

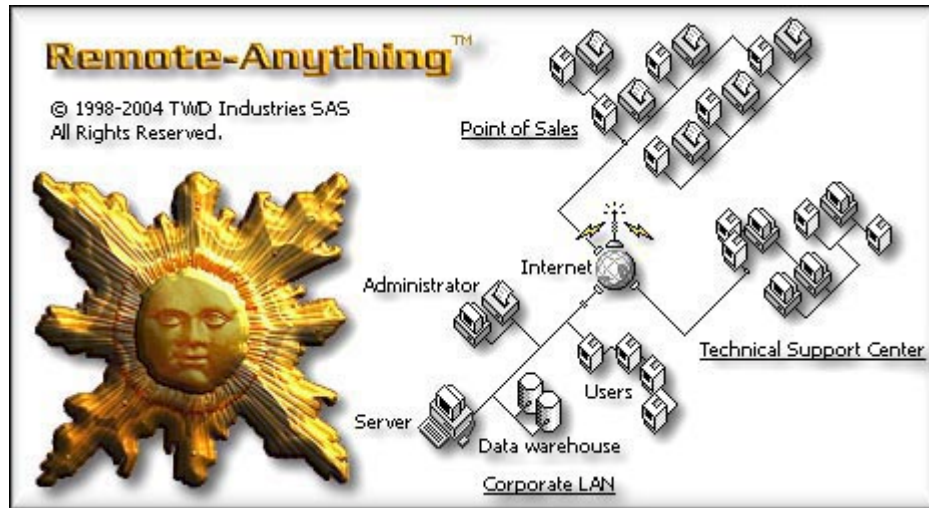


# Directory-Server



Version 4.11.12 for Windows (95, 98, Me, NT4, 2000, XP and 2003)

## • Reference Manual •



### • Copyright Notice

Copyright © 1998-2004 TWD Industries SAS. All Rights Reserved. Portions of the Directory Server are copyright 1992-2004 FairCom Corporation. "Faircom" and "c-tree Plus" are trademarks of FairCom Corporation and are registered in the United States and other countries. All Rights Reserved.




























### • Warnings





Product specifications and the contents of this document are subject to change without notice. This document has been prepared with our utmost effort. However, if there are any queries or errors please contact [eric.sanders@twd-industries.com](mailto:eric.sanders@twd-industries.com). This document may not be copied, translated or transcribed in any form in part or in entirety without TWD Industries' written permission.

### • Trademarks

Remote-Anything™, RA™, RA Gate™, RA Directory Server™ and RA DS™, are trademarks of TWD Industries SAS. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

# Table of Contents

 Copyright Notice.....	1
 Warnings .....	1
 Trademarks .....	1
 <b>Table of Contents</b> .....	<b>2</b>
 Wasn't technology <i>supposed</i> to make your life easier? .....	5
 System Specifications (minimum requirements).....	6
 <b>The Directory Server (DS)</b> .....	<b>7</b>
 <b>Benefits of the DS</b> .....	<b>7</b>
 TRANSPARENT for Proxies, Firewalls and Routers!.....	7
 How the DS works .....	8
 Why use several DS? .....	9
 Purpose of the DS.....	11
 ROI (Return on Investment) of the DS .....	12
 <b>Installing and uninstalling the DS</b> .....	<b>13</b>
 The DS Tray Icon.....	13
 The DS Options .....	13
 The DS Database .....	15
 <b>Uninstalling the DS</b> .....	<b>16</b>
 <b>Using the DS</b> .....	<b>17</b>
 The DS Main Dialog.....	17
 Configuring Masters and Slaves for the DS.....	18
 Deploy personalized Slaves on all the PCs of your LAN in just 10 seconds .....	19
 Help-Desk Centers: Automatically track and lookup newly deployed Slaves.....	20
 Configuring Master or Slave for a proxy server (Socks 4/5 and HTTP) .....	20
 Allowing Masters to access Slave PCs .....	20
 Setting up the Credentials.....	21
 Editing Master/Slave Options and Master User Credentials for a PC .....	22

☛ Querying the DS from <i>Masters</i> to locate and reach <i>Slave</i> users / PCs.....	22
☛ Using the DS from <i>Slaves</i> to send SOS Calls.....	23
☛ How to arrange PCs in Network Folders.....	25
☛ Real-time PC States .....	26
☛ Automatically Updating Master.exe and Slave.exe on all your PCs.....	27
☛ Real-time Application Inventory .....	27
☛ Real-time Hardware Inventory .....	28
☛ Track PC usage on a per user or per PC basis .....	28
☛ File Deployments .....	29
☛ The DS Load Button .....	31
☛ The DS HTTP Status Codes.....	33
☛ The Query Button.....	34
☛ Using the DS ODBC interface to make SQL queries .....	34
☛ The License Button .....	36
☛ The About Button .....	36
 <b>Troubleshooting the DS .....</b>	<b>37</b>
 <b>Performances of the DS .....</b>	<b>39</b>
☛ WinSock (the Windows TCP/IP stack) is the Bottleneck.....	40
☛ The Disk.....	41
☛ Processors.....	42
☛ Conclusion .....	43
 <b>How safe is the DS?.....</b>	<b>45</b>
☛ The Security of the DS.....	45
 <b>Passive Defense .....</b>	<b>45</b>
☛ Masters/Slaves are no longer listening to ANY port.....	45
☛ The Time Zone Filter.....	45
 <b>Active Defense .....</b>	<b>45</b>
☛ 2048-Bit Asymmetric RSA encryption .....	45
☛ 2048-Bit RSA Public Keys used for Symmetric Session Keys negotiation.....	46
☛ Replay protection .....	48
☛ Data integrity.....	48

☺ 128-Bit AES encryption (FIPS 197) and rotated Session Keys .....	48
☺ Why Encryption is Optional .....	49
☺ Buffer overflows protection .....	49
☺ No access to the system layer .....	49
☺ Monitoring and Logging .....	49
☺ Denial of Service protection .....	50
☺ Why not use established standards like SSL/TLS?.....	50
☺ Conclusion .....	51
🔍 <b>Technical Support .....</b>	<b>52</b>
🔍 <b>Program Updates .....</b>	<b>52</b>
🔍 <b>Small Glossary of the Network Terminology used in this Manual .....</b>	<b>53</b>
🔍 <b>License Agreement.....</b>	<b>55</b>

## 👁️ Wasn't technology *supposed* to make your life easier?

You have to access to 50 LANs distributed in 4 countries and you have to deploy remote-control to cut the costs involved in the maintenance of 10,000 PCs. Hell, that's around 80 routers and firewalls from various vendors to configure and you have to send skilled technicians to do the job. It will take months, it will hit your budget hard, there will be errors, new security issues and downtimes, and any future modification -like adding a single PC on a LAN- will force you to send people to fix the boxes again, and again.

You recall the large smiles of the sales reps and consultants who pocketed their big checks before leaving you with this mess and you think that *there should be a better way to do this*.

➡️ The TWD Industries DS makes this nightmare a relic of the past -and no other solution of the market is able to provide this feature: ***Secure Zero-Configuration Firewall Traversal***.

▶️ **Note:** If your ISP is maintaining a *managed router or firewall* for you then using the DS is your *only chance* to reach the PCs on your LAN (because you have no way to access or modify the configuration of this device).


BTW, isn't it nice to be able to access your PCs without digging into the sloppy documentation of your router or firewall and experiencing all the firmware bugs one by one each time you need to add NAT for a new user?

The DS saves you time as soon as you have to go through one blocking routing device but it does much more with centralized logs, inventory and credentials.

## System Specifications (minimum requirements)

- A PC or compatible, 386, 486, Pentium or higher
- 4 MB of free RAM or more (1MB for the Windows stack, plus the size required by the threads)
- Windows 95, 98, Millennium, NT4 (SP3), 2000, 2003 or XP.
- A VGA compatible Video Adapter or higher
- A Hard-Disk with 300 KB of free space (you need more space for the DS database)
- A Mouse and a Keyboard
- A Network Adapter or a Modem or a Cable (USB, parallel, etc.) to reach *Masters* and *Slaves*
- The TCP/IP protocol installed and working
- Winsock 2.0 (available since April 1996). Windows 95 users will have to download the Microsoft patch, W95ws2setup.exe (963 KB) from:

[http://www.microsoft.com/windows95/downloads/contents/WUAdminTools/S\\_WUNetworkingTools/W95Sockets2/Default.asp](http://www.microsoft.com/windows95/downloads/contents/WUAdminTools/S_WUNetworkingTools/W95Sockets2/Default.asp)

 **Note:** Optimal performances are achieved with appropriate hardware: among critical parts, a Network Adapter may double or triple the effective bandwidth -if the manufacturer is properly chosen. Some Windows Registry settings can also boost your connections (see the FAQ).

Please read the latest FAQ on <http://www.remote-anything.com> to learn more about performance hints and issues, TCP/IP installation, common problems, error messages, etc.

# The Directory Server (DS)

## Benefits of the DS

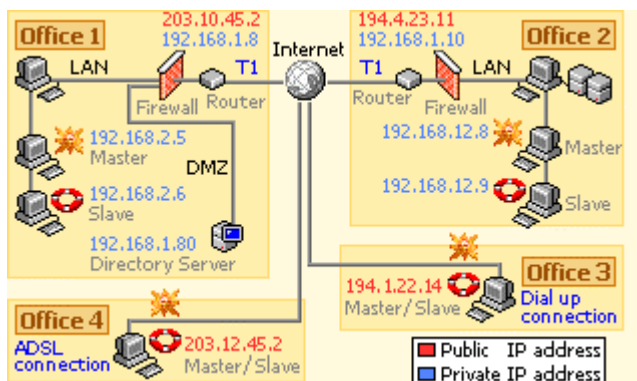
If you manage tens (hundreds, or thousands) of PCs then the following will be useful:

- ☛ reach Slave PCs on distant LANs with **no router/firewall setup** (no NAT, no port to open)
- ☛ Masters/Slaves **no longer listen to ports** so malicious users cannot detect or attack RA
- ☛ Masters/Slaves are automatically updated by the DS –**without rebooting any of the PCs**
- ☛ administrate groups of Master and Slave PCs and users from one centralized location
- ☛ define the Master rights to use a Slave PC on a per-user basis instead of on a password basis
- ☛ locate and reach a user or a PC even if you don't know his/her/its fixed or dynamic IP address
- ☛ allow Masters to search a Slave PCs/Users by user name/host name/MAC address/IP address
- ☛ allow Slave users to send SOS calls that will be processed by the first available Master user
- ☛ install or move Masters to new PCs without asking new registration keys to TWD Industries
- ☛ apply power-saving options from the DS on your remote Slave PCs to power-down displays

The DS implements **fault-tolerance**, **load balancing**, **mirroring** and **redundancy** to offer a scalable solution for a LAN or a WAN of up to 18,446,744,073,709,551,616 PCs. If you are out of processing power to manage your PCs, *just add a new DS!*

## TRANSPARENT for Proxies, Firewalls and Routers!

Save time with the configuration of those systems with the DS: using NAT or opening ports is *no longer necessary* to reach 'hidden' PCs located behind a router! There is no setup needed!



Any of the Masters (or Slaves) can interact with the other PCs of the WAN where RA is installed -*even if*.

- ☛ nobody knows the current (private or public) IP address of the remote PCs
- ☛ nothing has been done on routers/firewalls to route incoming connections or to open ports.

- Why “**Secure**”? A firewall blocks *incoming connections* to protect the PCs of your LAN. *Outgoing connections* are allowed so all users can share one single Internet access. With the DS, Masters and Slaves no longer need open ports because *instead of waiting for incoming connections they only make outgoing connections with the DS* (just like users who surf the Web). In addition, the DS uses AES encryption with a rotating *128-Bit session key* to protect your data.
- Why “**Zero-Configuration**”? Because you have *really* nothing to do to make it work and because there are *no* restrictions or compatibility requirements. The DS does not need a special technology, *it works in all the cases* (as long as the PCs of your LAN can initiate outgoing TCP connections on one port number).

► **Note:** In the case of a **proxy** : if your DS is not located on the Masters and Slaves LAN the proxy asks users to authenticate themselves in order to reach the Internet. In this case, Slave or Master cannot access the DS via Internet since the proxy is blocking connections that go outside of the LAN. The solution is to use the Master and Slave « Proxy » option which sends your username and password to the proxy -allowing Master and Slave to reach the Internet.

### ☛ How the DS works

When you *enable* the ‘DS’ option in Masters and Slaves, you can no longer establish direct connections from a Master to a Slave -using the Slave password to authenticate connections. Instead, the authentication process is performed by the DS:



- 1) Master queries the DS to locate a Slave PC (or a Slave user)
- 2) The DS checks the credentials of the ‘Master PC’ **and** ‘Master USER’ in its database
- 3) If Master is allowed to access this Slave PC then the DS returns the Slave information
- 4) Master establishes an AES 128-Bit encrypted connection with the Slave PC *through the DS*

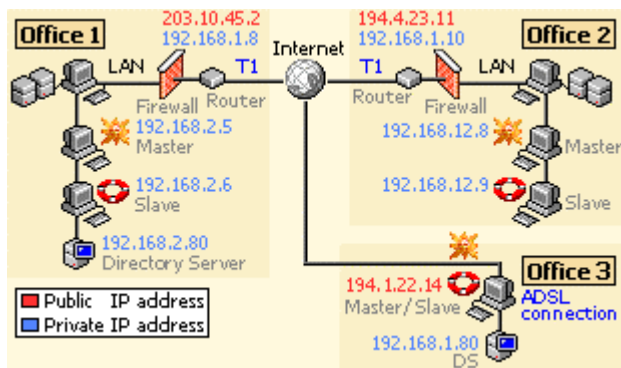


⇒ The DS machine can be located on any of your LANs or even outside of them –the only constraint is to make it reachable for all Masters and Slaves.

