



*Click&***DECiDE**
Le Décisionnel Polyvalent

NSI TRAINING BOOK

Part 2: Management Console Configuration

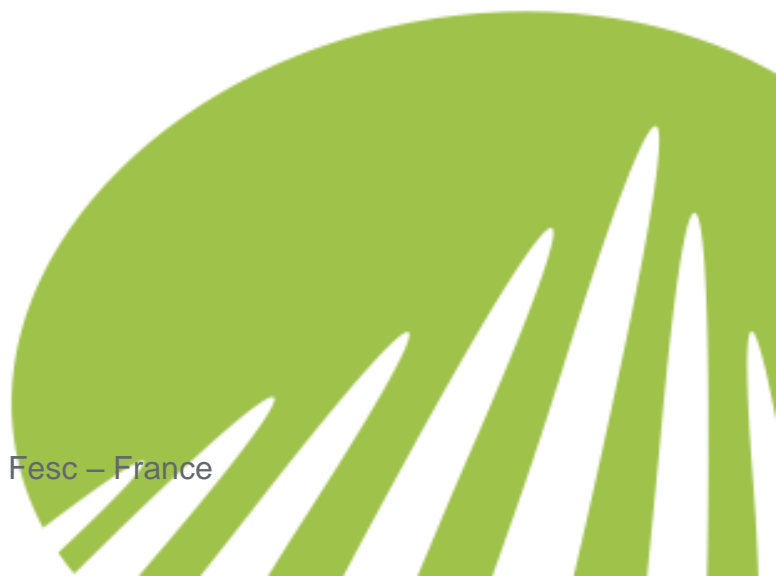
Click&DECiDE

Click&DECiDE ISO 27002

www.clickndecide.com

130 rue Baptistou, ZAE Nord, 34980 - Saint-Gély du Fesc – France

sales@clickndecide.com





Within this document, we are trying give you the knowledge to manipulate, operate and maintain Click&DECiDE NSI software.

Should you have any question about this document, or would you like some help, please contact:

Click&DECiDE SAS

Phone: +33 4 67 84 48 00

Email: support@clickndecide.com





Contents

Course Goals	8
4. Working with Click&DECiDE Management Console	9
4.1. Introducing Filters	9
4.1.1. Suggestions for Practice	10
4.2. Working with Click&DECiDE Management Console Backups	11
4.2.1. Suggestions for Practice	13
4.3. Introducing Agents/Parsers.....	16
4.3.1. Check Point (Real Time) Agent	16
4.3.2. Click&DECiDE Communication Agent.....	17
4.3.3. Event Scheduler Agent.....	19
4.3.4. Click&DECiDE Remote WMI Agent	20
4.3.5. Click&DECiDE Centralized WMI Agent.....	21
4.3.6. Click&DECiDE Ping Agent.....	22
4.3.7. Click&DECiDE Radius Agent	23
4.3.8. SQL Server Spyer.....	25
4.3.9. Flat File Parser	27
4.3.10. Syslog Parser ***REVIEW NEEDED (has changed in 10.3)***	34
4.3.1. SNMP Trap Listener	35
4.3.2. Suggestions for Practice	39
4.4. Working with Regular Expressions.....	46
4.5. Exporting Filters and Parsers.....	66
4.5.1. Suggestions for Practice	66
4.6. Importing Filters and Parsers	67
4.6.1. Suggestions for Practice	67
5. Working with Click&DECiDE Log Archive	69
5.1. Architecture	69
5.2. Introducing Click&DECiDE Log Storage.....	71
5.2.1. Suggestions for Practice	72
5.2.2. Exercise 2 - Adding a Store in File Action.....	72
5.2.3. Exercise 3 - Configuring the Store in File Action	72
5.3. Working with Click&DECiDE Log Storage Enriched CSV Format	
74	





5.3.1. Suggestions for Practice	75
5.4. Introducing Click&DECiDE Log Vault	77
5.4.1. Introducing Click&DECiDE Log Vault Settings	78
5.4.2. Suggestions for Practice	78
5.5. Introducing Click&DECiDE Log Vault Archives	81
5.5.1. Suggestions for Practice	81
5.5.2. Exercise 3 – Restoring Year/Month Level Archives	83
5.6. Introducing Click&DECiDE Log Replay	84
6. Working with the Click&DECiDE Alerting & Correlation Console	85
6.1. Introducing Alerts	85
6.2. Introducing the Alerting & Correlation Console	87
6.3. Correlated Alerts	91
7. Backing up and Restoring Click&DECiDE	92
7.1. Backing up Click&DECiDE Files	92
7.1.1. Click&DECiDE Spied Directory Backup	92
7.1.2. Click&DECiDE Database Backup	92
7.1.3. Click&DECiDE Configuration Backup	92
7.1.4. Click&DECiDE Log Storage Files Backup	93
7.1.5. Click&DECiDE Log Archive Files Backup	93
7.1.6. Click&DECiDE Web Portal Configuration Backup	93
7.1.7. Click&DECiDE Dashboards Backup	94
7.2. Restoring Click&DECiDE Backups	95
7.2.1. Suggestions for Practice	95
8. Troubleshooting	104
Reference Material	105
Contacting Click&DECiDE	106





Table of Figures

Figure 1 - ULA Fitlers	9
Figure 2 - Management Console Backup.....	11
Figure 3 - Saving a Backup of your Current Configuration	13
Figure 4 - Restoring a Backup.....	14
Figure 5 - Check Point (Real Time) Agent.....	16
Figure 6 - Click&DECiDE Communication Agent.....	18
Figure 7 - Event Scheduler Agent	19
Figure 8 - Remote WMI Agent Architecture	20
Figure 9 - Centralized WMI Agent Architecture	21
Figure 10 - Ping Agent	22
Figure 11 - Radius Agent	24
Figure 12 - SQL Server Spyer	26
Figure 13 - Flat File Generic Parser Configuration	29
Figure 14 - Flat File Generic Parser Date/Time Format.....	30
Figure 15 - Flat File Generic Parser General Parser Configuration	31
Figure 16 - Flat File Generic Parser Global Extra Fields.....	32
Figure 17 - Flat File Generic Parser Includes Parser	33
Figure 18 - Flat File Generic Parser Records Parser	33
Figure 19 - Syslog Parser Configuration	34
Figure 20 - Syslog Parser Log to File Mode	35
Figure 21 - SNMP Trap Listener	37
Figure 22 - Adding a Generic Parser: New Record Parser	39
Figure 23 - Adding a Generic Parser: Record Parser Configuration	40
Figure 24 - Adding a Generic Parser: Test Output.....	40
Figure 25 - Adding a Generic Parser: Configuration	40
Figure 26 - Adding a Generic Parser: Test Log File.....	41
Figure 27 - Adding a Generic Parser: General Configuration	41
Figure 28 - Creating a Custom Filter	42
Figure 29 - Creating Fields.....	43
Figure 30 - Creating the Send Mail Action	44
Figure 31 - Select Generic Parser in the drop-down list.....	47
Figure 32 - New Generic Parser Added.....	47





Figure 33 - Flat File Configuration 'Generic Parser'	48
Figure 34 - Records Parser Section	48
Figure 35 - New Pattern.....	49
Figure 36 - Parser Output: Alternation and Group and Naming.....	50
Figure 37 - Parser Output: Alternation and Group and Naming.....	50
Figure 38 - Parser Output: Naming	52
Figure 39 - Parser Output: Attributes and Values	53
Figure 40 - Parser Output: Attributes and their Corresponding Values ..	54
Figure 41 - Parser Output: Header Record	55
Figure 42 - Flat File Configuration 'Generic Parser': Records Parser	56
Figure 43 - Parser Output: Reference of a header	57
Figure 44 - Flat File Configuration 'Generic Parser': Includes Parser	59
Figure 45 - Flat File Configuration 'Generic Parser': New Include Parser	59
Figure 46 - Flat File Configuration 'Generic Parser': Include Parser Edited	60
Figure 47 - Flat File Configuration 'Generic Parser': Includes Parser	60
Figure 48 - Include Parser Configuration.....	61
Figure 49 - Include Parser Test Value	61
Figure 50 - Include Parser Test Result.....	62
Figure 51 - Parser Output: Referring Includes Record	63
Figure 52 - Includes Parser Named Captures.....	64
Figure 53 - Parser Output: Includes Parser Named Capture	65
Figure 54 - Log Archive Architecture.....	69
Figure 55 - Click&DECiDE Log Storage	71
Figure 56 - Click&DECiDE Log Vault.....	77
Figure 57 - Log Vault Settings	78
Figure 58 - Log Vault Archives	81
Figure 59 - Alerting & Correlation Console	87
Figure 60 - Alert Details	88
Figure 61 - Rule Properties	89
Figure 62 - User Profiles	90
Figure 63 - Click&DECiDE Web Portal Configuration Backup	94
Figure 64 - Click&DECiDE Configurator Device Selection	96
Figure 65 - Click&DECiDE Configurator Database Settings.....	97
Figure 66 - Configuration Backups	98
Figure 67 - Restoring Configuration Backup Files.....	99





Figure 68 - Restoring Web Portal Configuration	100
Figure 69 - Update Administration Settings	100
Figure 70 - Updating Database	101
Figure 71 - Stopping Click&DECiDE Task Manager	102
Figure 72 - Starting Click&DECiDE Task Manager	103





Course Goals

This course has been created to enable users to become familiar with Click&DECiDE NSI Products.



4. Working with Click&DECiDE Management Console

4.1. Introducing Filters

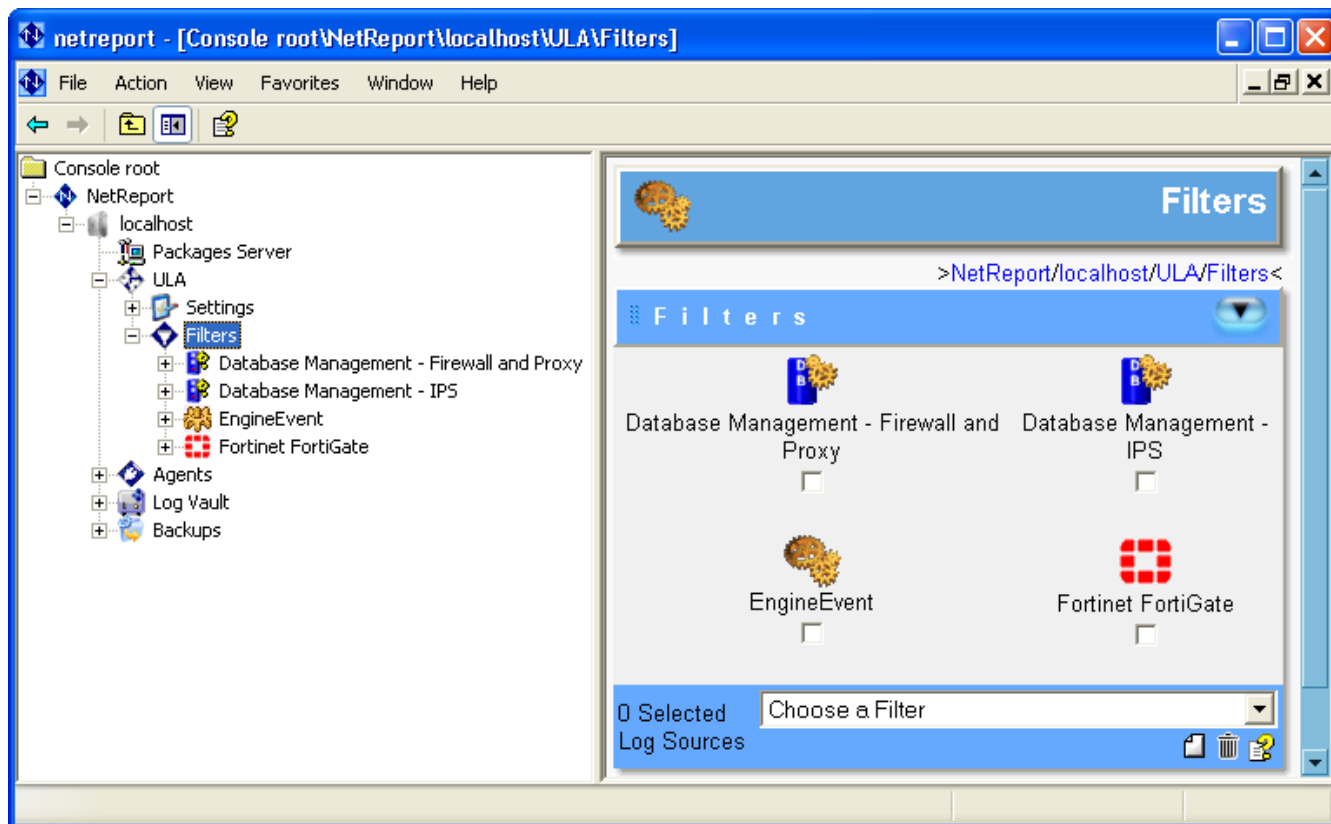


Figure 1 - ULA Filters

- Filters are specific to each Log format.
- Filters are unlimited.
- All Filters include their own:
 - Actions
 - Rules
 - Fields
 - Dictionary
- Pre-defined filters can be modified.


Click&DECiDE Filters allow you to define the Actions to execute (for example, writing in a database, sending e-mails, executing scripts and so on) based on customizable Rules. Any log system sends a frame containing an amount of information under the following format: (Attribute1, Value1); (Attribute2, Value2); (AttributeX, ValueX). The Rules system allows you to define the actions to execute based on given attributes and values. These attributes or values may or may not have a significant representation.





The Filters for the devices you selected in the Click&DECiDE Configurator will be automatically configured and appear in the Click&DECiDE Management Console. If you want to add filters for additional devices, this can easily be done by using the Click&DECiDE Management Console Filters screen. By default, only the EngineEvent filter is installed. The EngineEvent filter is installed as a standard and cannot be removed because Click&DECiDE uses it internally to handle errors.

4.1.1. Suggestions for Practice

1. Select **Start> All Programs> NetReport> Management Console**.
2. Enter your Login and Password.
3. Select **Console root> NetReport> ULA> Filters**.
4. Select **Microsoft Internet Information** Server from the drop-down menu.
5. Click the  **New** icon in the toolbar. Note the new **Microsoft Internet Information Server** filter is added.
6. Select **Console root> NetReport> [localhost]> ULA> Filters> Microsoft Internet Information Server> Actions> Insert into ww_rawdata**.
7. Check that **Create Table** is selected and **Drop Table** is cleared.
8. Click **Create Table !** in the tool bar at the base of the **Insert into ww_rawdata** pane to create the table

Note: You will lose all the data in the ww_rawdata table if you create a table.

9. Click **OK** in the warning message.
10. Note the **All Statements succeeded** message at the base of the **Insert into ww_rawdata** pane.
11. Select **Console root> NetReport> [localhost]> ULA** and note the asterisk next to the **ULA** branch.

Note: The asterisk indicates that you must save the changes you made.

12. Click **Apply Changes**. The asterisk disappears indicating that your changes have been saved.





4.2. Working with Click&DECiDE Management Console Backups

Click&DECiDE Backups simplify and automate your configuration backup. Click&DECiDE provides three types of backups to ensure that the user's settings are backed up each time the Click&DECiDE Configuration Wizard is run or a Migration is performed. In addition, the user can perform a backup at any moment via the Click&DECiDE Management Console.

Note: Click&DECiDE restores backups for Click&DECiDE Versions with the same major Version number, but not for different major versions. For example, any backups made in Click&DECiDE Version 10.1 cannot be restored in Click&DECiDE Version 11.0.

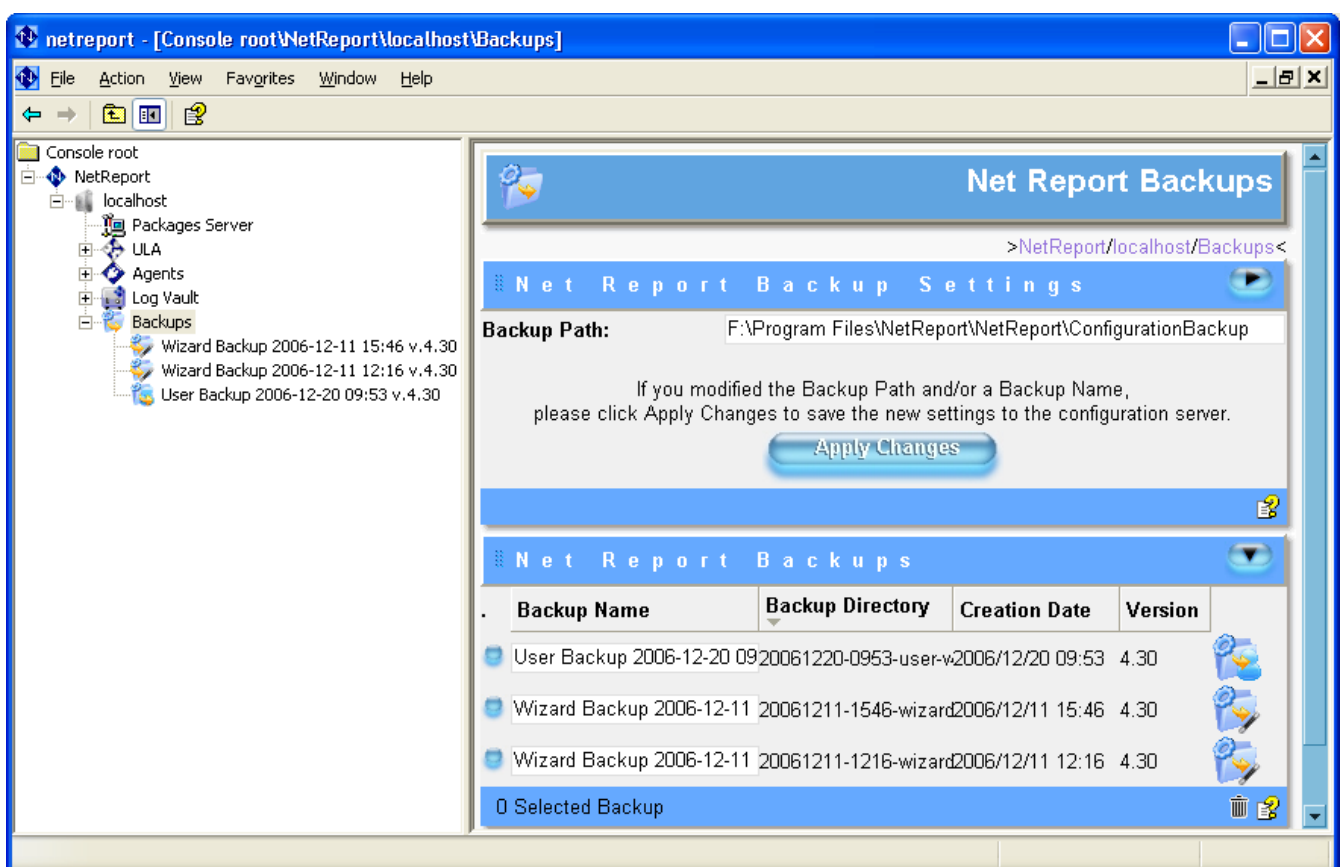


Figure 2 - Management Console Backup

Migration Backup: the backup of the configuration of the previous version of Click&DECiDE, when migrating from this version to the new version of Click&DECiDE.

Wizard/Configurator Backup: the backup of your configuration just before you launch the Click&DECiDE Configurator.





User Backup: a backup which the user can make at any moment via the Click&DECiDE Management Console to ensure that their configuration is backed up.

Each backup is available in the **Backups** branch in the Click&DECiDE Management Console root tree structure and its name can be customized by the user. The Backups are loaded one-by-one to optimize performance.

The Backups are ranked in chronological order in the left Console root pane. The most recent Backup is at the top of the Backups branch.

Each backup's configuration is disabled except for the Copy feature which is available for those elements which can be copied, for example Actions, Fields, Rules and Dictionaries. This enables the user to copy such elements from a backup to their current configuration.

The Click&DECiDE Backups section summarizes key information concerning each Backup.

Backup Name: the Backup Name

Backup Directory: the directory where the Backup is located in the Backup Path.

Creation Date: the date the Backup was created on.

Version: the Click&DECiDE Monitoring Center Version that the backup is related to.



4.2.1. Suggestions for Practice

4.2.1.1. Saving a Backup of your Current Configuration

You can save a backup of your current configuration (a User Backup) at any moment by following the steps below:

1. Select **Console root> NetReport> localhost**.

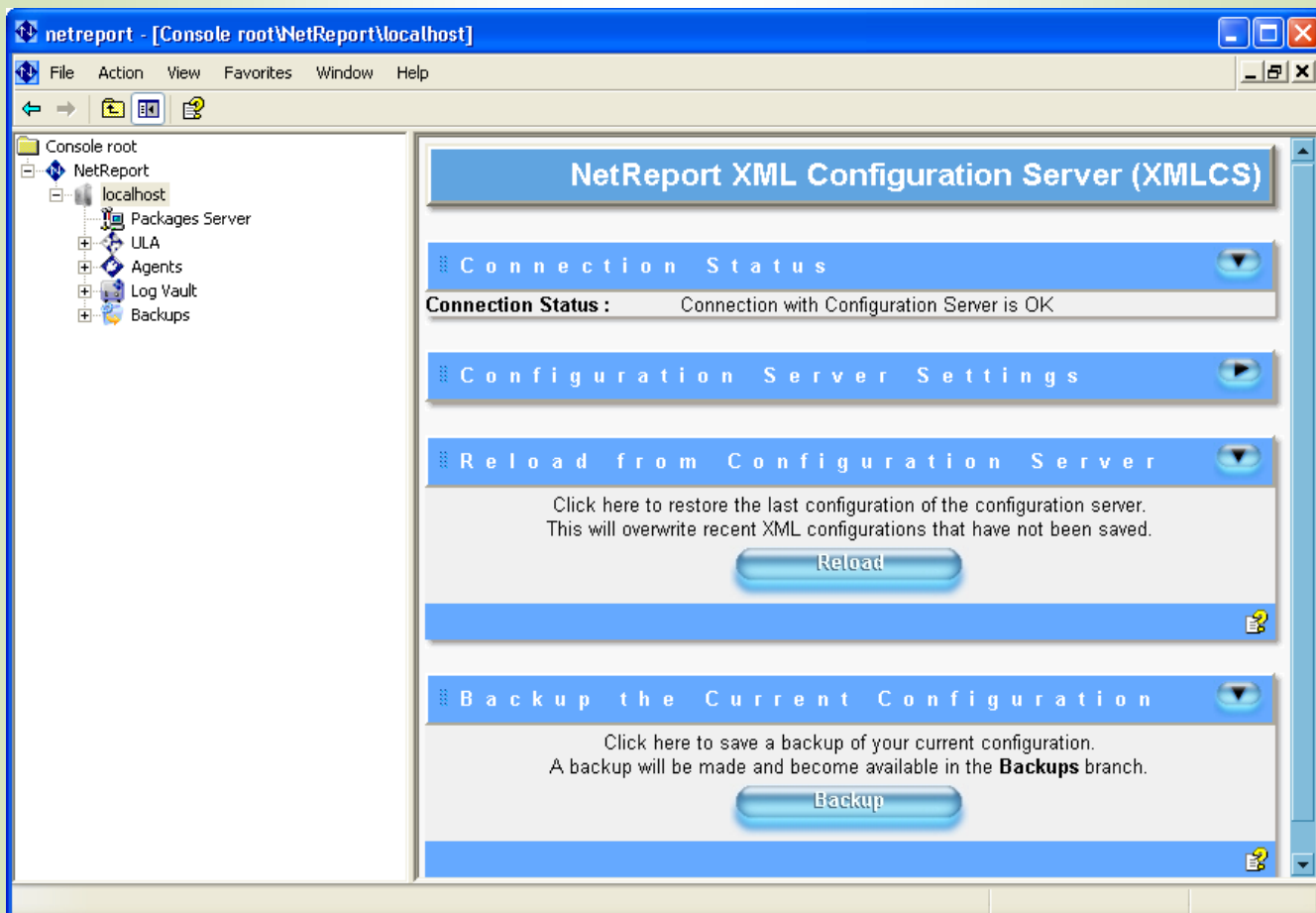


Figure 3 - Saving a Backup of your Current Configuration

2. Click the **Backup** button.



4.2.1.2. Restoring a Backup

1. Select **Console root> NetReport> [localhost]> Backups> [XBackup]**

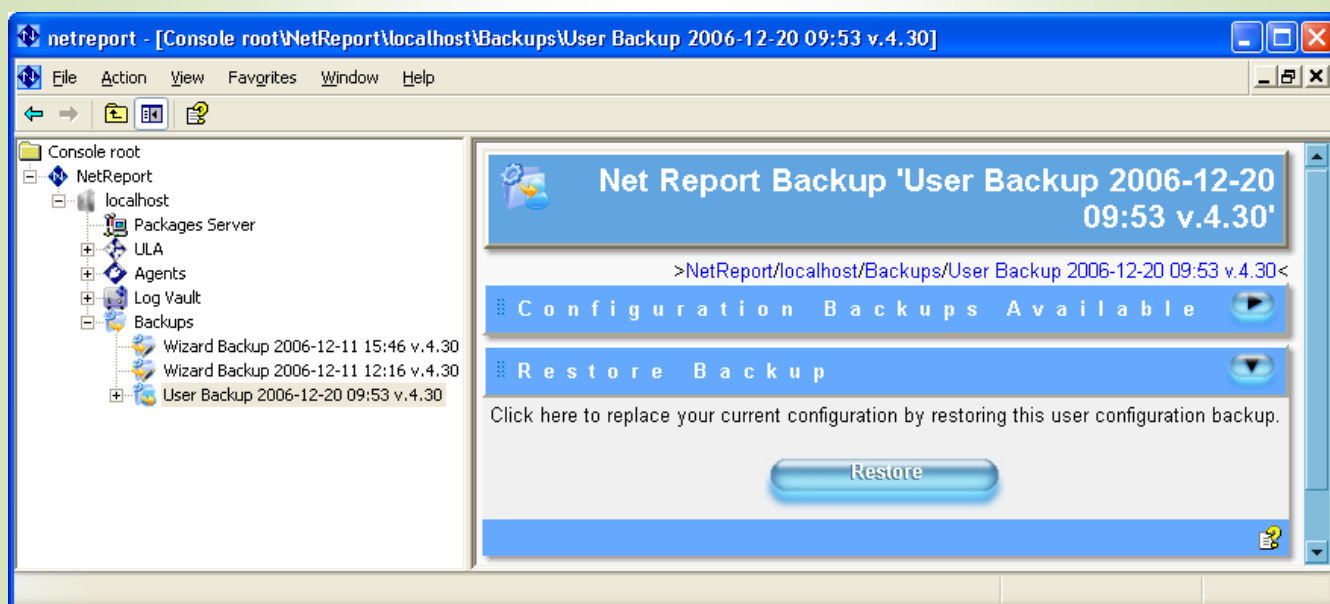


Figure 4 - Restoring a Backup

2. Click the **Restore** button

Or

2. Copy elements from the backup to the active configuration, for example, Actions, Rules, Fields, Dictionaries, certain Agent configurations and so on...

4.2.1.3. Exercise 1 - Modifying the Backup Path

To modify the Backup Path, please follow the steps below:

1. Select **Console root> NetReport> localhost> Backups** in the left Console root pane. The Click&DECiDE Backups screen appears in the right pane.

Note the default **Backup Path** where Click&DECiDE Backups are backed up:

..\Program Files\NetReport\NetReport\ConfigurationBackup

2. Modify the **Backup Path**, if you want your User Backups to be backed up in a path other than the default **Backup path**. The Migration and Wizard Backups will continue to be backed up in the default **Backup Path**.





3. Click the **Apply Changes** button to save the new **Backup Path** settings to the configuration server.

4.2.1.4. Exercise 2 - Modifying the Backup Name

To modify the Backup Name, please follow the steps below:

1. Select **Console root> NetReport> Local host> Backups** in the left **Console root** pane. The Click&DECiDE Backups screen appears in the right pane.
2. Modify the **Backup Name** for the Backup you want to customize it as appropriate. In this example the User Backup is renamed: **Customer Backup 2005-12-16**.
3. Click **Apply Changes** to save the new **Backup Name** setting to the configuration server.



4.3. Introducing Agents/Parsers

- Agents are used to collect device logs from the appropriate source.
- Agents parameters can be modified via the Click&DECiDE Management Console.
- Agents for devices with existing support are automatically configured by the Click&DECiDE Configuration Wizard according to the respective Parser (Flat File or Syslog).
- To access the **Agents** branch select **Console root>NetReport>Localhost>Agents**.

