

whitepaper

	page
☐ INDEX	
↳ 01. introduction	01
ProactivaNET® – Leading tool in administration of networked PCs	01
Specific characteristics of ProactivaNET®	01
Which products form part of ProactivaNET® ?	02
1. ProactivaNET® Inventory : <i>Automatic audit and inventory</i>	02
2. ProactivaNET® Service Desk : <i>Incidents Management</i>	02
↳ 02. Technical description of the products	03
Architecture and components	03
a) audit agents	04
b) conditions for running the agents	05
c) System to incorporate data on server	06
d) central repository for the data	06
e) Web application	06
f) Data access interface	06
Technologies used	07
Technical requirement	07
Other installation requirement	07
↳ 03. Implementing and updating the solution	08
Implementation schedule	08
Scheduled updates and new versions	08

ProactivaNET® >>> Leading tool in the administration of networked PCs

When a computer network grows to a significant size, it becomes very costly to manually keep the information on the computers, their settings and characteristics and the installed software licences up to date. In this case we need to use an automated solution that will check and update the state of the network at low cost, whilst also allowing us to manage any incidents that come about and automatically install upgrades and/or new programmes.

ProactivaNET® is the solution that allows you to automatically manage your network, generating an inventory that is always up-to-date and providing you with details on the state of your computer network:

- ↘ Incorporated hardware and software and characteristics (versions, licence control...).
- ↘ System configuration.
- ↘ Automatic, configurable installation of software throughout the network.
- ↘ Management of incidents generated by any hardware or software element in the network.

This solution is of great utility, since it allows administrators to carry out a series of key tasks for the correct administration of the computer network:

- ↘ Detection of computers with obsolete **hardware** and automatic classification in the different **locations**.
- ↘ Reports on licences installed and their level of use, along with detection of unauthorised software.
- ↘ Detection of outdated antivirus software.
- ↘ Reports on DLL and executable file versions.
- ↘ Detection of registration keys and flexible queries on the configuration of the computer.
- ↘ Alerts on changes in the network.
- ↘ Identification of user access to the computers.
- ↘ Registration of warranties and administrative details of each system.
- ↘ Installation of new applications or security upgrades in selected network elements.
- ↘ Changes of settings in the network computers selected automatically.
- ↘ Creation of incidents, integrated with all the inventory data, in line with ITIL practice.

specific characteristics of ProactivaNET®

ProactivaNET® also offers other specific characteristics, making it unique in its range:

- ↘ **Extremely light** implementation, data traffic volume and setting up.
- ↘ **Totally flexible implementation**, particularly notable in networks that go beyond the LAN, geographically scattered, with laptops, low quality connectivity, computers that are only connected occasionally...
- ↘ Generation of an **open central data repository**, which can be integrated with your management system.

which products form part of ProactivaNET®?

The administration of any computer network can benefit from an automated tool that helps in the management of the inventory and the incidents generated by the network, and in the automatic distribution of software,

although it is in medium-to-large or geographically scattered organisations where the benefits and savings of this solution are most notable.

The **ProactivaNET®** family of products comprises three independent products, fully integrated and mutually complementary, sharing key information for better management and administration of the network:

↘ **ProactivaNET® Inventory** – Tool specialised in drawing up inventories for networked PCs

↘ **ProactivaNET® Service Desk** – Tool for the management of incidents based on ITIL methodology

1. **ProactivaNET® Inventory: *Automatic audit and inventory***

ProactivaNET® Inventory is the leading tool in the management, administration and automatic inventory of networked PCs. With practically insignificant network traffic and extremely light implementation and commissioning, it allows you to obtain complete information on any component in the computer network right from the start. The audits and personalised fields, along with the integration with Active Directory and the other products in the suite, make it a must have-tool for all computer administrators.

Software delivery allows us to automatically deploy and install software packages on selected computers in a fully unattended way, avoiding the configuration of any additional components in the targeted equipment.

3. **ProactivaNET® Service Desk: *Incidents management***

ProactivaNET® Service Desk facilitates the management of incidents, from initial registration through to close, incorporating international standards of good practice such as ITIL, **ProactivaNET® Service Desk** allows integration with **ProactivaNET® Inventory**, with both forming a basic tool to optimise any IT service.

technical description of the products

architecture and components

The tools which form part of the **ProactivaNET®** suite are modular systems, formed by independent systems and elements which exchange information and interact amongst themselves. Thanks to this modularity, **ProactivaNET®** can adapt for implementation in very diverse environments.

Each **ProactivaNET®** tool is made up of the following main elements:

- a. Audit agents, who will audit each one of the networked PCs. (only in ProactivaNET® Inventory)
- b. A **relational database** where all the information regarding the computer system is stored.
- c. A **Web application** to exploit the database information.