► **Note:** *Master users and Master PCs* must have the necessary credentials in the DS database to be able to access *Slave PCs*.

### ☺ Why use several DS?

This may be necessary if you are using a really huge number of PCs or if you really need a true redundant solution. One DS will be enough for tenths of thousands of PCs. Real fault-tolerance can be achieved *without* expensive hardware (like fail-safe load-balancing routers).



You can chain several DS in order to merge the databases from one DS to another (left picture).

If a DS stops responding Masters and Slaves will automatically use the other DS (redundancy).

When a DS is started, it checks if another DS has a more recent database and if so, it synchronizes its database with the other DS.

Up to 16 DS can be chained this way to provide real-time redundancy and load-balancing. See the DS options later in this document to learn how to setup the **DS database synchronization**.

Tip: The DS is a Windows Service. As such, it can be restarted automatically (this is a Windows 2000/XP feature) if -for any reason- it has been stopped unexpectedly. This would lead to an interruption of service of less than 10 seconds (if Windows is not crashed).

If Windows is crashed, having two DS machines will allow the traffic to be processed by the second machine if the first server no longer responds.

Having two DS is also used to make sure that load balancing can be handled properly: in case too many connections are received on the first DS then this DS will redirect connections to the second DS. This, however, is only likely to happen with thousands of Slave PCs. See the 'Performances' chapter for more information about how much a single DS can take.

## 🔑 Purpose of the DS

🖥️ DS.exe (250 KB) is a HTTP Server written in portable C++ (with no dependencies or DLLs) like 🌟 Master.exe (285 KB) or 🚫 Slave.exe (80 KB). The DS will be used by:

### 🔑 Masters

- to check the credentials of a Master User trying to reach a Slave PC/User (Slaves using a DS will reject connections that are not authenticated by the DS)
- to lookup a LAN/WAN computer or user in the DS database (Masters can search a Slave PC by Network, User Name, IP address, MAC address, etc.)
- to be notified of pending SOS calls issued by Slaves
- to update themselves automatically (the DS will update remotely all the Masters it can reach)

### 🔑 Slaves

- to send SOS calls (Masters will be notified of SOS calls by the DS)
- to update themselves automatically (the DS will update remotely all the Slaves it can reach)

### 🔑 Network Administrators

- to monitor PCs (powered PC, hardware inventory, OS version, who is logged in, who is connected to the Internet, who asked help, who helped who, when, how long, etc.)
- to modify the options of all Master and Slave PCs from one centralized location
- to define credentials for Master Users/PCs (allowing them to access some of the Slave PCs)
- to define alerts (Is a specific machine used? Is a specific User logged in? Are critical resources of some machines reaching a dangerous level? Etc.)
- to manage PCs (deploy programs, modify privileges, search files on the LAN or WAN, etc.)
- to audit the DS database (PC usage history, RA usage history, memory usage, etc.)
- to trace a stolen notebook (as soon as it connects to the Internet, you can reach it)

▶ **Note:** Whether the DS is installed on a LAN or connected to the Internet, all your Master and Slave PCs need to be able to reach their DS: (the DS can use a dynamic IP address)

- If a Master cannot access the DS then the Master will not be able to query the DS database and will not be able to reach Slaves (or to be notified of SOS calls)
- If a Slave cannot access the DS then it will not be possible for a Master to establish a connection with the Slave (and the Slave will not be able to send SOS calls)

⇒ This model offers the best possible security scheme (and reduces the cost of ownership of both PCs and RA) since credentials, PC usage and history are stored and administrated from a centralized location updated in real-time.

▶ **Note:** Since Master and Slave PCs no longer listen on RA port numbers no hacker will be able to detect that RA is running and will not even be able to attack Masters or Slaves. For the same reason, port scanners will no longer see that your machines are using RA. This makes RA the safest remote-control solution available on the market (because you cannot break something that you cannot even detect or reach).

### 🔹 ROI (Return on Investment) of the DS

The DS and RA are offering unique innovative features that make your life easier and safer.

The U.S. Environmental Protection Agency estimated that an organization can save \$10 to \$50 per computer annually by enabling power management features that place a computer monitor into a low-power “sleep” mode during periods of inactivity.

The DS allows you to define *-and deploy-* such a power-saving scheme on remote PCs with a simple mouse click *–even on versions of Windows that do not support power-saving schemes.* You can define default values for your ‘Networks’ (groups of PCs) and you can create override settings for specific PCs as needed.


⇒ *This feature alone can make RA and the DS pay for themselves in less than six months!*

Most of our customers can migrate to RA for the amount they use to spend *each year* in the program updates, support and maintenance fees of a product from the competition.

That’s what we call ROI.

Many small businesses and large accounts are migrating from other solutions to TWD Industries’ products to reduce their recurring fixed costs.

## 🔧 Installing and uninstalling the DS

➡ To install a DS, login as 'Administrator' and then copy and run  DS.exe in the folder of your choice (C:\DS or C:\Program Files\DS are good choices). Once installed, the DS runs as a Windows Service so it will start automatically at boot time.


The DS has to be installed on a PC that Masters and Slaves can reach (this may be on the Masters and/or Slaves LAN or anywhere else). The DS machine can have a dynamic IP address providing that:

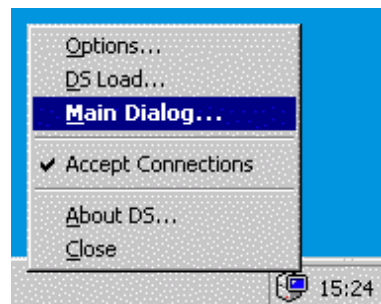
- Masters & Slaves know the DNS/NetBios name of the DS machine (Examples: 'twd-industries.com' or 'twd\_server1')

Once installed the DS will be immediately operational, listening for Master and Slave 'alive' packets. The only thing you will have to do then is to define credentials as explained later in this document.

### 🟡 The DS Tray Icon

➡ The DS will show a Tray Icon that gives you access to the DS functions.

This Icon is **black** when not accepting connections, **blue** when accepting connections, and shows a **green** arrow when performing database mirroring or synchronization: 

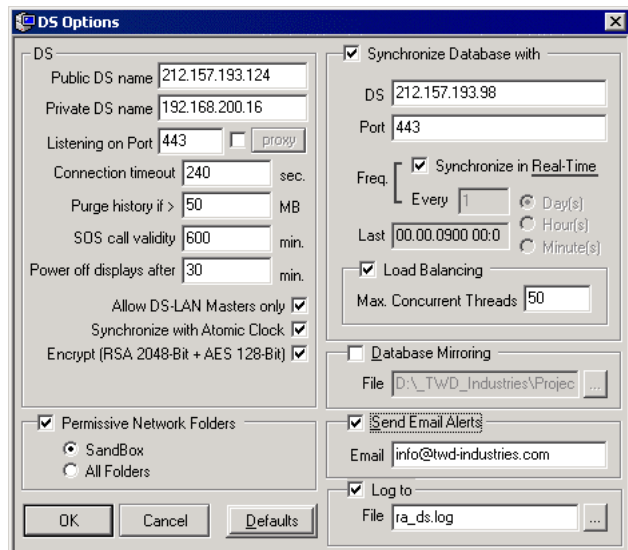


### 🟡 The DS Options



This button displays the Options dialog box below:

- **Public DS Name:** the public DNS Name or public IP address used by Masters and Slaves to access the DS from the Internet.
- **Private DS Name:** the private DNS Name or private IP address used by Masters and Slaves to access the DS from the DS LAN.
- **Listening on Port:** the Port number used by the DS to listen for incoming connections.
- **Connection Timeout:** (seconds) The DS cuts connections if responses are not quick enough.
- **Purge history if >:** prevent the States Table from growing forever and reset it if needed.
- **SOS call validity:** SOS calls are automatically deleted if they are not answered within this delay.
- **Power off displays after:** this is the default power-saving value to apply for Slave PCs.
- **Allow DS-LAN Masters only:** Masters that are not located on the DS LAN will not work.
- **Synchronize with Atomic Clock:** automatically keep the clock of the DS machine up to date.
- **Encrypt (RSA 2048-Bit + AES 128-Bit):** use RSA encryption for AES session key negotiations.
- **Permissive Network Folders** Masters can access the selected Network Folder(s) if they are allowed to access at least one Slave PC of the Network Folder(s) of interest.
  - **Log To:** keeps a DS activity log in the NT/2000 System Event Log and/or in a simple ASCII file.
- **Synchronize Database with:** use another DS to make sure that, in real-time or at a given interval of time, DS databases will be synchronized. During scheduled synchronizations, you cannot use the DS user Interface (in order to keep consistent with the exchanged information) but the DS is normally handling incoming connections from Master and Slave PCs. When this option is enabled Masters and Slaves automatically use the other DS if their primary DS is no longer responding.
- **Load Balancing:** the DS will redirect incoming connections to the co-DS if needed.
- **Max. Concurrent Threads:** the DS will redirect incoming connections if this value is reached.
- **Database Mirroring:** the path used to keep a copy of the DS database. Note: the mirroring feature is disabled as long as the Main DS dialog is opened (because it can be used to add Networks). If we just mirrored in real-time the database, the disk and CPU load would have been doubled - leading to poor scalability. So, instead, we use the following strategy: if there is no incoming connection for one hour (and if the database has changed since the last backup), the DS stops accepting incoming connections just the time to make a backup copy of the database (this should



be a matter of seconds, minutes if you have a big database). If you need more accurate mirroring strategies, you should consider RAID 5 controllers and disks or a co-DS.


## The DS Database

Once run, the DS will create the following database files: (in the .\db sub-directory)

- Network.dat           The Networks (Network ID and Description, DS, eventual Gateway, etc.)
- Computer.dat        The Master and Slave PCs (Master/Slave/DS, MAC address, Hostname, etc.)
- State.dat            The characteristics of a PC at a time (On/Off, user name, OS, CPU, RAM, etc.)
- mOptions.dat        The Masters options (port, log file, DS, Gateway, view only, FPS, etc.)
- sOptions.dat        The Slaves options (port, log file, DS, Gateway, Tray Icon, IP Filtering, etc.)
- OpenNetwork.dat    The credentials of a Master User (this User can access a given Network)
- OpenSlave.dat       The credentials of a Master User (this User can access a given Slave PC)
- EndUsers.dat        The Users of your PCs (Master credentials may be assigned to some users)
- SOS.dat             The list of SOS Calls sent by Slaves (when, by who, on which PC, etc.)
- Application.dat     All the applications of your WAN (Application name, version, etc.)
- AppInvent.dat      The Application Inventory (on which PCs, installation/un-installation date, etc.)
- Hardware.dat        All the Hardware of your WAN (Hardware name, type, version, etc.)
- HwrType.dat         Each category of hardware (CPU, RAM, Storage, Video, Controllers, etc.)
- HwrInvent.dat      The Hardware Inventory (for which PCs, installation/removal date, etc.)

As you can see, all the activity on your LAN or WAN will be stored in the DS Database: when a PC is not used, when a User opened a Windows session, when he asked support from a Master User and when he got help, how long, and from whom.

In addition, all the changes on your PCs are recorded (logged User, RAM, Disk, OS, NIC, modem, Internet connection, etc.) so you have a pretty handy record of the maintenance activity as well (the RAM and Disks status are stored when they are critical: less than 2MB RAM or less than 20MB disk, or when the RAM status change is larger than 10MB).

 A look at the main DS dialog lets you find which PC needs more RAM or more disk space.

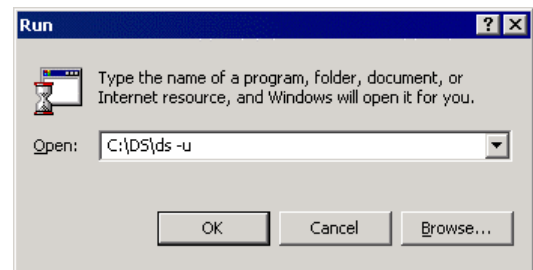
**Note:** The DS will allow you to accurately estimate the costs associated with all this activity (PC usage, Internet use, PC maintenance, etc.) and will allow you to find all the details of an event: *who was involved, when, and from where.*

In the future releases, the DS will provide sophisticated reporting tools to query the DS database and create custom reports and Database exportations.

## Uninstalling the DS

To uninstall the DS, just run the DS.exe with the `-u` parameter as shown below:  
(use the Windows “Start” menu and then the “Run” command)

This will remove the DS Service from the Service List of the Windows Service Control Manager.





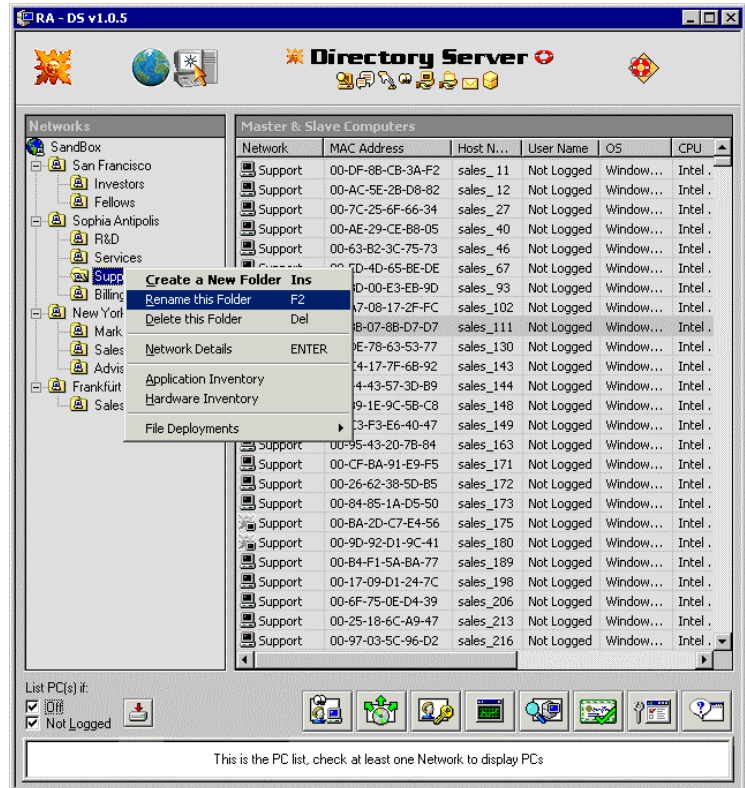
## Using the DS

### The DS Main Dialog

This dialog shows the **Network** and the **Computer Lists** (Masters and Slaves).