4.3.1. Check Point (Real Time) Agent

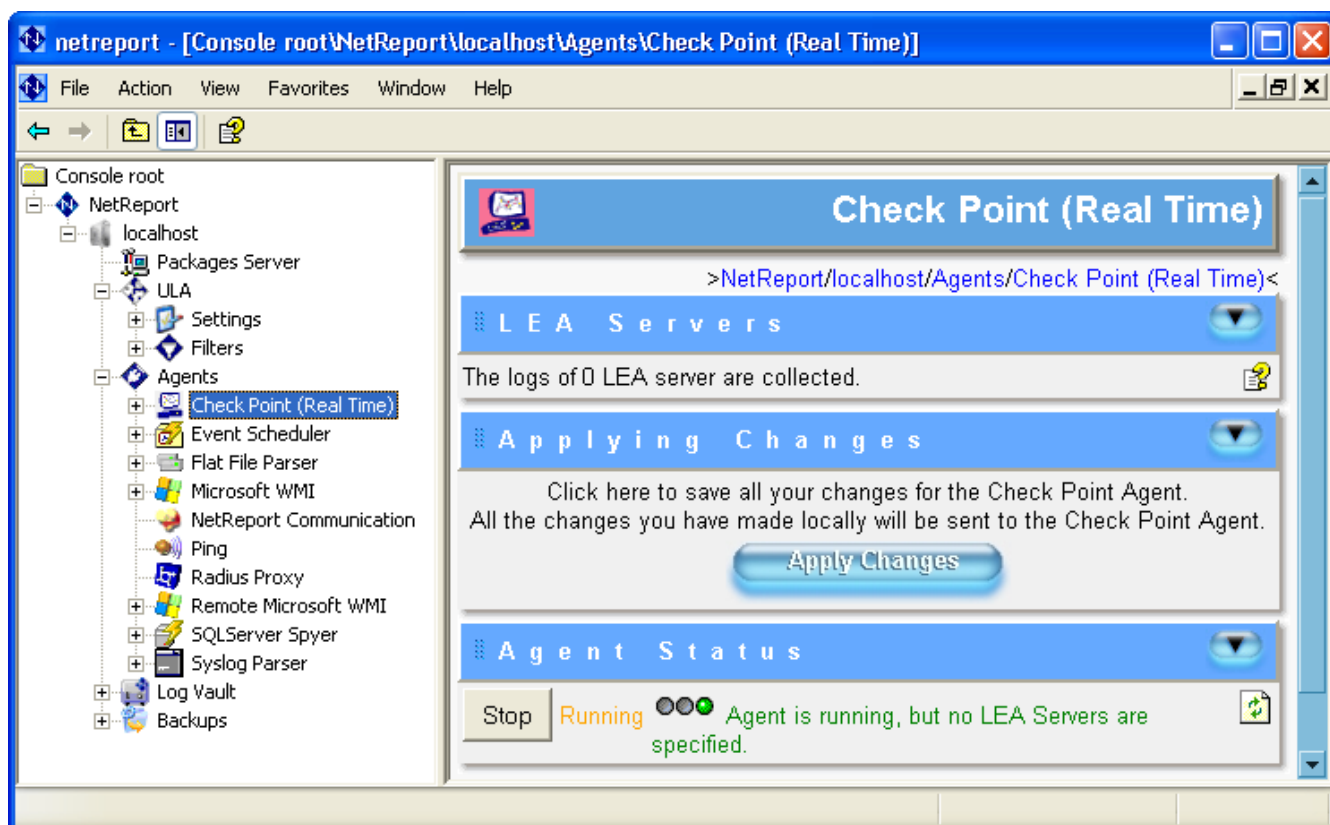


Figure 5 - Check Point (Real Time) Agent

Log Export API (LEA) specification enables events logs from the VPN-1/FireWall-1 (from the company Check Point) to be exported to other companies' applications. The Check Point (Real Time) agent must be installed on a machine that can communicate with the FireWall-1. The FireWall-1 must be setup to accept connections from the Check Point (Real Time) agent (that is, the LEA and OMI's ports, User Ids and authentication passwords' configuration).

A report generating application can use LEA to get the history and real time values of a user's connection activity counters through the firewall. It allows the administrator to check





the activity and prevent congestion. An intrusion or hostile activity detector could use LEA to detect the access attempts and the security gaps in its information system.

The Check Point (Real Time) agent sends records (NELRF) coming from one or several CheckPoint (FW1) NG Firewalls or lower to the Universal Log Analyser (ULA). For the NG versions, the agent allows server filters to be placed in order to only request pertinent information. The LEA API is based on the normal OPSEC API.

4.3.2. Click&DECiDE Communication Agent

Several ULA (Universal Log Analyser) concentrators might need to communicate or transmit information to each other that a specific Engine will be able to handle better than another. Each Engine has an agent responsible for communicating with other ULA Servers via their Click&DECiDE Communication Agent. This avoids duplicating actions in all the ULA concentrators based on one event, and also increases performance levels.

To understand the procedure in more detail, please read the information below.

- Each Engine has an agent responsible for communicating with other ULA Servers via their Click&DECiDE Communication Agent, through the TCP/IP network. This agent works on a client/server type organization.
- The agent's configuration page enables the connection parameters to be configured as a server.
- The **Connection to another ULA** initialization enables the connection parameters to be defined towards another Click&DECiDE Communication (COM) agent as a client.
- To send a log to another ULA concentrator, the **Send to another ULA** Action is used.
- The communication between two agents uses the Click&DECiDE Extensible Log Record Format (NELRF) and is encrypted with a shared secret.
- A Shared Secret is defined in the Server's configuration and any client knowing this shared secret can connect to the Server and send a NELRF to the engine working on the same machine as the COM Server.

The Server listens to a TCP port, definable in its configuration, and is able to receive a string in a NELRF format, and send it to the Click&DECiDE Filter Engine of the machine that it is working on. The Client is an object that knows how to connect to a server and send a NELRF string. For other Click&DECiDE Communication Agents to communicate with the ULA concentrator in your console, you must define your Agent's connection parameters in the Agents menu.



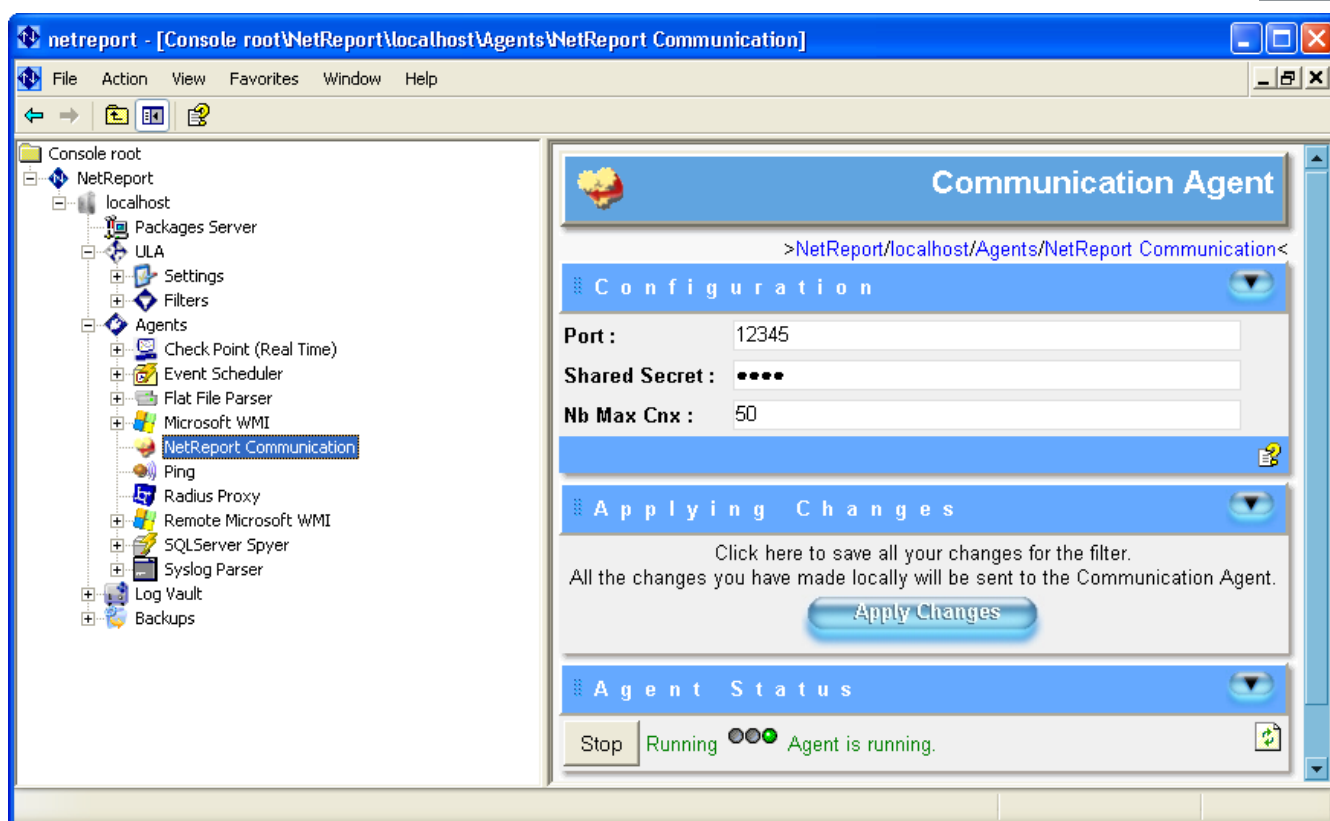


Figure 6 - Click&DECiDE Communication Agent

Port: the COM Agent's port as a server.

Shared Secret: the Shared Secret that the client must know to send a record in the NELRF format to the COM server. The COM server must know this Shared Secret as well. It enables you to code the communications towards this Agent.

Nb Max Cnx: the maximum Number of connections authorized on the COM Server.



4.3.3. Event Scheduler Agent

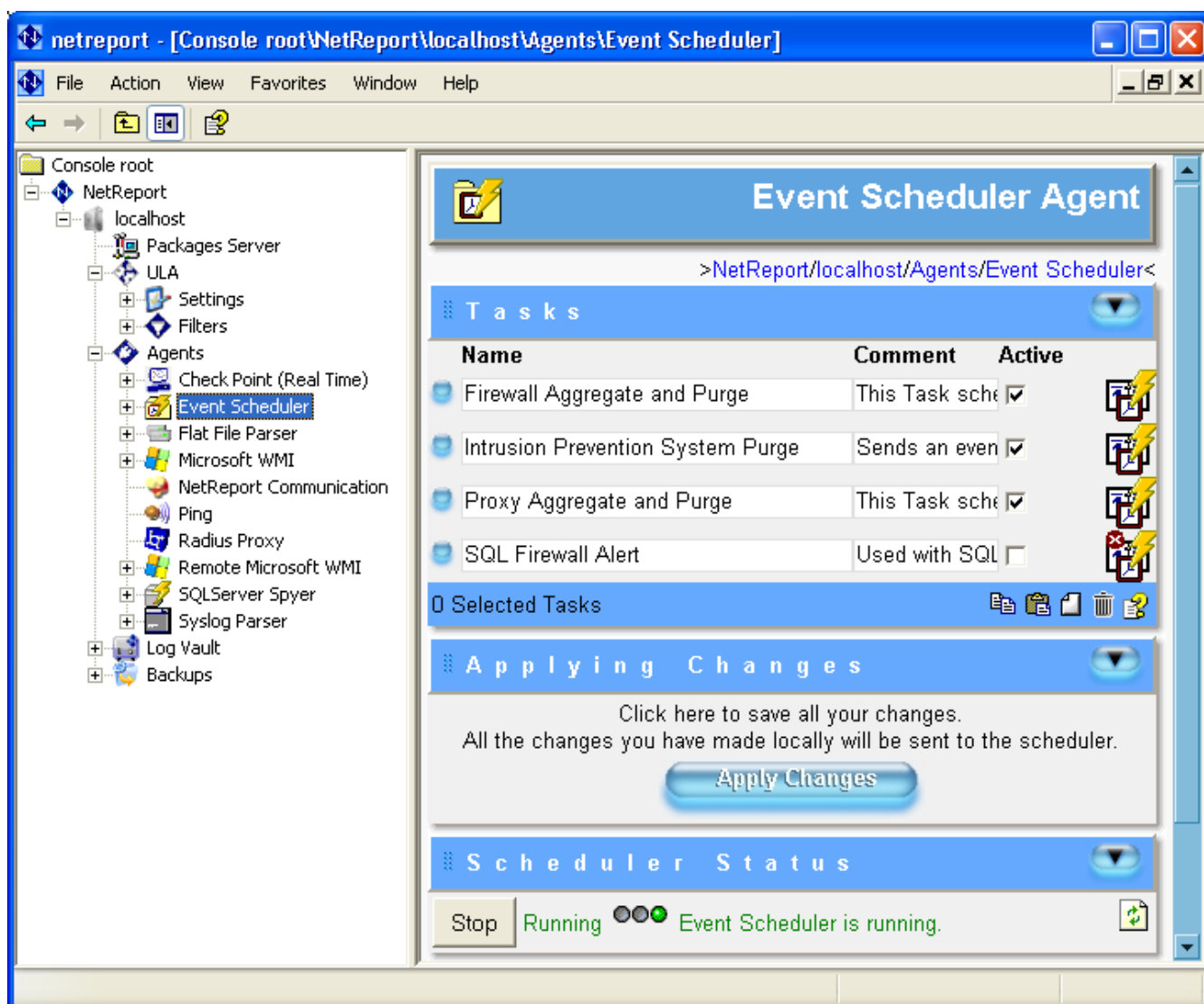


Figure 7 - Event Scheduler Agent

The Click&DECiDE Event Scheduler agent allows you to create triggers that will send an event to the Click&DECiDE engine at a specified frequency. The Click&DECiDE Event Scheduler agent uses the Task Scheduler integrated in Windows. A task is created with each trigger, whose program is in VBScript, which sends an event to the local Click&DECiDE Filter Engine.



4.3.4. Click&DECiDE Remote WMI Agent

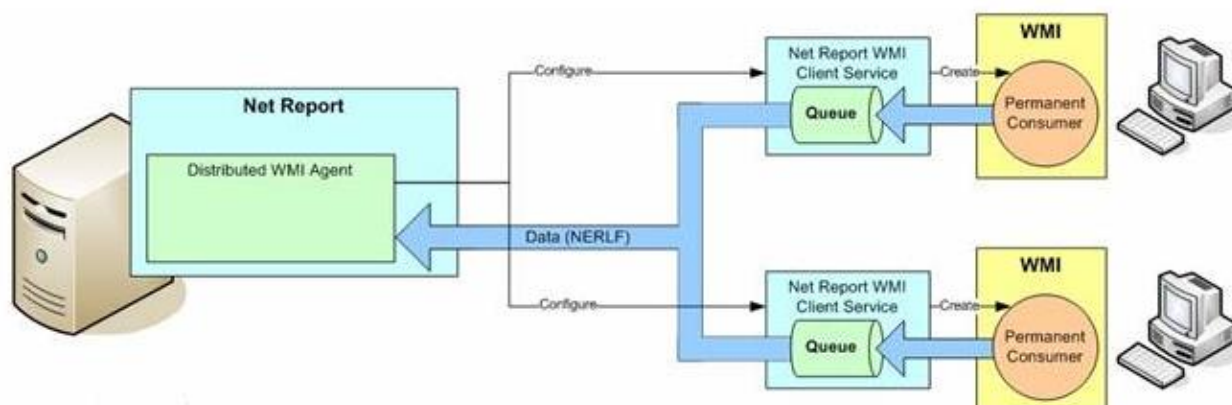


Figure 8 - Remote WMI Agent Architecture

Configure the Click&DECiDE Remote WMI Agent via the Click&DECiDE Configurator. The Click&DECiDE Remote WMI Agent requires the Click&DECiDE Remote WMI Service program to be installed on each computer you want to monitor. The program transfers the data to the Click&DECiDE Filter Engine. The Click&DECiDE Remote WMI Agent provides better WMI performance at distance than the Click&DECiDE Centralized WMI Agent. Log treatment is performed directly by each client, which liberates resources for the Click&DECiDE Filter Engine and the data transfer is fully controlled by **Click&DECiDE**.

Before configuring the Remote WMI Agent parameters please perform the following steps:

1. Ensure you have selected the computers you want to monitor via the Click&DECiDE Remote WMI Agent dialog boxes in the Click&DECiDE Configurator.
2. Install the Click&DECiDE Remote Microsoft WMI Service.
3. Configure the Audit Policy and the Audit Object Access for Files and Directories in Microsoft Explorer via the Microsoft Local Security Policy console as well as configuring the Microsoft Event Viewer Application, Security and System Logs.

To learn how, please follow the following link:

[http://www.clickndecide.com/downloads/WebDoc/ConfGuides/Net%20Report Configuration Guide for Remote Microsoft WMI.pdf](http://www.clickndecide.com/downloads/WebDoc/ConfGuides/Net%20Report%20Configuration%20Guide%20for%20Remote%20Microsoft%20WMI.pdf)

The Remote WMI Agent screen is made up of five sections:

- General Configuration
- WMI Computer Lists
- Available WMI Consumers
- Applying Changes



- Agent Status

Port: the port number you defined in the Click&DECiDE Remote WMI Service for the service to connect to Click&DECiDE on.

Maximum Number of Connections: enter the maximum number of clients connecting to each computer scanned (10 by default).

WMI Computer Lists

Lists the active Computer Lists you defined in the Click&DECiDE Configurator.

Note: Clicking the Modify Computer List icon takes you directly to the <Monitored Computers> screen where you can configure the computers and the Active consumers.

Available WMI Consumers

Lists the WMI Consumers which are available to activate along with their description?

Note: Clicking the modify consumer icon leads you to the specific configuration details for the WMI Consumer you selected.

4.3.5. Click&DECiDE Centralized WMI Agent

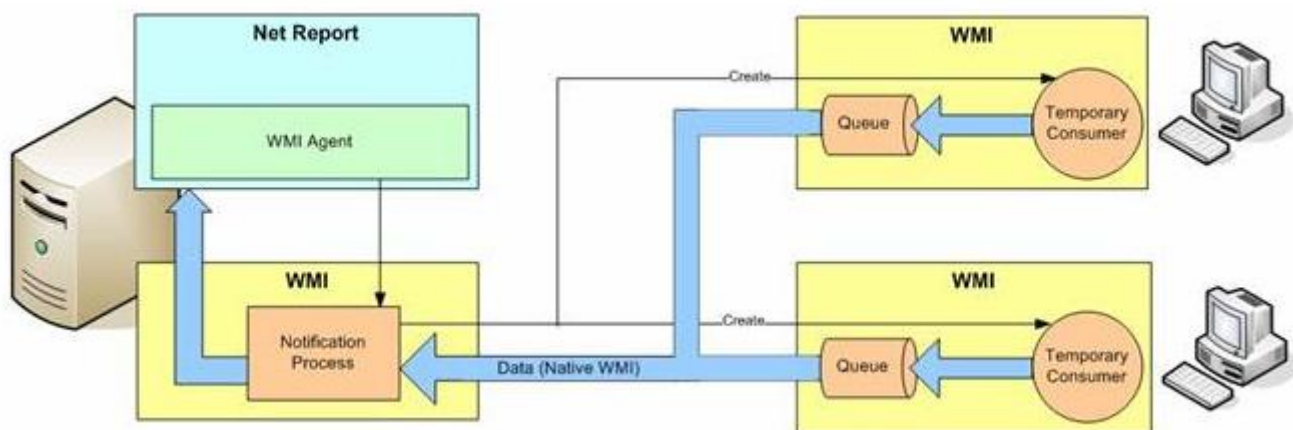


Figure 9 - Centralized WMI Agent Architecture

With the Click&DECiDE Centralized WMI agent, the server treats all the WMI logs and the data transfer is managed by the WMI API. Please note that it is difficult to control performance with the Click&DECiDE Centralized WMI Agent.

For more information on configuring WMI with [Click&DECiDE](#), please use our online Device Support Manuals and Online Management Console User Help.



4.3.6. Click&DECiDE Ping Agent

PING stands for Packet Internet or Inter-Network Groper. PING is a program that allows you to verify if a specific active IP address exists. It is a utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. This program is often used for diagnostic purposes.

PING can be used to know the response time (round trip) between two machines. The PING program works in the following manner: it sends a packet with a size that you can personalize to the address you choose and gives you the total transmission time with the response. PING uses the ICMP/IP protocol, sends an echo request to the defined address and waits for an ICMP Echo reply type response. The non-response does not necessarily mean that the distant device is not working, as in some cases some security or router equipments can prevent these requests from reaching the equipment.

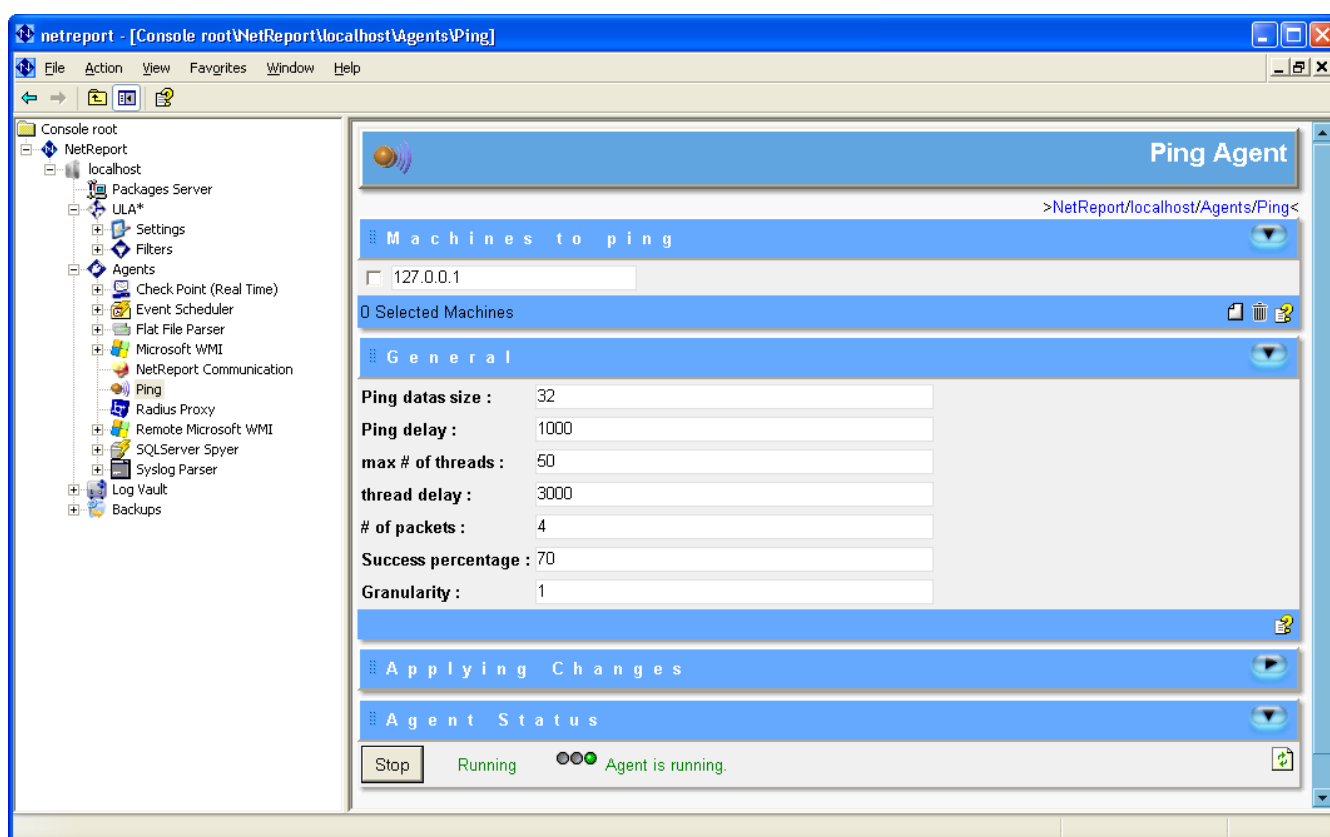


Figure 10 - Ping Agent

Machines to ping: enter the IP Addresses for the machines you wish to ping.

Ping Data Size: 32 bytes are available by default (1 to 65000). Size (in bytes) of the packet that is sent to the machine which is present on the network that has to be tested (for each packet sent).





Ping Delay: the delay (in milliseconds) for a response from the machine which is present on the network that has to be tested, and after which the Agent considers that the machine has not responded. 1000 milliseconds are available by default

Max # of threads: the maximum number of threads. 10 threads are available by default. The maximum simultaneous number of threads matches the maximum number of machines that can be tested at one time.

Thread delay: The delay for each thread between each processed machine (in milliseconds). 3000 milliseconds are available by default.

of packets: the number of packets. The number of packets sent to each processed machine. Four are available by default.

Success percentage: the minimum percentage for the program to estimate that the processed machine has responded sufficiently to the packets sent, and is on the network. 30% is available by default.

For example, if # of packets is configured with 4, and 3 responses are received from the processed machine, the success percentage is $\frac{3}{4} = 75\%$.

Granularity: 1 is available by default. Due to the bad settings of a defective cable or network interface card, a situation may occur where a machine's status appears connected and then disconnected, and then connected again within a short period of time. This can generate a significant amount of events which are sent to ULA. The Ping agent can limit the amount of events sent to ULA, with the help of the Granularity parameters that represent the minimum delay (in minutes) between two events sent to ULA.

4.3.7. Click&DECiDE Radius Agent

RADIUS is short for Remote Authentication Dial-In User Service. RADIUS is an authentication and accounting system. RADIUS is a client/server protocol that enables you to authenticate the users who access a requested service. RADIUS enables a company to maintain users' profiles in a central database for all the remote servers to share. It provides better security, enabling any company to define a global policy that will be administrated in a centralized manner.

The Radius protocol manages what is agreed as the 3As:

- **Authentication:** manages the users' authentication.
- **Authorization:** manages the users' rights.
- **Accounting:** accounts for what the users do during their session (how many bytes received and sent during the session and so on).



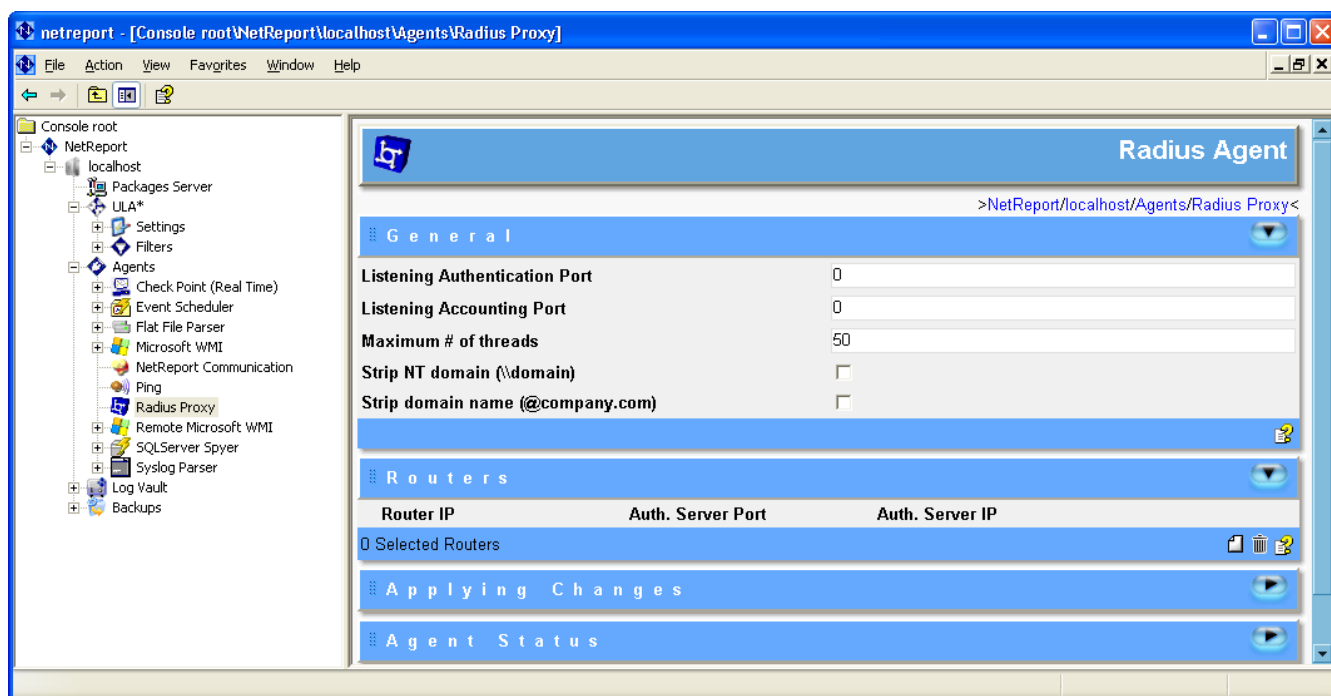


Figure 11 - Radius Agent

Listening Authentication Port: 1812

Listening Accounting Port: 1813

Maximum Number of Threads: 50

Strip NT domain (\\domain): removes the domain name \\domain\ preceding the content of attribute 1 that sends the User-Name back in certain configurations. For example, \\domain\Dupont will be received as Dupont.

Strip domain name (@company.com): removes the @company.com part that can follow the content of attribute 1 that sends the User-Name back in certain configurations. For example: Dupont@company.com will be received as Dupont in this case.