There are other mechanisms which complete the operation of the system, such as:

- d. **Parameterisation** of the audit of each PC and of the communication mechanisms between products.
- e. **System for incorporation of automatic data** in the databases.
- f. **User browser** to access the web application (MS Internet Explorer).

By way of example, there is an outline of the components and internal connections of **ProactivaNET® Inventory** (product with greatest number of components):

a] audit agents

ProactivaNET® Inventory has several audit agents capable of extracting information from the computer system:

- ↘ **Agent Win32:** panagent.exe is a small executable file (approx. 300Kb), which, as it is run locally on a PC, can audit the PC and issue an XML data package containing all the information regarding the machine (hardware, software and system configuration).
- ↘ **Active Directory Agent.** An audit agent which obtains information stored in the Active Directory and integrates it in ProactivaNET® Inventory with the other data obtained by the previous agents.

The **Win32 Agent** can also be distributed as embedded **ActiveX** in a webpage (such as the corporate intranet portal), thus providing additional forms of distribution.

The agents are designed to collect the information from all the **Windows** operating systems, whether clients or servers. The agents take information from each computer, basically from the operating system **APIs**, from the **BIOS** of the machine and from **registration keys**.

The information it obtains may vary slightly depending on the audited operating system, this being grouped together as follows:

- ↘ **Hardware characteristics:** data regarding processor, RAM, model, BIOS version, used and available HD, video cards, audio cards, peripherals, etc.
- ↘ **System data:** Operating system, service pack, explorer, network environment data, environment variables, shared resources, logins and domain, etc.

- ↘ **Installed software data:** Applications installed, version and installation date.
- ↘ **File existence data:** search for files in the folder structure. It also obtains the file creation date.
- ↘ **Configuration and registration:** The agent searches for registration keys and obtains their values, allowing us to obtain any data on the configuration of the computer.

Whenever we so wish, we can configure the agent to run and gather exactly the information we need at each moment. This configuration basically parameterises:

- ↘ Which registration keys will be audited
- ↘ Which files will be detected

With the information obtained, the agents generate a data packet in XML format, compressed and encrypted using RSA (public/private key encryption), which can be saved to disc as a text file or sent directly to the application.

The main characteristics of the Audit Agent of ProactivaNET® are:

- ↘ **Minimum traffic.** The reduced size both of the executable file and the XML packet generated for each machine (approx 5 Kb) make the system extremely light and easy to implement, whilst it can be run over the network without saturating it, even with narrow broadband, or over the Internet.
- ↘ **Low impact.** The agents do not disturb the normal operation of the client computer, since they run, extract the information and close, without any resident modules. Execution does not usually take longer than 1.5 seconds on average, and it can be run in the background without disturbing the user's work.
- ↘ **Robustness.** If we come across any potential problems after running the agents, these simply close. They do not produce any error in the computer, nor do they impede or obstruct the operation of the other applications.
- ↘ **Independence.** The agents do not need to be installed, as they run independently from the rest of the system modules, and do not require any external element to complete the audit.
- ↘ **Flexibility.** The agents have a large number of parameters which allow their behaviour to be modified. This allows easy adaptation to the characteristics of the client network.
- ↘ **Safety.** The information generated by the agents is encrypted at source with a public/private key, for greater security in the traffic of data.

b] conditions for running the agents

There are several ways to explain the way the ProactivaNET® Inventory audit agent works:

- ↘ The Win32 agent (panAgent.exe) can be run directly from a **script log-in line** when users log in. In this manner we have a single executable file, which will generate a new XML report every time a user logs in on each one of the machines of the domain.
- ↘ It is also possible to configure the PCs for them to run this file when **starting up** the PC (start group, registration key), generating an XML report on each machine with each start up.
- ↘ From the **command line** we can also run an agent found in a file, in an e-mail, on a floppy disk, etc., allowing us to include in the inventory computers which do not have a network connection, or which are scheduled to run every certain period of time.
- ↘ The audit agent in **ActiveX** can be deposited in web pages frequently visited by the users of the network, meaning every time they access the page the ActiveX will run and carry out their work.

All these formulae can be combined simultaneously in a single environment, in order to ensure that all computers are included in the inventory, regardless of their situation.

In most cases, it is sufficient to have a single file with the agent in the network, meaning the cost of updating to new versions is practically nil.

c] system to incorporate data on the server

There are also several possible systems to send the data from each running of the agents to the application server, giving the implementation enormous flexibility. These are the most common mechanisms:

- Every time the agent generates the XML data batch, it can **send it online** to the server, either by ODBC or SMB, or by simply using the POST method. The only requirement is to have **TCP-IP connectivity**.
- Should we not have online access to the application server when running the programme, the result of the audit can be temporarily stored as a text file in XML format, which will then be sent to the server from any computer which has a connection.