If you select one **Network** then the PCs of this group will be listed in the Computer List. Create a Network with the 'INS' key (rename it with the 'F2' key and delete it with the 'DEL' key –or just right-click it to get a menu).

The Computer List is showing a real-time list of available PCs for the selected Network (Masters or Slaves that are sending 'alive' packets to the DS).



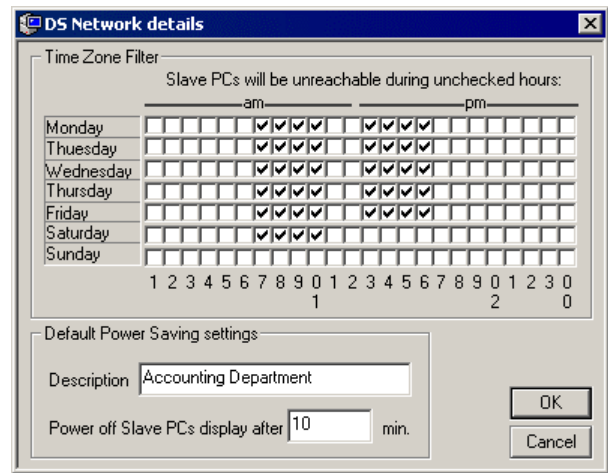
- Off
- Not Logged

These checkboxes allow you to filter the Masters and Slaves listed in the Computer List. If you check 'Off' then you will also see the computers that are unavailable (offline) but stored in the DS database. If you check 'Not Logged' then you will also see available (online) computers that are not being used by someone.

**Note:** The main dialog box should \*NOT\* be open all the time because it uses CPU and network resources to maintain a real time list of PCs for the selected Network. If you need to monitor such a list you should use a Master instead.

The **'Network Details'** menu item that you get with a mouse right-click (see image above) displays the dialog box on the right. You can define a default **Time Zone Filter**, rename the Network Folder or define the default **Power-Saving** options for this Network.

The default Network settings (Time Zone Filter and Power-Saving) are overridden if you define Slave settings for a specific PC.



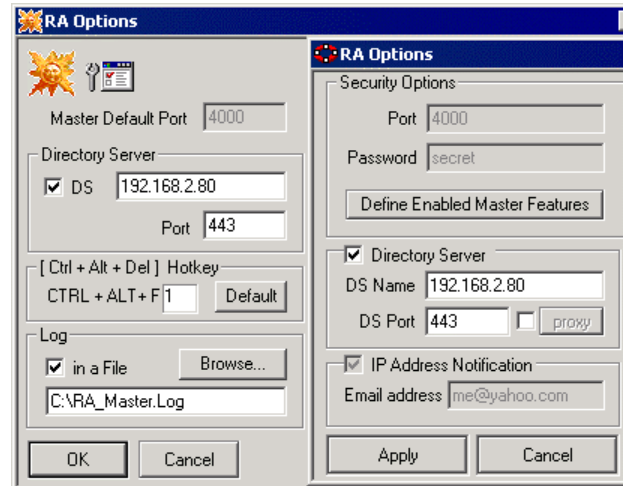
### ☛ **Configuring Masters and Slaves for the DS**

Once installed, the DS is working as soon as Masters and Slaves can reach it. Then, they send 'alive' packets to fill the DS Database with information about:

- PCs (Master and Slave PCs, with their options, state, RAM and Disk levels, etc.)
- Users (each time a new User is logged on a PC, he is added to the Database)

Configuring Masters and Slaves for the DS is simple. Two options are related to the DS: **'DS'** and **'Port'**.

Check the **'DS'** check box and enter the DS IP address (or DNS name) and port number in Masters and Slaves.



- For Masters and Slaves that are located on the DS LAN assign them the PRIVATE IP address of the DS.
- For Masters and Slaves that are NOT located on the DS LAN assign them the PUBLIC IP address of the DS (if the DS machine has no public IP address then this will be the public IP address of your router which implements a NAT table to route incoming connections from outside the LAN to the private IP address of the DS machine).

- For Masters and Slaves installed on roaming laptops that are located on the DS LAN only part of the time and are also used at Home then assign them the DNS NAME of the DS so they will always be able to lookup the DS (this requires a DNS server for your LAN and for the Internet).
- If you do not have a permanent connection to the Internet and/or have no fixed routable IP address to provide for the DS machine then you can use a dynamic DNS name (see [www.noip.com](http://www.noip.com)) so Masters and Slaves will be able to reach the DS from anywhere in the world. (**Note:** if your DS machine is behind a router then you still have to use port forwarding (NAT) on the router to redirect incoming connections to the private IP address of the DS machine)

Here is an example of configuration for the Option Dialogs of DS, Masters and Slaves:

DS Configuration

DS Public Name: 212.111.222.333

DS Private Name: 192.168.1.10

DS Port: 80

Master/Slave located on the DS LAN

DS: 192.168.1.10 (DS Private Name)

DS Port: 80

Master/Slave located outside of the DS LAN

DS: 212.111.222.333 (DS Public Name)

DS Port: 80

► **Note:** This configuration can be done **before you deploy Slaves** by using a **personalized** Slave.exe file that will contain the DS information. Using a personalized Slave.exe file will save you time and will avoid configuration errors since you will only have to run the Slave.exe file to install it and configure it (the procedure to make a personalized Slave.exe file is documented in the RA Manual).

👉 **Deploy personalized Slaves on all the PCs of your LAN in just 10 seconds**

Once you have created a personalized Slave file, you will want to deploy it on remote machines. This is as simple as just copying and running the Slave.exe file on the target PC.

A free tool called psexec.exe available from [www.sysinternals.com](http://www.sysinternals.com) can just do that (copy and run a personalized Slave file) on all the PCs of your domain. Just open a DOS box and type:

**psexec \\\* -u domain\administrator -p password -c -d -i "C:\my\_Slave.exe"**

Example: psexec \\192.168.124.145 -u domain\mike -p secret -c -d -i "C:\my\_Slave.exe"

To deploy Slave on a single machine, replace \\\* by \\192.168.124.145 for example.

## 🔑 Help-Desk Centers: Automatically track and lookup newly deployed Slaves

If you provide Help-Desk services and receive phone calls, email or web-based support requests then assigning an incident ticket or a customer code to a new Slave BEFORE it is deployed is very useful. As soon as you see the expected Slave identifier in the DS or Master list you can access the Slave PC remotely.

Personalized Slaves can **be automatically stored under a given Network folder** (they create the Network folder if it does not exist yet in the DS database) and use the PC Description of your choice. You just have to rename the “Slave.exe” file like this: “**Network#pcDescription.exe**” before you deploy (or ask the customer to download) this Slave file on a PC.

Examples: “NY\_Sales#Paul’s Laptop.exe”, “NY\_Sales#.exe” or “HelpDesk#Ticket2452.exe”.

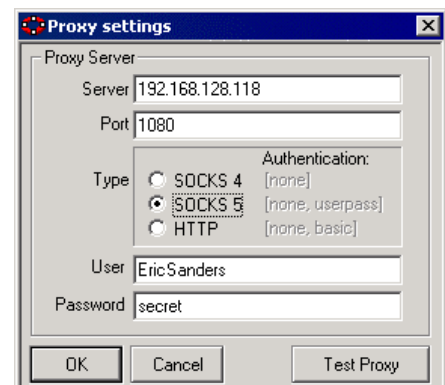
You can send an email to your customer with a link to your web site that will specify a ticket code in the URL that points to the CGI on your web site in order to rename the Slave.exe file downloaded by the customer according to the ticket code.

Then, the newly deployed personalized Slave will register with your DS in the Network Folder specified by the ticket code and you will be able to find it immediately in DS or Master (the "Permissive Networks' DS option allows Masters to reach newly deployed Slaves without creating new access rights in the DS).

## 🔑 Configuring Master or Slave for a proxy server (Socks 4/5 and HTTP)

The ‘**proxy**’ option of the Master and Slave Options dialog boxes (see the pictures above) displays the dialog on the right. You can define the parameters of your proxy server to allow Masters and Slaves to reach a DS via the Internet.

This option is useless if the DS is located on the Master and Slave LAN.



## 🔑 Allowing Masters to access Slave PCs

After all PCs and Users are registered in the DS Database, you can define User Credentials (the right for a User to use a Master PC to access a given number of Slave PCs).

⇒ In order to make the DS operational, you only have to:

1. **Install the DS**
2. **Deploy Masters and Slaves on your LAN/WAN (NT script, Logon script, email, etc.)**
3. **Wait that PCs and Users are listed in the DS Database (it is done automatically)**
4. **Authorize Master PCs in the DS Database (if you don't they will not accept to work)**
5. **Define User Credentials (so Master Users can use Master PCs to access Slave PCs)**

The steps 4 and 5 can be done at the same time in the dialog documented below.

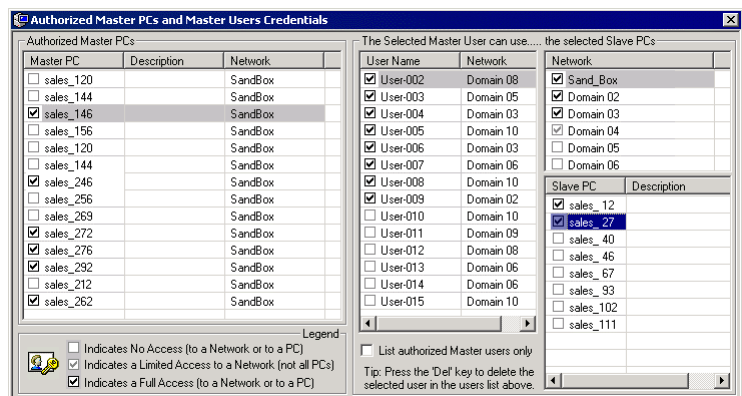
## 🔑 Setting up the Credentials



This button calls the Credentials dialog box below:

🔑 This dialog allows you to:

- Authorize a Master PC (so a Master User can use this Master PC to access Slave PCs)
- Select Master Users (among all Users so a User can use any Master PC)
- Select the Networks a Master User can access (an 'Open' Network grants access to all its Slave PCs)
- Select the Slave PCs that a Master User can access.



▶ **Note:** To open rights for a Network or a Slave PC, you have to select one Master User.

In order to establish a connection to a Slave PC, a User has to:

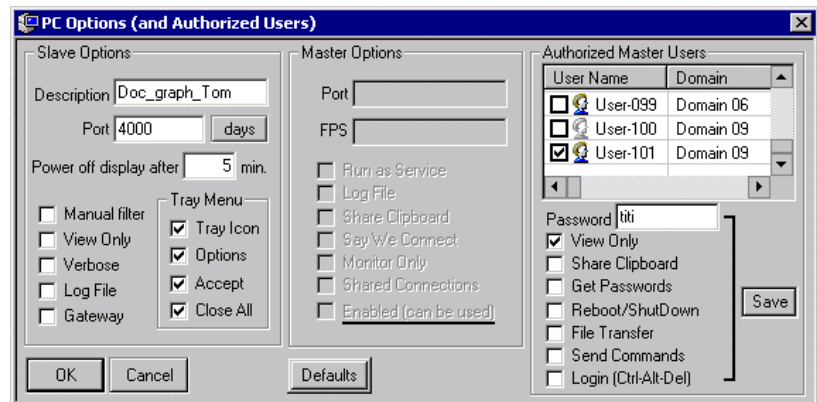
- be an Authorized Master User
- have credentials to access this Slave PC (or all the PCs of the same Network)
- use an Authorized Master (a PC where Master.exe is authorized by the DS)

**Note:** If a Master User has credentials for a Network, he can access all the Slaves of this Network. If you define credentials for a specific Slave then they will override the eventual existing credentials of its Network.

## Editing Master/Slave Options and Master User Credentials for a PC

Just double-click one PC in the Computer List to edit the Master and Slave Options and define the Master Users that can access this PC. Once saved in the DS Database, the new RA options will be updated on the distant PC when the DS will hear about this remote PC.

This dialog is handy to modify the setting for one single PC. Another dialog (see the 'Credentials button') allows you to define Master User credentials for all your PCs at the same time (here, Master options are grayed because there is no Master installed on this PC).




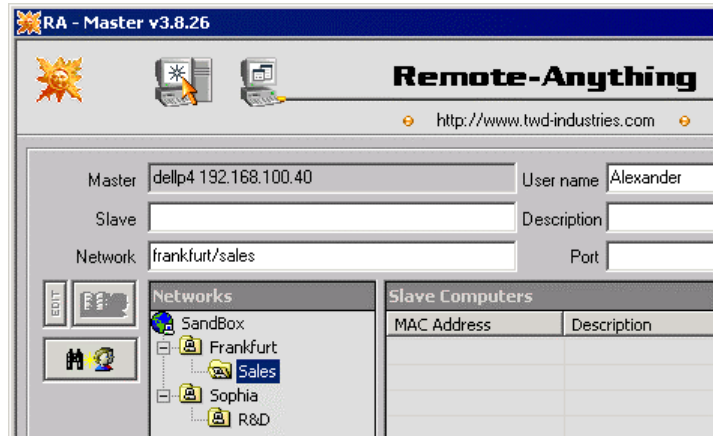
## Querying the DS from Masters to locate and reach Slave users / PCs

The DS allows **authorized Master users** to send request in order to find *Slave* users and PCs on a LAN or WAN. The search values can be one or a mix of:

- user name (the name users type to open Windows sessions)
- machine name (DNS or NetBIOS names – type it in the 'Slave' edit box)
- IP address (the *private* IP address – type it in the 'Slave' edit box)
- MAC address (the network adapter's MAC address – type it in the 'Slave' edit box)
- Network (the name of the 'Network' where the Slave PC is located)

Just enter the search values in the relevant fields of the main Master dialog box (if you want to filter the list of online

PCs) and press the  button to populate the 'Slave Computers' list with the Slave PCs that the Master user is allowed to reach.