Router IP: router's IP address.

Authentication Radius Server Port: Radius authentication server's port. Note that the default port is: 1812 (Radius standard). However this can be modified, Port 1645 is the old standard port.

Authentication Radius Server IP: Radius authentication server's IP address.

Router Shared Secret: the Shared Secret used between the router and the RADIUS Agent. It is not mandatory if the Shared Secret is the same as the RADIUS Server's, as long as the RADIUS Agent transfers the Accounting frames to the RADIUS Accounting Server.





Accounting Radius Server IP: the Accounting Radius Server IP address, usually the same as the RADIUS Authentication server's. If this address is not indicated, it will take the Authentication Server's by default.

Accounting Radius Server Port: the Radius Accounting Server's Port: 1813 is proposed (that is, the RADIUS standard). This can be modified (for example, Port 1646: based on the old standard).

Note: if this field is not filled in, no Accounting frame will be sent to the Radius Accounting Server since Click&DECiDE will then handle the Accounting frames. In this case, it is mandatory to have typed the Router's Shared Secret because it is used by Click&DECiDE's Radius Agent to send the Accounting acknowledgement of delivery to the Router.

Reply Timeout: the response's time limit. 10 seconds is proposed by default.

Radius Server Shared Secret: the Shared Secret used between the Radius Agent and the Radius Server. If it is not indicated, the Router's Shared Secret will be used. It is not mandatory to indicate the Shared Secret here if it is the same as the Router's as long as the Radius Agent transfers the Accounting frames to the Radius Accounting Server.

Add Proxy State: if the Radius Server supports this function, this parameter indicates where the IP was sent from. However, it does not indicate the IP of the machine on which the Radius Agent is installed.

Proxy State Format: holds the syntax used in the Proxy State's parameter's value (that is, attribute 33), the %1 will automatically be replaced by the original IP address. If the Add Proxy State check box was selected, the Radius agent will add attribute 33 to the frame with the following value:

Proxy_NAS_IP: xxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the original IP address.

4.3.8. SQL Server Spyer

Several services offer to write their logs directly in a database (for example, IIS). If it streamlines the work for Click&DECiDE, it cannot generate actions when an event that is particularly important occurs. This is the SQL Server Spyer Agent's purpose.

As its name suggests, this agent only works with SQL Server (8+) and despite its name, the SQL Server Spyer does not really "spy" on SQL Server. It simply creates triggers that will notify Click&DECiDE's engine when a certain row is inserted in a table. Nevertheless, to make things work, it is necessary to configure the machine that the database is running on.



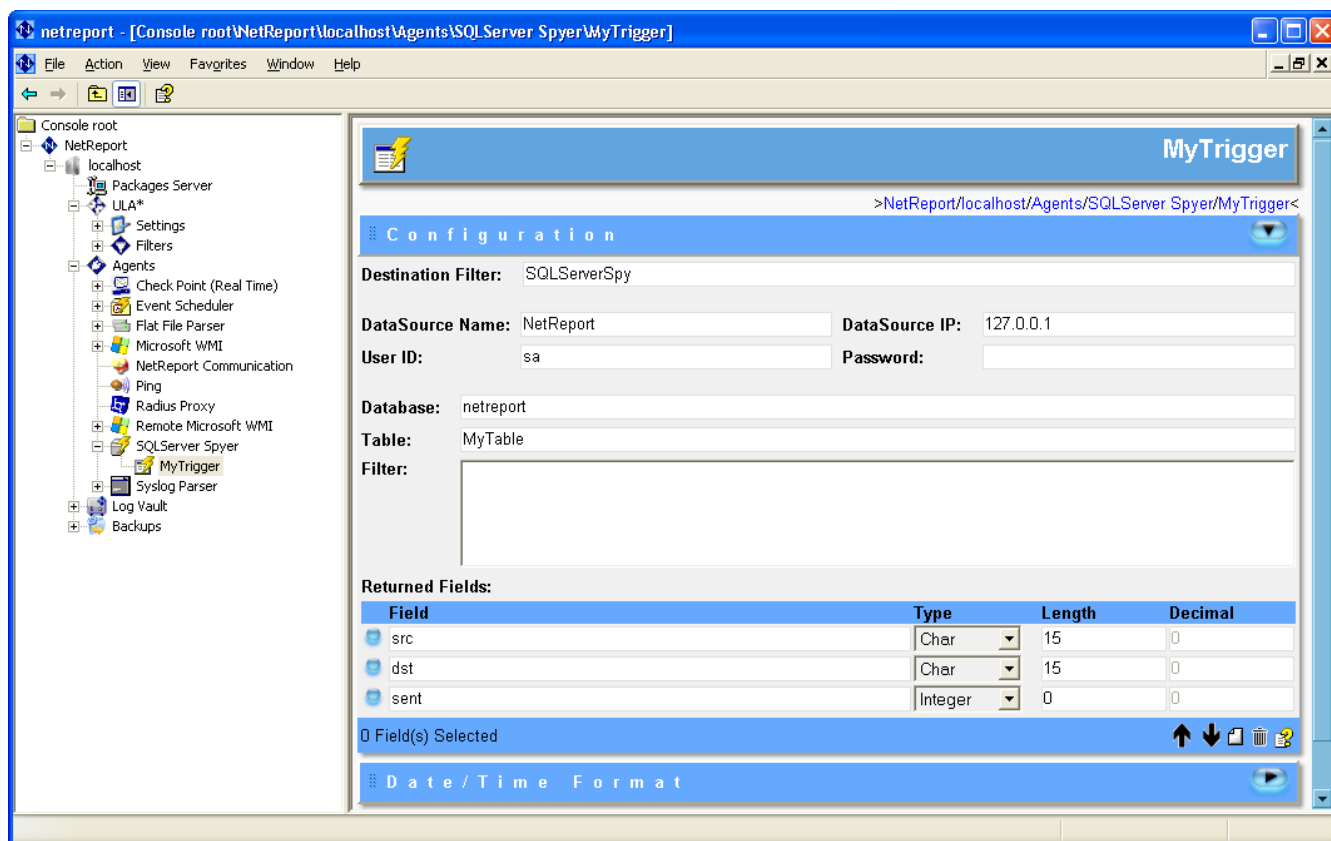


Figure 12 - SQL Server Spyer

Destination Filter: the Click&DECiDE filter that will process the event generated by the trigger.

User ID: login for data source name (please see the DDI Initialization section).

Password: the password for data source name (please see the DDI Initialization section).

DataSource IP: the IP address of the machine where the database is running. This is the value that will be sent in the NRAgentIP field.

Database: the name of the database. If no name is defined, the default database (master) will be used.

Table: the name of the table where you want to create a trigger on.

Filter: the WHERE clause of the Transact-SQL language that specifies the type of row that will generate an event when inserted.

Returned Fields: the fields of the table returned when an event occurred (it is not necessary to return all the fields). Please note that the global size of the returned field cannot exceed 8000 characters. As a consequence, all the fields containing strings will be truncated to 255 characters.





4.3.9. Flat File Parser

Click&DECiDE provides four main types of Flat File Parser:

- The Generic Parser
- The Tabular Parser
- The W3C Parser
- The Replay Parser

Device Breakdown by Flat File Parser

The following devices have device-specific Flat File Parsers which are based on the following type of parser:

Generic Parser

- Aladdin eSafe
- Apache
- ARKOON Network Security
- Cisco PIX
- Clavister
- Fortinet FortiGate UTM
- IBM Lotus Domino
- ISS Proventia IPS
- Juniper Networks NetScreen
- Juniper NSM
- McAfee IntruShield
- Microsoft Exchange 2000
- Microsoft Exchange 2003
- Microsoft Exchange 5.5
- Microsoft Internet Connection Firewall
- MIMESweeper
- NETASQ
- netfilter ipchains
- netfilter iptables
- Novell BorderManager
- Olfeo
- Postfix
- Radius Cisco Secure
- Radius Telefonica
- Radware Defense Pro
- Replay – Check Point FireWall-1 (LEA)
- Replay – Microsoft WMI
- Replay – Radius
- SendMail
- SNORT FAST





- SNORT FULL
- SNORT Syslog
- SonicWALL
- SonicWALL (Syslog Format)
- Squid
- Squid Reverse Proxy
- SquidGuard
- Stonesoft StoneGate
- Symantec Gateway Security
- Symantec Raptor Firewall
- Trend Micro IMSS for Linux eMgr
- Trend Micro IMSS for Linux Virus
- Trend Micro IMSS for Windows eMgr
- Trend Micro IMSS for Windows ISNT
- Trend Micro IMSS for Windows Virus
- Trend Micro IWSS
- WatchGuard
- WatchGuard (WELF Format)
- WatchGuard (XML Format)

Tabular Parser

- Check Point Firewall (Command Line)
- Check Point Firewall (GUI)
- Microsoft ISA Server (Native Format)

W3C Parser

- Microsoft Internet Information Server (Real-Time)
- Microsoft Internet Information Server (Static)
- Microsoft ISA Server (W3C Format)
- Blue Coat
- F5 WebAccelerator
- NetApp NetCache
- NetApp NetCache v5.5
- NetApp NetCache v6

Replay Parser

- Replay - Check Point FireWall-1 (LEA)
- Replay - Microsoft WMI
- Replay - Radius



4.3.9.1. Introducing the Generic Parser

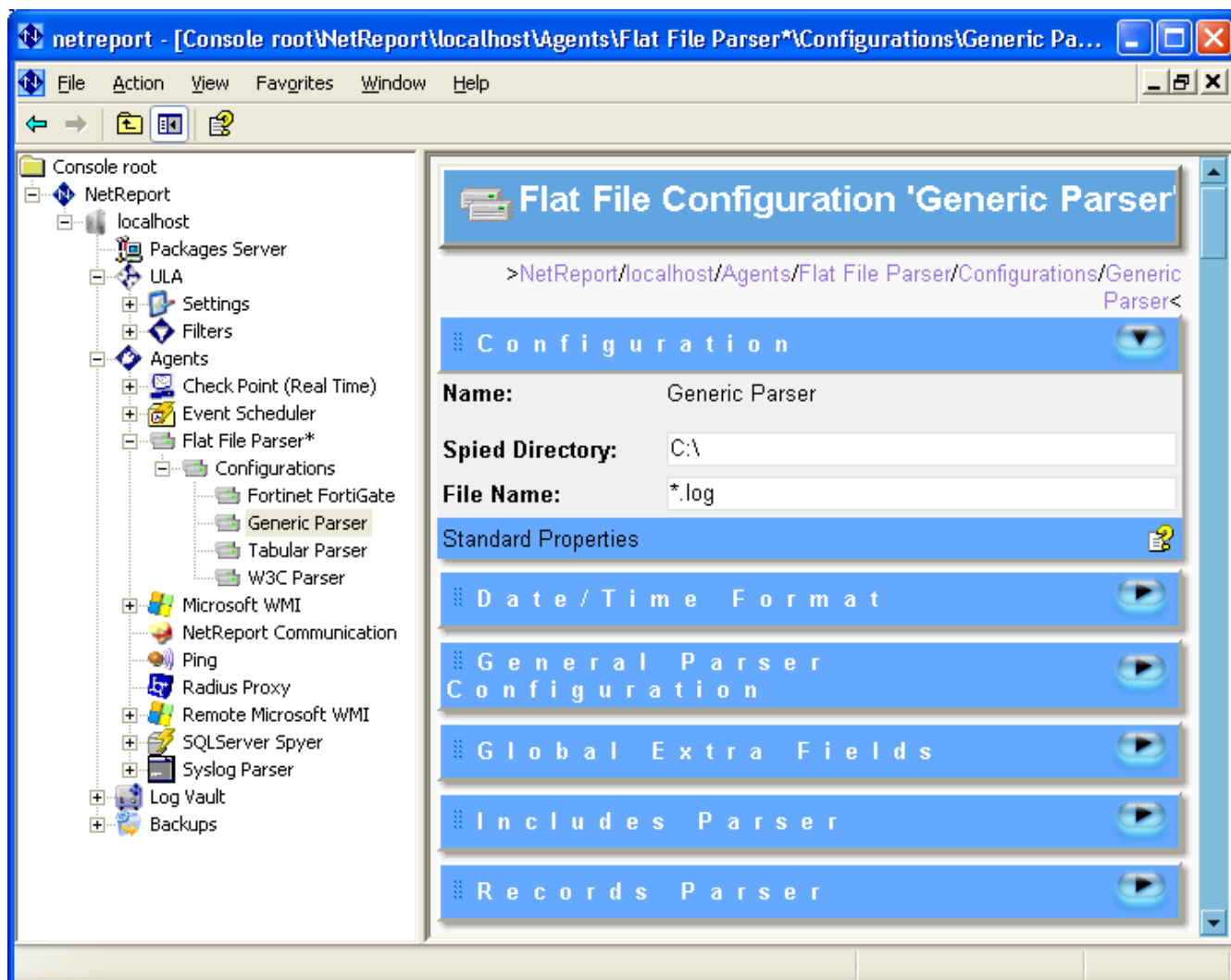


Figure 13 - Flat File Generic Parser Configuration

The Generic Parser screen is made up of six sections:

- Configuration
- Date/Time Format
- General Parser Configuration
- Global Extra Fields
- Includes Parser
- Records Parser

4.3.9.2. Configuration

The Configuration section enables you to configure the directory you want Click&DECiDE to spy on and the file name format of your flat file logs.



Name: the Flat File Parser name.

Spied Directory: the directory where the device logs are. Click&DECiDE will spy on this directory and treat the logs inside it.

File Name: the default file name for your logs. The default value is *.log.

4.3.9.3. Date/Time Format

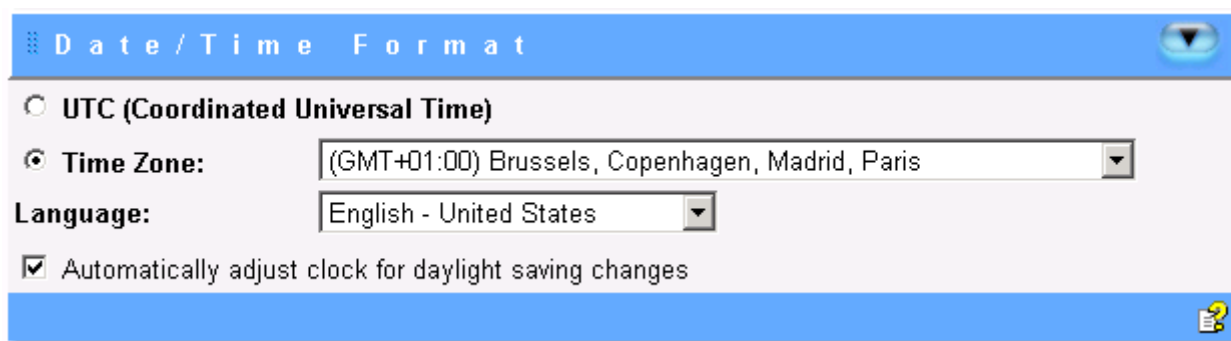


Figure 14 - Flat File Generic Parser Date/Time Format

Click&DECiDE collects your security device logs and converts them from their specific Time Zone into Coordinated Universal Time (UCT) before they are analyzed. For Click&DECiDE to correctly convert the date/time values in your logs to UCT, you must indicate the Time Zone parameters which characterize your Device's configuration. Please note that if your device is configured for UTC then Click&DECiDE will simply leave the time data in UTC.

For Click&DECiDE to translate the dates used in your logs, above all, the month (for example, January, janvier, gennaio, enero etc...) you must select the language options which are relevant to each of your device(s). Click&DECiDE will then be able to translate the dates used in your logs.

To configure the Time Zone for your Device, either indicate the Time Zone where your device is physically located (if you are configuring Click&DECiDE for several devices in different countries then you will need to select each of the many Time Zones for these devices) along with whether Daylight Saving Time (DST) Adjustment applies to the device. Or select the UTC (Coordinated Universal Time) offset if the device is configured for Coordinated Universal Time.

UTC (Coordinated Universal Time): for Click&DECiDE to correctly treat date/time values in your logs, you must indicate whether or not your device is configured to use the UTC (Coordinated Universal Time) offset.

Time Zone: the Time Zone for the log, that is where your device is physically located.

Language: the language the log is in.





Automatically adjust clock for daylight saving changes: select this check box if the Date/Time parameters of your device are configured to adjust for Daylight Saving Time (DST). That is, where clocks are set one hour or more ahead of standard time to provide more daylight at the end of the working day during late spring, summer, and early autumn.

4.3.9.4. General Parser Configuration

Figure 15 - Flat File Generic Parser General Parser Configuration

Destination Filter: the Click&DECiDE filter that will process the event generated by the trigger.

Search for Header:

- **No Header:** if the file's parsing is interrupted then Click&DECiDE will start parsing where it left off.
- **Only One header:** if the file's parsing is interrupted then Click&DECiDE will go through the file from the top of the file until it finds the first header and it will then start parsing using this header from where it was interrupted.
- **Several Headers:** if the file's parsing is interrupted then Click&DECiDE will go through the file from where it was interrupted and will go backwards through the file looking for the first header. It will then start parsing using this header from where it was interrupted.
- **Don't Know:** if the file's parsing is interrupted then Click&DECiDE will go through the file from the top of the file to where it was interrupted, it will then start parsing using the last header it found from where it was interrupted.

Record Separator: the character used to identify a logical boundary between adjacent records in your log file. The default value is \n.

Disable Backward Compatibility with Version 4.20 or Earlier: selecting this check box will disable backward compatibility with the parsers in Version 4.20 or Earlier. From Click&DECiDE Version 4.30 and greater the Syslog and Flat File Parsers have been





optimized. If you want to use the previous versions of the Syslog and Flat File Parsers (that is, those in Click&DECiDE Version 4.20 and earlier) then clear this check box.

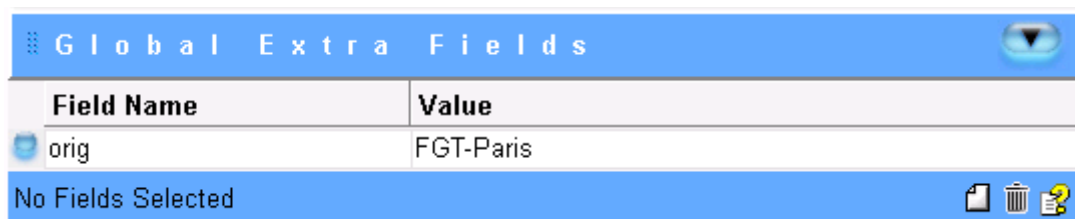
Text Delimiter: the character the log file uses to encapsulate text. The default value is ". If **Disable Backward Compatibility with Version 4.20 or Earlier** is checked, this character will be automatically removed at the beginning and at the end of the text.

String as Null Value: how the value Null is represented. If the parser encounters an attribute with this specific value, it will automatically replace this value with an empty string.

Include Record Separator: select this check box if you want to include the Record Separator.

4.3.9.5. Global Extra Fields

This section allows you to add additional information that may not be present in the logs; for example, the name of the device that generated the logs.



Field Name	Value
orig	FGT-Paris

No Fields Selected

Figure 16 - Flat File Generic Parser Global Extra Fields

Field Name: the name of the Global Extra Field.

Value: the field's value.

Includes Parser

To make the regular expressions as readable and user friendly as possible, Click&DECiDE enables you to create predefinitions. For each one of them, a name and a pattern must be defined.





Pattern: the Include's pattern.

4.3.9.6. Records Parser

This is the list of regular expressions used to parse the logs for a device. You can define several regular expressions. The parser will use the first one that matches.



Header: select this checkbox to define a pattern for the header.

Number: the record number, you can move the record up and down in the list via the up and down arrows.



4.3.10. Syslog Parser ***REVIEW NEEDED (has changed in 10.3)***

Syslog is an abbreviation for System Log. Syslog is a journal for all events within a system. On most UNIX operating systems, the journal for daily events, the applications and some network devices are affected by a service (that is, a daemon under UNIX) called syslogd. The device must be configured to send the data from the event journal to the Click&DECiDE Agent. When a log is received, it is sent to the first configuration that meets the header criteria. Up and down arrows can be used to order the configurations.

Configuration

Name: Syslog Trace

Criteria:

☐ Client IP =

☐ Facility =

☐ Severity =

☐ Hostname =

☐ Process Name =

Message:

Mode:

Standard Properties

Figure 19 - Syslog Parser Configuration

Name: the Syslog Parser name.

Client IP: the IP address of the machine transmitting the Syslog message.

Facility: the value of the Facility field of the Syslog message. (0 - 23).

Note: the Facility and Severity fields are not directly transmitted in the Syslog message. They are transmitted through the Priority field with the relation: $\text{priority} = \text{Facility} * 8 + \text{Severity}$.

Severity: the value of the Severity field of the Syslog message. (0 - 7).

Note: add a comparison sign in the case of Facility and Severity if appropriate. The values ""(null string) and -1 are interpreted as a "criteria not specified":

Hostname: the value of the Hostname field of the Syslog message.

Process Name: the value of the Process Name field of the Syslog message.





Message: which part of the message should be parsed. Three choices are available:

- **Parse the whole Syslog message.**
- **Parse only the 'msg' part.**
- **Parse only the 'content' part.**

Mode: how the Syslog message should be treated. Three choices are available.

- **Send Record:** sends a record to the Click&DECiDE Engine.
- **Log to File:** this option enables you to define the Base File Name for the flat file via the Base File Name field.
- **Log to File and Send Record:** this option enables you to define the Base File Name for the flat file via the Base File Name field.

Figure 20 - Syslog Parser Log to File Mode

Base File Name: how the Syslog message should be treated. Select the folder or file name you want to add a splitter to and then select one of the following five splitters.

- **IP Splitter:** splits the file path and/or file name by the IP Address of the Device sending the Syslog, when the IP address changes a new flat file will be created in the directory you define.
- **Year Splitter:** splits the file path and/or file name by Year, when the year changes a new flat file will be created in the directory you define.
- **Month Splitter:** splits the file path and/or file name by Month, when the month changes a new flat file will be created in the directory you define.
- **Day Splitter:** splits the file path and/or file name by Day, when the day changes a new flat file will be created in the directory you define.
- **Hour Splitter:** splits the file path and/or file name by Hour, when the hour changes a new flat file will be created in the directory you define.

4.3.1. SNMP Trap Listener

SNMP messages may be initiated by either the network management system (NMS) or by the network element. An SNMP TRAP is a message which is initiated by a network element and sent to the network management system. For example, a router could send a message





if one of its redundant power supplies fails or a printer could send an SNMP trap when it is out of paper.

The idea behind trap-directed notification is that if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for the manager to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.

After the manager receives the event, the manager displays it and can choose to take an action based on the event. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

SNMP Versions

The SNMP protocol has benefited from major upgrades since its introduction in 1988. Many network elements support only SNMPv1 and SNMPv2c. Support for SNMPv3 is minimal.

Version	Description
SNMPv1	SNMPv1, which implements community-based security
SNMPv2c	SNMPv2 with community-based security
SNMPv2u	SNMPv2 with user-based security
SNMPv2	SNMPv2 with party-based security
SNMPv3	SNMPv3, which implements user-based security

Terminology

MIB: The SNMP MIB, or Management Information Base, is a collection of variables which is shared between the NMS and the network element (NE). In general "a MIB" refers to group of management objects, all relating to the same general management task. This is more strictly a "MIB module" or "MIB file". "The MIB" of an agent or management tool is the collection of all MIB modules known to that particular application. The MIB is extensible, which means that hardware and software manufacturers can add new variables to the MIB. These new MIB definitions must be added both to the network element and to the network management system.



OID: An Object ID (OID) is a way of identifying a particular management object, as a sequence of numerical sub-identifiers.

4.3.1.1. Introduction to the Click&DECiDE SNMP Trap Listener Agent

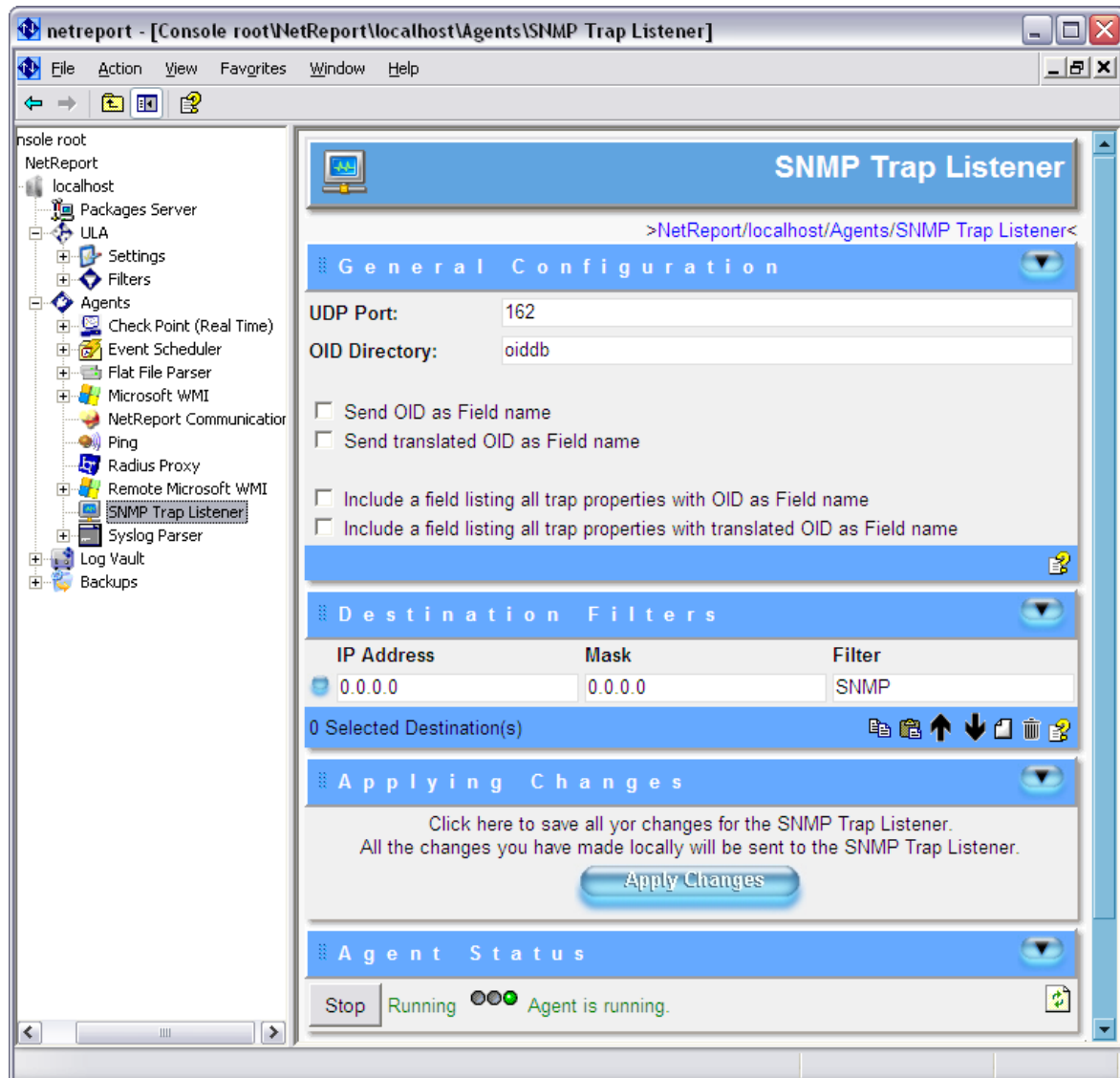


Figure 21 - SNMP Trap Listener

SNMP Trap Listener Agent is used to listen to traps received from the NET-SNMP / UCD-SNMP snmptrapd trap daemon, it can also translate SNMP traps into easy to understand messages.

SNMP Trap Listener listens to traps, parses them and sends them to a specific filter. The filter can then be configured to perform actions or send alerts. You can configure the SNMP Trap Listener to send printer specific traps to a filter and network device specific traps to





another. Based on the information extracted from the trap by the SNMP Trap Listener, the filter can assign the severity as critical and also associate an email action.

The default port through which the traps are received is 162.

4.3.1.2. General Configuration

UDP Port: Universal Serial Bus Port, this is 162 for SNMP Traps by default.

OID Directory: the directory where the CSV (Comma Separated Values) file with the OID definitions is located. The default directory is relative to the installation directory, for example: **C:\Program Files\Click and DECiDE\NS\oidb**.

Note: by default Click&DECiDE does not provide any CSV files with the OID definition but Click&DECiDE can generate these files from the MIB if needed. Please contact **Click&DECiDE's** Technical Support Team for more information.

Once a trap has been received, the SNMP Trap Listener parses it. The result is a list of OIDs and their values. You can choose to send the list as it is (with the OID sequence of numerical sub-identifiers as field name) to the ULA filter or you can choose to translate the OID sequence of numerical sub-identifiers (using the definitions in the **OID Directory**) into a more user-friendly name choose both.

Send OID as Field name: sends the Object ID as a field name.

Send translated OID Field name: sends the translated Object ID as a field name. This requires the CSV File with the corresponding OID definitions.

