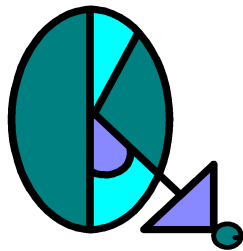


NetAdmin

White Paper Version 5.0



Overview

The information contained in this document is subject to revisions or improvements at any time without prior notice within the framework of the program's evolution. The software described in this document is distributed under a license agreement and shall be used or copied only in conformity with the stipulations of this agreement. Unless specifically authorised by this agreement, any reproduction of the software on any support whatsoever is illegal. Any copy or transmission of this manual in any form or by any means, electronic or mechanical, including photocopying, recording, on information storage and retrieval systems, without prior written permission of OÏKIALOG SAS is prohibited by the law.

Calyx SSO, Calyx Crypto and NetAdmin are registered trademarks of **OÏKIALOG SAS**.

Protect is a registered trademark of **ICZ Group**.

DOS/Windows are registered trademarks of MICROSOFT Corporation.

Outlook, Outlook Express and Internet explorer are registered trademarks of MICROSOFT Corporation

Notes is a registered trademark of LOTUS Corporation.

SAP is a registered trademark of SAP GMBH.

VPN1 is a registered trademark of CHECKPOINT Corporation

© Copyright 1997-2008 OÏKIALOG SAS, all rights reserved.

Summary

1	NETADMIN PRESENTATION	5
1.1	INTRODUCTION	5
1.2	SYSTEM DESCRIPTION	5
1.2.1	<i>NetAdmin server</i>	5
1.2.2	<i>NetAdmin agent</i>	5
1.2.3	<i>Communication Principles</i>	5
1.3	NEW FEATURES	6
•	LDAP SYNCHRONISATION OF THE TREE STRUCTURE	6
•	OPTIMISATION OF NETADMIN AGENT WAKEUP	6
•	OPTIMISATION OF THE ACCESS TO THE ERROR REPORTS	6
•	ALERTS MECHANISM	6
1.4	REQUIRED CONFIGURATION	6
1.4.1	<i>Required configuration console / server</i>	6
1.4.2	<i>Agent required configuration</i>	7
1.5	DATABASE DEFINITION	7
1.5.1	<i>Microsoft Data Engine (MSDE)</i>	7
1.5.2	<i>Microsoft SQL Server</i>	7
1.5.3	<i>Oracle 8.1.7 or 9.2</i>	7
2	NETADMIN CONSOLE	8
2.1	OVERVIEW	8
2.2	GENERAL ORGANISATION	8
2.2.1	<i>Console tree</i>	8
2.2.2	<i>Detailed Configuration Panel</i>	9
2.2.3	<i>Station system characteristics</i>	9
2.3	NETADMIN AGENT SCRIPT	9
2.4	USER MANAGEMENT	9
2.4.1	<i>SAM base importation</i>	9
2.4.2	<i>LDAP directory synchronization</i>	9
2.4.3	<i>User token configuration</i>	9
2.4.4	<i>User photo management</i>	10
2.4.5	<i>Users badges affectation</i>	10
2.5	DELEGATION OF THE ADMINISTRATION	10
2.5.1	<i>Definition of the operations accessible to a NetAdmin user</i>	11
2.5.2	<i>Definition of the access rights of the NetAdmin user to the objects</i>	11
2.6	ANALYSE OF THE ADMINISTRATOR'S LOG	12
2.7	LOG ANALYSE	13
3	NETADMIN SERVER	14
3.1	OVERVIEW	14
3.2	BLACK LIST AND WHITE LIST	14
3.3	LOG PROCESSING	14
4	NETADMIN AGENT	14
4.1	OVERVIEW	14
4.2	NETADMIN AGENT DEPLOYMENT	15
4.3	AUTOMATIC AFFECTATION OF THE NEW STATIONS	15
4.4	MANAGEMENT OF FURTIVE NETWORK CONNECTIONS	15
5	SOFTWARE DEPLOYMENT	15
5.1	OVERVIEW	15
5.2	STRATEGIES IMPLEMENTATION	15
5.3	MANAGEMENT OF THE ENVIRONMENT VARIABLES	16
6	MANAGEMENT OF USERS	16
6.1	DYNAMIC MANAGEMENT OF USERS	16
6.2	VALIDITY DATE AND BADGE DEACTIVATION	16
6.3	BACKUP OF THE BADGE CONTENTS	16
6.4	CENTRALIZED MANAGEMENT OF CONFIDENTIAL INFORMATION	17

7	ENCRYPTION KEYS MANAGEMENT	17
8	APPLICATIONS MANAGEMENT	17
9	TOOLS AND UTILITIES	18
9.1	DATABASE BACKUP AND RESTORE	18
9.2	MANAGEMENT AND ANALYZES OF LOGS AVAILABLE IN THE CONSOLE	18
9.3	ALERTS SYSTEM.....	18

1 NETADMIN PRESENTATION

1.1 Introduction

NetAdmin software allows you to perform the deployment and the configuration of applications in a centralized manner. It allows to deploy and configure the whole set of Calyx Suite products.

NetAdmin is made up of 3 distinct elements:

- An administration console: this software allows the administrator to set up his deployment and configuration strategy from the workstation on which the console is installed. It is installed by default on the server but might also be installed on an other workstation on the network.
- A server : its task is to store the installation programs of the products which are likely to be deployed but also to store the administrator defined configuration sent to the workstations of the network as well as reports and logs generated by the stations and consulted by the administrator.
- An agent: installed on each workstation to administrate, it is responsible for the communication with the NetAdmin server and the application of the installation strategies and the administrator's configuration for that workstation.