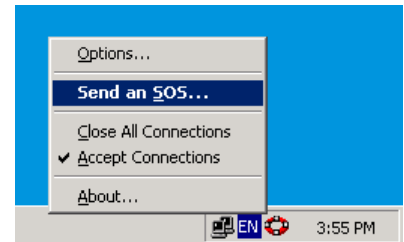
⇒ Then, to reach a Slave PC, just select it and press one of the buttons below:



This will connect Master and Slave via the DS *if Master has the right to use the feature you have selected with this Slave PC.*

### ☛ Using the DS from Slaves to send SOS Calls

When using the DS, Slave users who send an SOS will not send it to a specific Master but instead will send it to the DS. The DS then will broadcast the SOS to all the available Master users that are allowed to provide assistance to this Slave PC.



Slave SOS Calls will be signaled to Master users by displaying smiley icons 😊 until a Master provides assistance to the Slave users requesting help.

Each of the smiley icons gives an idea of the delay that the Slave user is experiencing –from hope to despair:

😊 😐 😱 😞 allowing Master users to identify priorities.

MAC Address	Gateway	IP Address	Hos
00-C0-F0-1C-E7-FA	192.168.100.10	192.168.100.10	astc
00-E0-29-64-5D-F3	192.168.100.20	192.168.100.20	durc
😊 00-50-BA-E6-52-97	192.168.100.8	192.168.100.8	Dua
00-50-BA-E6-25-61	192.168.10.16	192.168.10.16	lase
00-50-BA-E6-32-86	209.237.155.68	192.168.10.42	tech
00-50-BA-E6-51-23	209.237.155.68	192.168.10.44	tech
00-50-BA-E6-52-17	209.237.155.68	192.168.10.45	tech
😊 00-50-BA-E6-55-11	209.237.155.68	192.168.10.58	dev
00-50-BA-E6-62-27	209.237.155.68	192.168.10.59	dev
😊 00-50-BA-E6-34-17	209.237.155.68	192.168.10.61	dev
00-50-BA-E6-21-25	209.237.155.68	192.168.10.65	dev
00-50-BA-E6-97-80	209.237.155.68	192.168.10.82	sale
00-50-BA-E6-11-97	209.237.155.68	192.168.10.84	sale
😊 00-50-BA-E6-72-99	209.237.155.68	192.168.10.85	sale

⇒ The DS logs all Master-Slave connections and all SOS Calls so you will be able to identify the time spent by your support staff at maintenance and assistance on your LAN / WAN.

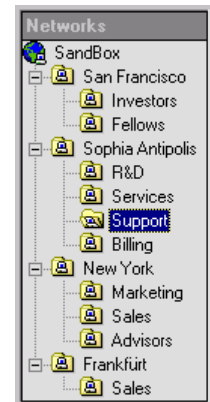
On the top of the unique security provided by the DS, the ability to reach any user or PC behind firewall and/or routers without configuration *-or to have any user be able to reach you-* is a dramatic improvement over what the Help Desk market offered so far.



## 🔑 How to arrange PCs in Network Folders

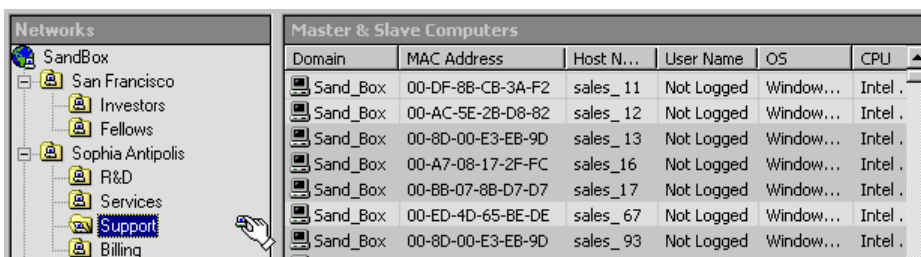
🔑 If you need to work with a lot of PCs then you may find it more convenient to organize your PCs in 'Networks'. There is no obligation for you to use several Networks to split your list of PCs -this may just be more convenient.

💡 Because the DS will associate each Master and Slave PC with the appropriate Network and will pass the information to all Masters then this work is done one time only.



The default '**SandBox**' Network is provided to collect PCs that do not (yet) belong to a user-defined Network. It may be useful to indicate new PCs when new Masters or Slaves will be installed in the future.

➡ To edit a Network name just click on one item of the tree. Press the [INS] key to create a Network. Press the [ENTER] key to save a change (or the [ESC] key to cancel changes). Press the [DEL] key to delete a network.























In order to associate PCs with a Network, just drag & drop PCs from the Computer List to the Networks Tree.

▶ **Note:** You can move PCs from one Network to another Network at any time but it is far easier to deploy your Master and Slaves by Networks and wait that they are listed in the DS. Then, you can drag & drop them in just one step in the appropriate Network and deploy RA on another Network, drag & drop them in a new Network folder, and so on...

## 📡 Real-time PC States

When listed in the main DS dialog, PCs have an icon that specifies their state:

-  The DS just started and has not heard about this PC yet
-  The PC is Offline
-  The PC is Online and that's a Slave PC
-  The PC is a Slave PC that has been marked as to be remotely uninstalled ASAP
-  The PC is Offline and locked by the Time Zone Filter
-  The PC is Online and that's a Slave PC locked by the Time Zone Filter
-  The PC is Offline and unlicensed (deployed without enough licenses in the DS)
-  The PC is Online and unlicensed (deployed without enough licenses in the DS)
-  The PC is Online and that's a Slave Gateway PC
-  The PC is Online and that's a Slave PC and it is running a Screen Saver
-  The PC is Online and that's a Slave PC and nobody is currently logged in
-  The PC is Online and that's a Master PC
-  The PC is Online and that's a DS machine
-  The PC is Online and that's a Slave PC currently controlled by a Master
-  The PC is Online and that's a Slave PC currently monitored by a Master
-  The PC is Online and that's a Slave PC currently exchanging files with a Master
-  The PC is Online and that's a Slave PC which just sent an SOS Call
-  The first SOS Call has not been processed yet and the user has sent another SOS
-  The second SOS Call has not been processed yet and the user has sent another SOS
-  The third SOS Call has not been processed yet and the user has sent another SOS

These icons allow you to quickly check in real-time the workload of the PCs *on your WAN*:

- Where is a given user?
- Who is logged on a given PC?
- Which PCs are not used?
- Which PCs are remotely accessed by RA or asking help?
- What are the memory and disk levels of a given PC?
- Where is the weakest or the most powerful PC?
- What are the PCs that have a modem?
- Is this PC currently connected to the Internet?

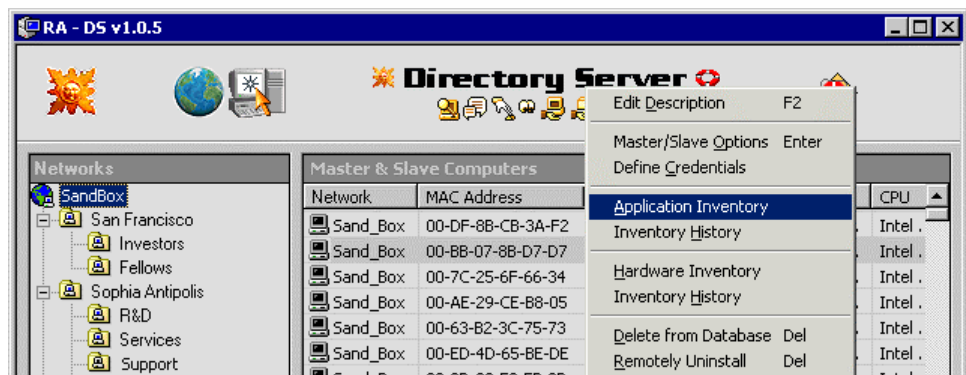
## ☛ Automatically Updating Master.exe and Slave.exe on all your PCs

💡 The burden of deploying personalized Masters and Slaves on each Group of end-users is a one-time issue because *Masters and Slaves will keep their options when the DS will automatically update them with new versions.*

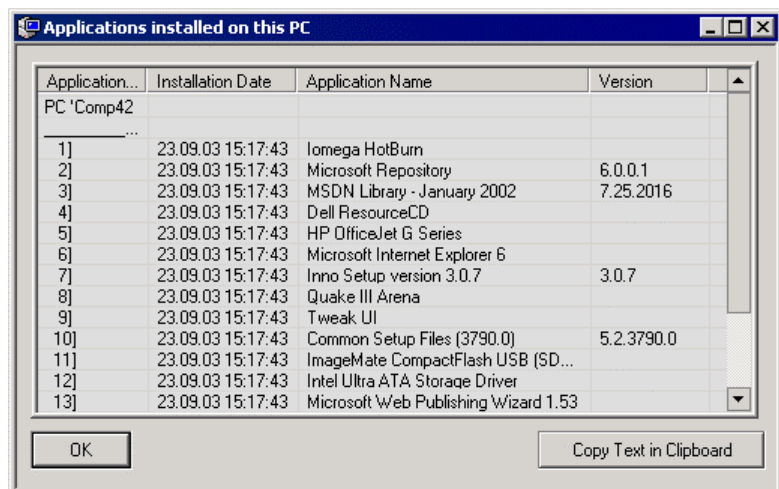
The only thing that you will have to do is to copy the new versions of Master.exe and Slave.exe in the DS folder. The DS will detect them and will attempt to remotely update all the distant Masters and Slaves until they use this new version.

## ☛ Real-time Application Inventory

You can list the applications installed on any PC with a **right-click** on the PC of interest in the DS dialog box (see the picture on the right side). This will display a menu which allows to edit the **PC description** which may be used with the **Recycle** option (see 'The License button') or to **Delete** or **Remotely Uninstall** the selected PC.

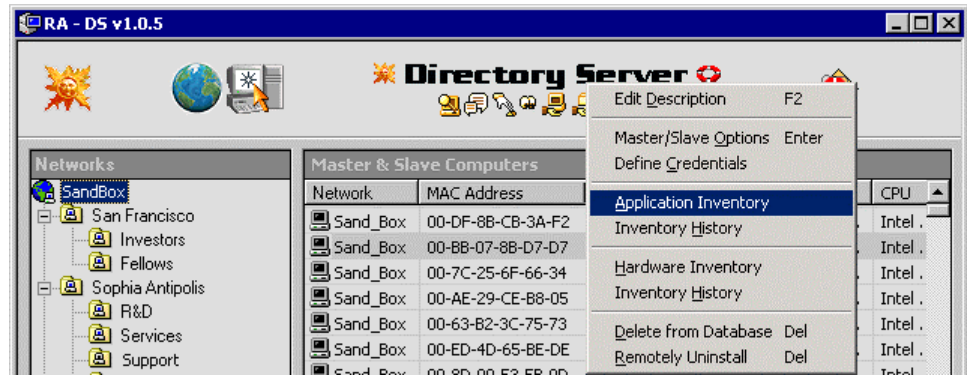


The **Application Inventory** menu item displays a dialog which lists the current applications installed on this PC and the **Inventory History** item lists un-installation dates as well so you can track if an application has been removed and reinstalled –how many times and when.

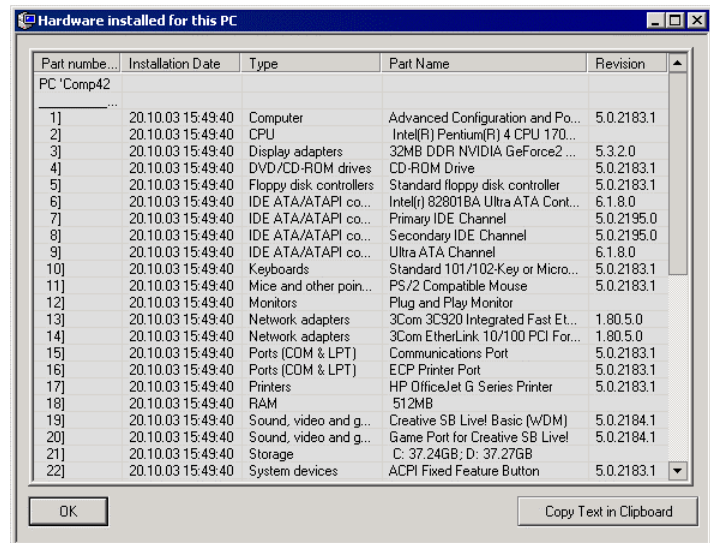


## ☛ Real-time Hardware Inventory

To list the hardware installed on any PC right-click the PC of interest in the DS dialog box to get a pop up menu (see the picture on the right side).



The **Hardware Inventory** menu item displays a dialog which lists the current hardware installed on this PC and the **Inventory History** item lists un-installation dates as well so you can track if a part has been removed and reinstalled –how many times and when.



## ☛ Track PC usage on a per user or per PC basis



This button displays the dialog box below:

☛ The Track dialog box allows you to generate a .RA movie and/or a text log file that will record the user activity during all the Windows sessions –for a given Slave PC or for a given User that will log on any of the Slave PCs managed by your DS.