You can also send additional fields that contain the list of OIDs and their values in a single string to the ULA. Once again you can choose to send the OID sequence of numerical sub-identifiers or its translation.

Include a field listing all trap properties with OID as Field name: includes a field with all the SNMP trap properties with the Object ID as the field name.

Include a field listing all trap properties with translated OID as Field name: includes a field listing all the SNMP trap properties with the translated OID as the field name. This requires the CSV File with the corresponding OID definitions.





4.3.1.3. Configuring the Destination Filter Section

The **Destination Filter** section enables you to define the IP Address and the mask for the device sending the SNMP Trap to Click&DECiDE and to define to which destination filter the SNMP Trap should be sent. You can thus send incoming traps from low priority devices (such as printers) to a filter and send incoming traps from high priority devices (such as routers) to another filter.

4.3.1.4. Working with the Agent Status Section

The SNMP Trap Listener Agent's status in this example is: Running. This indicates that it is listening. If you want to stop the agent, click the **Stop** button. The **Stopped** status will then be displayed and a **Start** button appears for you to restart it. If you want to start the agent, click the Start button. The **Started** status will then be displayed.

4.3.2. Suggestions for Practice

4.3.2.1. Exercise 1 - Adding a Generic Parser

1. Add a Generic Parser
2. Add an Includes Parser with the
 - a. **Name:** value
 - b. **Pattern:** `[^\s]+`
3. Add a **Records Parser** with the Pattern:
(?<value:First Name>)\s+(?<value:Second Name>)\s+(?<value:Town>)\s+(?<value:Country>)\s+(?<value:Telephone Number>)

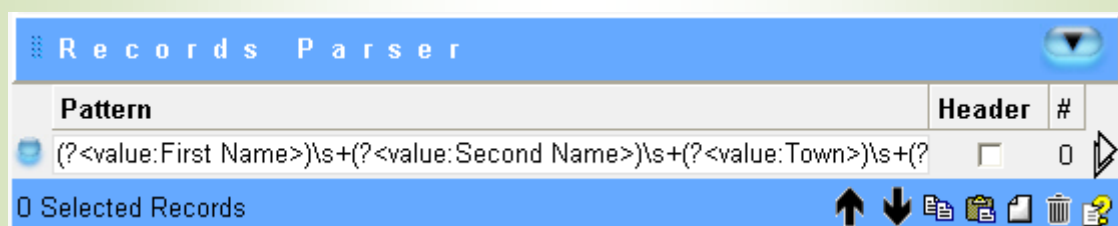


Figure 22 - Adding a Generic Parser: New Record Parser



4. Click the arrow icon to the right of the pattern to add a **Test Value**:

In this example:

John Smith Paris France 0033165237455

Figure 23 - Adding a Generic Parser: Record Parser Configuration

5. Click **Test**. The **Output** appears.

Figure 24 - Adding a Generic Parser: Test Output

6. Click **OK**.

7. Enter the **Spied Directory**: C:\Logs

8. Enter the **File Name**: *.log

Figure 25 - Adding a Generic Parser: Configuration



9. Create a plain text file and enter three lines of data respecting the format:

First Name Second Name Town Country Telephone Number

Note: remember to add a carriage return at the end of each log row.

In this example:

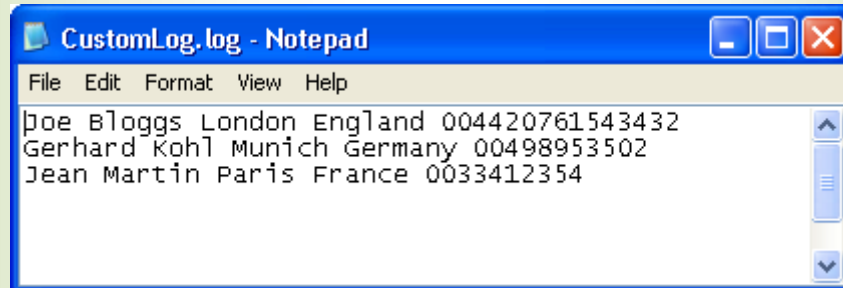


Figure 26 - Adding a Generic Parser: Test Log File

10. Save the log file with the File Name: CustomLog.log in C:\Logs.

11. Enter the **Destination Filter**: MyCustomFilter

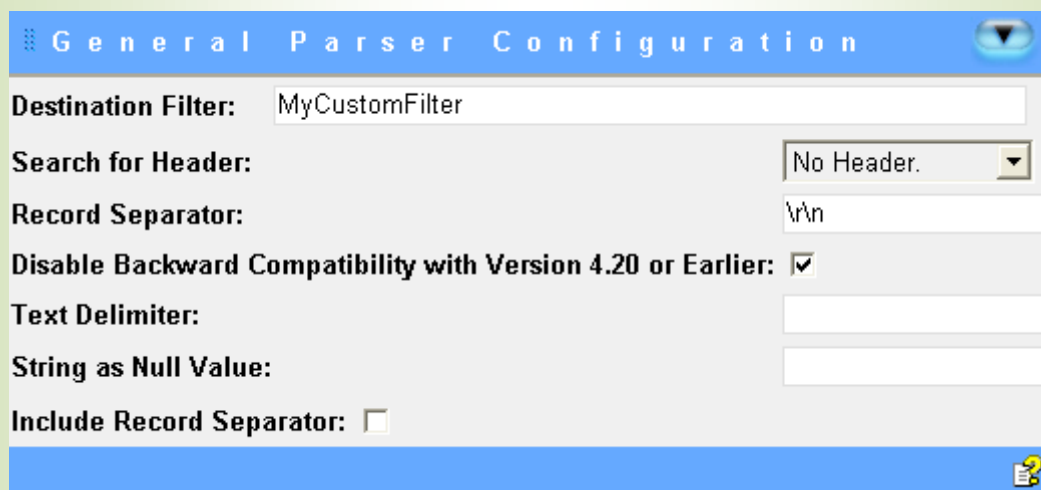


Figure 27 - Adding a Generic Parser: General Configuration

12. Select **No Header** in the **Search for Header** drop-down list.

13. Enter the **Record Separator** \r\n.

14. Select Console root> NetReport> [localhost]> ULA > Agents> Flat File Parser.

15. Click Apply Changes.



4.3.2.2. Exercise 2 - Creating a Custom Filter

1. Select **Console root> NetReport> [localhost]> ULA > Filters.**
2. Add a **Custom Filter** from the drop-down list, click New.
3. Enter the filter name as: **MyCustomFilter.**

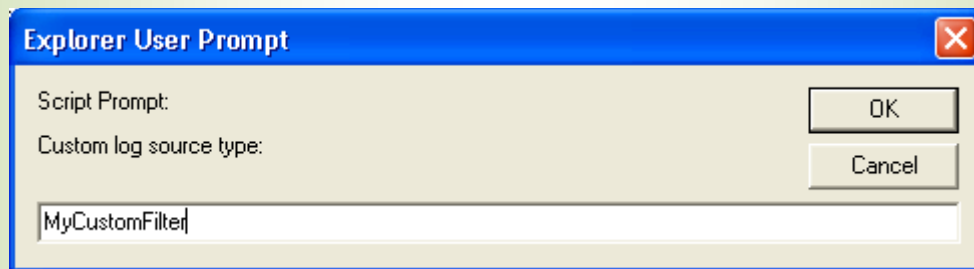


Figure 28 - Creating a Custom Filter

4. Click **OK.**

4.3.2.3. Exercise 3 - Creating Fields

1. Select Console root> NetReport> localhost> ULA> MyCustomFilter > Fields
2. Click the **New** icon to add a field. The _New Field row appears.
3. Rename the field:
 - a. **Name:** FirstName
 - b. **Type:** String
 - c. **Expression:** Record("First Name")
4. Create a new field with the following properties:
 - a. **Name:** SecondName
 - b. **Type:** String
 - c. **Expression:** Record("Second Name")
5. Create a new field with the following properties:
 - a. **Name:** Town
 - b. **Type:** String
 - c. **Expression:** Record("Town")
6. Create a new field with the following properties:
 - a. **Name:** Country
 - b. **Type:** String
 - c. **Expression:** Record("Country")



7. Create a new field with the following properties:
 - a. **Name:** Phone
 - b. **Type:** String
 - c. **Expression:** Record("Telephone Number")
8. Create a new field with the following properties:
 - a. **Name:** Mail_From
 - b. **Type:** String
 - c. **Expression:** Server.GetEnv("Mail_From")
9. Create a new field with the following properties:
 - a. **Name:** Mail_To
 - b. **Type:** String
 - c. **Expression:** Server.GetEnv("Mail_To")

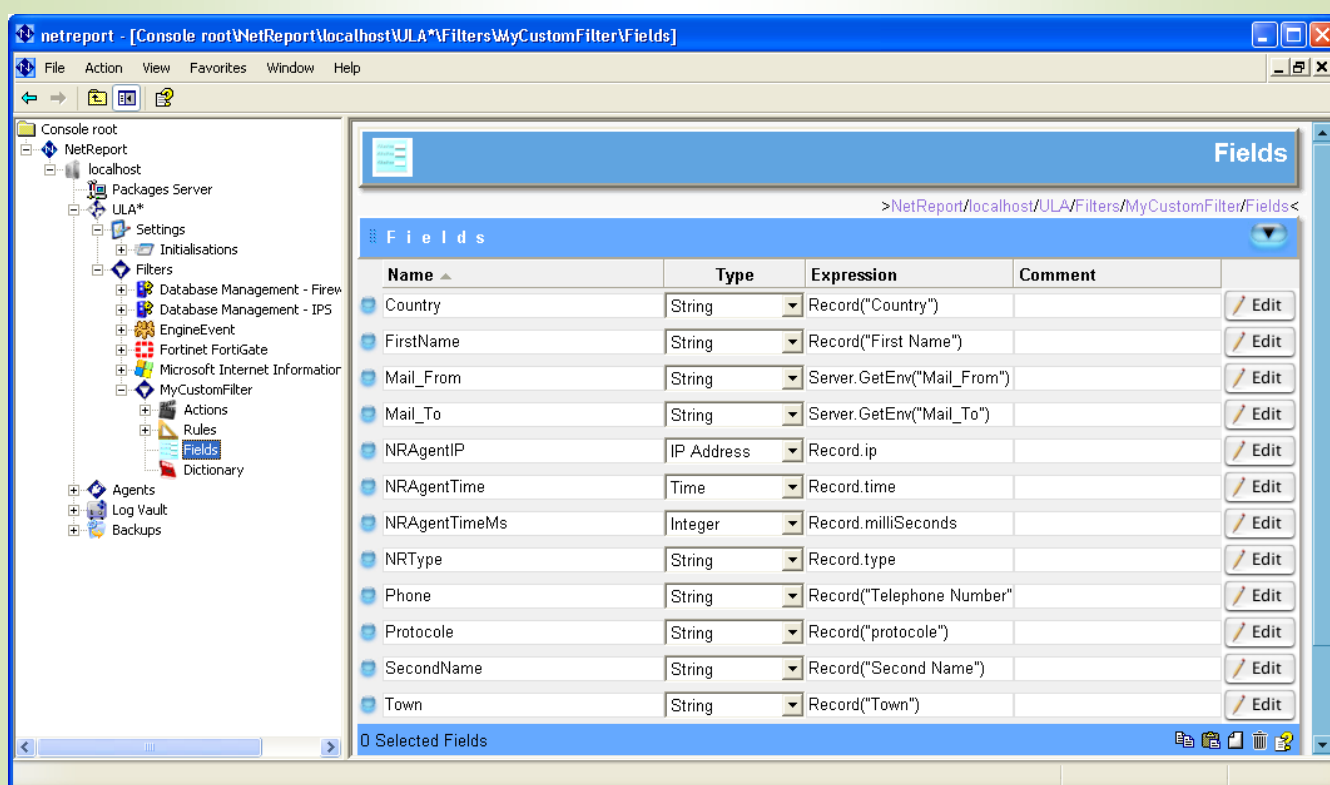


Figure 29 - Creating Fields

4.3.2.4. Exercise 4 - Creating the Send Mail Action

1. Select **Console root > NetReport > localhost > ULA > MyCustomFilter > Actions**.
2. Select the **Send Mail** action from the drop-down list.

3. Click the **New** icon.
4. Click the **Edit** icon to the right of the **Send Mail** row.
5. Enter the **Subject**: New Log Row in Log File
6. Type First Name: in the Message:
7. Select the **FirstName** field from the drop-down list.
8. Click the **New** icon to add the field.
9. Type Second Name: in the Message
10. Select the **SecondName** field from the drop-down list.
11. Click the **New** icon to add the field.
12. Type **Town** in the **Message**
13. Select the **Town** field from the drop-down list.
14. Click the **New** icon to add the field.
15. Type **Country** in the Message.
16. Select the **Country** field from the drop-down list.
17. Click the **New** icon to add the field.
18. Type **Telephone Number**: in the Message
19. Select the **Phone** field from the drop-down list.

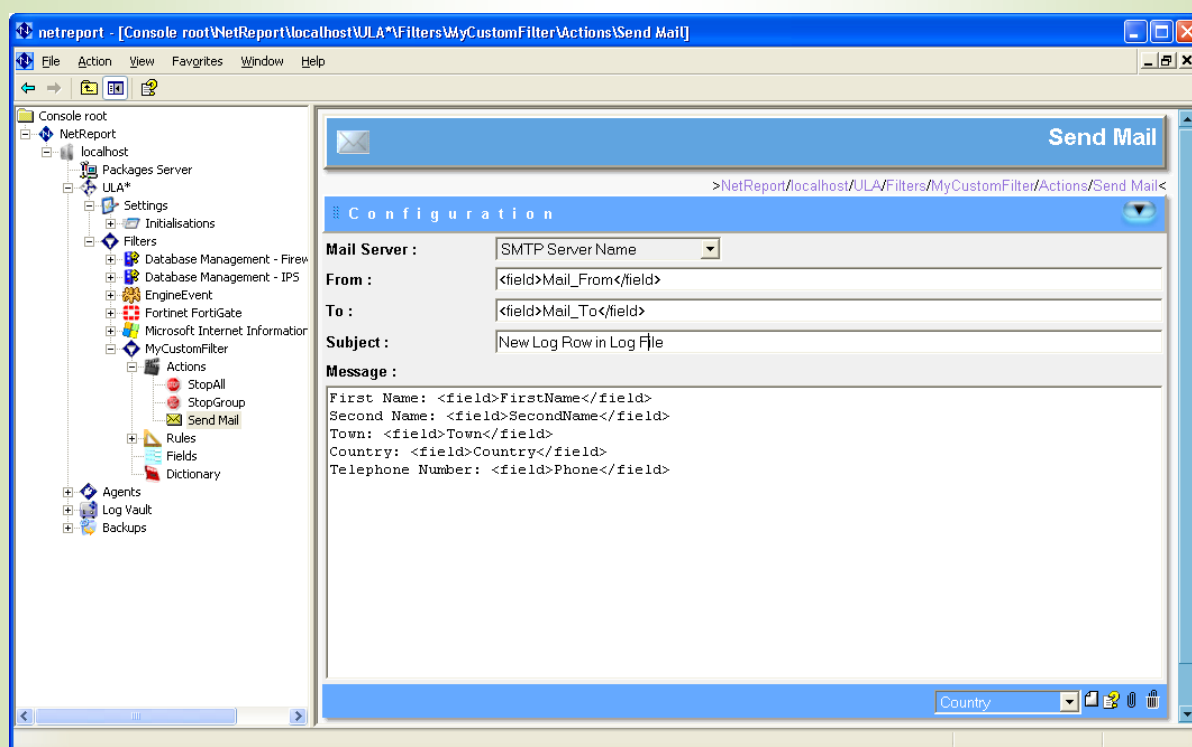


Figure 30 - Creating the Send Mail Action



4.3.2.5. Exercise 5 - Adding a New Rule

1. Select **Console root> NetReport> localhost> ULA> MyCustomFilter > Rules> New rules group**.
2. Click the **New Rule** icon.
3. Double-click the **Action** cell for the new rule to display the drop-down list.
4. Select the **Send Mail** action.

4.3.2.6. Exercise 6 - Defining SMTP Server Name and Mail Address Settings

1. Select **Console root> NetReport> localhost> ULA> Settings > Initialisations> SMTP Server Name**.
2. Check that the **SMTP Server Name** you configured via the Click&DECiDE Configurator is correct and functional for sending e-mails during the Training Course.
Note: ask your Trainer to give you an appropriate SMTP Server for the Training Course.
3. Select **Console root> NetReport> localhost> ULA> Settings > Initialisations> Mail Addresses**.
4. Enter the appropriate **“Mail To”** address, for example your e-mail address. **Note:** please enter an address which you can use to test e-mails from Click&DECiDE during the Training Session.
5. Select **Console root> NetReport> localhost> ULA**.
6. Click Apply Changes.

4.3.2.7. Exercise 7 - Parsing the CustomLog.log File

1. Create a copy of the CustomLog.log file in C:\Logs.
2. Wait for three e-mail messages to arrive in your inbox.
3. Add an additional row to the CustomLog.log file and add a carriage return, save the file.
4. Wait for another e-mail to arrive alerting you to the new line that was added to the CustomLog.log file.





4.4. Working with Regular Expressions

For the following examples we will be using the Generic Parser in the Click&DECiDE Management Console. Through Exercises 1 – 10 we will give examples of how to:

- Write Regular Expressions via the Records Parser.
- Parse Test Values.
- Test the expressions.
- Create Header Records.
- Use the Click&DECiDE Includes Parser.

To get started, create a Generic parser and add regular expressions via the Records Parser, please follow the steps below.

Exercise 1 - Creating a Generic Parser, Using the Records Parser to Create Regular Expressions

Steps

1. Launch the Click&DECiDE Management Console, select **Start> All Programs> NetReport> Management Console**. The **Login** dialog box appears.
2. Enter your **Login** and **Password**. The Click&DECiDE Management Console appears.
3. Select **NetReport> [localhost]> Agents> Flat File Parser> Configuration** in the left **Console Root** pane.



4. Select **Generic Parser** in the drop-down list.

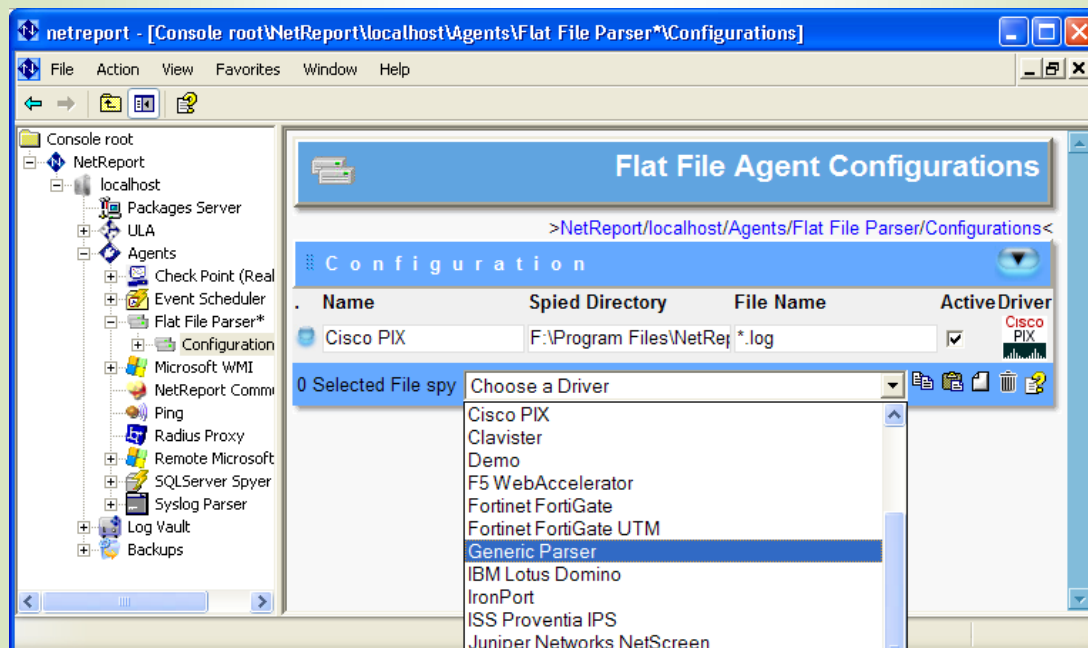


Figure 31 – Select Generic Parser in the drop-down list

5. Click **New** to add the Generic Parser.

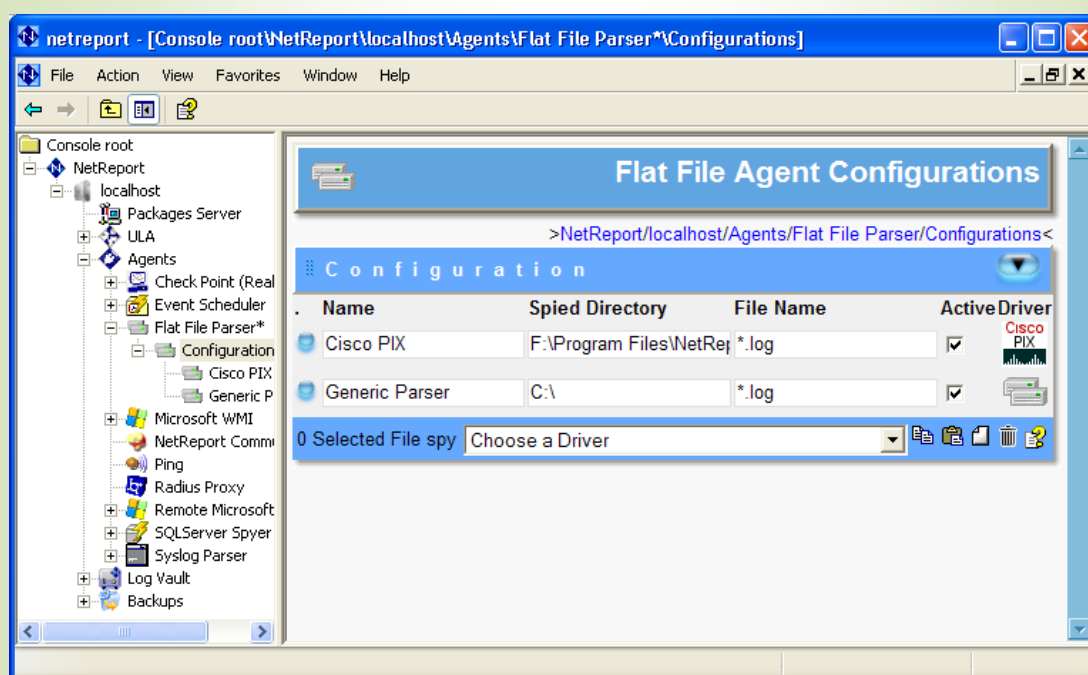


Figure 32 - New Generic Parser Added

6. Click  **Edit this spied configuration** to the right of the Generic Parser row.

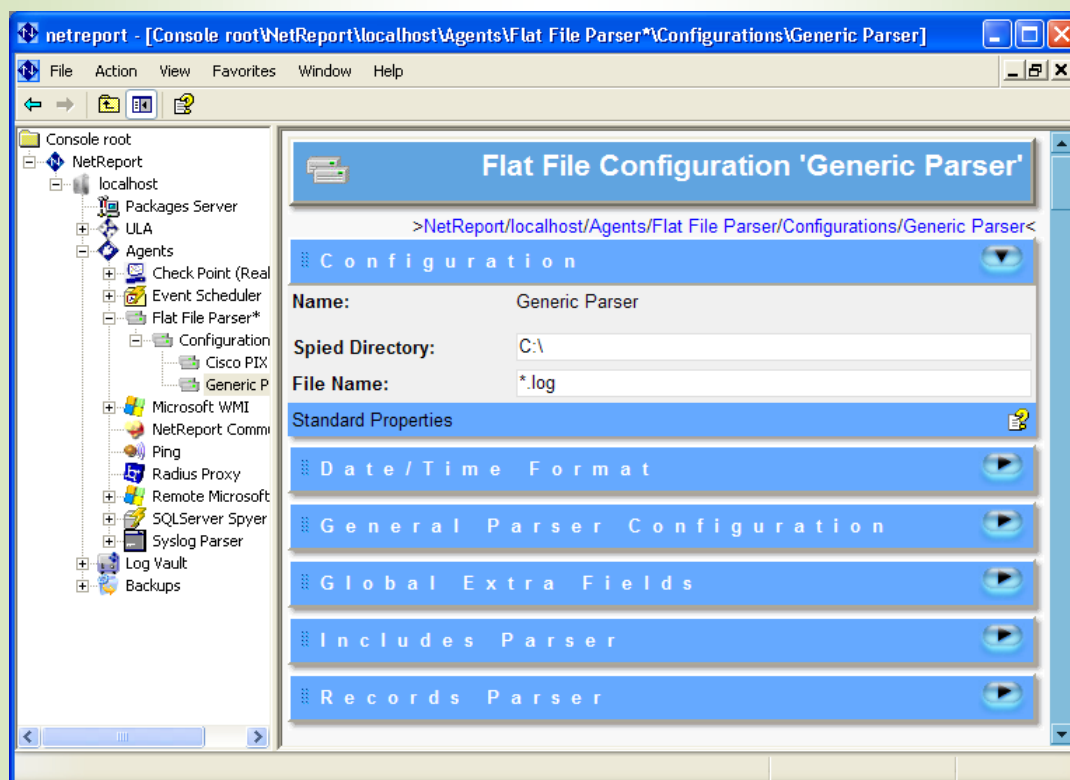


Figure 33 - Flat File Configuration 'Generic Parser'