The mechanism of agent – server communication developed for NetAdmin allows you to get rid of the rights constraints linked to the domain and so, to manage a multi-domain network through the same NetAdmin server.

The possibility to install the administration console apart from the NetAdmin server lets you share the network management between different users.

Once the server and a console are installed, you have the possibility to configure the agent's installation and the different products of the Calyx Suite but also to define its strategies.

After the agent's installation, the administration console allows to display the different products of the Calyx Suite already installed on the workstation, to update it and apply the strategies defined by the administrator through the administration console.

1.2 System description

1.2.1 NetAdmin server

The server is made up of 2 elements: a web server and a database. These two elements can be installed on a unique server or on two servers.

- Database: the database is used for the storage of strategies defined by the administrator, some system and configuration information brought back by the agents, the log files and the reports. That Database can be either an SQL Server 2000 (not provided with NetAdmin) or an MSDE 2.0 database (provided with NetAdmin), or Oracle 8.1.7 or 9.2 (not provided with NetAdmin).
- Web Server: the Web server is a proprietary server and its task is to build and interface between the agents and the database. When the agent contacts the server, it retranscribes the received requests so as to forward it to the database and then send the information obtained from the database to them.

1.2.2 NetAdmin agent

The agent is a service executed under the system account that allows to perform the administrator's defined operations thanks to the administration console. It is in charge of installation, update and uninstallation of the Calyx Suite's products, but also of the configuration and the collection of information concerning the workstation and the Calyx Softwares installed on it.

1.2.3 Communication Principles

Two communication methods are defined in NetAdmin:

- Agent – Server communication: The communication between agents and server lays on the http protocol in a periodical manner. The agents wake up periodically and contacts the server on a port defined at the installation of NetAdmin.
However, it might be sometimes necessary to wake up the agent without waiting for the end of its reconnection delay: that is why, each agent is listening on a port defined during the installation of NetAdmin server. The administration console uses that port to contact the agent and obliges it to wake up.
Every connection between Agent and Server is encrypted. Encryption keys are generated during the initialization of each connection and exchanged in a secured way through an asymmetrical encryption mechanism using algorithm RSA (length of key 1024 bits).

- Console – Server NetAdmin Communication: the communication between an administration console and the NetAdmin server is performed through an ODBC link.

1.3 New features

- **Backup of the data stored in badges**

NetAdmin 4.7 allows through the Agent – Server communication the synchronized backup to the data stored in the user badges. Activated per station or stations group, this feature makes it possible to realize a backup of the data stored in the badge in the NetAdmin server at each modification of them.

In case of lost or renewed badge, the NetAdmin administrator will restore the saved data in the new badge affected to the user.

- **LDAP synchronisation of the tree structure**

The LDAP request of NetAdmin allows since version 4.7 to synchronize the list of users existing in directories or part of directories and to synchronize also the groups and the tree structure of the directories.

The LDAP synchronisation type allows the NetAdmin administrator to automatically obtain the user tree structure corresponding to that defined in the company directory.

The synchronization of the tree structure allows also keeping coherence after modifications of the company directories.

- **Optimisation of NetAdmin agent wakeup**

The NetAdmin agent wakeup mechanisms have been optimised in version 4.7 in order to be more powerful:

- A random delay has been added to the agent wakeup when connection activation is detected. During a VPN connection, it is established after the connection activation. An immediate wakeup after detection of the connection does not allow contacting the server. The wakeup random delay allows to be sure that the Agent – Server communication is realized after the VPN activation VPN.
- During the agent wakeup from the NetAdmin console, the administrator can define a delay during which each selected station will be waked-up remotely. This feature allows realizing a wakeup by group of stations without taking risks to synchronize NetAdmin agents and to create a peak of activities on the server and on the network.

- **Optimisation of the access to the error reports**

The 4.7 NetAdmin console integrates a synthetic interface showing the whole reports that include error message. All reports generated by stations are always available station per station but this new interface allows having a global vision of the read and non read error reports.

A notification system announces to the administrator the generation of the new report.

- **Alerts mechanism**

Since the version 4.7, an alert mechanism allows sending messages to the administrators in case of events opposite to the defined security strategies. This alert mechanism allows also:

- Announcing every Calyx software uninstallation realized through the “Add / Remove Program” interface of the workstations.
- Sending SMTP message (mail).
- Sending SNMP message.
- Receiving SNMP messages in the internal trap of the NetAdmin console.

1.4 Required configuration

The NetAdmin server should rather be installed on a server that is member of a Windows NT or 2000 domain. The use of a file server is recommended since the installation on domain controller risks to have a negative impact on the performance of NetAdmin and on the controller itself.

1.4.1 Required configuration console / server

The administration console and the NetAdmin server need the following resources:

- An Intel Pentium processor operating at 500 MHz at least.
- At least 200 Mo of disk space knowing that the size of the database evolves on the number of workstations and users to administer.
- From 256 Mo up to 512 Mo of RAM depending on the database size.
- A network card supporting the TCP/IP protocol and a fix IP address.

- Windows NT4 Service Pack 6 minimum or Windows 2000 Service Pack 2. However some server operating systems are recommended.

Besides, before the installation of NetAdmin server, you have to choose which database environment you wish to use:

- Microsoft Desktop Engine 2.0 (MSDE).
- Microsoft SQL Server 2000.
- Oracle 8.1.7 or 9.2.