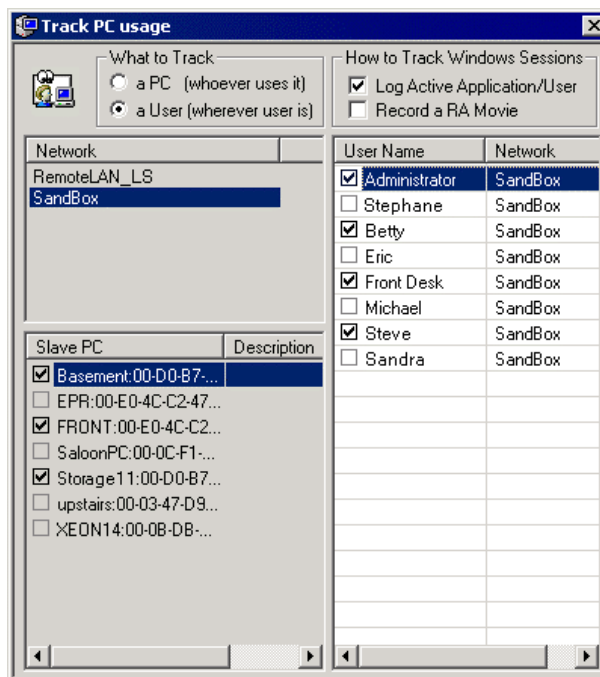
The text log file will just store the title of the active window and the application name for each user.

The RA movie will store all the screen changes.

The files are located in a sub-folder of the DS folder (DS\Tracking\Network Folder\User or PC).

With the NT Windows Task Manager opened on the “Performance” tab, a RA Movie file of 130 MB is created for a whole day (24 hours) of tracking.

CPU usage stays below 10% during RA Movie file tracking to avoid slowing down Slave PCs.



## File Deployments

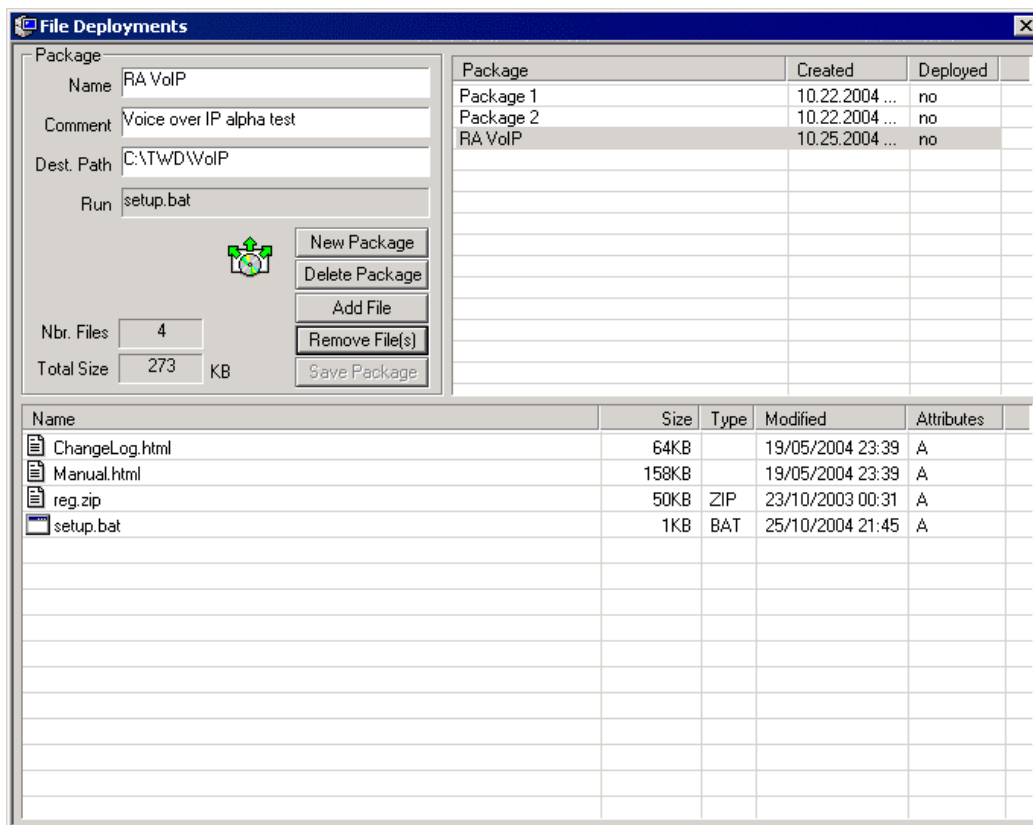


This button displays the dialog box below:

Here you can **create, edit** or **delete** Packages that the DS will deploy on request.

To indicate the setup file to **run** click on the icon of the package file.

**Dest. Path** can be an absolute PATH or contain any of the system folders below:

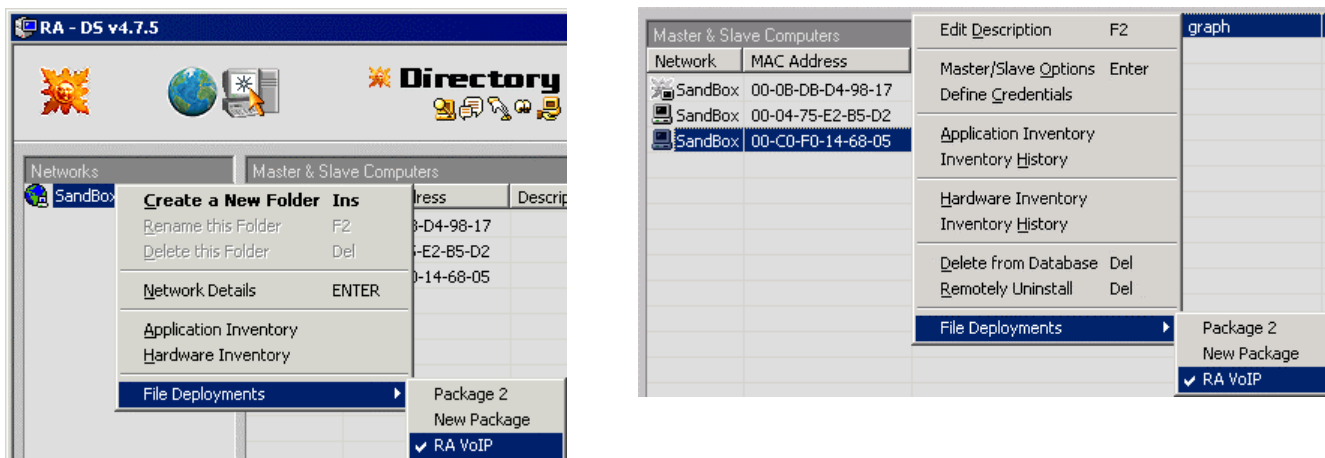


- %windir% (C:\WINNT or C:\Windows)
- %programfiles% (C:\Program Files)
- %system% (C:\WINNT\SYSTEM32 or C:\Windows\SYSTEM32)
- %commonappdata% (C:\Documents and Settings\all users\Application Data)
- %commondocuments% (C:\Documents and Settings\ all users \Documents)

Using such a %systemdirectory% will install the package files in the expected destination folder whatever the actual system drive and path are on each destination PC.

The **Run** file (if any) you have defined by clicking the icon of a package file will be run after all package files have been copied. This will allow you to copy package files in other directories, to install drivers and register dlls, etc. It can be any executable file (\*.exe, .bat, .vbs, .js) or even a data file (\*.msi, \*.txt, \*.doc) as long as the corresponding program is already installed on the destination PC to be invoked by Windows.

Once a package is saved, you can ask the DS to deploy it on all the **Slave PCs** of a Network Folder (see the picture below on the left) or on one PC only (see the picture on the right).

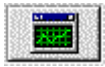


When a Package is ticked in a File Deployment menu the destination you selected (a Network Folder or a single PC) will receive this package. You can enable or disable deployments by simply ticking or un-ticking a menu item.

By deploying on a whole Domain and then by disabling (unselecting) the deployment for a single PC you can quickly define exceptions within a Network Folder.

When a package is fully deployed, the menu item is ticked and grayed to indicate success. You can watch the progress of a Network Folder Package by simply checking which of the PCs already received it.

## 🔘 The DS Load Button

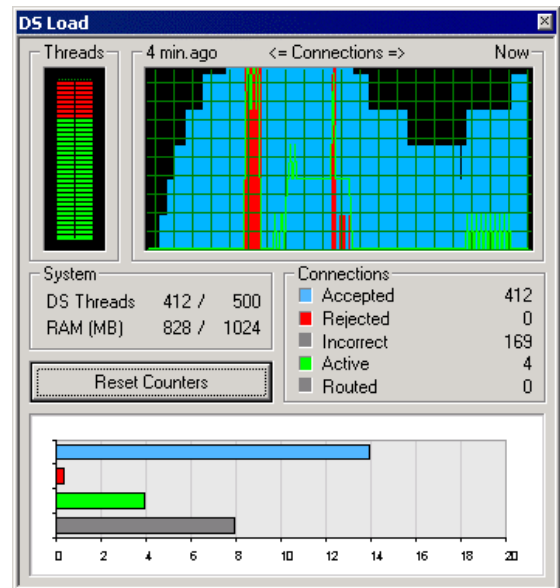


This button calls the DS Load dialog box below:

- 🔘 The DS Load dialog box is an efficient way (it uses less than 1% of the CPU resources) to monitor the DS activity. **Rejected Connections** allow you to discover that the **Max. Concurrent Threads** option has been set to a too small value or that this machine is overloaded.

- 🔘 If you see **Incorrect Connections**, you may find that a hacker is trying to access your DS.

(As the DS will only answer connections sent from Masters and Slaves that are listed in the DS database, any other connection will be rejected).



If your DS is listening on port 80, one may think that the DS is a Web Server (which it seems to be since it then uses the HTTP port, but the DS only answers a few of all the possible HTTP requests and does not use the verbose and unsafe HTTP protocol).

**Incorrect Connections** may be valid HTTP requests that are not supported by the DS. As a result, you may want to have a look at the DS log for further investigations (in order to find who is trying to use your DS, and to do what).

A 'guardian' thread monitors the activity of the pool of threads of the DS. If one thread of the pool is blocked or lasts a too long time it is simply killed.

▶ **Note:** Some OS faults called 'Heisenbugs' (OS bug that disappears as measures are taken to

eliminate it. Example: it could be a timing bug in an I/O device driver that only appears when the CPU load is high or the driver is used in a faster processor. Inserting code to isolate the bug (hides it) can make your life miserable. The DS will do its best to cope with them.



## ☛ The DS HTTP Status Codes

The DS supports a few of the HTTP codes a HTTP server returns (highlighted below in blue).

Code	Name	Explanation	(URI: Uniform Resource Identifier)
<b>100 Informational codes</b>			
100	Continue	A partial request has been received. Submit the rest of the request.	
101	Switching Protocols	Agreement to switch the version of the HTTP protocol.	
<b>200 Successful codes</b>			
200	OK	The request completed successfully.	
201	Created	The request resulted in the creation of a new URI.	
202	Accepted	The request has been accepted for processing, but is not processed yet.	
203	Non-Original Source	The data returned may come from a proxy.	
204	No Content	No data available for the request, do not change the current document view.	
205	Reset Content	The client should reset the current document view.	
206	Partial Content	The server is responding with the results to a partial GET request.	
<b>300 Redirection codes</b>			
300	Several Choices	There are several locations that satisfy the client request.	
301	Moved Permanently	The client should permanently reset the current URI to be the URI specified.	
302	Moved Temporarily	The client should update the current URI with the requested URI.	
303	See Other	The client should use a different URI, performing another GET request.	
304	Not Modified	Target URI has not changed since the client's cached version was retrieved.	
305	Use Proxy	The requested entity must be accessed through a proxy.	
<b>400 Client Error codes</b>			
400	Bad Request	The request was not understood by the server.	
401	Unauthorized	The request requires user authentication.	
402	Payments Required	The request requires a payment by the client.	
403	Forbidden	The authenticated user does not have permission to access this resource.	
404	Not Found	The specified resource does not exist.	
405	Method Not Allowed	The request method is not supported by this server.	
406	None Acceptable	The resource may not have the proper content type for the client.	
407	Proxy Auth. Required	The client must first authenticate with the proxy.	
408	Request Timeout	The client did not complete the request in time.	
409	Conflict	The request could not be completed due to a resource conflict.	
410	Gone	The resource is no longer available.	
411	Length Required	The server requires a content-length header in the client's request.	
<b>500 Server Error codes</b>			
500	Internal Server Error	An unexpected condition prevented the server from completing the request.	
501	Not Implemented	The server does not support the request received.	
502	Bad Gateway	The gateway could not access the upstream server.	
503	Service Unavailable	The server is unable to handle the request at this time.	
504	Gateway Timeout	The upstream server did not respond to the gateway in time.	

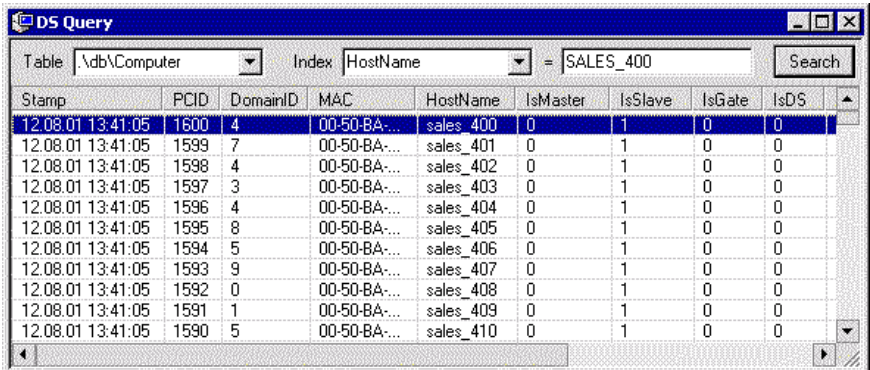
## The Query Button



This button displays the Query dialog box below:

You can list and search records of all the Tables of the DS Database by Index.