7. Select the **Records Parser** section.

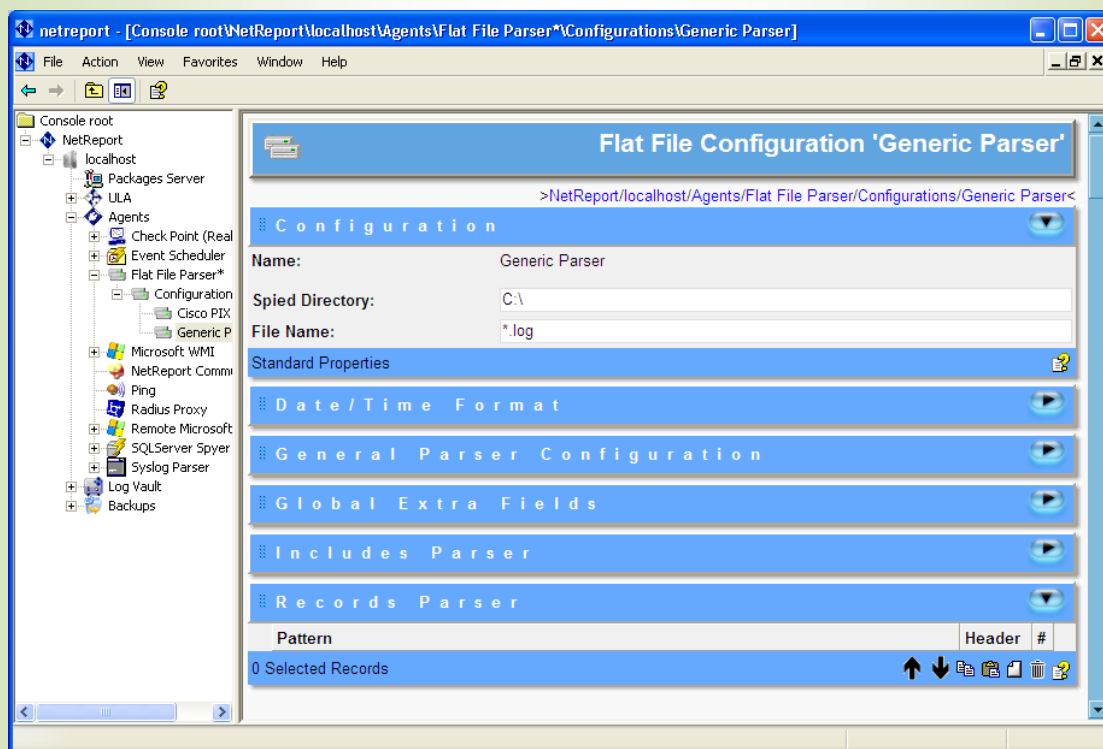


Figure 34 - Records Parser Section

8. Click  **New** to add a new pattern (regular expression).

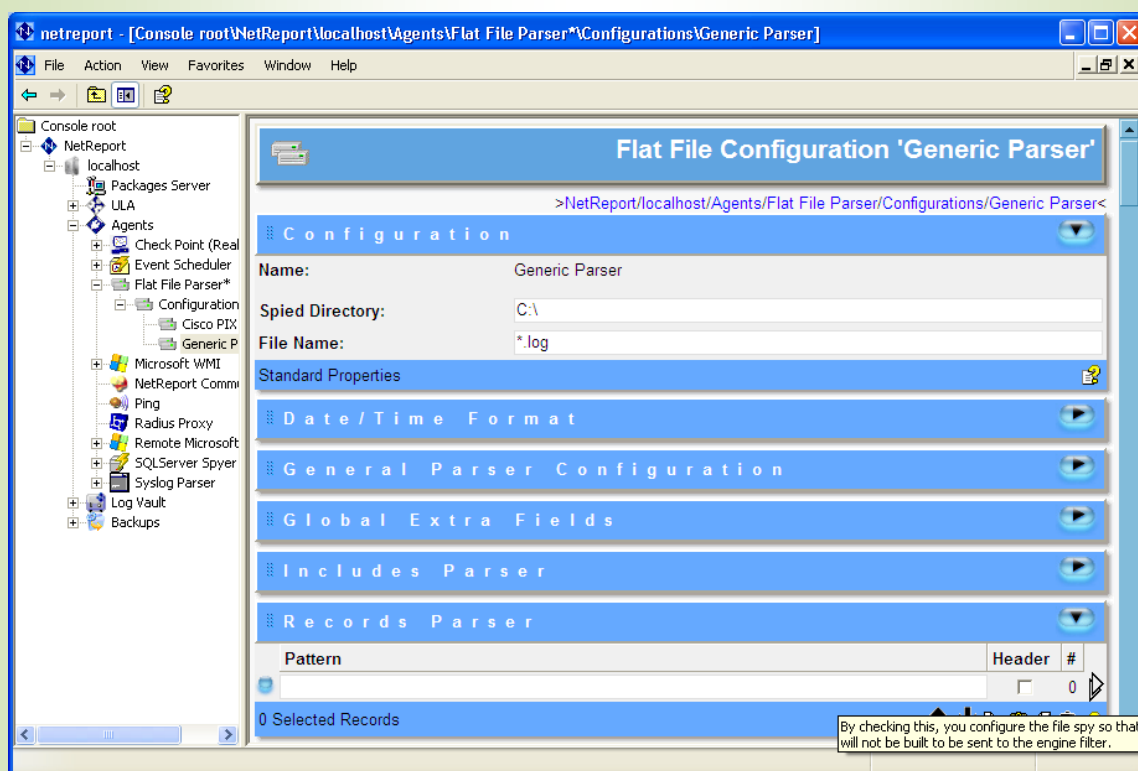



Figure 35 - New Pattern



9. Click  **Edit Pattern** to write the regular expression, add a test value and test the expression.

Exercise 2 - Alternation and Grouping

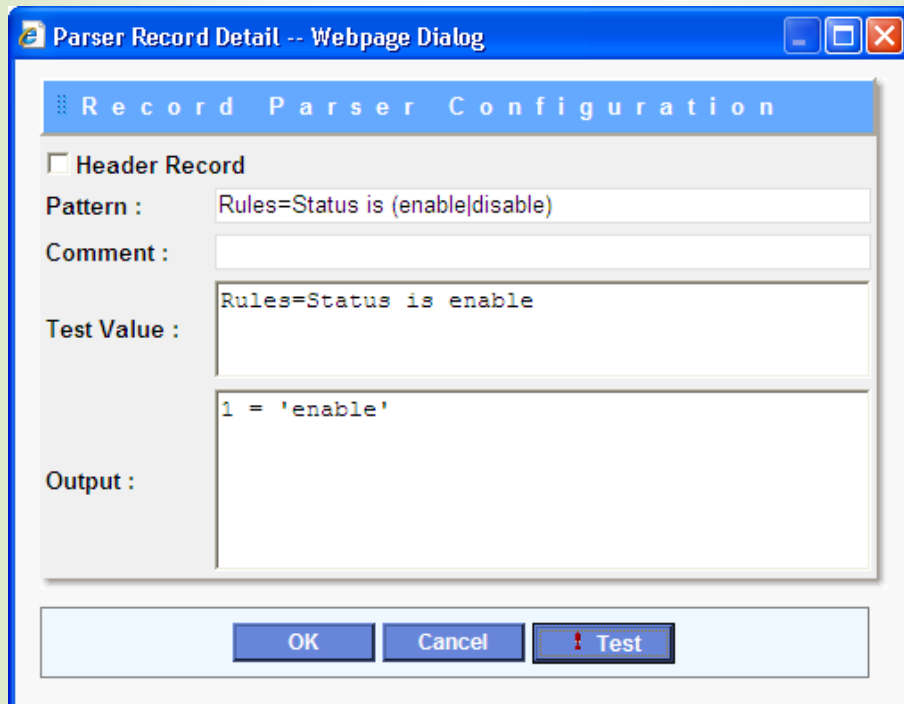
If you do not want to capture a substring but need parentheses to group the substring, use the '?' operator to avoid capturing. For example, to see if a rule's status is Enable or Disable we could use the following regular expression:

Rules=Status is (enable|disable)

Steps

1. Click  **New** to add a new **Pattern** via the **Records Parser**.
2. Click  **Edit Records Parser**.
3. Enter the following pattern in the **Pattern** field:
Rules=Status is (enable|disable)
4. Enter the following **Test Value**:
Rules=Status is enable

5. Click **Test** and note the **Output**.



Parser Record Detail -- Webpage Dialog

Record Parser Configuration

☐ Header Record

Pattern : Rules=Status is (enable|disable)

Comment :

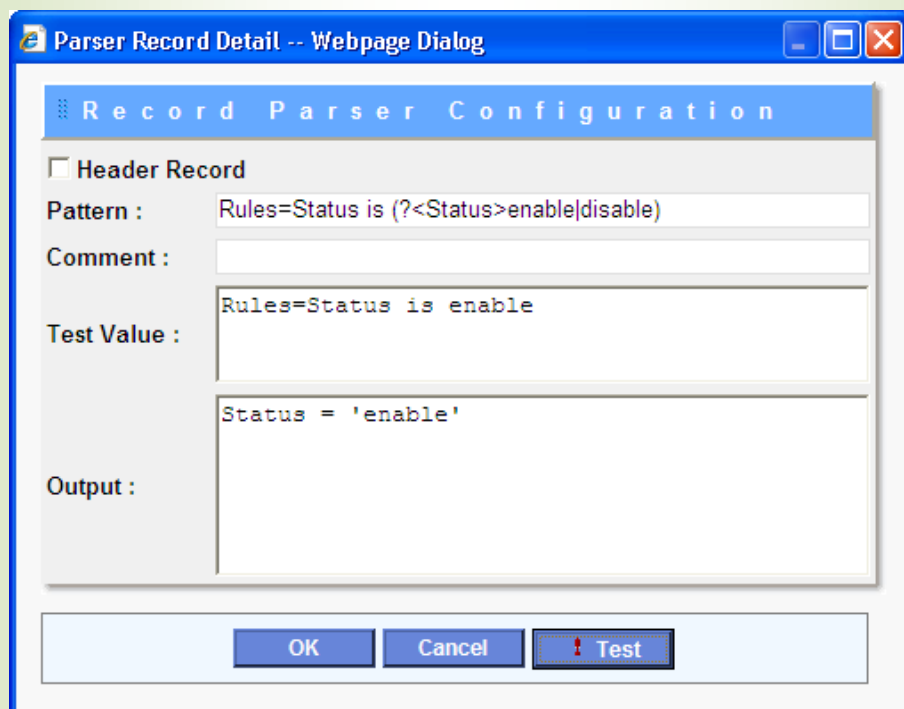
Test Value : Rules=Status is enable

Output : 1 = 'enable'

OK Cancel **Test**

Figure 36 - Parser Output: Alternation and Group and Naming

6. Note the **Output** displays a numbered match: **1='enable'** without a name. To name the capture, modify the pattern as follows.
7. Modify the pattern by adding **?<Status>** before enable|disable: Rules=Status is (?<Status>enable|disable)



Parser Record Detail -- Webpage Dialog

Record Parser Configuration

☐ Header Record

Pattern : Rules=Status is (?<Status>enable|disable)

Comment :

Test Value : Rules=Status is enable

Output : Status = 'enable'

OK Cancel **Test**

Figure 37 - Parser Output: Alternation and Group and Naming





8. Note the effect of (?<Status>) in displaying a named capture. Note that the capture is no longer numbered.

Information

If we analyze the above expression (pattern) we can note the following key points:

Character	Comments
	or 'pipe' means 'or', for example enable disable matches enable or disable.
(enable disable)	Matches either enable or disable. For example (none enable disable) would match none or enable or disable.
(?<Status>)	Names the capture 'Status'.

Exercise 3 - Extracting Fields



A log line will typically list several fields separated by separators or tabs. Below is a very simple line:

George-Smith-49

To parse this line and extract each field we could use the following expression:

(?<name>[^-]+)-([^-]+)-([^-]+)

Steps

1. Click  **New** to add a new **Pattern** via the **Records Parser**.
2. Click  **Edit Records Parser**.
3. Enter the following pattern in the **Pattern** field:
(?<name>[^-]+)-([^-]+)-([^-]+)
4. Enter the following **Test Value**:
George-Smith-49



5. Click **Test** and note the **Output**.

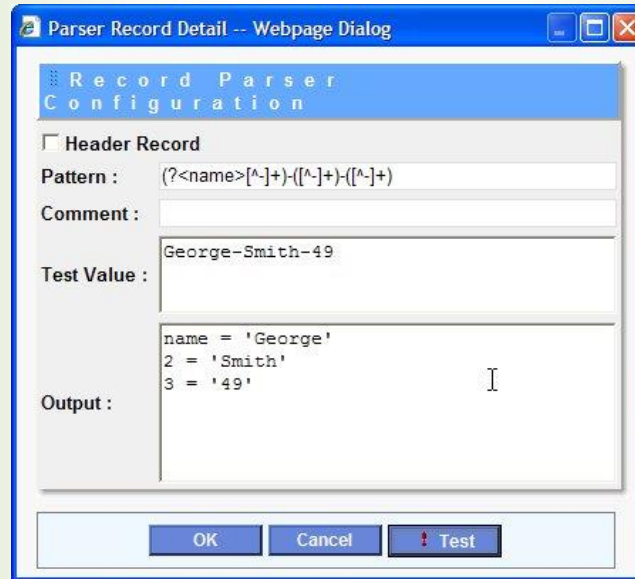


Figure 38 - Parser Output: Naming

Information

If we analyze the above expression we can note the following key points:


Character	Comments
(?<name>[^-]+)	Captures the name, in this case 'George'. Captures all characters except the – (endash) one or more times.
([^-]+)	Captures all characters except the – (endash) one or more times.

Exercise 4 - Matching Attributes and Values

To display all the attributes (for example, Firstname, Surname, Age) in a row, followed by all the values (for example, George, Smith, 49) in the row below, we could use the following expression:

```
(?<att>[^=]+)=(?<val>[^;]+);?
```

Steps

1. Click  **New** to add a new **Pattern** via the **Records Parser**.
2. Click  **Edit Records Parser**.



3. Enter the following pattern in the **Pattern** field:

`(?<att>[^\=]+)=(?<val>[^\;]+);?`

4. Enter the following **Test Value**:

Firstname=George;Surname=Smith;Age=49

5. Click **Test** and note the **Output**.

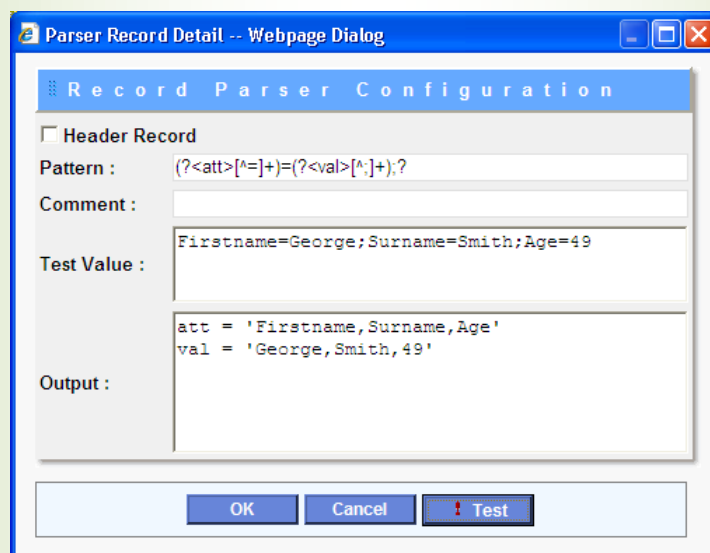


Figure 39 - Parser Output: Attributes and Values

Information

If we breakdown the expression above, we can note the following points:

Character	Comments
<code>(?<att></code>	Captures the attribute name.
<code>[^\=]+</code>	Matches all characters except = (equal to) one or more times.
<code>(?<val></code>	Captures the value.
<code>[^\;]+</code>	Matches all characters except ; (semi-colon) one or more times.
<code>;?</code>	Matches 0 or once what preceded, in this case the ; semi-colon.



Exercise 5 - Displaying Each Attribute with its Value

To display the attributes in a row (for example, Firstname, Surname, Age), followed by each attribute separately with its specific value (for example, Surname = Smith), we could use the following expression:

```
(?<att>[^=]+)=(?<&att>[^;]+);?
```

Steps

1. Edit the previous Pattern, replace `<val>` by `<&att>`:
`(?<att>[^=]+)=(?<&att>[^;]+);?`
2. Keep the previous **Test Value**:
`Firstname=George;Surname=Smith;Age=49`
3. Click **Test** and note the **Output**.

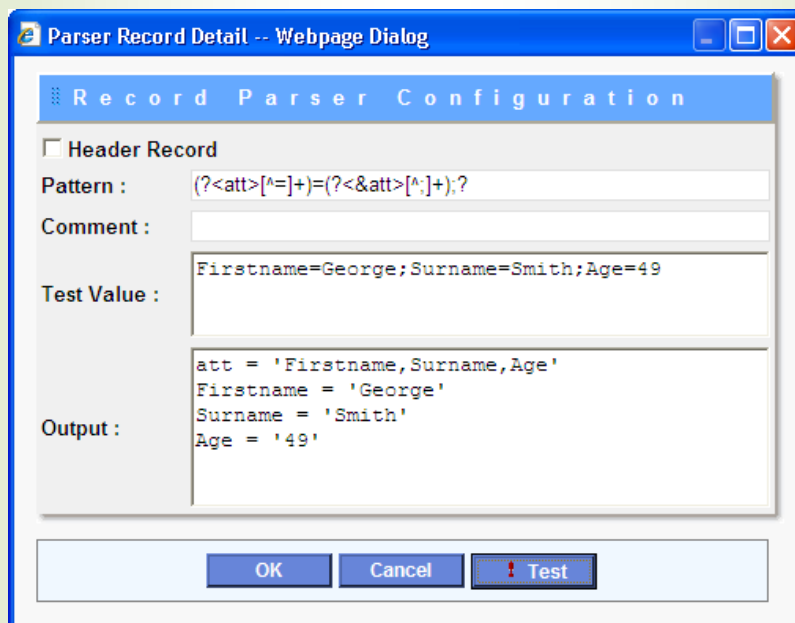


Figure 40 - Parser Output: Attributes and their Corresponding Values

Information

If we breakdown the expression above, we can note the following points:

Character	Comments
(?<att>	Captures the attribute name.
[^=]+	Matches all characters except the = (equal to) one or more times.







(?<&att>	Analyses the Attribute's value with reference to the Attribute Name captured.
[^;]+	Matches all characters except the ; (semi-colon) one or more times.
;?	Matches 0 or once what preceded, in this case the ; semi-colon.

Exercise 6 - Defining a Header Record

It is possible to create a Header Record, that is, a pattern which is used to parse the header in a log file. In this example, we are going to use the following pattern:

```
#field (?:(?<$att>[^;]+);?)+
```

Steps

1. Click  **New** to add a new **Pattern** via the **Records Parser**.
2. Click  **Edit Records Parser**.
3. Select the **Header Record** check box.
4. Enter the following pattern in the **Pattern** field:

```
#field (?:(?<$att>[^;]+);?)+
```
5. Enter the following **Test Value**:

```
#field Firstname;Surname;Age
```
6. Click **Test** and note the **Output**.

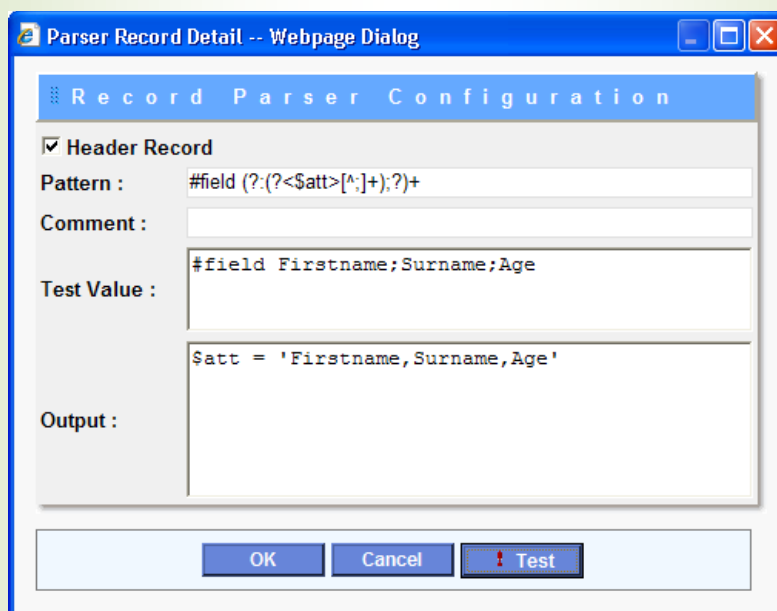


Figure 41 - Parser Output: Header Record



Information

If we breakdown the expression above, we can note the following points:

Character	Comments
#field	Matches #field
?:	Regroups what follows between parenthesis.
\$att	Stores the attribute name for it to be used as reference later (please see Exercise 7).
[^;]+	Matches all characters except the ; (semi-colon) one or more times.

Status: if we return to the **Flat File Configuration 'Generic Parser'** screen we can note the following patterns have been added and that **Pattern** number 3 (#3) is selected as a **Header Record**.

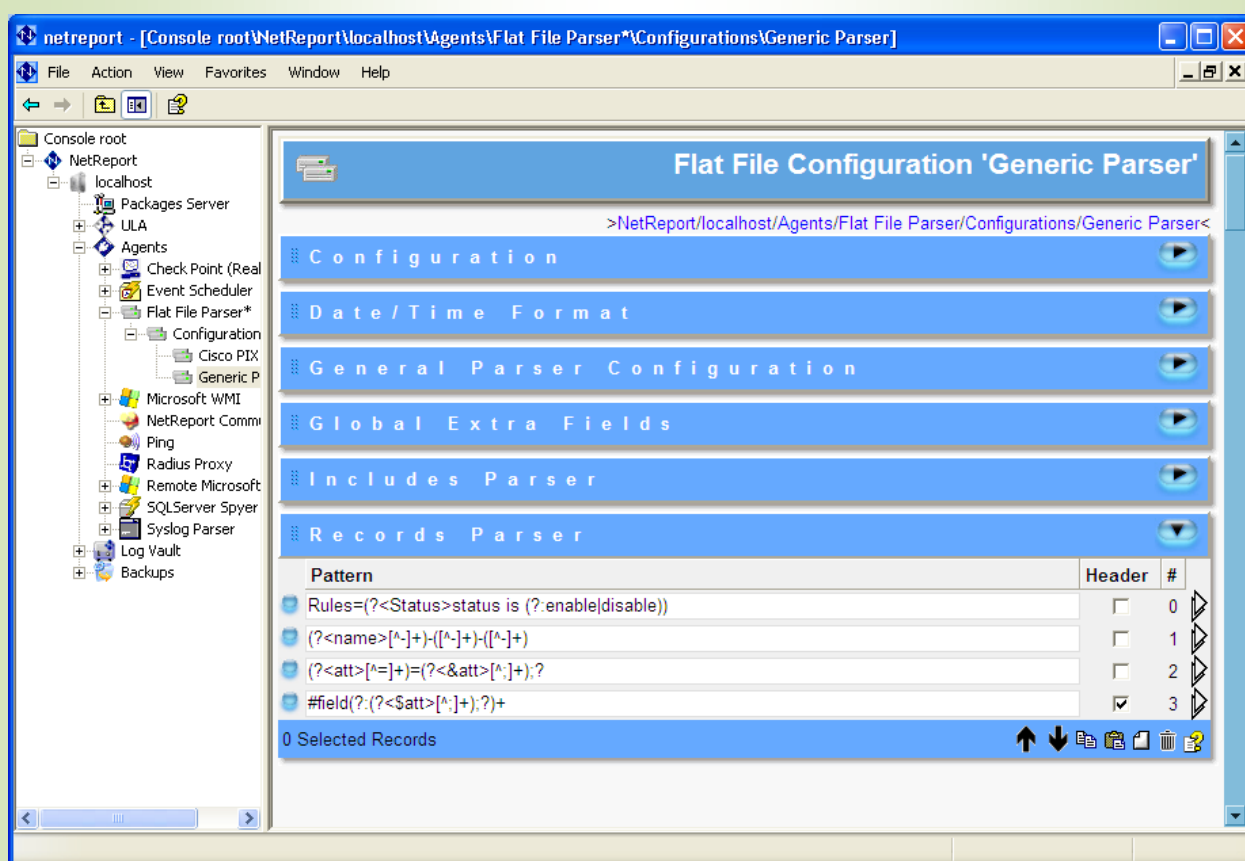




Figure 42 - Flat File Configuration 'Generic Parser': Records Parser

Exercise 7 - Parsing with reference to a Header Record

We are now going to parse a new record with reference to the Header Record we created in Example 6, using the following pattern.

```
(?<&$att>[^;]+);?
```

Steps

1. Click  **New** add a new **Pattern** via the **Records Parser**.
2. Click  **Edit Records Parser**.
3. Enter the following pattern in the **Pattern** field:

```
(?<&$att>[^;]+);?
```
4. Enter the following **Test Value**:
George;Smith;49
5. Click **Test** and note the **Output**.

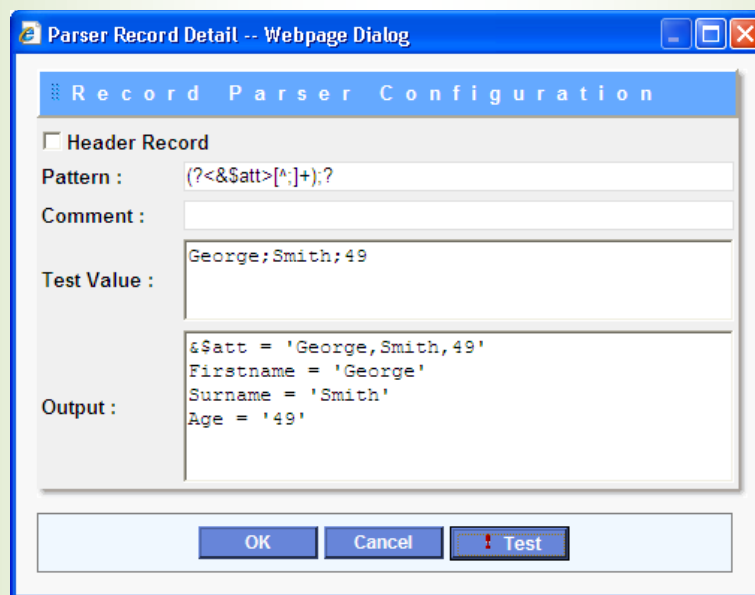


Figure 43 - Parser Output: Reference of a header



Information

If we breakdown the expression above, we can note the following points:

Character	Comments
<&\$att>	Refers to the \$att which we defined in the Header Record in Example 6.
[^;]+	Matches all characters except the ; (semi-colon) one or more times.
;?	Matches 0 or once what preceded, in this case the ; semi-colon.

Exercise 8 - Creating Includes Parser Patterns

To make regular expressions as readable and user friendly as possible, Click&DECiDE enables you to create predefinitions. For each one of them, a name and a pattern must be defined. For this example we are going to use the following test pattern:

Src=192.168.0.1;dst=15.12.12.01;user=George;Service=80

We therefore need to create Includes Parser patterns for numbers, letters and IP Addresses. For this example we are going to create the following patterns:

Name	Pattern
num	[0-9]+
alpha	\w+
ip	[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}

To add these patterns via the Includes Parser, please follow the steps below:



Steps

1. Select the **Includes Parser** section.

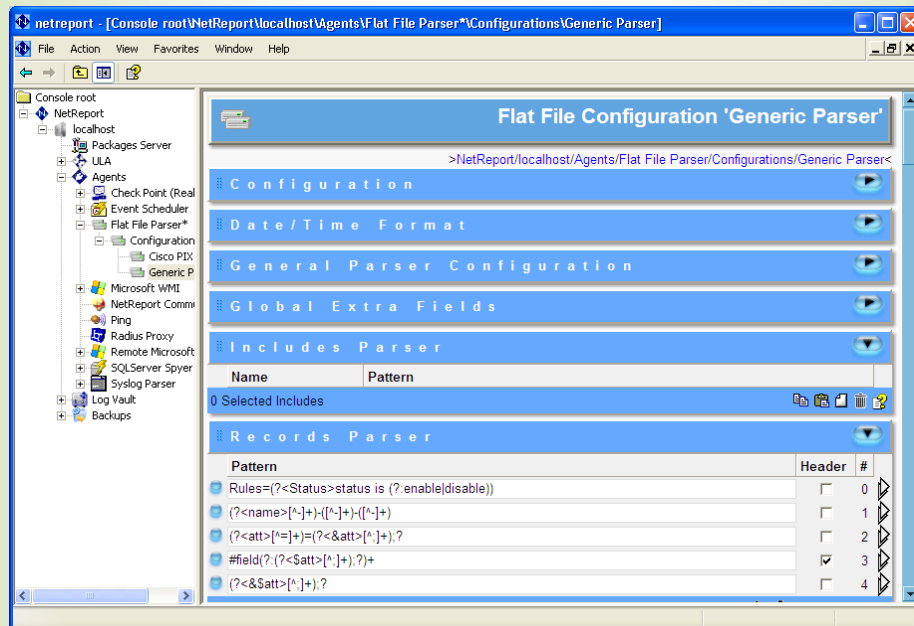


Figure 44 - Flat File Configuration 'Generic Parser': Includes Parser

2. Click **New** to add a new pattern (regular expression). **Note:** for each Include you must define the following:
 - a. **Name:** the name of the Include.
 - b. **Pattern:** the Include's pattern.