1.4.2 Agent required configuration

The NetAdmin agent requires at least the following resources:

- 1 Mo of disk space on the client workstation.
- An extra disk space for the installation of the software to deploy. For further information, see the manual of each software you wish to deploy via NetAdmin.
- 32 Mo of RAM.
- The agent can be installed on one of the following operating systems: Windows 95, Windows 98, Windows NT4 Service Pack 3 or higher, Windows 2000 Service Pack 1 or higher, Windows XP.
- Internet Explorer version 4 or higher.
- Since Windows XP Service Pack 2, it is necessary to configure the XP firewall in order to allow the communication between the agent and the server.

1.5 Database definition

The database required to NetAdmin operation can be either Microsoft Data Engine 2.0 (MSDE) or Microsoft SQL Server 2000. However, it is possible for you to start the installation with MSDE and then to migrate toward Microsoft SQL, just installing it on the server where MSDE is installed.

1.5.1 Microsoft Data Engine (MSDE)

Microsoft Data Engine (MSDE) provided with the NetAdmin software.

- It allows the use of a database up to 2 Go.
- It offers 5 simultaneous connections to the database. Thus the number of consoles connected at the same time to the database is 5.

1.5.2 Microsoft SQL Server

Microsoft SQL Server is not provided with the NetAdmin Software. You have to get it separately.

- It permits an unlimited storage capacity.
- The number of simultaneous connections is unlimited.
- Several administration tools are provided as a standard.

1.5.3 Oracle 8.1.7 or 9.2

Oracle is not provided with the NetAdmin Software. You have to get it separately.

- It permits an unlimited storage capacity.
- The number of simultaneous connections is unlimited.
- Several administration tools are provided as a standard.

2 NETADMIN CONSOLE

2.1 Overview

The NetAdmin console is the unique interface allowing a remote configuration of both the agents and the NetAdmin server. That console ensures the configuration and the deployment of the Calyx products on the network, resting on a management per station and station groups.

The administration console is directly connected to the SQL Database through the ODBC links defined during the NetAdmin installation. That administration console can be installed on a different machine from those that host the database or the server.

2.2 General organisation

The NetAdmin console is composed of three main parts:

- A tool bar and a menu allowing accessing a certain number of tools and some server general parameters applied to the database and the console.
- A tree on the left hand side of the console's screen.
- The right hand side of the console's screen concerns the details of the parameters, configuration or logs related to the selected element of the tree. Depending on the selected element, that right part can be divided in two pans.

The general console's appearance evolves to show the state and/or the selected element's configuration in the left hand side tree.

2.2.1 Console tree

The tree corresponds to the left part of the console. That tree is made up of six main nodes:

- The **All the groups** node: it contains the list of the administrated stations through the NetAdmin server. These stations are classified in a group sub tree allowing to simplify the management of the different possible configurations. By default, each group or station inherits its configuration from the parent's group.
- The **User** node allows the management of the Spy Killer users. The management can be performed by a user group so as to simplify the restrictions management. A user belonging to the sub tree can be assigned 1 to 5 badges (USB badge, smartcard, fingerprint) and a list of encryption.
- The **Domain** node allows to access the Network Neighbourhood and to visualisation of the visible machines on the network in each domain. The interest of the domain node is to integrate the visible machines names in the sub tree « All the groups » with drag and drop.
- The **SAM request** node allows to perform some users importations from the user names recorded in a local or remote SAM base. In the sub tree of the SAM request node, the list of the requesters. From each one of the requesters, it is possible to import the present users with drag and drop.
- The **LDAP request** node allows to perform some users importations from those listed in a directory interfaced thanks to the Ldap protocol. In the sub-tree of the Ldap request node appears the Ldap requesters list toward the different directories. An Ldap synchronisation mechanism allows the administrator to automatically import all the users appearing in the defined directories but also to delete the users in the sub tree, those who have been removed from the directories.
- The **Encrypting key** node: the sub tree of this node contains the list of the encryption keys stored in the database and administrable with NetAdmin. From this node, it is possible to assign some encryption keys to a user or a user group simply by "drag and drop" on the users or on the users group.
- The **Application** node: the sub-tree of this node contains the list of applications settings for which the authentication is managed by Calyx SSO. In this node, it is possible to import Calyx SSO configuration files, to realize the apprenticeship of the authentication window and web pages and to affect the settings to the stations or stations' group.

2.2.2 Detailed Configuration Panel

The detailed configuration panel constitutes the right part of the screen and aims at presenting the configuration details matching the selected object in the tree. Thus, the data displayed in the panel will be different according to the sub-tree in which the object is located. Sometimes, the right part of the screen is not used (as when an encryption key is selected).

2.2.3 Station system characteristics

The Workstations System information is brought back by the NetAdmin Agent to the NetAdmin Server as soon as the installation is finished. This information is updated each time the agent wakes up.

The system information collected is:

- NetAdmin agent listening port.
- Physical Memory available.
- Number and type of processors.
- List of the existing partitions, size and available disk space.
- List of the services either stopped or running.
- List of the devices either stopped or running.
- Internet Explorer version installed on the client.

2.3 NetAdmin agent script

As NetAdmin agent starts, it is possible to execute a script on the clients' workstation. That script is a batch that can contain all the useful commands with that type of file.

2.4 User management

The **User** node is the root of the tree allowing the centralised management of the Calyx Users from the NetAdmin Console. This tree can contain two types of objects: users and groups. A group contains users whose restrictions will be those of the group. The name of a user or a group is unique in the **User** tree set.