Fields ending with 'ID' are referring to a record of another Table (like 'NetworkID' in the Computer.Dat Table).



The screenshot shows the 'DS Query' dialog box with the following table of records:

Stamp	PCID	DomainID	MAC	HostName	IsMaster	IsSlave	IsGate	IsDS
12.08.01 13:41:05	1600	4	00-50-BA...	sales_400	0	1	0	0
12.08.01 13:41:05	1599	7	00-50-BA...	sales_401	0	1	0	0
12.08.01 13:41:05	1598	4	00-50-BA...	sales_402	0	1	0	0
12.08.01 13:41:05	1597	3	00-50-BA...	sales_403	0	1	0	0
12.08.01 13:41:05	1596	4	00-50-BA...	sales_404	0	1	0	0
12.08.01 13:41:05	1595	8	00-50-BA...	sales_405	0	1	0	0
12.08.01 13:41:05	1594	5	00-50-BA...	sales_406	0	1	0	0
12.08.01 13:41:05	1593	9	00-50-BA...	sales_407	0	1	0	0
12.08.01 13:41:05	1592	0	00-50-BA...	sales_408	0	1	0	0
12.08.01 13:41:05	1591	1	00-50-BA...	sales_409	0	1	0	0
12.08.01 13:41:05	1590	5	00-50-BA...	sales_410	0	1	0	0


This dialog is useful to list records by the order of your choice (you have to select the corresponding index). You can also search by index any table of the database like RA Connections, PC usage, and check the States of a PC for a given period of time to verify the free RAM level and the Disk(s) levels.

 A future release of the DS will allow you to edit the records directly from this dialog box.

## Using the DS ODBC interface to make SQL queries

SQL (Structured Query Language) is the method used for accessing data through ODBC (Open Database Connectivity). By using the DS ODBC interface you can query the DS database with SQL requests.

The DS ODBC interface grants you real-time (read) access to the DS database from your favorite ODBC compliant spreadsheet, report tool or custom solution. Microsoft Access, Word, Excel, Powerbuilder, Borland Delphi, Crystal Pro Report Writer and Visual Basic are just a few among the thousands of available ODBC compliant applications.

 **Note:** Some of our customers need this access to link the DS and their invoicing system so each new Remote-Anything SOS Call is -automatically- added to the Slave user account and properly invoiced at the end of each month.

Other users need to process the information pushed by all their Slave PCs (like inventories) in order to monitor their equipments, apply specific rules or raise alerts and eventually take an appropriate action by using Masters or the DS to reply to the Slaves PCs or users who need an immediate answer.

The screenshot shows the Microsoft Access database design view. The Relationships pane displays several tables and their fields:

- DOMAIN:** DeleteFlag, Stamp, DomainID, Description, ParentID, Level, PowerSaving, Days, Changed.
- COMPUTER:** DeleteFlag, Stamp, PCID, DomainID, IsMaster, IsSlave, IsGate, ChatSession, VoIPSession, MAC, HostName, Description, sSocket, mSocket, mOptsID, sOptsID, StateID, onDSLAN, AppDepl, PowerSaving, sSessionKey, mSessionKey, sSessionIV, mSessionIV, Tracked, TrackID, Changed.
- APPLICATION:** DeleteFlag, Stamp, AppID, AppName.
- HARDWARE:** DeleteFlag, Stamp, ID, Desc.
- HWRINVENT:** DeleteFlag, Stamp, PCID, HwrID, TypeID, Ver, DateInstalled, DateRemoved.
- ENDUSER:** DeleteFlag, Stamp, UserID, DomainID, MasterUser, Sex, Name, Email, Phone, Fax, Title, Password, Comment, RSAKeyID, Tracked, TrackID, Changed.
- CONNECTION:** DeleteFlag, Stamp, mPCID, mUserID, sPCID, sUserID, OnOff, RC, FB, Chat.
- STATE:** DeleteFlag, Stamp, StateID, PCID, State, UserID, IPAddr, OnOff, OS, CPU, RAM, Disks, NIC, Internet, Modem, Printer.
- SO5:** DeleteFlag, Stamp, PCID, UserID, DomainID, Closed, Text, Urgency, Gateway, IPAddr, UserName, Port.
- HWRTYPE:** DeleteFlag, Stamp, ID, Desc.

Below the design view, three data tables are displayed:

**APPLICATION : Table**

DeleteFlag	Stamp	AppID	AppName
+	1085421296	1	Adobe Acrobat 6.0.1 Standard
+	1085421296	2	Adobe Download Manager 1.2 (Remove Only)
+	1085421296	3	Adobe Reader 6.0
+	1085421296	4	Alexa Toolbar
+	1085421296	5	AMS Server
+	1085421296	6	AnswerWorks Runtime
+	1085421296	7	COMPVision
+	1085421296	8	e-Sword
+	1085421296	9	Internet Explorer Q831167
+	1085421296	10	lomega Automatic Backup
+	1085421296	11	LiveReg (Symantec Corporation)
+	1085421296	12	LiveUpdate 1.80 (Symantec Corporation)
+	1085421296	13	LiveUpdate Administration Utility
+	1085421296	14	Microsoft BackOffice 4.0

**ENDUSER : Table**

Stamp	UserID	DomainID	MasterUser	Sex	Name
+	1092403526	4	0	0	0 gguz
+	1092403526	5	0	0	0 idia
+	1092403526	6	0	0	0 tscan
+	1092403526	7	0	1	0 DOT
+	1093932539	8	0	1	0 Eric

**COMPUTER : Table**

IsGate	ChatSession	VoIPSession	MAC	HostName	Descripti
+	1	0	0 00-20-18-D9-3A-5F	HomeOffice	
+	1	0	0 00-00-56-4F-85-D7	DESK4	
+	0	0	0 00-0D-56-29-A8-B5	Russell	
+	0	0	0 00-04-75-E2-B5-D2	EPROXYGATE	
+	0	0	0 00-0B-DB-D4-98-17	XEON_4	

The DS ODBC interface is a DS option charged separately. If your DS license key lists the ODBC option then you can ask for the ODBC Interface package which will install automatically once copied in the DS folder.

## ☛ The License Button

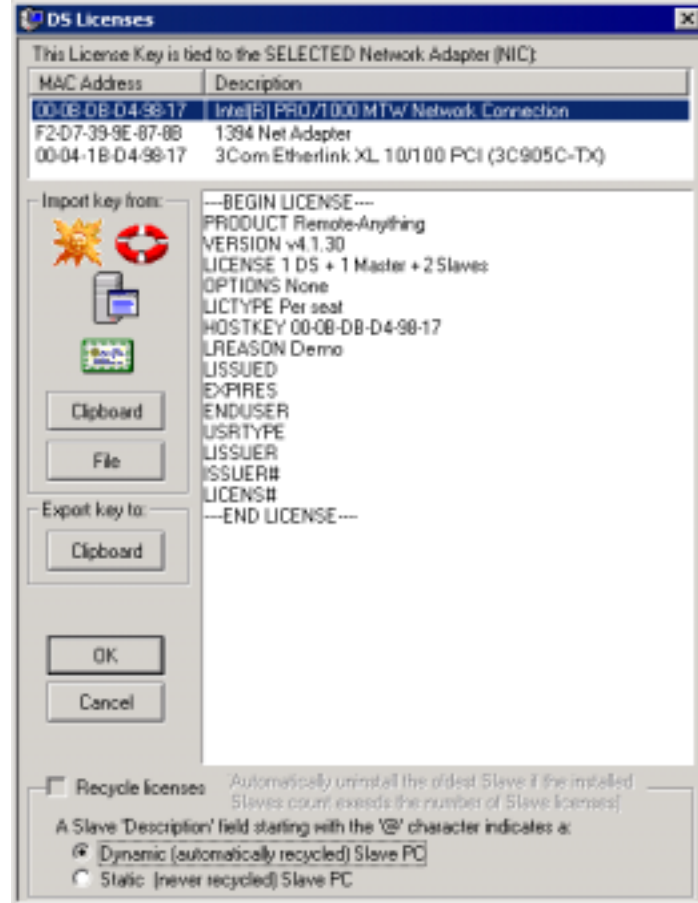


This button displays the License dialog box below:

As Masters no longer need a License Key with the DS, the DS needs one License Key. This DS License Key allows you to use the licenses you have purchased.

This key is based on the MAC address of the network adapter of your choice –just select the one you want to be used in the list.

The **'Recycle licenses'** option remotely uninstalls and replaces in the DS database the oldest Slave with a new incoming Slave PC (easier 'on-demand' deployments). You can also define exceptions with Slave PCs that will not be recycled or the inverse (Slave PCs that will be recycled).



## ☛ The About Button



This button displays the About dialog box below:

It show the number of active connections at a this moment and lists the web sites from which you can get information and support about TWD Industries' products.



## Troubleshooting the DS

Once correctly configured the DS will work out of the box. If it does not then either the Master/Slave or the DS configuration is incorrect. Please follow the procedure below:

Make sure that you are using the latest version of RA and of the DS, log on as 'Administrator' on each machine and:

### DS

- stop the DS Service from the Control Panel
- overwrite the old DS.exe file with the latest release
- delete the ../db sub-folder to reset the database
- restart the DS Service

### Masters

- close the Master application if it is running
- overwrite the old Master.exe file with the latest release
- restart the Master application

### Slaves

- stop the Slave Service from the Control Panel
- overwrite the old Slave.exe file with the latest release
- restart the Slave Service

Make sure all Masters and Slaves have the 'DS' option enabled, the correct DS 'Private', 'Public' IP addresses (or DNS names) and port number registered so they can send 'alive packets' to the DS (see 'Configuring Masters and Slaves for the DS' for more details).

If you are not sure of the ability of a Master/Slave PC to reach the DS then use telnet:

```
telnet <DS_IP_Address> <DS_Port_Number>      (ex: telnet 212.128.14.45 80)
```

If telnet fails to establish a connection with the DS then you have a routing problem. Check the way this Master/Slave PC is supposed to use in order to reach the DS machine and identify the point of failure with Trace Route:

```
tracert <DS_IP_Address>      (ex: tracert 212.128.14.45)
```

When Masters and Slaves register in the DS database you should see them listed in the main DS dialog box under the default Network (Sand\_Box). This process should take 3 or 4 minutes maximum.

After PCs and users are listed in the DS database, click on the 'Credentials' button to authorize Master PCs and Master USERS (and allow some Master users to access some Slave PCs).

If no PC is listed in the DS database then the configuration of the DS or of the Master/Slave PCs is incorrect. You have to return to the top of this troubleshooting procedure to find what's wrong and fix it.

Then, run a Master (using a NT user account that was registered in the DS as an authorized Master user) to query the DS. You can just push the 'search' button of the Master without typing anything in the 'Slave' or 'User' fields of the Master dialog box.

Slave PCs should be listed in the Master dialog box. Select any of them and click on the 'Remote Control' or 'File Transfer' button to establish a connection.

If you get the error message 'Access Denied' then you have not defined credentials for this Master PC or for the NT user account that you are logged into. Define credentials in the DS database and then try again to query the DS from this Master PC.

If no Slave PC is listed in the Master then check that this Master user has been allowed to access at least one Slave PC, and check that this Slave PC is online.

## 🎯 Performances of the DS

The DS is an optimized program. TWD Industries worked hard to provide a really scalable solution that will not hurt your budget because of crazy hardware requirements. Typical connections are accepted, handled, logged and closed in *0.05 second*. The DS was the only active application on our Windows 2000 Pro machines and the 'DS Load' dialog box was the only dialog on the screen (other windows were closed to save CPU).

The tests below do not reflect the maximum number of PCs a DS can handle (*this is directly related to the amount RAM rather than limited by the CPU*) but only focused on the worse case conditions your DS can meet under heavy DoS (denial of service) attacks.

### ➡ DELL OptiPlex GX400



CPU: Intel Pentium 4 1.7 Ghz, 256 KB L2 cache  
RAM: 512 MB PC800 (100 Mhz) RDRAM  
HDs: 2 40 GB IDE (7,200 tpm)  
NIC: 10/100 MB 3Com EtherLink

This machine handled 175 connections per second (85-90% CPU usage).

This represents 15,750 PCs sending 'alive packets' every 90 seconds to the DS.

### ➡ DELL PowerEdge 4600



CPUs: 2 Intel Pentium III Xeon 1.8 Ghz, 512 KB L2 cache  
RAM: 1 GB PC1600 (200 Mhz) DDR EEC SDRAM  
HDs: 2 hot-plug 18 GB SCSI Ultra3/U160 (15,000 tpm)  
NICs: Broadcom 1 GB and Intel 10/100 MB Ethernet

This machine handled 180 connections per second (50-55% CPU usage).

This represents 16,200 PCs sending 'alive packets' every 90 seconds to the DS.

With more connections, then the CPU usage brutally reached 100% (but was still OK).

The PowerEdge server costs much more than the OptiPlex desktop PC (and is supposed to be much more powerful) but has apparently similar performances. *How is it possible?*

## 👉 WinSock (the Windows TCP/IP stack) is the Bottleneck

The performances described in the above tests are likely to be much better in the real World because:

- we tested the most critical part of the activity of the DS: receiving Masters and Slaves attempts to register –an operation that takes place only during the initialization of the DS, not during the normal use (the DS is supposed to be always on so the initialization took place only one time)
- we did not conduct the tests with tens of thousands of real PCs (we just used a few PCs to send simulated connections to the DS). Because of this, we were limited in the number of connections per second for a given destination because of the TIME-WAIT state. This is a ‘by-design’ TCP/IP limitation and this is why a test is not relevant unless it is conducted with tens of thousands of physically networked PCs (something that we do not have at our disposal at TWD Industries):

**When a TCP connection is closed, the connection resources at the node that initiated the close are put into a wait state, called TIME-WAIT, to guard against data corruption if duplicate packets linger in the network (ensuring both ends are done with the connection). This can deplete resources required per-connection (RAM and Ports) when applications frequently open and close connections.**

⇒ The DELL PowerEdge server will handle much more connections than the DELL Optiplex desktop PC because it still has plenty of CPU and RAM resources available. Remember that the tests stressed the DS machine with constant incoming connections –something that you will never experience under normal operating conditions unless the DS is under attack (an even in this case, the DS will reject the connections it cannot handle to stay operational).