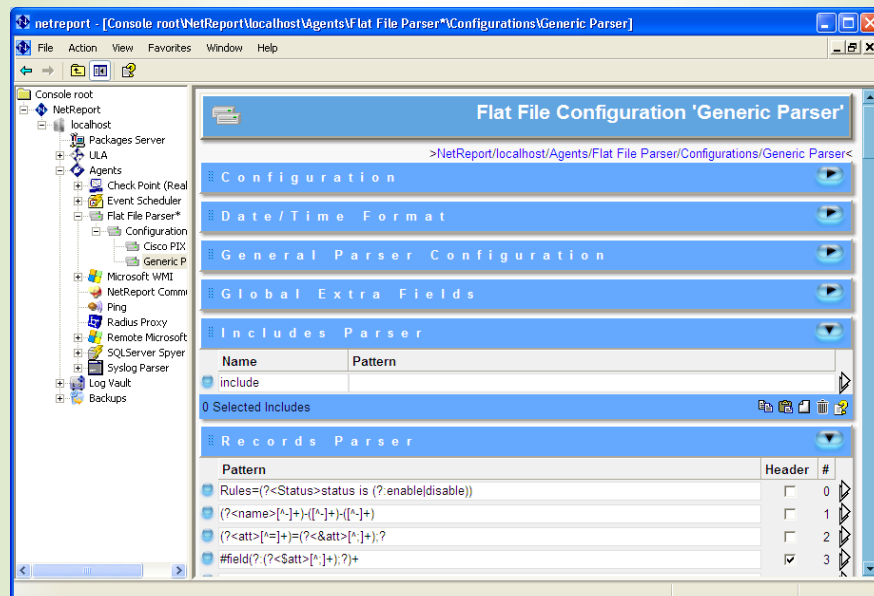


Figure 45 - Flat File Configuration 'Generic Parser': New Include Parser



3. Replace the 'include' **Name** by num and enter the **Pattern**: [0-9]+:

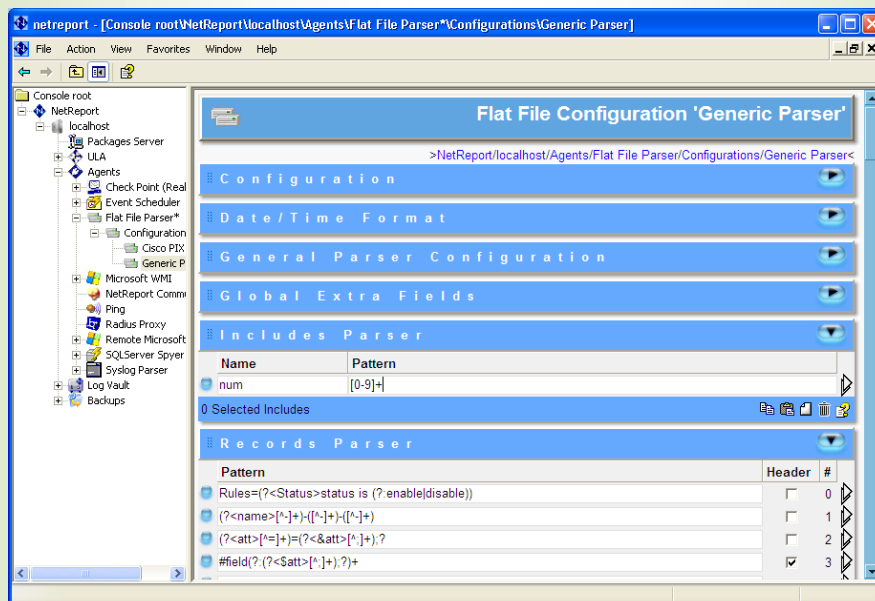


Figure 46 - Flat File Configuration 'Generic Parser': Include Parser Edited

4. Create the following two Includes predefinitions

Name	Pattern
alpha	\w+
ip	[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}

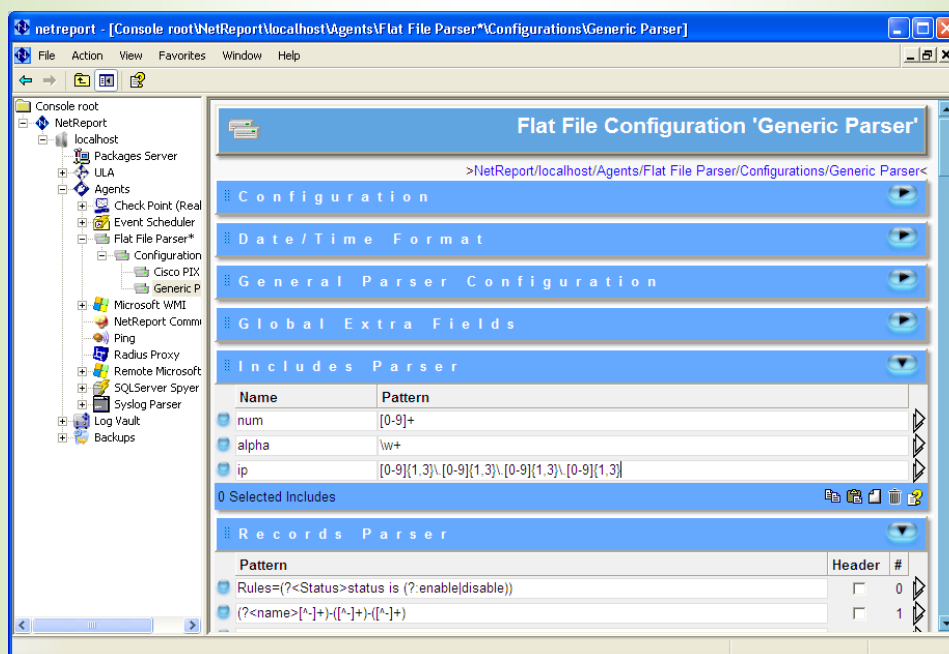



Figure 47 - Flat File Configuration 'Generic Parser': Includes Parser



5. Click  **Show Include Detail** to the right of ip to edit the ip Include predefinition. The **Include Parser Configuration** dialog box appears.

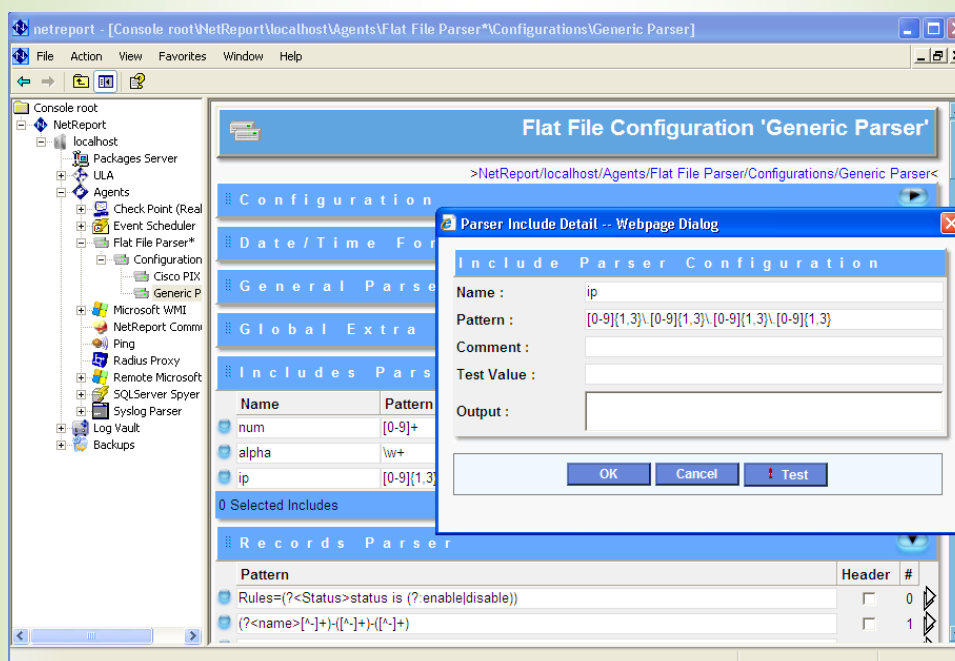


Figure 48 - Include Parser Configuration

6. Enter an IP Address as a **Test Value**, for example: 192.168.0.1:

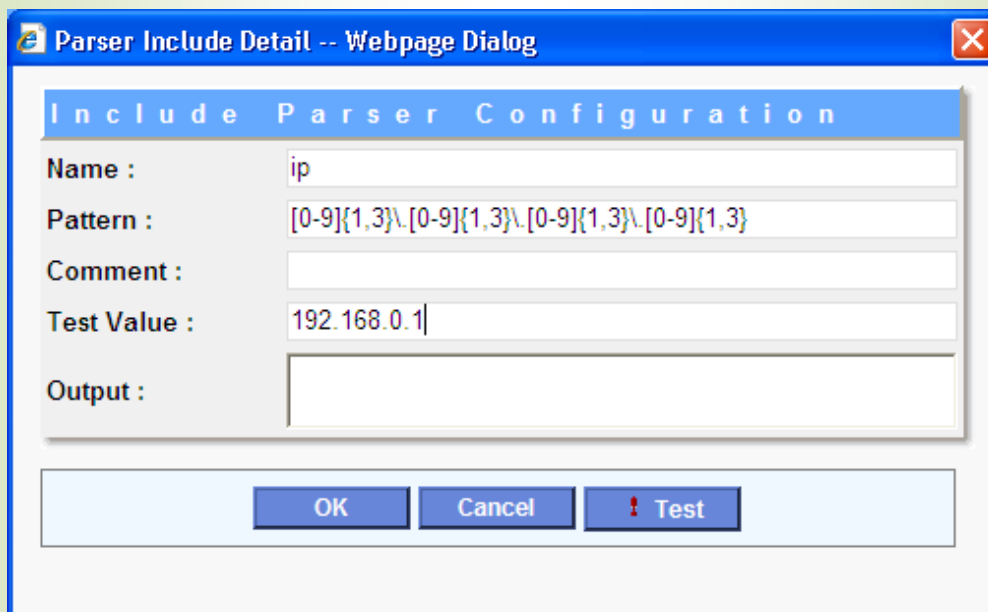


Figure 49 - Include Parser Test Value



7. Click **Test** and note the **Output**.

Parser Include Detail -- Webpage Dialog

Include Parser Configuration

Name : ip

Pattern : [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}

Comment :

Test Value : 192.168.0.1

Output : true

OK Cancel Test

Figure 50 - Include Parser Test Result

Exercise 9 - Parsing a Record with the Includes Parser

To parse a record using the Includes Parser definitions we defined in Example 8, please follow the steps below.

Steps

1. Select Records Parser Patterns # 2 and #4.
2. Click **Delete** to delete these patterns.
3. Click **New** to add a new **Pattern** via the **Records Parser**.
4. Click Show Includes Detail.
5. Enter the following pattern in the **Pattern** field:
src=(?<ip:Source>);dst=(?<ip:Destination>);user=(?<alpha:User>);service=(?<num:Service>)
6. Enter the following **Test Value**:
Src=192.168.0.1;dst=15.12.12.01;user=George;Service=80



7. Click **Test** and note the **Output**.

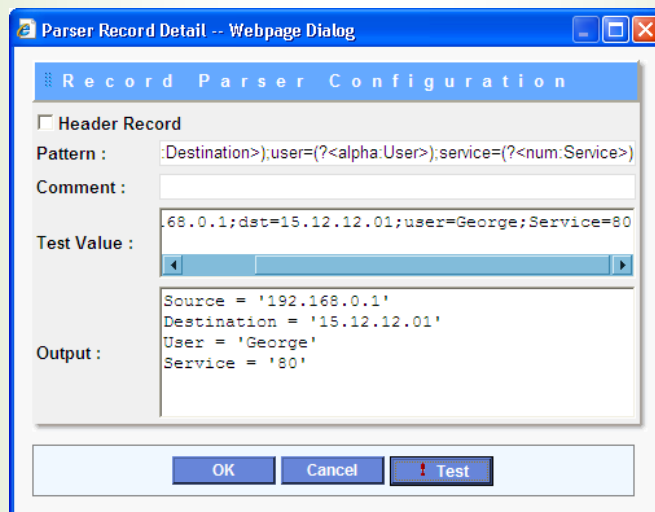


Figure 51 - Parser Output: Referring Includes Record

Information

If we breakdown the expression above, we can note the following points:

Character	Comments
(?<ip:Source>)	Captures the value for the Includes Parser 'ip' which we defined in Example 8.
(?<ip:Destination>)	Captures the value for the Includes Parser 'ip'.
(?<alpha:User>)	Captures the value for the Includes Parser 'alpha'.
(?<num:Service>)	Captures the value for the Includes Parser 'num'.



Exercise 10 - Includes Parser Named Captures

To parse a record using an Includes Parser named capture, please follow the steps below.

Steps

1. Create the following Includes predefinitions:

Name	Pattern
src	(?<ip:Source>)

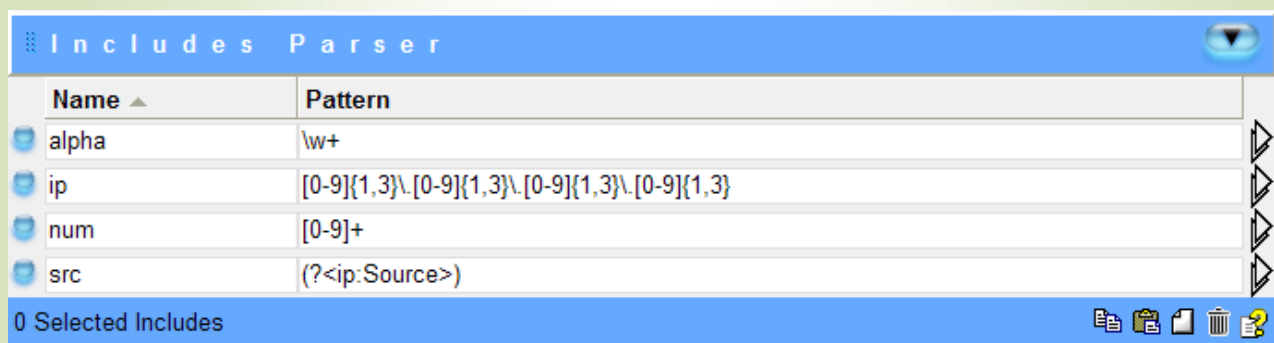



Figure 52 - Includes Parser Named Captures

2. Click  **Show Includes Detail** to the right of the **Records Parser** pattern we created in Example 8:
 src=(?<ip:Source>);dst=(?<ip:Destination>);user=(?<alpha:User>);service=(?<num:Service>)
3. Modify the beginning of the above pattern to refer to the src Includes predefinition we just defined as follows:

Replace

src=(?*ip:Source*>);dst=(?<ip:Destination>);user=(?<alpha:User>);service=(?<num:Service>)

by

src=(?*:src*>);
 dst=(?<ip:Destination>);user=(?<alpha:User>);service=(?<num:Service>)



4. Click **Test** and note the **Output**.

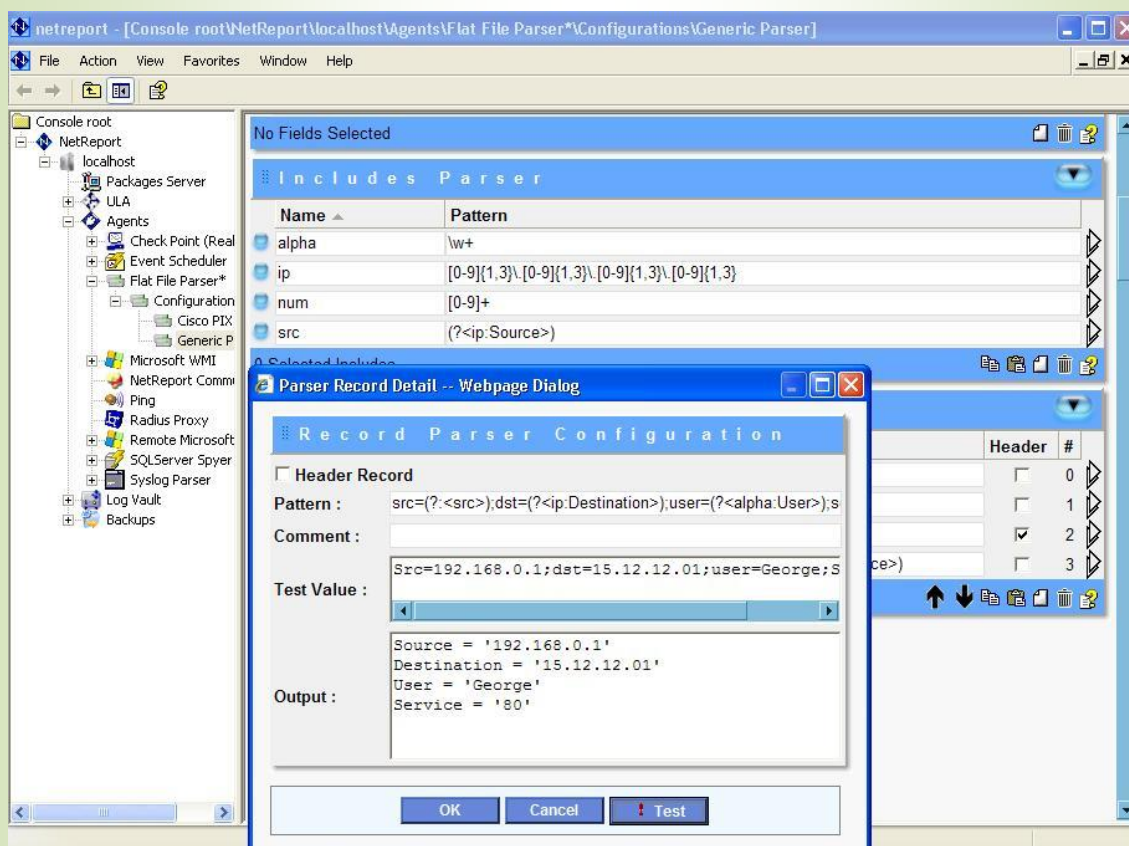


Figure 53 - Parser Output: Includes Parser Named Capture

Information

If we breakdown the expression above, we can note the following points:

Character	Comments
(?:<src>)	Captures the value for the Includes Parser 'src' which we defined in Example 9.





4.5. Exporting Filters and Parsers

Export any Click&DECiDE Filter and Parser(s) in a matter of clicks. Installing, integrating or managing technical support for Filters and Parsers is now even easier. Click&DECiDE's Filter and Parser Export Feature enables you to export and save filters and all the associated parsers. Filters and parsers can easily be exported – enabling easy update and support management.

4.5.1. Suggestions for Practice

When you export a Filter you export all the associated Flat File and Syslog parsers. Please follow the steps below to export a Filter and its Parsers from the Click&DECiDE Management Console.

1. Select **Start>All Programs>Click&DECiDE> Management Console** in the **Start** menu. The **Click&DECiDE Login** dialog box appears.
2. Enter your **Login** and **Password** and click **OK**. The **Click&DECiDE Management Console** loading screen appears followed by the Click&DECiDE Management Console.
3. Select **Console root> NetReport> localhost> ULA> Filters** in the left **Console root** pane.
4. Right-click on the Filter you want to export. In this example the **Cisco PIX filter**. The context menu appears.
5. Select **Export Filter and Parsers...** The **Save As** dialogue box appears.
6. Select the export destination folder and enter the File name you want for the Filter you export and click **Save**. In this example, my_cisco_pix_filter.
Note: the File format by default is *.xml. Please ensure you export Filters in *.xml format.
7. Note the **Warning** message. Click **Yes** to overwrite or **No** to enter another File Name if the file already exists.
8. Note the **Status** message. Click **OK**.

Status: your filter and parsers have been successfully exported.





4.6. Importing Filters and Parsers

Import any Click&DECiDE Filter and Parser(s) in a matter of clicks. Installing, integrating or managing technical support for Filter and Parsers is now even easier. Click&DECiDE's Filter and Parser Import Feature enables you to save filters and all the associated parsers. Filters and parsers can easily be imported – enabling easy update and support management.

4.6.1. Suggestions for Practice

When you import a filter, you import the filter along with each of the associated parsers. To import a Filter and/or its Parsers, please follow the steps below:

1. Select **Start>All Programs>Click&DECiDE> Management Console** in the **Start** menu. The **Click&DECiDE Login** dialog box appears.
2. Enter your **Login** and **Password** and click **OK**. The **Click&DECiDE Management Console loading** screen appears followed by the Click&DECiDE Management Console.
3. Select **Console root> NetReport> localhost> ULA> Filters** in the left **Console root** pane.
4. Right-click the **Filters** branch to reveal the context menu.
5. Select **Import Filter and/or Parsers...** The Open dialog box appears.
6. Select the filter you want to import. In this example, my_cisco_pix_filter.xml.
7. Click **Open**. The **Import Filter and/or Parsers** dialog box appears.
8. Click **Yes** at the base of the **Do you want to import the “Cisco PIX” filter** message.

Note: if you click **Yes** your current configuration for this filter will be overwritten.

9. Click **Yes** at the base of the **Do you want to import the “Cisco PIX” flat file parser** message.

Note: if you click **Yes** your current configuration for this flat file parser will be overwritten.

10. Click **Yes** at the base of the **Do you want to import the “Cisco PIX” syslog parser** message.

Note: if you click **Yes** your current configuration for this syslog parser will be overwritten.



WMI Warning: if you have imported a Microsoft WMI Filter then you will be asked if you want to import the active WMI consumers for both the Microsoft WMI Agent and the Remote Microsoft WMI agent.

11. Click **Yes** if you want to import the active Remote WMI consumer(s)
12. Note the status message and click **OK**.
13. Note the addition of the new Filter and Parsers in the left console root pane.
14. Apply changes at each branch marked by an asterisk. In this example, please click the **Apply Changes** button at the following branches:
 - a. Console root> **Click&DECiDE**> local host> ULA
 - b. Console root> **Click&DECiDE**> local host> Agents> Flat File Parser
 - c. Console root> **Click&DECiDE**> local host> Agents> Syslog Parser

Status: The Filter and its associated parsers have been successfully imported.



5. Working with Click&DECiDE Log Archive

5.1. Architecture

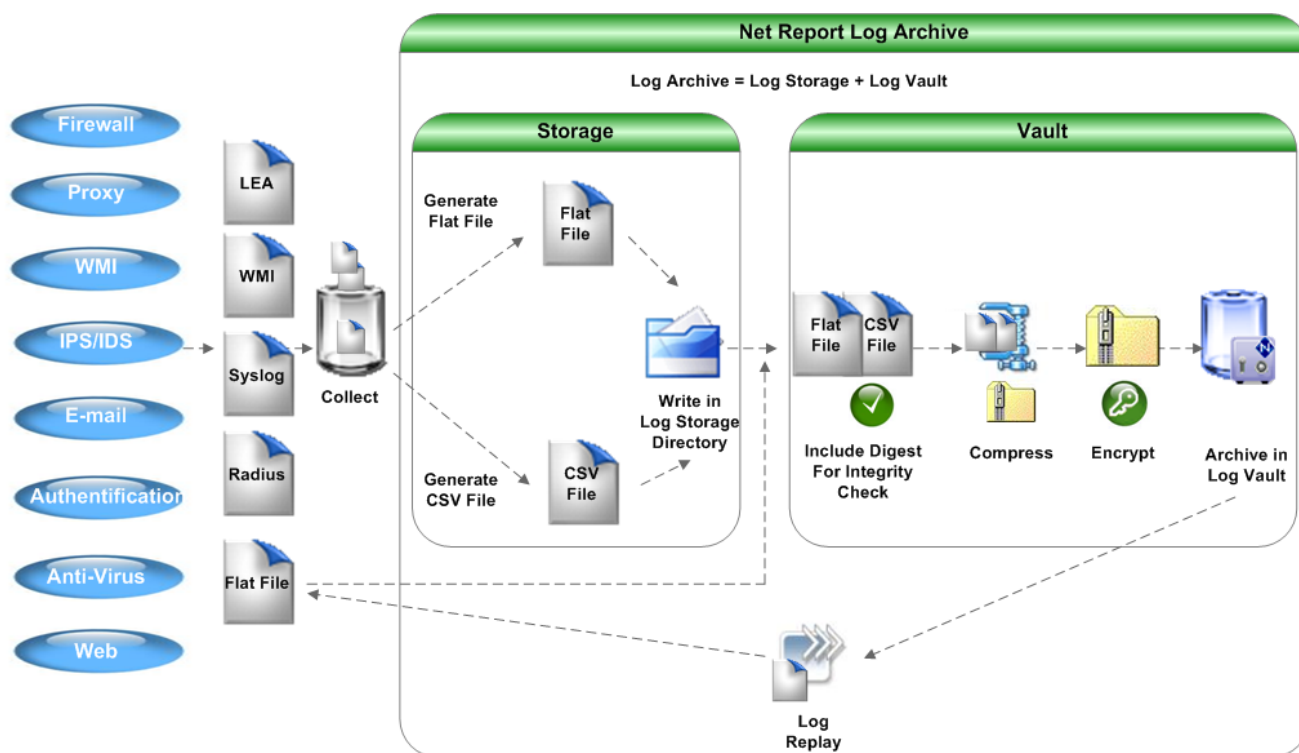


Figure 54 - Log Archive Architecture

Increasingly stringent compliance requirements have prompted best practices groups to recommend more reliable log data archival strategies. Retaining secure log archives is critical to proving regulatory compliance and can be used as legal evidence in court proceedings. A complete record of access, activity, and configuration changes for network devices provides an audit trail for security policy validation.

Automated data retention

By automating the entire log data archival process, Click&DECiDE Log Archive minimizes administration costs while providing more secure log data capture and retention. Click&DECiDE Log Archive is easy to use, requiring minimum installation.



Key Points

- Recuperate all your log files: in the following formats: Syslog, Flat File, API (LEA, WMI, Radius). Offers Two Complementary Storage Modes:
- Raw Data Storage (Sarbanes-Oxley, Basel II etc...)
- Enriched CSV Format Data Storage (in original context; RDNS, Groups etc...).
- Log Replay: Replay your logs in their original context for forensic enquiries.
- Sign, Compress and Encrypt your Files: Day-to-day file treatment (files are named by device or by date).
- Archives: Stores unaltered log data for long-term storage. Legislation such as Sarbanes-Oxley, Basel II recommend retaining and protecting log data for up to seven to ten years.
- Enterprise Scalability: connects to external storage networks for infinite Scalability.

Key Benefits

- Automation: automates the entire log data archival process.
- Minimizes administration costs.
- Provides more secure log data capture and retention.
- Assists with network problem remediation. IT managers can mine log data for root-cause analysis to aid in system recovery and damage cleanup after a security or performance incident.
- Increases network performance.
- Improves availability.
- Aids in decision support.

Note: Click&DECiDE Log Archive (Log Vault and Log Storage) are part of the Click&DECiDE Monitoring Center product. To use Click&DECiDE Log Vault please ensure that you have a license certificate for Click&DECiDE Monitoring Center.



5.2. Introducing Click&DECiDE Log Storage

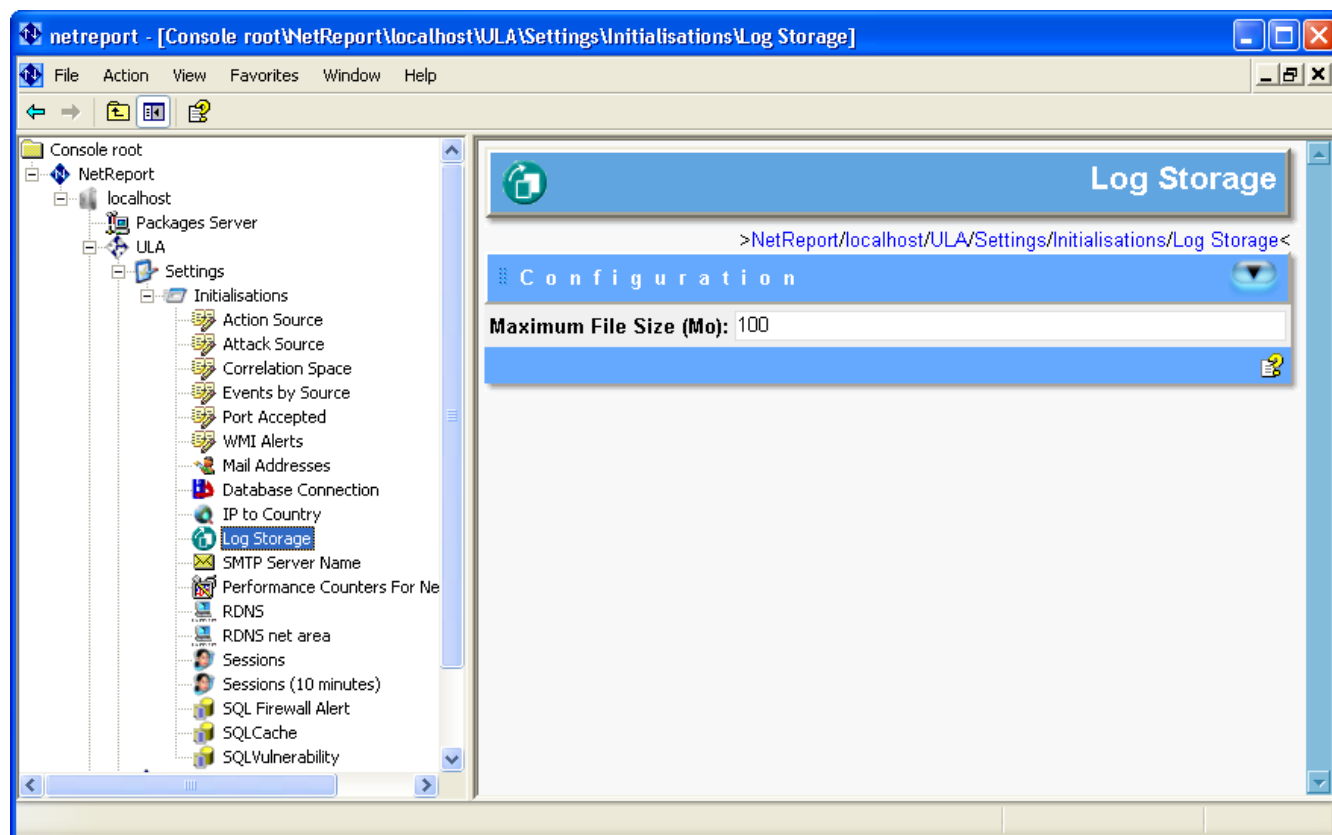


Figure 55 - Click&DECiDE Log Storage

Click&DECiDE Log Storage is one of the key components of Click&DECiDE Log Archive. Click&DECiDE Log Storage enables you to store your logs (from several devices in several formats: Syslog, WMI, Check Point LEA...) in log files (in Flat Files) for archival. Click&DECiDE Log Storage thus stores your raw data either in its:

- Original Format: for raw data storage (for International Regulations such as Sarbanes-Oxley, Basel II, LSF etc...).
- Enriched CSV Format.





5.2.1. Suggestions for Practice

5.2.1.1. Exercise 1 - Working with the Log Storage Initialization

To configure the maximum file size of a log file that you want to store, simply set the size required in the Configuration drop-down section in the Log Storage Initialisations screen. To do so, please follow the steps below:

1. Select **Console root> NetReport> Localhost> ULA> Settings> Initialisations> Log Storage** in the left **Console root** pane.
2. Enter the maximum file size for your logs in the **Maximum File Size (MB)**. Thus when your log file reaches this size, the file will be closed and a new log file will be used (with the addition of the following suffix: **_002**. The index will be incremented for the files that follow when the maximum file size is reached again). Please note that by default the Maximum File Size (MB) field value is 100MB.
3. Select **Console root> NetReport> Localhost> ULA** in the left **Console root** pane.
4. Click the **Apply Changes** button to apply the modifications made.