2.4.1 SAM base importation

The SAM bases contain the information of the defined users' accounts for a server or a workstation of Windows NT4 type, Windows 2000 or Windows XP. The administration console of NetAdmin allows you to define some Calyx users using this information. To success you have to define one or several requesters pointing towards local or remote databases.

2.4.2 LDAP directory synchronization

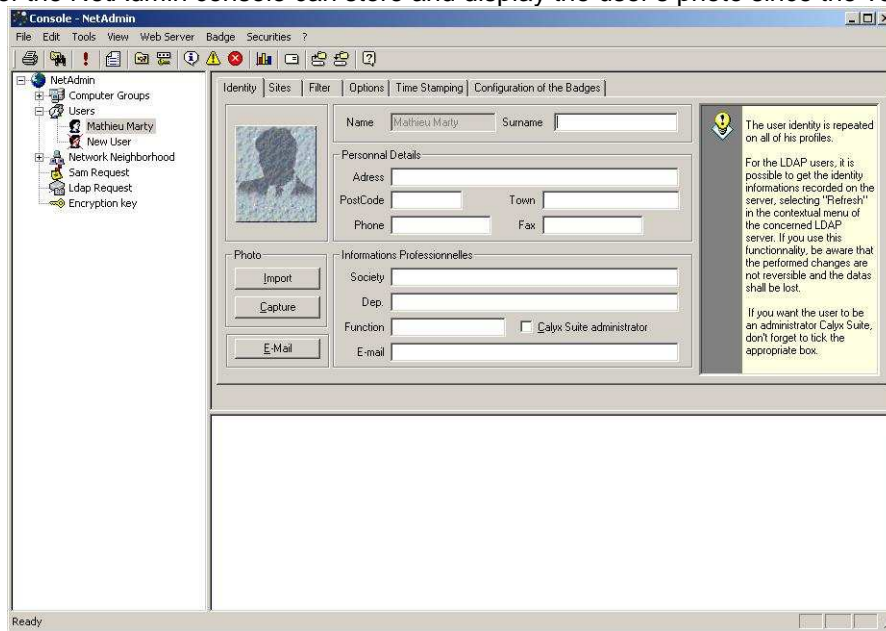
The Ldap directory servers contain the data concerning the members of a company. If your company has set up such a server, you can import these data in order to create some new Calyx users. This synchronization can be applied to the users but also to the groups existing in the directory.

2.4.3 User token configuration

The NetAdmin console allows to define up to 5 badges or fingerprints for a single user. These badges can be of the same type or different types.

2.4.4 User photo management

The user's identity of the NetAdmin console can store and display the user's photo since the version 4.6.



The “Import” button allows importing the photo stored in a jpeg, bmp or gif file. The “Capture” button starts an interface allowing making the acquisition of the photo since some different sources (digital camera, webcam, etc.).

A specific table of the database gives a simple access to data of the user (last name, first name, photo, serial number) in a format that can uses an external graphical token customisation tool.

2.4.5 Users badges affectation

The enrolment of the badges to the users is made in the NetAdmin console. However, the badge can be enrolled remotely (if the badge is not in the same location than the console). Some available tools on the workstations allow to realize an enrolment remotely. These tools are available when the user is logged in and even though when he is logged out.

2.5 Delegation of the administration

The NetAdmin administrator can delegate his administration rights:

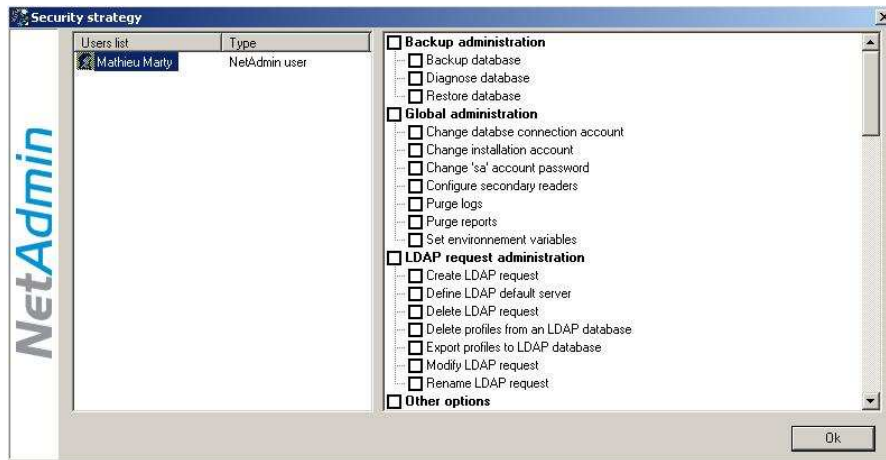
- Completely to another NetAdmin administrator.
- Partially to a NetAdmin user.

The rights limitations of the NetAdmin users are made at 2 levels:

- It is possible to limit the list of the operations that the NetAdmin user can make. For example, a NetAdmin user can have the right to administrate the users and no right to administrate the station.
- For each object the tree of the NetAdmin console (user, group of users, station, group of stations, requester, encryption key, etc.), it is possible to affect some access rights to the different NetAdmin user. For example: a NetAdmin user can have full access on a group of user, read only on the encryption keys, and no access on the whole stations.