Microsoft states that WinSock 2.2 has the following performances with Windows 2000:

1. Windows 2000 Server has been tested with over 200,000 simultaneous TCP connections (Microsoft does not specify if the connections transmit something... and say nothing about the hardware or the time necessary to reach this number of connections. It is likely that it was not done on an Intel-platform...)
2. Internet Information Services (IIS) on Windows 2000 was highly ranked in SPECWeb96, handling more than 25,000 HTTP requests per second (Microsoft does not specify the hardware platform and the amount of memory used here ... notice that we are now far from the 200,000 connections above...)
3. Windows 2000 was used to set a land speed record of more than 750 Megabits-per-second (Mbps) on a transcontinental gigabit network consisting of 10 hops (Microsoft does not provide the Trace Route listing [latency]... and does not specify if 10 bytes or 10 GB were sent to calculate the transfer rate...).

Note: Winsock 2.x’s code is borrowed from BSD Unix... while Winsock 1.x was coded by Microsoft.



Back to reality now:

- On Windows 9x, the OS *limit* is 100 connections. You can edit this value (a DWORD for Windows 95 and a STRING for Windows 98/Me) in the Registry: [HKLM/System/CurrentControlSet/Services/VxD/MSTCP/MaxConnections](#). Keep in mind that if you set it to 200 or higher then Windows 9x/Me will be far less reliable.
- On Windows NT4 and Windows 2000 it depends on the available RAM but the OS limit is the size of the non-paged memory pool. On **Intel platforms** this pool cannot exceed 1/8 of the total physical RAM -with a hard-coded limit of 128MB on NT4 and 256MB on 2000 (so having more than 2GB of RAM is helpless in our case on Windows 2000). This leads -in theory- to a limit of 12,800 connections on NT4 and 25,600 on 2000 (alive TCP connections use 10KB). In practice, real-life users report that they hit the wall before 10,000 connections. Why? Simply because the Windows core threads (in the thousands), the Services and all the applications will be competing with your application for space in the limited non-paged memory pool.

Conclusion: do your own tests before you count on the official Windows benchmarks.

⇒ For the DS, the consequence is clear: one 2GB RAM Intel-based Windows 2000 server will be able to manage millions of PCs and will be limited to around 10,000 concurrent RA users doing file transfers or remote control *at the same time*.

Not many Help-Desk centers serve 10,000 customers at the same time so one unique DS machine should be more than enough for most needs.

## 🗨 The Disk

Unless the DS is running on a machine with *enough RAM to hold the entire database*, performance will be dictated by how fast the database is read or updated by the disk.

A Wide Ultra SCSI-3 hard drive provides about 75 non-sequential (random) and 150 sequential I/O operations per second. The transfer rates are not the bottleneck. The bottleneck is due to the 75/150 I/O transfers per second limitation:

$$(75 \text{ random I/O operations per second}) \times (8 \text{ KB transfer}) = 600 \text{ KB per second}$$

With only random disk read or write a disk will transfer at most 600 KB (0.6 MB) per second!

A hard drive consists of a set of drive platters with a set of arms with read/write heads that can move across the platters and read or write information from the drive platters. The heads and arms need to move in order to find the location of the hard drive platter that Windows asked to update. If the data is located on non-sequential locations on the hard drive platter, it takes significantly more time for the hard drive to move the disk arm and head to all of the necessary hard drive platter locations. The time difference between the non-sequential versus sequential case is significant, about 50 milliseconds per non-sequential seek versus approximately 2-3 milliseconds for sequential seeks.

## 🔴 Processors

When the disk is overloaded, the CPU usage grows and immediately after the memory usage grows too. This is simply because the connections cannot be processed in a timely fashion. As a result, Windows does its best to queue them. Unfortunately, this has a disastrous effect because doing this (dumping them in RAM and then on disk) is the slowest possible task.

That's a bad idea since the PC is already overloaded. This is like putting oil on your wheels while you are pushing the breaks pedal down to the metal. It does not help.

To save Windows from itself TWD Industries designed the DS so it will reject connections when the server is not able to cope with the workload -until the situation is back to normal. At least, this prevents Windows from crashing the server. Now, the only consequence of an oversized workload is that the DS rejects the connections that it cannot handle (if no load-balancing is available).

When the CPU is not the bottleneck, something else is the bottleneck (a primary candidate being the disk subsystem because disks are the slowest part of a computer), so the CPU is being wasted. The CPU is usually the hardest resource to expand (above some configuration specific level, such as four or eight on many current systems), so it should be seen as a good sign that CPU utilization is more than 95%.

The response time of transactions should be monitored to ensure they are within reason; if not, >95% CPU usage may simply mean that the workload is just too much for the available CPU resources. In this case, either CPU has to be increased or workload has to be balanced.


Look at the Performance Monitor (Perfmon.exe) counter "*Processor: Processor Time %*" to make sure all processors are consistently below 95% utilization on each CPU. "*System:Processor Queue*" is the processor queue for all CPUs on a Windows NT system.


If "*System: Processor Queue*" is greater than 2 per CPU, it indicates a CPU bottleneck. When a CPU bottleneck is detected, it is necessary to either add processors to the server or reduce the workload on the system.

## **Conclusion**

If you are going to increase the number of users that the server is to support then you will have to (in order of efficiency):

- Store the whole DS database in a RAM disk (so random disk seeks will be much faster)
- Add RAID 5 disks to your server (to reduce the random disk seek latency statistically)
- Add a caching controller (to prevent random disk seeks from happening when possible)
- Add RAM to your server (to prevent random disk seeks from happening when possible)
- Add a processor (to add processing power if the CPU is overloaded)




 The DS database has been designed to be compact: you can count approximately 1 MB for 1,000 PCs so 1 GB of free space on disk leaves room for 1,000,000 PCs.

 A 2 GB RAM Intel-based Windows 2000 DS server will be able to manage millions of PCs and will be limited to around 10,000 concurrent RA users doing file transfers or remote control *at the same time*.


Not many Help-Desk centers serve 10,000 customers at the same time so one unique DS machine should be more than enough for most needs.

It is likely that you will never have to invest in a lot of expensive hardware for the DS.

## Remote Administration of the DS

The  DS can be remotely installed, configured and used by installing  Slave.exe on the DS machine. Doing this, you can access the DS from any  Master PC -providing that you have the appropriate credentials (or password if you are using a Slave which is not tied to a DS) to access the DS machine.

You can either use a Slave tied to this DS or a Slave not tied to a DS: it may be safer to use a Slave that does not need the DS to be operational (this will allow you to start and stop the DS, do some database file maintenance, etc. even if the DS is not running).

 A simple 'RA - Individual Pack' (1 Master + 1 Slave) will do the job!

# How safe is the DS?

## The Security of the DS

The DS is handling critical information about a network. This may not be a real issue if you are using the DS on a LAN (because this information is already publicly available on your LAN) but most DS users will use it with a WAN. That's why the DS security has been carefully studied before being implemented.

## Passive Defense

### Masters/Slaves are no longer listening to ANY port

⇒ This makes them invisible for an attacker since they cannot be reached. Because they cannot be reached, nobody can even try to attack them. That's the *security "by design"*.

### The Time Zone Filter

⇒ This makes it impossible for authorized Masters to reach Slaves during the hours of your choice for each day of the week. Only a DS administrator can modify this option so no remote user can bypass this security even if a Master user or Master PC is compromised or working after hours.

## Active Defense

### 2048-Bit Asymmetric RSA encryption

RSA, one of the most widely used asymmetric encryption methods, relies upon the fact that factorization of large prime numbers is difficult. 'Asymmetric' comes from the fact that it uses two keys: a public and a private key. The private key cannot be derived from the public key without excessive effort –excessive in this case meaning something more than all the computational power available in the (known) universe. What is considered infeasible today may be feasible tomorrow but there is no way to protect us against this.

The mechanism that makes public key cryptography so useful is that data that has been encrypted with a private key can only be decrypted with the corresponding public key –and

reciprocally. It is not possible to decode encrypted data with the key used to encode the plain-text message. Other differences with symmetric encryption: asymmetric encryption is 1,000 times slower and the encrypted message is much larger than the original message. That's why asymmetric encryption is mostly used to code symmetric keys –and not data.

Why using a 2048-Bit RSA key while the symmetric AES key is only 128-Bit long? Well, public keys need to be much larger to ensure the same level of security that is possible with a much smaller symmetric key. A 80-Bit symmetric key has approximately the same strength as a 1024-Bit public key.

During the August 1999 RSA challenge a RSA 512-Bit digit was factored. This required 35.7 CPU-years distributed on 292 workstations and high-speed computers, plus a massive amount of storage for intermediate results. Calendar time was 3.7 months. This considerable effort has to be repeated for each RSA key to crack. This means that a 512-bit RSA key can be cracked -if it is worth spending so much resource (\$1,000,000).

While RSA 1024-Bit keys are supposed to be safe during 5 years, a RSA 2048-Bit key is for long-term secrets that are supposed to last more than 10 years. This sounds good.

### 🔑 **2048-Bit RSA Public Keys used for Symmetric Session Keys negotiation**

How to setup a secure session between a server and a remote client over an unsafe link like the Internet is a difficult problem that has been studied for many years. Protocols like Diffie-Hellman have been proposed but they are vulnerable to man-in-the-middle attacks. Patches like SRP or PAK exist but are patented and add to the connection initialization overhead.

Our feeling at TWD Industries is that security must come from a simple publicly available design –not from a so complex scheme that nobody is willing to spend the time necessary to analyze it and say if it is really safe or just too complex to be understood at first glance. If people can find at first glance that the security scheme is safe then that's far better.

⇒ When registered the DS creates a 2048-Bit RSA Key. During the personalization process Masters and Slaves receive the public RSA key while the DS keeps the private RSA key secret. Each Master user also gets a private 2048-Bit RSA key to allow the DS to authenticate Master users without possibility for Masters to repudiate connections.


When a Master or a Slave is signing up with the DS, the DS encrypts a (true) randomly generated 128-Bit symmetric session key with its RSA private key, signs it and sends it to Master/Slave. Then, Master/Slave decrypts it with its public RSA key, checks if it matches the signature and starts an encrypted session with the DS if all goes well.

Since nobody has access to the DS RSA private key no session key can be forged by an attacker. If a pirate has access to the DS machine then he will surely prefer to add credentials for an external Master rather than trying to find the DS private key to try later man-in-the-middle attacks. Pirates are not masochists.

How safe this security scheme is? Let's see all the possible cases:

- A man-in-the-middle\* is replacing the random symmetric key by something else:
  - since he does not know the DS private key the signature does not match the symmetric key and Master/Slave closes the connection. The attack fails.
- A stranger\* Master/Slave is trying to access the DS:
  - if he does not know the public key the signature does not match the symmetric key and the DS closes the connection. The attack fails.
  - if he knows the public key (he got it from someone in your organization) the signature matches the symmetric key and the DS starts a normal session.
    - if that's a Slave then it will show up in the DS list as a PC that can be controlled by Masters once credentials have been defined. That's not a security issue.
    - if that's a Master then, depending on the fact that he knows (or not) a valid Master user name, password and the corresponding RSA key:
      - he will impersonate a valid Master since he got all the secrets (the DS public key, the Master user name and its associated password and RSA key) from someone in your organization. The restrictions attached to this Master user will apply: reachable Slaves, time-zone filter (restricted hours).
      - he will not be able to get anything from the DS until the DS administrator has explicitly enabled the new Master PC and then defined credentials, a password and generated and sent a private RSA key for this new Master user. The attack fails.

[\*] See the note below.

 **Note:** If the “*Allow DS-LAN Masters only*” DS option is enabled then man-in-the-middle and stranger Master attacks are possible only if it is conducted by someone acting from within your LAN. As long as your LAN is not compromised these attack cannot be performed. *In all the cases, man-in-the-middle attacks fail.*

⇒ The DS can be used by a stranger Master ONLY IF mobile Masters are allowed AND a Master user from your organization gave all the secrets to a pirate. At this stage, this pirate has probably the key of your office door so one may wonder why he would bother to use RA while he has physical access to your machines during the night or during weekends.

If you need to allow mobile Master users then restrict the access rights of Master users. Accountants must not be able to access R&D machines. If one of your Master users happens to divulge confidential information then the leaks will be limited to his credentials.

In order to prevent Denial of Service or brute force attacks targeting the session key exchange (which consumes CPU resources by crushing large prime numbers) a first round of authentication is processed *before* session keys are negotiated.

### 🔒 **Replay protection**

⇒ Encryption and hashing are initiated with 'salted' values (values nested in meaningless data) and initialization vectors that take the current date and time into account. This means that replay attacks cannot take place because the values used in a past session cannot be used again in a future session.

### 🔒 **Data integrity**

⇒ Because encryption does not prevent data modification every chunk of data sent over the wire also uses Hash based Message Authentication Codes (HMAC) to check the integrity of the message. Only the owners of the private symmetric key are able to make and verify an HMAC. An impostor will not be able to forge an HMAC. Those symmetric keys are random session keys that are different from the encryption session keys.

### 🔒 **128-Bit AES encryption (FIPS 197) and rotated Session Keys**

⇒ Advanced Encryption System (AES) is the secure encryption standard designated by the Federal Information Processing Standard (FIPS) 197. All the connections are encrypted with AES 128-Bit private session keys. The session keys are rotated randomly and random padding is used to prevent plain text attacks. Any connection that transfers corrupted data (data that remains meaningless after decryption) is immediately closed –protecting the DS from unauthorized connections and man-in-the-middle or hijacked-connections attacks.