5.2.2. Exercise 2 - Adding a Store in File Action

To add a Store in File action, please follow the steps below:

1. Select **Console root> NetReport> Localhost> ULA> Filters> MyCustomFilter> Actions** in the left **Console root** pane. The **Actions** screen appears.
2. Select **Store in File** in the drop-down menu at the base of the **Actions** screen.
3. Click the **New** icon in the toolbar at the base of the **Actions** screen.
4. The **Store in File** row appears at the base of the **Actions** table.
5. Modify the **Name** and **Comment** columns for the new **Store in File** action in order to customize it for your needs.

5.2.3. Exercise 3 - Configuring the Store in File Action

To configure the **Store in File** action, please follow the steps below:

1. Select **Console root> NetReport> Localhost> ULA> Filters> MyCustomFilter> Actions> Store in File** in the left Console root pane. The **Store in File** screen appears.
2. Configure the following fields accordingly:





Log Storage Initialization: the name of the Click&DECiDE Initialization enabling Click&DECiDE to recuperate the COM object which writes in the file.

Destination Directory: the directory where the file will be stored. You can add environment variables to customize the Destination Directory. By default the Destination Directory is on the same disk as Click&DECiDE was installed on. Click&DECiDE recommend that the Destination Directory is on a separate disk from that which Click&DECiDE is installed on.

File Name: the name of the file which is made up of specific fields.

Log Record: the data to stock in the file which can be expressed by Click&DECiDE fields. The drop-down list to the right of the Log Record field can be used to insert a field in the Log Record field. Simply select the field you want to add and click the New icon. By default the Log Record field contains the NRRecord field, which contains the log in a refined nelfr form.

Record Separator: the record separator which should be written following the record in the file. By default, it is fixed as `\r\n` (carriage return for Windows), however it can be empty.

Write in File in XML Format: when this option is active, the action writes the record (in general a refined form of nelfr) in an XML file, in order to manage the document's start and end tags (`<document>...</document>`). Otherwise, the record is written in the file as is.

Note: when the file in question has reached the size you defined in the corresponding Initialization, or if it changes format (to XML), the next file is used by adding the suffix `_iii` which starts at `_002` and is incremented for each new file.





5.3. Working with Click&DECiDE Log Storage Enriched CSV Format

Terminology

CSV: Comma-separated Values format. Data is stored in text form, with data items separated by commas. CSV is also referred to as Comma Delimited. This is a popular format for transferring data from one application to another, because most database systems are able to import and export comma-delimited data. Each column value is separated by a comma from the next column's value and each row starts a new line. CSV format files are generally used for exchanging data with spreadsheets and relational databases.

Introducing the Click&DECiDE Store in CSV Format File Actions

If you selected to store your logs in CSV Format files in the Click&DECiDE Configuration Wizard then a Store [TableName] in CSV Format File action will automatically be created in the Click&DECiDE Management Console. For example Store px_rawdata CSV Format File action to store the fields in the Proxy raw data table in a comma delimited *.csv file. Each string type field will be delimited by straight quotation marks and the list separator which corresponds to your regional settings (for example the Comma , for US regional settings and the semi-colon ; for French regional settings).

Introducing the Default Click&DECiDE CSV File Name Format

By default, the *.csv files are named according to the following file name format:

[TableName].[MEDIA]_[ConfigurationName]_YYYYMMDD.csv

Where:

- **[TableName]:** is the name of the Device raw data table. For example, fw_rawdata for the Firewall raw data table and px_raw data for the Proxy raw data table.
- **[MEDIA]:** is the name of the Device Media. The Media are abbreviated as follows:
 - **FLF:** Flat File
 - **SYS:** Syslog
 - **LEA:** Check Point LEA
 - **WMI:** Windows Management Instrumentation
 - **SQL:** SQL Spyer





- **RAD:** Radius
- **PNG:** Ping
- **SCH:** Event Scheduler
- **COM:** Communication
- **[ConfigurationName]:** the name of the device Configuration. For example, Check Point FireWall-1.
- **[YYYYMMDD]:** the date format.
 - **YYYY:** four digit year. For example, 2005.
 - **MM:** two digit month. For example, 01 for January.
 - **DD:** two digit day. For example, 10.
- **.csv:** the Comma Separated Values file format.

5.3.1. Suggestions for Practice

5.3.1.1. Exercise 1 - Adding a Store in CSV Format File Action

If you want to add a Store in CSV Format File action in the Click&DECiDE Management Console then please follow the steps below. In this example we will add a Store in CSV Format File action to store the fields for the Firewall raw data table in a comma delimited *.csv file.

1. Select **Console root> NetReport> Localhost> ULA> Filters> MyCustomFilter> Actions** in the **left Console root** pane. The **Actions** screen appears in the right pane.
2. Select the **Store in CSV Format File** action in the drop-down list at the base of the **Actions** drop-down section.
3. Click the **New** icon in the toolbar at the base of the **Actions** drop-down section. The **Store in CSV Format File** row appears in the **Actions** table.
4. Click the **Edit Action** icon to the right of the **Store in CSV Format File** action row. The **Store in CSV Format File** screen appears in the right pane.
5. Note the **Log Storage Initialization**. This is the name of the Click&DECiDE Initialization enabling Click&DECiDE to recuperate the COM object which writes in the file.
6. Enter the appropriate **Destination Directory**. This is the directory where the file will be stored. You can add environment variables to customize the Destination Directory. By default the Destination Directory is on the same disk as Click&DECiDE was installed on. The default Destination Directory is NETREPORT_STORAGE%. Click&DECiDE recommend that the Destination Directory is on a separate disk from that which Click&DECiDE is installed on.





7. Note the **File Name** field. By default, the *.csv files are named according to the following file name format: [TableName].[MEDIA]_[ConfigurationName]_YYYYMMDD.csv
8. Select the **Insert into Database** action which corresponds to the Device raw data table whose fields you wish to store in the comma delimited *.csv file. In this example Insert into fw_rawdata is selected.
9. Select **Console root> NetReport> Localhost> Filters> Device> Actions** in the left **Console root** pane.
10. Modify the name of the **Store in CSV Format File** to the name you wish, in this example, Store fw_rawdata in CSV Format File.



5.4. Introducing Click&DECiDE Log Vault

The Click&DECiDE Log Vault screen enables you to:

- Edit the spied directory list, add a new spied directory or manage the list of spied directories.
- Apply the changes you made to the Log Vault Service
- Verify and Manage the Log Vault Status, start or stop Log Vault, refresh the status and so on.

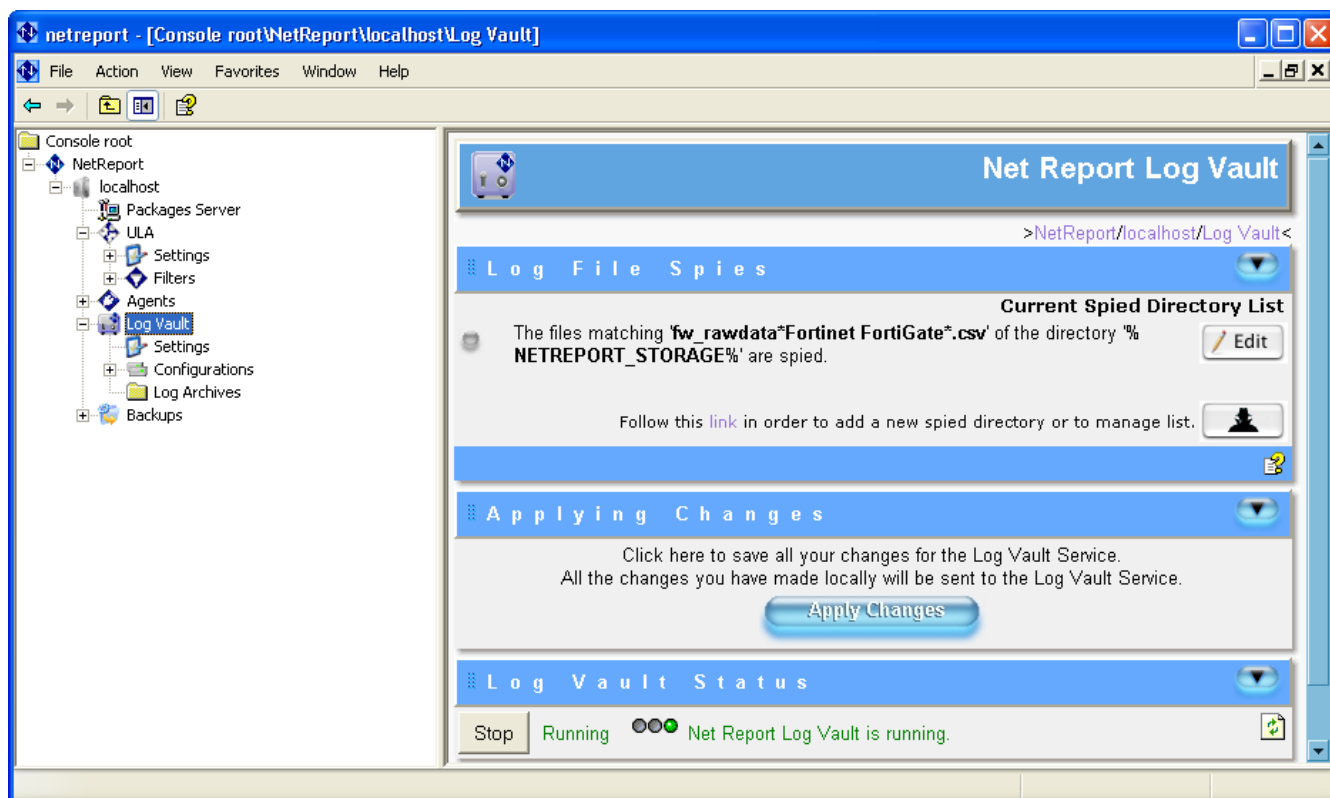


Figure 56 - Click&DECiDE Log Vault

5.4.1. Introducing Click&DECiDE Log Vault Settings

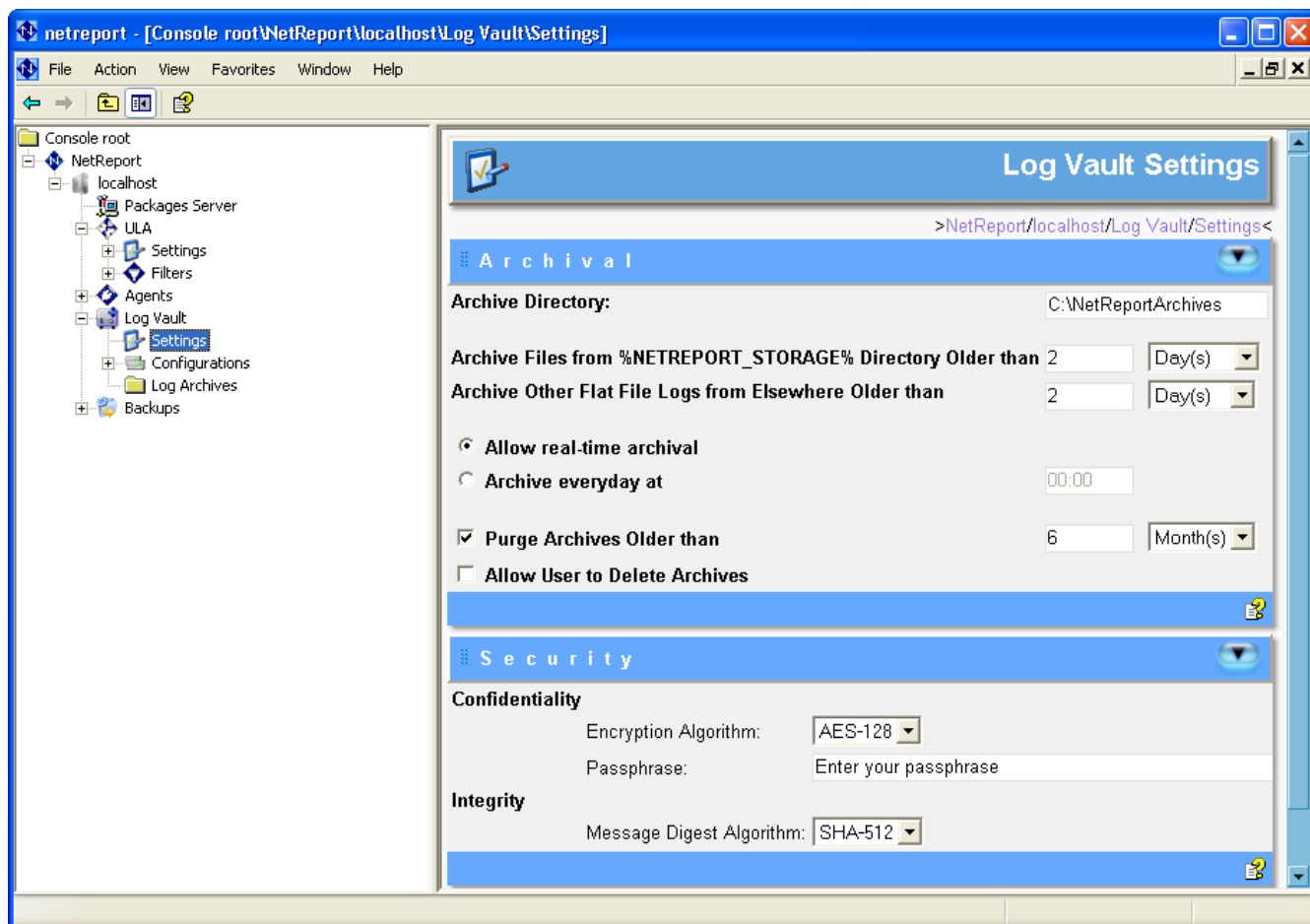


Figure 57 - Log Vault Settings

Click&DECiDE Log Vault spies on the directory you specified to spy on in the Log Vault > Configurations> Device - Spied Directory field. When Log Vault finds a file which is ready to be archived then it archives the file in the Archive directory you selected.

5.4.2. Suggestions for Practice

To configure the settings for the files you archive with Click&DECiDE Log Vault, please follow the steps below:

1. Select **Console root> NetReport> Localhost> Log Vault> Settings** in the left **Console root** pane. The **Log Vault Settings** screen appears.
2. Note the Fields to configure:

Archive Directory: the directory where Log Vault will archive your log files.

Archive Files from %NETREPORT_STORAGE% Directory Older than: enables you to select in Minute(s), Hour(s), Day(s) or Week(s) the frequency with which you wish Log Vault





to archive your files. For example if 2 Days is selected, then all files that are older than 2 days will be archived in the Archive Directory you specified.

Archive Other Flat File Logs from Elsewhere Older than: If your device logs are in flat file format originally then they do not need to be translated into CSV (Comma Separated Values) format by Click&DECiDE Log Storage, Click&DECiDE archives these "other" Flat Files by scanning the Spied Directory and archiving them in the Archive Directory you specify. This field enables you to select in Day(s) or Week(s) the frequency with which you wish Log Vault to archive your files. For example if 2 days are selected, then all files that are older than 2 days will be archived in the Archive Directory you specified.

Allow real-time archival: the Log Vault archives your files once a minute.

Archive everyday at: the Log Vault archives your files every day at the time you specify in the text box.

Purge Archives Older than: enables you to purge files that are older than a certain number of years. Note that the default value for this field is 7 years.

Allow User to Delete Archives: by default this check box is left clear. However, should you wish that users have the possibility to delete archives, simply select the Allow User to Delete Archives check box.

Encryption Algorithm: select the appropriate Encryption Algorithm. Note that AES is selected by default, this is the CryptoAPI algorithm name for the Advanced Encryption Standard algorithm.

Passphrase: enter the passphrase. A passphrase is basically a sentence or phrase that serves as a more secure password. A typical password is 6 to 8 characters, and often is a word that is present in a dictionary. That is very unsafe. A passphrase could be a complete sentence, preferably a nonsensical one. Such a sentence would be much harder to guess.

Message Digest Algorithm: produces the message digest.

3. Set the appropriate **Post Archival File Transfer** settings if necessary. Note that the Archive File Transfer check box is clear by default. If you want to transfer your archive files post archival, simply select the Archive File Transfer check box and select the appropriate Local Archive File Transfer method from the drop-down list to the right of the check box.

Archive File Transfer: select this check box if you want Click&DECiDE Log Vault to perform Post Archival File transfer.





Local Archive File Transfer: Click&DECiDE Log Vault transfers files from the Archive Directory to the directory of your choice. Specify the Destination directory in the Destination field.

FTP Archive File Transfer: Click&DECiDE Log Vault transfers files from the Archive Directory to a FTP site. Specify the Destination, Host Name, User and Password details for your FTP Site.

Passive Mode FTP Connection: by default FTP transfer is performed via Passive FTP. To enable Active FTP transfer clear the Passive Mode FTP Connection check box.

Note: the files transferred will either be in *.zip format or *.crp format (if you have selected to encrypt your files).

4. Select **Console root> NetReport> Local Host> Log Vault** in the left **Console root** pane.
5. Click **Apply Changes** to save the changes you have made.



5.5. Introducing Click&DECiDE Log Vault Archives

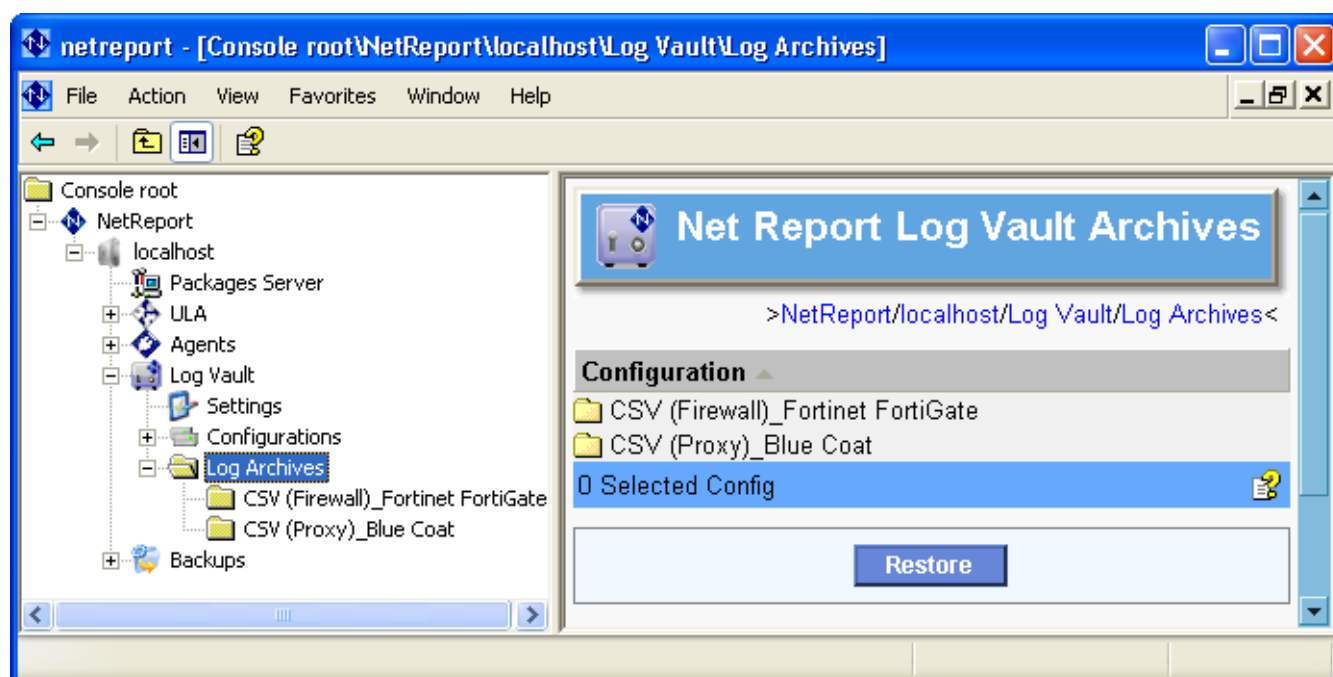


Figure 58 - Log Vault Archives

The Click&DECiDE Log Vault Archives branch enables you to manage your Log Vault Archives. You can easily navigate between the archives for different Device configurations, from month-to-month and year-to-year. You can restore or remove archives (according to the Archive Management rights which your System Administrator has granted) at any level in the Click&DECiDE Log Archives tree structure.

5.5.1. Suggestions for Practice

To manage your Click&DECiDE Log Vault Archives at the Configuration level, please follow the steps below:

5.5.1.1. Exercise 1 - Restoring Configuration Archives

To restore configuration archives, please follow the steps below:

1. Select **Console root > NetReport > Localhost > Log Vault > Log Archives** in the left **Console root** pane. The **Click&DECiDE Log Vault Archives** screen appears in the right pane.
2. Select the Configuration Archives you want to restore, by clicking the directory for the Configuration, for example FLF Check Point FireWall-1 to restore the Check Point Firewall-1 flat file archives.





3. Click **Restore**. The **Log Vault Restore** dialog box appears.
4. Enter the **Destination** directory where you want the Log Vault archive files to be restored to.
5. Note that the following check boxes are selected by default:

Unencrypt Archive Files: this unencrypts the *.crp files.

Uncompress Archive Files: this uncompresses the *.zip files to enable the extraction of the *.log and the *.cert signature file, for example, if you selected to sign your archive files with the signing algorithm.

Verify Archive Files' Integrity: verifies the message digest's integrity.

6. Note that the **Build tree to mirror current structure** check box is not selected by default. This option builds a tree structure in the Destination directory which you entered at the top of the Log Vault Restore dialog box in order to mirror your current archive tree structure.
7. Wait for your archive files to be restored, this may take some time.

5.5.1.2. Exercise 2 - Removing Configuration Archives

Before removing Click&DECiDE Log Vault Configuration Archives, please contact your System Administrator, as if your company Security Event archives are kept for long-term storage, removing them may have very serious legal implications. For example, if your company is seeking to conform to the Internal Control directives in Sarbanes-Oxley or Basel II, for example, then you must keep your enterprise Security Event logs for seven years and ten years respectively.

To remove configuration archives, please follow the steps below:

1. Select **Console root> NetReport> Localhost> Log Vault> Settings** in the left **Console root** pane. The **Log Vault Settings** screen appears in the right pane.
2. Select the **Allow User to Delete Archives** check box in the **Archival** drop-down section.
3. Select **Console root> NetReport> Localhost> Log Vault** in the left **Console root** pane.
4. Click **Apply Changes** to save that modifications you have made.





5. Select **Console root> NetReport> Localhost> Log Vault> Log Archives** in the left **Console root** pane. The **Click&DECiDE Log Vault Archives** screen appears in the right pane.
6. Select the Configuration Archives you want to remove, by clicking the directory for the Configuration, for example FLF Check Point FireWall-1 to remove the Check Point Firewall-1 flat file archives.
7. Click **Remove**.
8. Wait for your archive files to be removed, this may take some time.

5.5.2. Exercise 3 – Restoring Year/Month Level Archives

1. Select **Console root> NetReport> Localhost> Log Vault> Log Archives> Configuration> Year** in the left **Console root** pane. The **Click&DECiDE Log Vault Archives** screen appears in the right pane.
2. Select the archives for the Months of the year you want to restore.
3. Click **Restore**.
4. Enter the Destination directory where you want the Log Vault archive files to be restored to.
5. Note that the following check boxes are selected by default:

Unencrypt Archive Files: this unencrypts the *.crp files.

Uncompress Archive Files: this uncompresses the *.zip files to enable the extraction of the *.log and the *.cert signature file, for example, if you selected to sign your archive files with the signing algorithm.

Check Archive File Signature: verifies that the file signature *.cert file corresponds to the log file.

6. Note that the Build tree to mirror current structure check box is not selected by default. This option builds a tree structure in the Destination directory which you entered at the top of the Log Vault Restore dialog box in order to mirror your current archive tree structure.
7. Wait for your archive files to be restored, this may take some time.





5.6. Introducing Click&DECiDE Log Replay

Please contact your Click&DECiDE Training Advisor for more information on Click&DECiDE Log Replay.





6. Working with the Click&DECiDE Alerting & Correlation Console

6.1. Introducing Alerts

Click&DECiDE delivers over 100 alerts and examples of correlation by default. We provide single and multi-device alerts by default. Trusted alerts are sent by e-mail, SNMP Trap and Syslog. Administrators can easily use advanced function to create customized alerts and actions.

Click&DECiDE correlate events from a wide range of network devices to provide faster decision making and greater enterprise security. We provide an easy way to define the pattern of events, rules and corresponding actions to simplify the monitoring of network events. Click&DECiDE provides four possible correlation methods to correlate security events from different devices to identify security incidents and send trusted alerts:

1. Generate an alert when a fixed pattern is met.
2. Generate an alert when a threshold is met with a pre-defined session timeout (Memory Counter).
3. Generate an alert if either of the two above actions are identified, and correlated with information in a database, LDAP or a dictionary.
4. Generate an alert when the result of a query in the database meets certain criteria defined in the rule. This query can be scheduled. This method enables analysis over long periods of time such as port scans.

The benefits of event correlation can be very real. More efficient use of staff time and skills, as well as the prevention of revenue loss resulting from downtime is a major benefit. We mine and analyze huge volumes of data for your Enterprise. In many cases, these need to be analyzed in real-time and are useful in many security scenarios. Select predefined alerts, create specific actions or alerts and send alerts via:

- SMTP.
- SNMP.
- Pop-up.
- Alerting & Correlation Console.





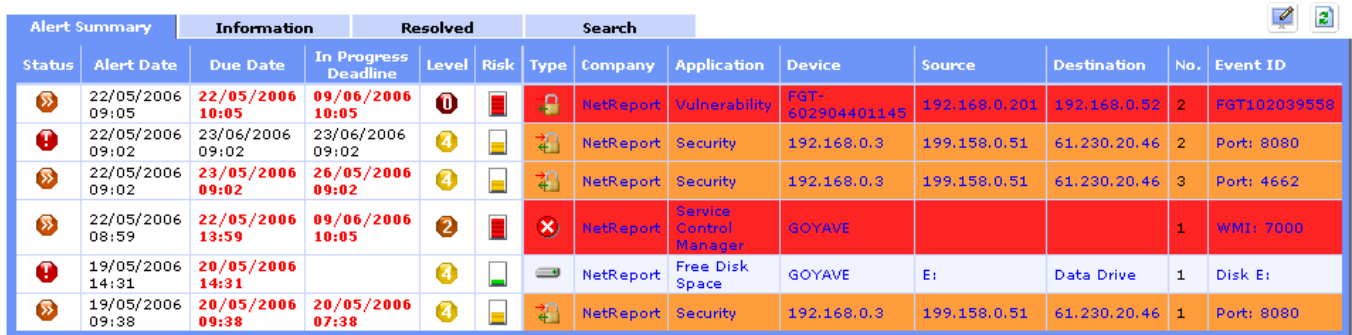
According to the pre-defined set of actions, several types of alerts or tasks can be executed:

- Write in the database.
- Send an e-mail.
- Generate a SNMP TRAP.
- Launch a script.



6.2. Introducing the Alerting & Correlation Console

Click&DECiDE provides a real-time HTTP Alerting & Correlation Console (ACC) for dynamic alert filtering and alert management. The Console is multi-user with advanced user profile management. The four tabs: Alert Summary, Information, Resolved and Search enable your IT Staff to quickly identify, isolate, filter and mitigate threats.



Alert Summary		Information		Resolved		Search							
Status	Alert Date	Due Date	In Progress Deadline	Level	Risk	Type	Company	Application	Device	Source	Destination	No.	Event ID
	22/05/2006 09:05	22/05/2006 10:05	09/06/2006 10:05	1		NetReport		Vulnerability	FGT-602904401145	192.168.0.201	192.168.0.52	2	FGT102039558
	22/05/2006 09:02	23/06/2006 09:02	23/06/2006 09:02	4		NetReport		Security	192.168.0.3	199.158.0.51	61.230.20.46	2	Port: 8080
	22/05/2006 09:02	23/05/2006 09:02	26/05/2006 09:02	4		NetReport		Security	192.168.0.3	199.158.0.51	61.230.20.46	3	Port: 4662
	22/05/2006 08:59	22/05/2006 13:59	09/06/2006 10:05	2		NetReport		Service Control Manager	GOYAVE			1	WMI: 7000
	19/05/2006 14:31	20/05/2006 14:31		4		NetReport		Free Disk Space	GOYAVE	E:	Data Drive	1	Disk E:
	19/05/2006 09:38	20/05/2006 09:38	20/05/2006 07:38	4		NetReport		Security	192.168.0.3	199.158.0.51	61.230.20.46	1	Port: 8080

Figure 59 - Alerting & Correlation Console

- **Alert Summary:** displays alerts that are either to be acknowledged or in progress. Alerts can easily be managed by clicking the In Progress or To be Acknowledged icons in the Status column.
- **Information:** displays Information type alerts.
- **Resolved:** displays the alerts that have been treated and resolved.
- **Search:** displays all the alerts, clicking any of the icons or hyperlinks enables you to filter and group alerts. For example, filter events through an IP Address.