2.5.1 Definition of the operations accessible to a NetAdmin user

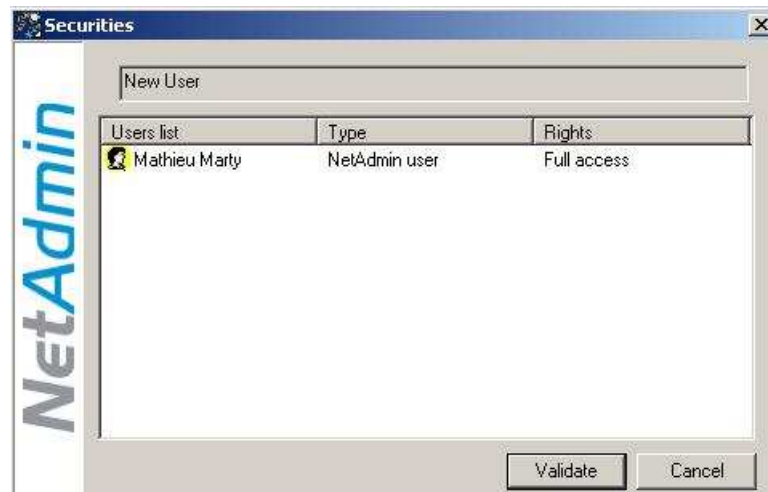
- In the NetAdmin console, select the entry "Security strategy" in the "Securities" menu. The following window appears:



- In the left part the list of NetAdmin users is displayed.
- Select a NetAdmin user.
- In the right part, define the operations that the selected user can make.
- Repeat the previous operations for each NetAdmin user and press on "OK" to close the window.

2.5.2 Definition of the access rights of the NetAdmin user to the objects

- In the tree of the NetAdmin console, select the object (user, group of users, station, group of stations, requester, encryption key, etc.) where you want to define access rights to the NetAdmin users.
- In the context menu of this object (right click), select the option "Set Securities". The following window appears:



- The list of the existing NetAdmin users is displayed. Select a user in the list.
- In the context menu of the selected NetAdmin user (right click), define the right to affect: Read only, No access, Full access.
- Check the box Apply on child objects if you want to propagate the access rights to the child's objects.
- Press on "Validate" to save the modifications.

2.6 Analyse of the administrator's log

The NetAdmin console logs the whole administration operations made by the NetAdmin administrator and the NetAdmin users. If the administration is delegated, the NetAdmin console allows the central administrators of the company checking the operations realized by the NetAdmin users.

The whole following action are logged:

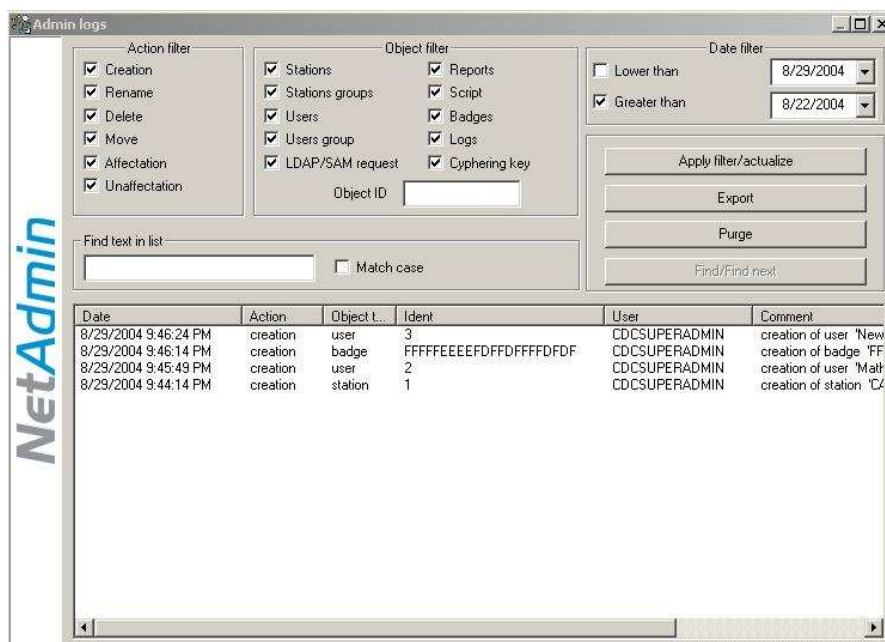
- Create an object
- Rename an object
- Remove an object
- Move an object
- Assign an object to another
- Unassign an object to another

The existing objects in the NetAdmin console are the following:

- Stations and group of stations
- Users and group of users
- SAMP and LDAP requesters
- Logs and reports
- Scripts
- Tokens
- Encryption keys

Each entry is completed with the date and the name of the NetAdmin administrator or user who has made the operation.