Because encryption does not prevent data modification every chunk of data sent over the wire also uses Hash based Message Authentication Codes (HMAC). This allows for data integrity.

128-bit symmetric encryption has never been broken. According to RSA Labs, it would take a trillion-trillion years to crack 128-bit encryption using today's technology. But if your organization needs to use larger session keys just drop us a line: the DS will just need to be recompiled to provide you with longer keys. The DS implements 128-Bit symmetric encryption for legal reasons but some organizations are allowed by their government to use larger keys.

### 🔑 Why Encryption is Optional

⇒ Given the obvious benefits of a proper encryption implementation one may wonder why this is an option for the DS. Well, some users have a safe WAN with leased lines and the only users are network administrators. Their work is about administrating hundreds of servers in a secure environment and they just need to access machines without wasting precious CPU cycles. Encryption is just a waste of CPU resources and a latency aggravation factor for them.

### 🔑 Buffer overflows protection

⇒ While the DS is not an HTTP server, it will look like one for the external world and will be using the port of your choice (80, 443 or 389 may be good choices). The DS is using one port only and it has been protected against oversized, malformed -or unknown HTTP requests (particular care has been taken to make sure that the DS is not exposed to buffer overflows or 'magic words').

### 🔑 No access to the system layer

⇒ The only thing that one can do with the DS is submitting new information or requesting existing information from the DS database. This way, as it is not possible to reach the file or with the system layer -or to interact with it by using scripts or compiled code (DLLs, ActiveX components, Java, VB script, etc.), using the DS is far safer than letting your users surf on the Web.

### 🔑 Monitoring and Logging

⇒ All requests and connections attempts are logged (in a log file) and you can monitor in real-time the DS activity with a 'Task-Manager like' dialog box.

### 🔒 Denial of Service protection

⇒ The DS has been extensively tested with huge workloads (up to 10 times the physical capacity of the server CPU). And TWD Industries has implemented security processes to prevent denial of service attacks: if the DS receives more requests than it can process then it simply discards the extra load (eventually redirecting it to a co-DS if any is defined in the options). Specific code has been added to stabilize the Windows TCP/IP stack (because it never recovers by itself when faced to an oversized workload -even if the workload slows down later...and ends by consuming all the RAM before crashing the system). The DS will not go down even if you are not there to take the appropriate actions to reduce an abnormal workload.

### 🔒 Why not use established standards like SSL/TLS?

The fact that many vendors rely on a widely used standard does not mean that this standard is secure. It just means that people believe what the standard promoters tell them. The DS has been designed to be as secure as possible and SSL/TLS are not secure enough for the DS. If the goal is really to make users safe then we find it criminal to tell users that they are secure when this is not the case –especially with critical business activities like e-commerce, remote-control tools or VPNs.

Having said this we have to explain why SSL/TLS are unsafe. The devil is (again) in the design: *it does not matter how good the encryption algorithm is if the authentication lacks.*

1. SSL/TLS *blindly* accepts *any* key providing that one Certification Authority (CA) among the *dozens* available *seems* to associate it to the *user name* you are expecting. What's wrong here? You have absolutely no control nor guaranty about how, where and for who the key was generated so you *cannot* be sure that a key is from the right person (*the DS instead associates each Master user with a unique private key and cannot be fooled about a key/owner pair since the DS is its own Certification Authority (CA).*
2. SSL/TLS protects the user name of the key but not the IP address. Since name resolution (DNS) is *not* protected it can be modified on the client side, the server side, or on any of the

involved DNS servers. How useful is it to have a successful authentication if you are not talking to the right person? *(going through the DS authentication is the only way to get in touch with a correspondent –and this is the DS who does the handshaking for you so you are sure that your peer is the expected one).*

3. Microsoft has experienced the limits of SSL/TLS the day someone called “Administrator” requested a Microsoft certificate from Verisign... and got it. Are you really believing that paying total strangers a small annual fee will make them take care about the security of your organization? If you have something to loose then think twice *(the DS allows you to avoid using third parties –saving your money and making sure that your business will stay for your eyes only).*
4. Most SSL/TLS *implementations* suffer from critical security breaches (a search “SSL + vulnerabilities” on Google reports 124,000 relevant links) that allow for remote execution of arbitrary code, denial of service and disclosure of sensitive information. As a result, SSL/TLS is far from being a guaranty of security for vendors and end-users.

SSL/TLS do not preserve the confidentiality and the integrity of your data. Worse, as the SSL/TLS traffic is encrypted nobody will notice that a pirate is playing with your financial information. With this in mind, SSL/TLS does not sound desirable to us.

## 👉 Conclusion

The DS security is using higher security standards than the most demanding client/server applications. At the same time, it also minimizes the costs involved in the deployment of the security scheme and does not delegate the most critical part of the security chain to any third party.

If a DS database is compromised, it is likely that the machine hosting the DS was compromised, not the DS. In this case, the attacker will have a list of your users but will not be able to reach them or their PCs.

Suggestions and feedback are welcome: ✉ [feedback@twd-industries.com](mailto:feedback@twd-industries.com)

For more information about security, please consult the RA Reference Manual.

## **Technical Support**

TWD Industries provides free Technical Support to registered users the first year and to users testing the product:

- Email: [support@twd-industries.com](mailto:support@twd-industries.com)
- Telephone: (Hours: 9:00 AM to 6:00 PM, Greenwich Meridian Time+1)
  - Voice +33 (0)492 940 510
  - Fax +33 (0)492 940 512

Please read the latest FAQ on <http://www.remote-anything.com> to solve common issues.

## **Program Updates**

New versions of the DS are free the first year for registered users, just download the latest version from:

<http://www.remote-anything.com/en/news.htm>

Our products are constantly evolving and so is your investment with TWD Industries.

## **Small Glossary of the Network Terminology used in this Manual**

Networking is a complex subject and many experienced computer users feel confused about some words they simply do not understand. So, here is a small introduction to networks that is intended to make you feel more comfortable with those barbarian terms.

**LAN (Local Area Network):** a private network of several PCs.

**WAN (Wide Area Network):** several interconnected LANs via leased lines or the Internet.

**IP (Internet Protocol):** this is a protocol (a language) used by computers and devices like routers, printers, etc. to communicate over a network. This is also the protocol used by the Internet. IP supports two transport protocols: TCP and UDP.

**TCP (Transport Control Protocol):** this is a connection-oriented protocol which involves two computers for an exchange of information (see it as a phone call: you dial to call someone, talk from both sides and then hang up). TCP is reliable since it checks that the packets it sends are received by the other end. RA is using TCP for 'remote-control' and 'file-transfer' sessions.

**UDP (User Datagram Protocol):** this is an unconnected protocol (see it as bottle you throw in a river: it may reach your friend located below but it may be lost). UDP is not reliable but is faster than TCP since it uses far less resources. RA is using UDP for the 'Chat', 'Wake-on-LAN' or 'Get Hardware Information' features.

**IP address (Internet Protocol address):** this is a 4-byte logical address (an address that can be defined by the user) used to reach another machine (or 'node') over the Internet or on a LAN (see it as the phone number you use to dial to talk to your mother). Some IP addresses are reserved:

- if it ends with zero(s): 137.50.4.0 or 137.50.0.0, then it specifies a network
- if it ends with 255: 13.4.2.255 or 13.4.255.255, then it defines a broadcast address (or a mask)
- if it starts with 127: 127.50.10.121 or equals 0.0.0.0, then it specifies the local machine
- if it starts with 0: 0.68.10.11 or 0.0.10.11, then it defines an address on the current network
- 255.255.255.255 is a 'limited broadcast' used on a LAN, it will be blocked by routers

Example of a valid IP address that can be assigned to a computer: 192.168.124.12

**Public or routable IP address:** this is an IP address that everybody can use on the Internet. Some of these addresses have been assigned to geographical regions:

- 194.0.0.0 – 195.255.255.255, Europe
- 198.0.0.0 – 199.255.255.255, North America
- 200.0.0.0 – 201.255.255.255, Central and South America
- 202.0.0.0 – 203.255.255.255, Pacific Area

Example of a valid public IP address: 213.18.124.12

**Private or non-routable IP address:** this is an IP address that can be ONLY used on a private LAN. As specified in the RFC 1597 issued in March 1994, the following IP addresses can be used for private networks:

- 10.0.0.0 – 10.255.255.255, allowing 1 network of 16,777,214 IP addresses
- 172.16.0.0 – 172.31.255.255, allowing 16 networks of 65,534 IP addresses each
- 192.168.0.0 – 192.168.255.255, allowing 256 networks of 254 IP addresses each

Example of a valid private IP address: 192.168.124.12

**WAN IP address:** this is the public (or routable) IP address of a Slave PC located on a LAN.

**NAT (Network Address Translation):** NAT is used to translate a private IP address to a public IP address. Example: a Master user can reach a Slave PC located on a private LAN via a router connected to the Internet doing NAT (see it as a phone center dispatching customer's incoming calls to the internal lines of a corporate building).

**NIC (Network Interface Card):** a network adapter (usually for Ethernet or Token Ring) that allows you to connect your computer to a local LAN.

**MAC (Media Access Control):** a 6-byte physical address (i.e. an address burned into the silicon of your hardware) which allows computers to translate (with the ARP protocol) a logical address like an IP address into something related to a physical device like a computer. The MAC address is supposed to be unique: the first 3 bytes are the manufacturers identifier and the rest is used to define  $2^{(3*8)} = 16,777,216$  unique cards for each manufacturer. Example: 00-50-BF-12-D4-98

## License Agreement

The software described in this document is provided with a License Agreement and may not be used without acceptance of the terms of this License. This software is licensed, not sold. The fee you pay entitles you to use the software, not to own it. The software is copyrighted material and its exclusive distribution rights are owned by TWD Industries SAS.

This is a legal agreement between you, the end user, and TWD Industries SAS, a French company.

**GRANT OF LICENSE** – This TWD License Agreement permits you to use one copy of the TWD Industries software product acquired with this License on any single computer, provided the software is in use on only one computer at any time. If you have several Licenses for the software then at any time you may have as many copies of the software in use as you have Licenses. The software is "in use" on a computer when it is loaded into the temporary memory (i.e. RAM) or installed into the permanent memory (e.g. hard disk, CD ROM, or other storage device) of that computer, except that a copy installed on a network server for the sole purpose of distribution to other computers is not "in use". If the anticipated number of users of the software will exceed the number of applicable Licenses, then you must have a reasonable mechanism or process in place to assure that the number of persons using the software concurrently does not exceed the number of Licenses.

**MANDATORY REGISTRATION.** This software contains technological measures that are designed to prevent unlicensed or illegal use of the software. The license rights granted under this license are limited to the first thirty (30) days after you first run the software unless you supply information required to register your licensed copy in the manner described on <http://www.twd-industries.com>. You can register the software through the use of the Internet or telephone; toll charges may apply. You may also need to register again the software if you modify your hardware or alter the software.

**COPYRIGHT** - The software is owned by TWD Industries or its suppliers and is protected by United States copyright laws, international treaty provisions, and all other applicable national laws. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that if the software is not copy protected you may either make one copy of the software solely for backup or archival purposes, or transfer the software to a single hard disk provided you keep the original solely for backup or archival purposes. You may not copy the Product manual(s) or technical and commercial written materials accompanying the software.

**OTHER RESTRICTIONS** – You may not rent or lease the software, but you may transfer your rights under this TWD Industries License Agreement on a permanent basis provided that you transfer all copies of the software and all written materials, and the recipient agrees to the terms of this agreement. You may not reverse engineer, decompile or disassemble the software. Any transfer must include the most recent update and all prior versions.

**LIMITED WARRANTY** – TWD Industries warrants for a period of 60 days from the date of receipt that the software will perform substantially in accordance with the accompanying Product Manual(s) and any TWD Industries supplied hardware accompanying the software will be free from defects in materials and workmanship under normal use and service for a period of one year from the date of receipt. Any implied warranties on the software and hardware are limited to 60 days and one (1) year, respectively.

**TECHNICAL SUPPORT AND PROGRAM UPDATES** – TWD Industries offers free technical support and free program updates the year that follows your first purchase of TWD Industries products. Then, technical support and program updates are charged annually (maintenance fee) at the rate of 10% of the total price of all your licenses. If the maintenance fee subscription has been discontinued for a while and then later restarted then the amount of the maintenance fee for the first new year of subscription is calculated as follows:  $\text{fee} = \text{fee} + ((\text{fee} \times \text{years}) / 2)$ . Further years of maintenance are then charged at the normal rate.

**CUSTOMER REMEDIES** – TWD Industries' entire liability and your exclusive remedy shall be, at TWD Industries' option, either return of the price paid or repair or replacement of the software or hardware that does not meet TWD Industries' Limited Warranty and which is returned to TWD Industries with a copy of your receipt. This Limited Warranty is void if failure of the software or hardware resulted from accident, abuse, or misapplication. Any replacement software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer.

**NO OTHER WARRANTIES** – TWD INDUSTRIES DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE ACCOMPANYING PRODUCT MANUAL(S) AND WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS.

**NO LIABILITY FOR CONSEQUENTIAL DAMAGES** – IN NO EVENT SHALL TWD INDUSTRIES or its suppliers be liable for any other damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use this TWD industries product, even if TWD industries has been advised of the possibility of such damages. In any case, TWD industries entire liability under any provision of this agreement shall be limited to the amount actually paid by you for the software.

**U.S. Export Controls:** You agree that you will not export or re-export these products to any country, person, entity or end user subject to U.S.A. export restrictions. Restricted countries currently include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea and Syria. You warrant and represent that neither the U.S.A. Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges.

This Agreement is governed by the French laws and the competent Tribunal is Antibes, France. Should you have any question concerning this Agreement, or if you desire to contact TWD Industries for any reason, please mail to: [info@twd-industries.com](mailto:info@twd-industries.com).