When the data of each machine reach the application server, they are first processed by way of a script, which transforms them before feeding them to the database:

- The script checks whether it is the first time for this specific machine, either to enter it as a new item in the network, or in order to compare with the previous audit for this machine, in case changes in the network need to be reported to the administrator (events and alerts).
- The script reads the XML file, normalises it and incorporates it in the SQL database. At this moment it can also parameterise the processing of the information in order to take different decisions:
 - The location of the computer is determined automatically by the script, through patterns for Hostname, IP, Domain, additional information added, subnetworks...
 - Configure specific alarms which trigger under certain conditions (little HD space available, little RAM, new applications installed...)
 - Separate the XMLs considered defective or strange, for assessment by the network administrator.
 - Any other "intelligent" decision which can be taken based on the data found.

d] central repository for the data

The central repository which stores the information of the computer audits is an open SQL database. It can be either MSDE (free MS SQL motor), MS SQL Server (7.0 or later) or Oracle (9i or later), and, in all cases, there is free access to the database and to the data stored in it. All the necessary documentation is provided, allowing for integration with the client's existing systems.

e] web application

The application which exploits the inventory data is implemented as a web application on the Microsoft IIS (Internet Information Service) server. The application is formed by pages developed in JavaScript, C# and .NET, using a development framework which allows quick implementation, robust results and a common, coherent interface.

This web application may reside in the same machine as the database, or in separate machines.

f] data access interface

The web application which manages the inventory can be accessed from any PC which has HTTP access to the server and MS IE browser version 6.0 or later, or IE version 5.5 updated with some components.

As it is not necessary to install any client software in order to access the inventory, the system administrator may access the data of his/her system from practically any point on the network.

Moreover, using IE for web browsing means we have an extremely simple and intuitive interface, which minimises the need to train users with regards to this application.

technology used

All the technologies used in the development of the tool are market standards, backed by companies such as Microsoft and Oracle.

- The **audit agents**. In the executable versions they are simply invoked from the command line using any means. In the ActiveX version they are embedded in any frequently visited webpage.
- The **result of an inventory** is a plain text file, with XML structure, meaning it can be integrated with any existing system.
- The **sending of data packages** via the client's network is done using http (POST dispatch to a webpage, over TCP-IP) or via ODBC.
- The **database** is open, in SQL. It can be implemented both in MS SQL Server, its free MSDE motor and with Oracle.
- The **Web application** which manages the computer system is programmed in JavaScript, C# and uses the .NET environment to make active pages (ASPX).

technical requirements

There are no specific hardware requirements. The software requirements are detailed below: (check for other configurations)

- W2000 Server operating system, or later
- SQL Server 7 or later, or Oracle 9i or later, and MSDE
- WEB IIS service enabled
- MS .NET framework 1.1

other installation requirements

- Token Ring and Ethernet networks are supported.
- The audited machines need Windows OS.
- IE 5.5 or later is required to access the web application.

implementing and updating the solution

implementation schedule

Not all PC networks are the same. Each organisation has its own singular network configuration, whilst the LAN configuration in a single office is only the simplest of the cases possible. Companies which group together several companies, with geographically scattered offices or with offices with no online connection to the main site, PCs in laboratories or facilities without any type of connectivity or with very poor lines... it is in these environments that **ProactivaNET®** beats all other inventory solutions.

The first step in any inventory project is the carrying out of the **consultancy and implementation study** most suitable for the needs of the organisation for which the inventory is to be completed.

Whatever the specific casuistry of the network upon which **ProactivaNET®** is implemented, our technicians will accompany you throughout the implementation process, until the system is fully up and running, thus guaranteeing **the successful implementation of the tool**.

scheduled updates and new versions

There is a continuous upgrade plan which publishes a new version of the product approximately once a year, incorporating new technical features and new functions.

Moreover, depending on the evolution of the product, different upgrade releases will be made available for small improvements necessary throughout the lifetime of the version.

The release subscription service gives automatic access to upgrades for all products through the supporting website, along with licences for upgrading to new versions which come onto the market during the lifetime of the product.

More information: www.proactivanet.com



Parque Científico Tecnológico de Gijón
Edificio I+D, s/n. – 33203 Gijón – Spain
Tels. (+34) 985 099 215

www.espiralms.com



Espiral MS is certified by AENOR for the design and development of web applications for systems management.

Our products satisfy the Capability Maturity Model Integrated (CMMI®) Level 2 as certified by the European Software Institute.

Espiral MS applies the best practice for IT Service Management and has support staff qualified as ITIL.