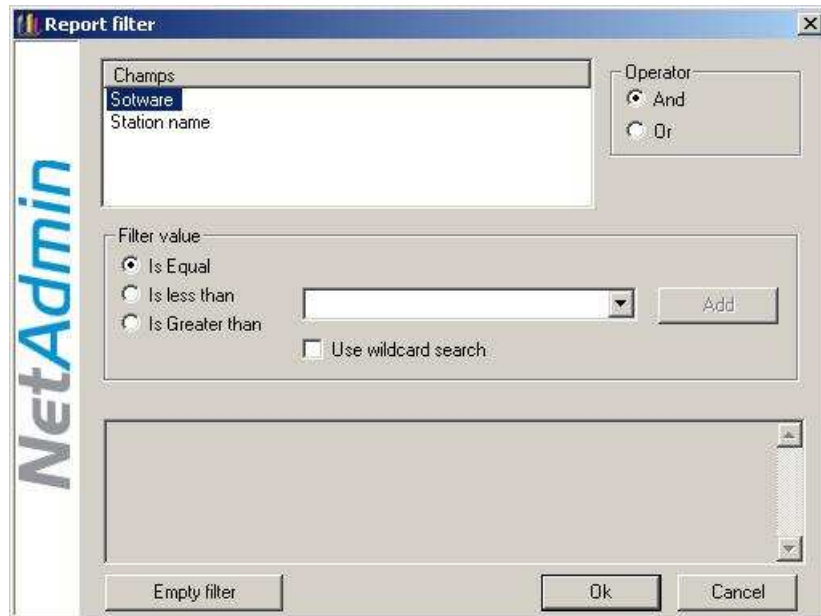
The interface of administrator logs displaying is available by selecting the entry "Admin logs" in the "Securities" menu of the NetAdmin console.



This interface presents a filter system that allows limiting the list of displayed logs.

2.7 Log analyse

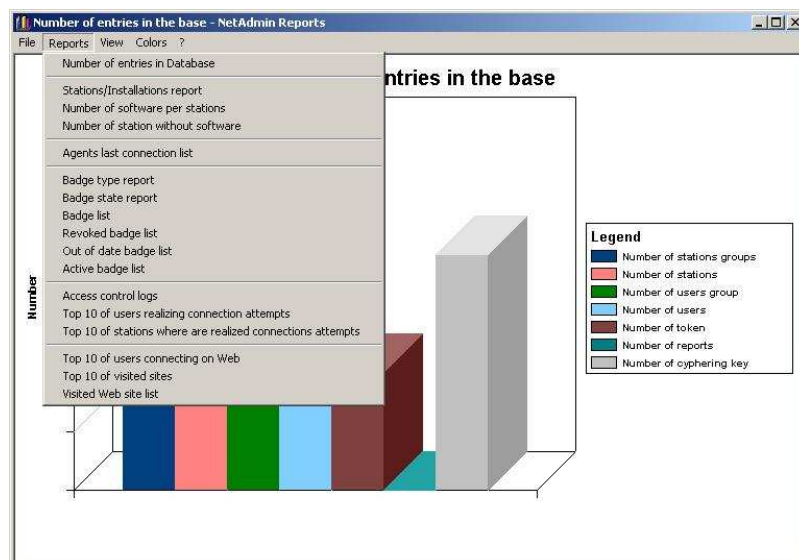
The NetAdmin console integrates a log analysis tool with a list pre-defined request. Each request can be configured at the generation of the report. This personalisation allows the user to define filters on the executed requests. It allows for example to realize a report concerning a specific part on the managed stations.



The result of the request is shown as a graphical report. The displayed format of the graphical report is defined by the user and can be modified at each moment. The available choices are:

- Pie
- 3D Pie
- Bar
- 3D Bar
- Detailed list of the elements found by the request

The log analyse tool is available since the Tools menu when you select the entry “Reports”.



The available reports are the following:

- **Number of entries in Database:** display the number of objects stored in the database sorted by type.
- **Stations / Installations report:** display the number of managed stations and the number of stations where is installed each products.
- **Number of software per stations:** display per software the number of stations where the software is installed.

- **Number of stations without software:** display per software the number of stations where it is not installed.
- **Agent last connection list:** display the stations list with the date of the last connection of each of them.
- **Badge type report:** display for each type of badge, the number of managed badges in the console.
- **Badge state report:** display the number of revoked, activated or expired badges.
- **Badge list:** display the detailed list of managed badges in the NetAdmin console.
- **Out of date badge list:** display the detailed list of the out of date badges.
- **Revoked badges list:** display the detailed list of the revoked badges.
- **Active badge list:** display the detailed list of the activate badges.
- **Access control logs:** display the detailed list of the connection tries of the users on the stations.
- **Top 10 of users realizing connection attempts:** display the list of the 10 users that have made to most important number of connection tries on the stations.
- **Top 10 of stations where are realized connection attempts:** display the list of the 10 stations where is made the most important numbers of connection tries.
- **Top 10 of users connecting on Web:** display the list of the 10 users that have made to most important number of connection tries on Internet.
- **Top 10 of visited sites:** display the list of the 10 most visited Web sites.
- **Visited Web site list:** display the detailed list of the visited Web sites.

3 NETADMIN SERVER

3.1 Overview

The NetAdmin server is a proprietary server whose task is to ensure the communication between the NetAdmin agents installed on the clients' workstations and the SQL database. The server and the NetAdmin console are thus the only process allowed to access the database consequently limiting the diffusion of the access rights to that database.

3.2 Black list and white list

It is possible to configure a list of IP addresses which connection attempt will be systematically refused or accepted by the NetAdmin server. That list is updated by specifying IP addresses or ranges of IP addresses.

3.3 Log processing

The NetAdmin server makes permanently to types of actions on the logs and reports sent by the NetAdmin agents.

- The Calyx Suite logs received by the NetAdmin server (access control logs, Internet access control logs) are cut and stored in the database in specific tables for each type of logs. The simple storage format of the Calyx Suite logs in the NetAdmin database allows the administrator to analyse this information through an external log analyse and correlation tool.
- The NetAdmin server limits the log and report volume stored in the database by removing the older logs. This automatic deletion can be configured in the NetAdmin console. The NetAdmin administrator defines by type of logs, the number of days of logs or reports to keep.

4 NETADMIN AGENT

4.1 Overview

The NetAdmin agent is a service executed on each client station and which task is to perform the management of the Calyx products installed on the workstation. The agent performs the installations, the updates and the uninstallation of the products, their configuration and locally applies the strategy assigned to the Calyx Suite users.

All these tasks are performed by the agent after it received the orders sent via the NetAdmin server. At start of the client station and then periodically, the NetAdmin Agent contacts the NetAdmin server. The Agent sends a report to the server concerning the state of its configuration (In particular, the list of the Calyx products installed locally) and then receives the tasks to perform.

Besides, it is possible from the NetAdmin console to wake up one or several agents so as to interrupt the waiting. As soon as it starts, the NetAdmin agents is listening the port on which it receives the wake up order. The value of this port is defined for each workstation or station group in the administration console. The default port defined is 1024. As the message arrives the agent immediately contacts the NetAdmin server.

4.2 NetAdmin agent deployment

The NetAdmin agent can be deployed on the workstations through 3 different ways:

- By using the auto-installation feature of the NetAdmin console: this solution allows the administrator to deploy on the workstations remotely through the NetAdmin console. The advantage of this solution is that it is the most simple and do not ask any other action. The installation of the NetAdmin agent is completely invisible for the user. However, it can be used only on Windows NT4, 2000 and XP stations and requires the station to be connected on the network when the administrator uses it.
- Manual installation of the NetAdmin agent: this solution is the less simple because it requires a direct intervention on the workstations.
- Generation of a customised package: this package, generated in the NetAdmin console allows to define a setup including the installation program of the NetAdmin agent, the installation parameters and an account with administrator rights. The advantage of the solution is that it allows integrating the installation of the NetAdmin agent into the existing scripts of the users. It allows the administrator to automatically install the NetAdmin agents on all new stations added on the network.

4.3 Automatic affectation of the new stations

If the installation of the NetAdmin agent is made with a customised package, the station that appears in the NetAdmin console automatically affected to the stations' group used to create the customised package.

Example:

If the company has different remote sites, the administrator defines in the NetAdmin console a stations' group per site and a customised package for each site. Each station where the agent is installed appears directly in the NetAdmin console in the group that corresponds to the site.

4.4 Management of furtive network connections

The NetAdmin agent detects the activation of the network connection. For each detection, the NetAdmin agent wakes up randomly in a maximum delay of 3 minutes and connects to the NetAdmin server.

This feature ensures that there is a periodical connection of the NetAdmin agent to the server even if the agent is installed on a laptop that uses only a RTC connection.

5 SOFTWARE DEPLOYMENT

5.1 Overview

After the installation of the server and the agent deployment, it is possible for the administrator to set up a deployment policy of the Calyx products on one or more stations of the Network.

5.2 Strategies implementation

Once the installation of the NetAdmin server and its console is done, and after the deployment of the NetAdmin agent and Calyx products on the client stations, it is possible to remotely deploy the configuration strategies of these softwares.

- From the NetAdmin administration console, the software strategies are defined and stored in NetAdmin server database.
- As the agent connects to the NetAdmin server, it indicates the list of the Calyx Suite applications installed and administrable by the server through NetAdmin.
- The NetAdmin server provides the strategy to apply for each Calyx Suite application available on the client station and administrable with NetAdmin.
- The NetAdmin server transmits the list of Calyx Suite applications to install, update or uninstall.
- The NetAdmin agent performs the installation tasks, update and uninstallation specified by the server.

In case of error during the start of the strategies, and during the installation, update or uninstallation, a report is sent by the agent toward NetAdmin server. These reports are available in the NetAdmin console.

During the agent wake up, the software strategies are applied. If the connection between agent and server is successful, new software strategies are applied. If the connection fails, the last software strategies received by the agent are reapplied.

5.3 Management of the environment variables

All the configurations requiring an access path definition towards a file or a folder on a station are done through a wizard which allows as well as possible to define the writing format of this path. This wizard proposes in particular to the administrator the whole of the possible combinations of environment variables which make it possible to define this access path.

6 MANAGEMENT OF USERS

This management can be carried out by group users in order to make easier the management of the restrictions. A user being in this under tree structure can be assigned from 1 to 5 badges (USB keys, smart card, fingerprint) as well as a list of encrypted keys.

6.1 Dynamic management of users

This method of management of Calyx users is based on the use of a LDAP directory to which we add an object in the diagram. It applies only to Calyx Users defined starting from this directory and only on stations whose parameter setting allows dynamic management of Calyx users.

During the log on, the NetAdmin agent is connected to the directory and downloads on the station customers' identification information of the whole of user's badges and fingerprints (if this information is present in the directory).

The NetAdmin agent announces in the data base through the Web server the fact that this user is now deployed on this station. In the NetAdmin console, the user appears deployed as if that had been done manually.

If the user or one of his badges is removed from Calyx users' base of NetAdmin server, then the modification is propagated to stations where user already connected.

6.2 Validity date and badge deactivation

The NetAdmin console enables you to define validity dates for your various users' badges. Before and after this validity period, the user's badge is deactivated. This one will not be able to thus use this badge to reach one of the stations.

This deactivation function can be used manually in order to block in a temporary way the use of a badge.

6.3 Backup of the badge contents

In their traditional usage, Calyx suite and NetAdmin uses the badges as secured storage support for confidential information (System credential information, Application and Web form credential information, encryption keys, etc...).

NetAdmin offers the administrator to realize a synchronized backup of the data stored in the users' badges. Being activated per station or per stations' group, this feature allows at each modification of the stored data to realize a backup on the NetAdmin server.

The main advantages are:

- In case of lost or forgotten badge, it is possible to restore the backup data in the new badge affected to the user.
- Keep a system where all the confidential data are stored in a secured external support (USB key or smartcard) and are never stored directly on the workstation.

Principle of operation:

- A user wishes to connect on a client workstation on which he is authorized to reach. He inserts his badge or put his fingerprint on the reader.
- In the case of a biometric system, he enters his username.
- He enters his PIN.
- Calyx SSO uses the data stored in the badge.
- In case of modification of one of the data, the agent sends the modifications to the NetAdmin server.
- When the badge is replaced, the administrator enrolls a new badge to the user in the NetAdmin console and restores the credential information in it.

6.4 Centralized management of confidential information

In their traditional operation, Calyx Suite and NetAdmin use badges like protected storage supports of confidential information (connection system information, applicative and Web authentication information, encryption keys, etc...).

NetAdmin suggests the administrator a second operating mode which consists in storing the whole of the confidential information in the NetAdmin server and in temporarily transmitting them on the workstation after user authentication using his badge.

The main advantages of this second method are as follows:

- Support of types of badges on which it is impossible to record information (Example: ASK public transport card, French Health Professional Card, etc...)
- Faster adaptation to owner's badges used by new customers.
- Capacity to reallocate confidential data towards a new badge in the event of loss or of stole.
- No diffusion of confidential information in the event of loss or of stole of badges. Indeed no information is stored there.
- Greater flexibility in use and greater mobility for users using biometrics devices. When those change their password, this modification is reflected not locally but in the NetAdmin data base.

Principle of operation:

- A user wishes to connect on a client workstation on which he is authorized to reach. He inserts his badge or presents his fingerprint.
- In the case of a biometric system, he enters his username.
- He enters his PIN.
- Agent transmits to the NetAdmin server an authentication request from the user.
- In the event of acceptance, the NetAdmin server transmits confidential information package to agent who store it encrypted locally.
- In the event of modification of one of data by the user, agent transmits modifications to the NetAdmin server. If network communication is stopped, he preserves the modification to transmit it later.
- A local mask containing confidential information of X last users can be preserved on stations in order to allow an operation in fail-safe mode (no network connection between client and server).

7 ENCRYPTION KEYS MANAGEMENT

The NetAdmin console allows to manage the encryption keys of Calyx Crypto in a centralised manner.

The generation of encryption keys in the badges is performed with SetBox from Calyx crypto. That application is installed on the whole set of machines on which Calyx crypto is installed.

Through the NetAdmin console, it is possible, to read the keys existing on the inserted token and to store them securely in the NetAdmin database.

The NetAdmin console allows to allocate some encryption keys to the Calyx Suite users and to deploy their badges remotely.

8 APPLICATIONS MANAGEMENT

The NetAdmin console allows to manage centrally the configurations of Calyx SSO linked to the management of the authentication for the standard application and the Web forms.

The whole settings are composed of:

- The definition of the authentication window, of the change password window and the invalid password windows for modal application.
- The definition of the authentication form, of the change password form and the invalid password form for Web application.
- The definition and the affectation to the applications of the password strategies.

These configurations can be made either with Calyx SSO tools and imported in the NetAdmin console or either directly in the NetAdmin console. In order to simplify the administration of the applications, the Calyx SSO interfaces and theses available in the NetAdmin console are the same.

9 TOOLS AND UTILITIES

9.1 Database backup and restore

The NetAdmin console offers as a standard, a save tool of the database. That tool allows to do some punctual save of the set of configurations of the stations and users.

This tools of saving and restoration is particularly interesting in case of the use of an MSDE database since it is provided without nay administration tool.

Besides, a save of a NetAdmin/MSDE database can be restored in an SQL server database.

However, the save of a MSDE database through the NetAdmin console requires the NetAdmin console and the MSDE database to be installed on the same workstation.

9.2 Management and analyzes of logs available in the console

NetAdmin collects the logs generated by Calyx software on stations and incorporate them in the NetAdmin data base. Since the NetAdmin console, the administrator can thus consult the whole of this information. The logs available are as follows:

- Access logs to workstations: the administrator visualizes connections carried out on stations by users.
- Access logs to Internet: the administrator visualizes Internet connections carried out by users.
- Access logs to the administration console: allows to trace access carried out to the administration console level.
- Save logs: these logs allow to save each data base save operation carried out through one of the NetAdmin administration console.

It is possible to limit logs visualization following a date stamping and either only date by date.

An automatic mechanism makes it possible NetAdmin to carry out an automated removal of oldest logs and reports. This mechanism parameter by fixing the duration during which logs and reports must be preserved.

9.3 Alerts system

The NetAdmin alerts system allows sending messages to the administrators in case of events opposite to the security strategy. These alerts can be sent through 2 ways:

- Sending the message in SMTP (mail) by defining the mail server, the displayed sender and the recipient addresses. It is also possible to define if the message is sent in plain text mode or in HTML mode.
- Sending the message in SNMP mode by defining the address of the server.

This configuration of the sending mode is defined per station or group of stations.

These alerts allow:

- To announce all uninstallation of Calyx Suite realized from the Add / Remove Programmes interface on the workstation.
- To send all messages appearing in the Trace window of the agent. This feature allows the administrator to analyse the incident of the NetAdmin agent without going directly on the workstation.