The Alerting & Correlation Console enables you to display up to sixteen fields, as follows:

Alert Date,	Due Date/ In Progress,	Level,	Risk,
Type,	Application,	Device,	Source,
Destination,	Number,	Event ID,	Description,
Dependency,	Company,	Last User,	Last Comment.

Clear icons and color schemes highlight the priority of alerts and the management due dates. Hyperlinks enable you to navigate between the tabs and access alert relevant links online.

Easily centralize and manage the status of your aggregated alerts via the Management, History and Extra Information tabs:

- **Management:** details concerning the aggregated alert, the alert status, easily modify the status, due date etc... and forward the alert by SNMP, E-mail or Syslog. Clicking



the Manage this Alert... button enables you to edit the Alert management parameters via the Edit Alert tab.

- **History:** track alert mitigation by user profile and follow previous Alert Management modifications made to the Alert, along with the date, user profile and comments made.
- **Extra Information:** additional information, displayed according to the parameters selected. Possibility to generate daily, weekly and monthly OLAP cubes for IP Source and or IP Destination.

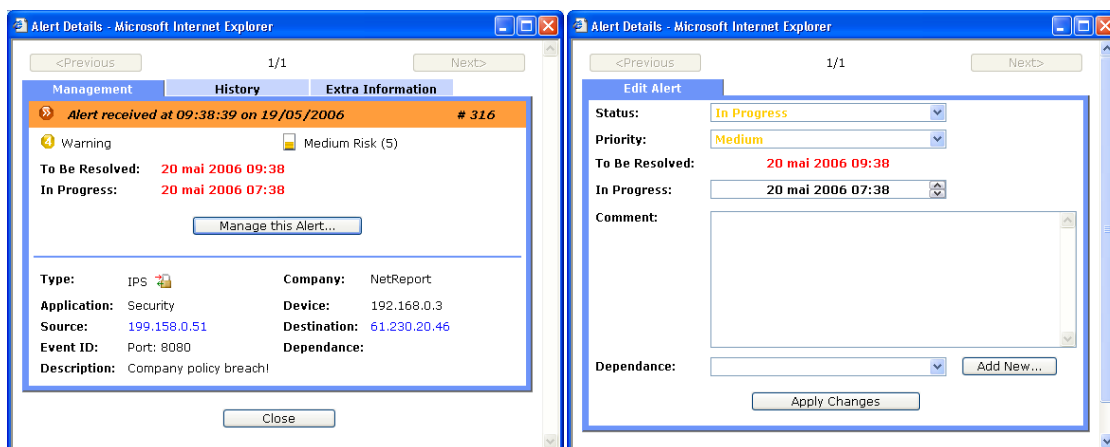


Figure 60 - Alert Details



Advanced Configuration Panel

The Alerting & Correlation Console Configuration Panel enables you to manage User Profiles, Filtering Rules and column display features in real-time.

- **Column Display:** enables the user to select the columns they want to be displayed in the Alerting & Correlation Console.
- **Filtering Rules:** enables the user to add and edit filtering rules according the criteria they define.

Rule Properties - Microsoft Internet Explorer

New Rule

Hide alerts older than 2 days that meet the following criteria:

Status: IGNORE

Priority: IGNORE

Level: IGNORE

Risk: IGNORE

Type:

Company:

Application:

Device:

Source:

Destination:

Event ID:

Dependence:

Description:

This field can use the same syntax as a LIKE condition in SQL.
For example, "%computer%" will match the alerts with the word "computer" anywhere in its description.

OK Cancel

Figure 61 - Rule Properties





User Profiles: enables Administrators to define, edit and delete user profiles and assign permissions.

The screenshot shows a web interface with three tabs: "Column Display", "Filtering Rules", and "User Profiles". The "User Profiles" tab is active. It displays two user profiles: "ACC_ADMIN" and "ACC_GUEST".

ACC_ADMIN Profile:

- Grant Admin Rights: ☒
- Buttons: Add New Rule...

ACC_GUEST Profile:

- Rename or Delete Profile... (with edit/delete icons)
- Grant Admin Rights: ☐
- Table of rules:

Edit	#	Status	Priority	Level	Risk	Type	Company	Application	Device	Source	Destination	Event ID	Description	Dependence
	2								GOYAVE					
	3						Netreport							

Buttons: Add New Rule...

Figure 62 - User Profiles





6.3. Correlated Alerts

Please contact your Click&DECiDE Training Advisor for more information on Correlated Alerts.





7. Backing up and Restoring Click&DECiDE

7.1. Backing up Click&DECiDE Files

This section explains the files and directories to backup for Click&DECiDE. Note this document gives the directories which Click&DECiDE proposes by default, please replace the directories as appropriate. Please note that the default Click&DECiDE drive is drive C, if you installed Click&DECiDE on another drive then replace drive C which is used for the paths in this section by the appropriate drive.

7.1.1. Click&DECiDE Spied Directory Backup

Backup the log files in the directory you selected for Click&DECiDE to scan via the Click&DECiDE Configurator or the Click&DECiDE Management Console.

7.1.2. Click&DECiDE Database Backup

Backup the netreport database.

7.1.3. Click&DECiDE Configuration Backup

If you used the Click&DECiDE Configurator: then the Click&DECiDE configuration you parameterized will be automatically backed up when you click either the **Apply** or **OK** buttons in the Click&DECiDE Configurator. Click&DECiDE will automatically create a directory (YYYYMMDD-HHMM-wizard-vXXX) with your configuration in the following directory:

C:\Program Files\NetReport\NetReport\ConfigurationBackup

If you performed an advanced configuration via the Click&DECiDE Management Console: then you must click the **Backup** button to save this configuration in the following branch in the Click&DECiDE Management Console:

Console root> NetReport> localhost

Click&DECiDE will create a directory (YYYYMMDD-HHMM-user-vXXX) with your configuration in the following directory:






C:\Program Files\NetReport\NetReport\ConfigurationBackup

7.1.4. Click&DECiDE Log Storage Files Backup

Backup the files in the following directories

C:\NetReportStorage

 **Note:** The %NETREPORT_STORAGE% Environment Variable defines the default directory for Click&DECiDE Log Storage Actions.

 **Note:** Log Storage generates files in Native and/or Enriched CSV Format for temporary storage before they are archived by Click&DECiDE Log Vault. Log Storage does not treat other Flat File Logs which can be directly archived in the Click&DECiDE Archive Directory.

7.1.5. Click&DECiDE Log Archive Files Backup

Backup the log archive files you selected to store over the long-term (for example for seven to 10 years) in the Click&DECiDE Log Vault

C:\NetReportArchives

7.1.6. Click&DECiDE Web Portal Configuration Backup

Backup the Web Portal Configuration .bck file that is generated by the **Click&DECiDE Administration Manager**.

7.1.6.1. Suggestion for Practice

1. Start **Click&DECiDE Administration Manager**: Start> All Programs> Click and DECiDE> Administration Manager.



2. Go to **File> Backup Security Database**

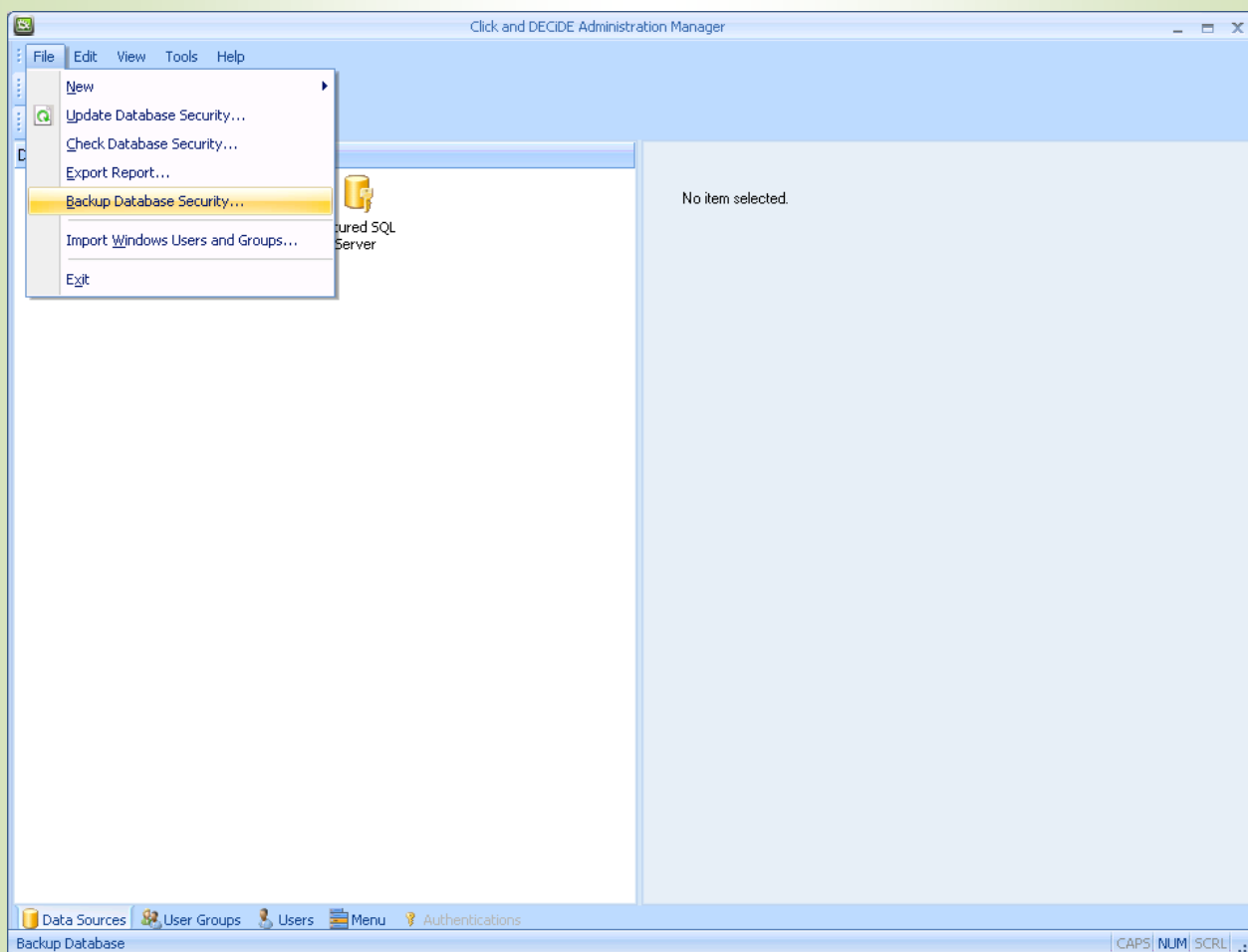


Figure 63 - Click&DECiDE Web Portal Configuration Backup

3. Save the Security Database configuration into a .bck file.
4. Close **Click&DECiDE Administration Manager**.

7.1.7. Click&DECiDE Dashboards Backup

Backup the directories in which you have saved all non-default *.wfv files which you may have installed or modified via the Click&DECiDE Tool Kit, Click&DECiDE Device Support Center...

If you have set scheduled Dashboard generation tasks via the Click&DECiDE Web Portal then backup the following file:

C:\Program Files\NetReport\WebPortal\d7tasks.xml





7.2. Restoring Click&DECiDE Backups

This section explains how to restore your Click&DECiDE configuration from the files and directories you backed up.

This section is divided into seven tasks. Please perform the tasks in the order in which they are presented:

Task 1: Restoring the netreport Database and Installing Click&DECiDE Version X.X

Task 2: Parameterizing Settings via the Click&DECiDE Configurator

Task 3: Restoring Configuration Backup Files via the Click&DECiDE Management Console

Task 4: Restoring Web Portal Configuration

Task 5: Updating the netreport Database via the Click&DECiDE Configurator

Task 6: Restoring Standard and Non-Standard Scheduled Dashboard Generation Tasks

Task 7: Restoring Log Archive Files and Non-Default Report Files

Note this section gives the directories which Click&DECiDE proposes by default, please replace the directories as appropriate. Please note that the default Click&DECiDE drive is drive C, if you installed Click&DECiDE on another drive then replace drive c which is used for the paths in this document by the appropriate drive.

7.2.1. Suggestions for Practice

7.2.1.1. Task 1: Restoring the netreport Database and Installing Click&DECiDE Version X.X

1. Restore the netreport database.
2. Install Click&DECiDE Version X.X.
3. Select the parameters you wish in the InstallShield Wizard.



7.2.1.2. Task 2: Parameterizing Settings via the Click&DECiDE Configurator

1. Select a device that you configured in your previous configuration when the Click&DECiDE Configurator appears.

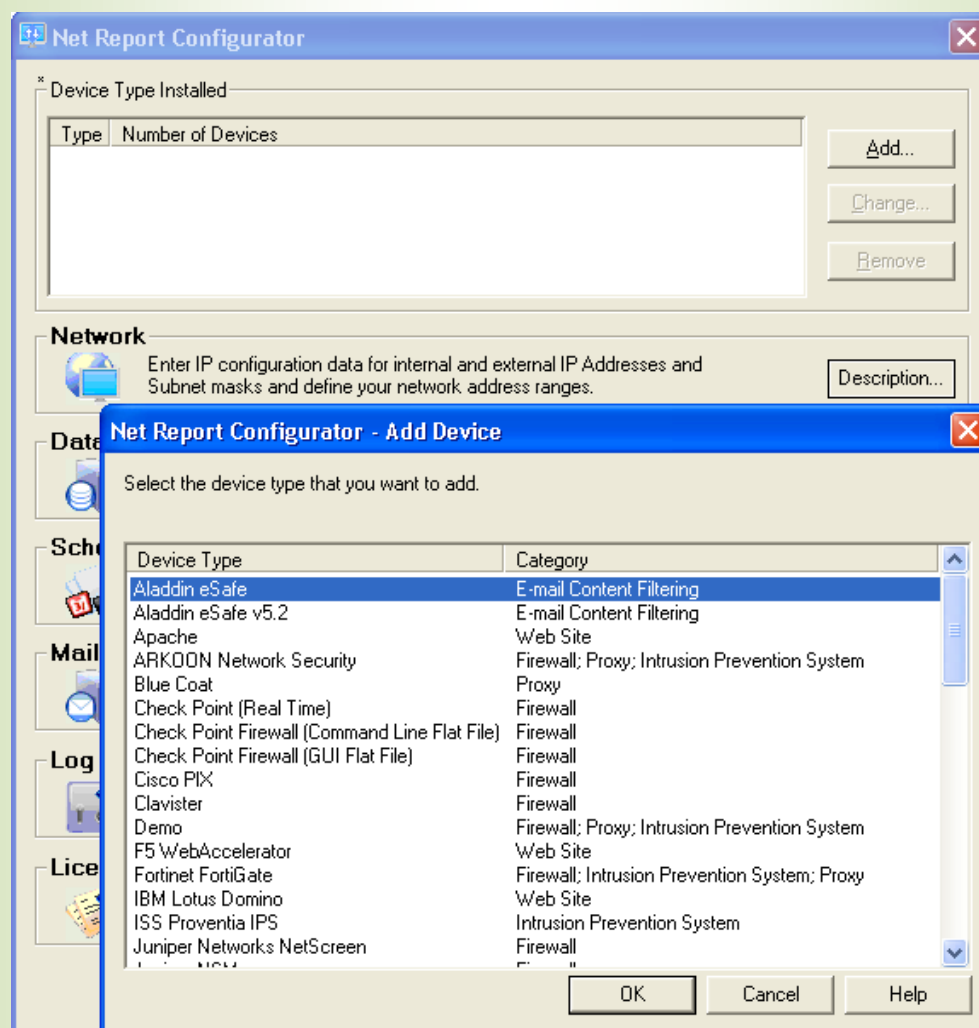


Figure 64 - Click&DECiDE Configurator Device Selection

2. Select the **Settings...** button to the right of the **Network**, **Scheduled Tasks**, **Mail Server** and **Log Archive** zones and click **OK** for each of the settings. Note that your initial settings will be restored in the tasks which follow.
3. Select Database **Settings...**



4. Enter your **Click&DECiDE Login** in the **Password** and **Confirm** text boxes.

Net Report Configurator - Database Settings

Database Connection Settings

☒ Use an existing Database Server Type: **SQL Server (MSDE, 2000, 2005)** Server Name: **LYCHEE**

☐ Install MSDE Installation Directory:

Warning: MSDE is for test purposes only.

Net Report Database Administrator Login
This Administrator Login creates the 'netreport' User and Database.

User ID: **sa** Password: **Test**

Net Report Login

User ID: **netreport** Password: ********* Confirm: *********

Database Update Settings
Configure the update settings for the netreport Database.

☒ Update Database

☐ Do not execute SQL scripts now (only generate).
Manually execute your SQL scripts later.

☐ Delete existing data

Database Time Zone Settings

☐ Use UTC offset (Coordinated Universal Time)

Time Zone: **(GMT+01:00) Brussels, Copenhagen, Madrid, Paris**

☒ Adjust for Daylight Saving Time (DST)

OK **Cancel** **Help**

Figure 65 - Click&DECiDE Configurator Database Settings

5. Click **OK**.
6. Click **Apply**. Wait for the Click&DECiDE Configurator to update your settings.



7.2.1.3. Task 3: Restoring Configuration Backup Files via the Click&DECiDE Management Console

1. Copy the Click&DECiDE Configuration Backup files to the following directory:
C:\Program Files\NetReport\NetReport\ConfigurationBackup

Note about Click&DECiDE Configuration Files: the files you copied during your backup of the ConfigurationBackup directory (with sub-directories with the format YYYYMMDD-HHMM-wizard-vXXX or YYYYMMDD-HHMM-user-vXXX) from the following directory:

C:\Program Files\NetReport\NetReport\ConfigurationBackup

2. Select **Start> All Programs> NetReport> Management Console**.
3. Enter your **Login** and **Password**.
4. Click **OK**.
5. Select **Console root> NetReport> [localhost]> Backups** in the left **Console root** pane.

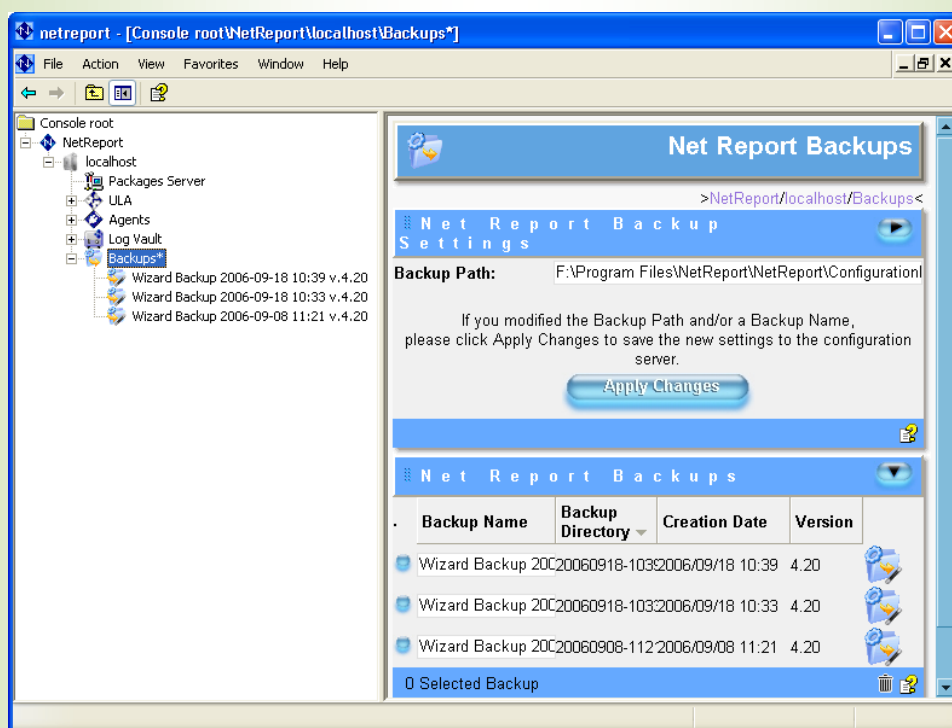


Figure 66 - Configuration Backups

6. In the left **Console root** pane right-click on the backup you want to restore.

7. Select **Restore Configuration** in the context menu.

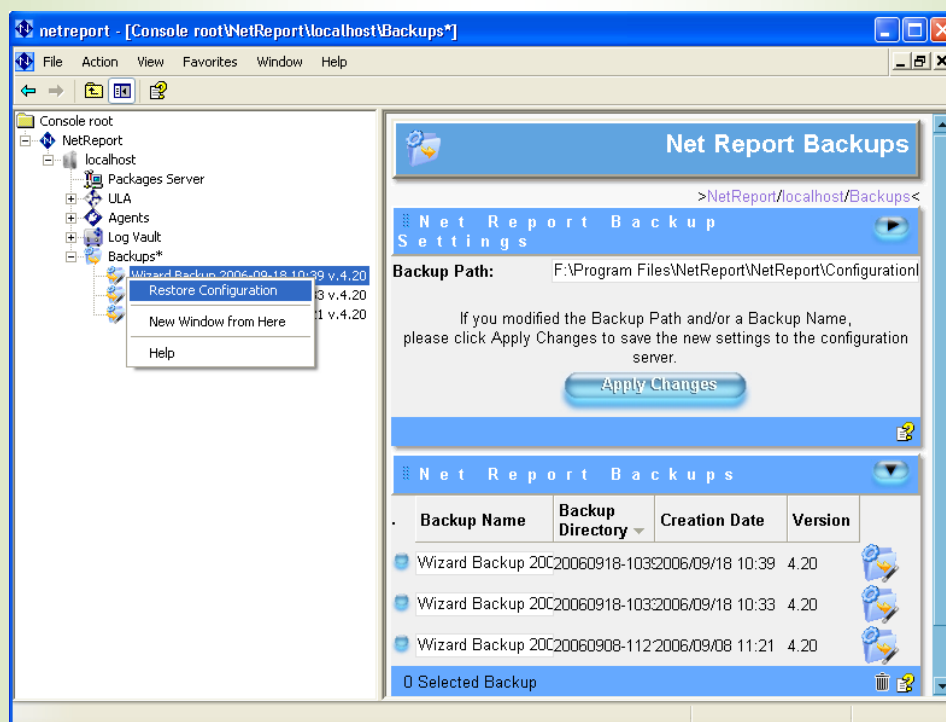


Figure 67 - Restoring Configuration Backup Files

8. Click **Yes** when the **Do you really want to restore the “XXX” backup for the “[localhost]” configuration server** message appears. Wait for your Configuration to be restored.
9. Click **OK** when the status message appears.
10. Select **File> Exit**.
11. Click **Yes** when the **Save Console settings to netreport.msc** message appears.
12. Click **Yes** when the **Do you want to save all your changes to the “[localhost]” configuration server** message appears.



7.2.1.4. Task 4: Restoring Web Portal Configuration

1. Locate the Security Database backup file (.bck).
2. Double click on the file. **Administration Manager** asks if you want to restore the Security Database.

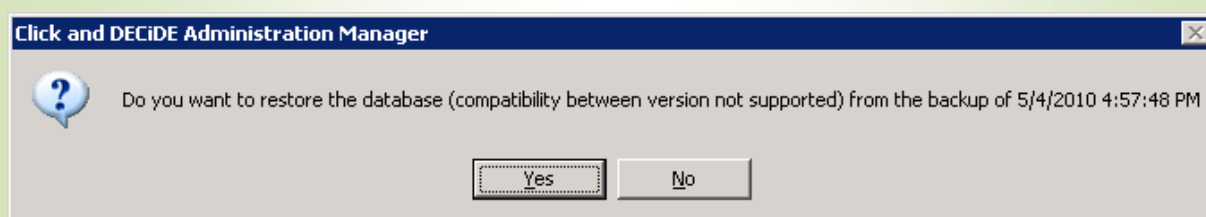


Figure 68 - Restoring Web Portal Configuration

3. Click **Yes**.
4. Verify that your configuration is correct.
5. Click **Update Security** icon

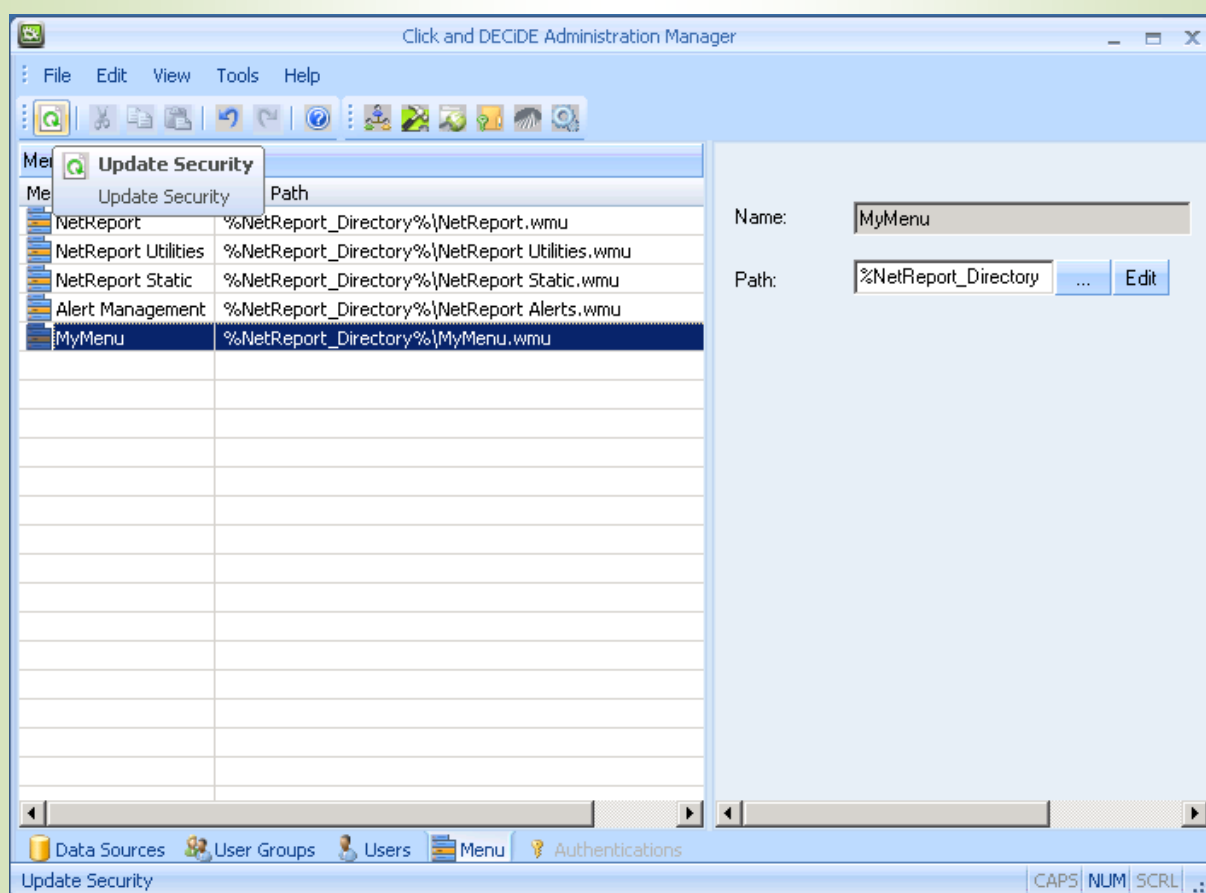


Figure 69 - Update Administration Settings

6. Click **OK**.
7. Close **Administration Manager**.



7.2.1.5. Task 5: Updating the Database via the Click&DECiDE Configurator

1. Select **Start> All Programs> NetReport> Configurator**. The **Click&DECiDE Configurator** appears.
2. Select the **Update Database** check box.

Net Report Configurator - Database Settings

Database Connection Settings

☒ Use an existing Database Server Type: **SQL Server (MSDE, 2000, 2005)** Server Name: **LYCHEE**

☐ Install MSDE Installation Directory:

Warning: MSDE is for test purposes only.

Net Report Database Administrator Login

This Administrator Login creates the 'netreport' User and Database.

User ID: **sa** Password: **Test**

Net Report Login

User ID: **netreport** Password: Confirm:

Database Update Settings

Configure the update settings for the netreport Database.

☒ Update Database

☐ Do not execute SQL scripts now (only generate).
Manually execute your SQL scripts later.

☐ Delete existing data

Database Time Zone Settings

☐ Use UTC offset (Coordinated Universal Time)

Time Zone: **(GMT+01:00) Brussels, Copenhagen, Madrid, Paris**

☒ Adjust for Daylight Saving Time (DST)

OK **Cancel** **Help**

Figure 70 - Updating Database

3. Enter your Click&DECiDE Database Administrator Login **User ID** and **Password**.
4. Click **OK**.
5. Click **Apply**. Wait for the **Click&DECiDE Configurator** to update your settings.



7.2.1.6. Task 6: Restoring Standard and Non-Standard Scheduled Dashboard Generation Tasks

1. Select **Start> Control Panel> Administrative Tools> Services**. The **Services console** appears.
2. Right-click the **Click&DECiDE Task Manager** service.
3. Select **Stop** in the context menu.

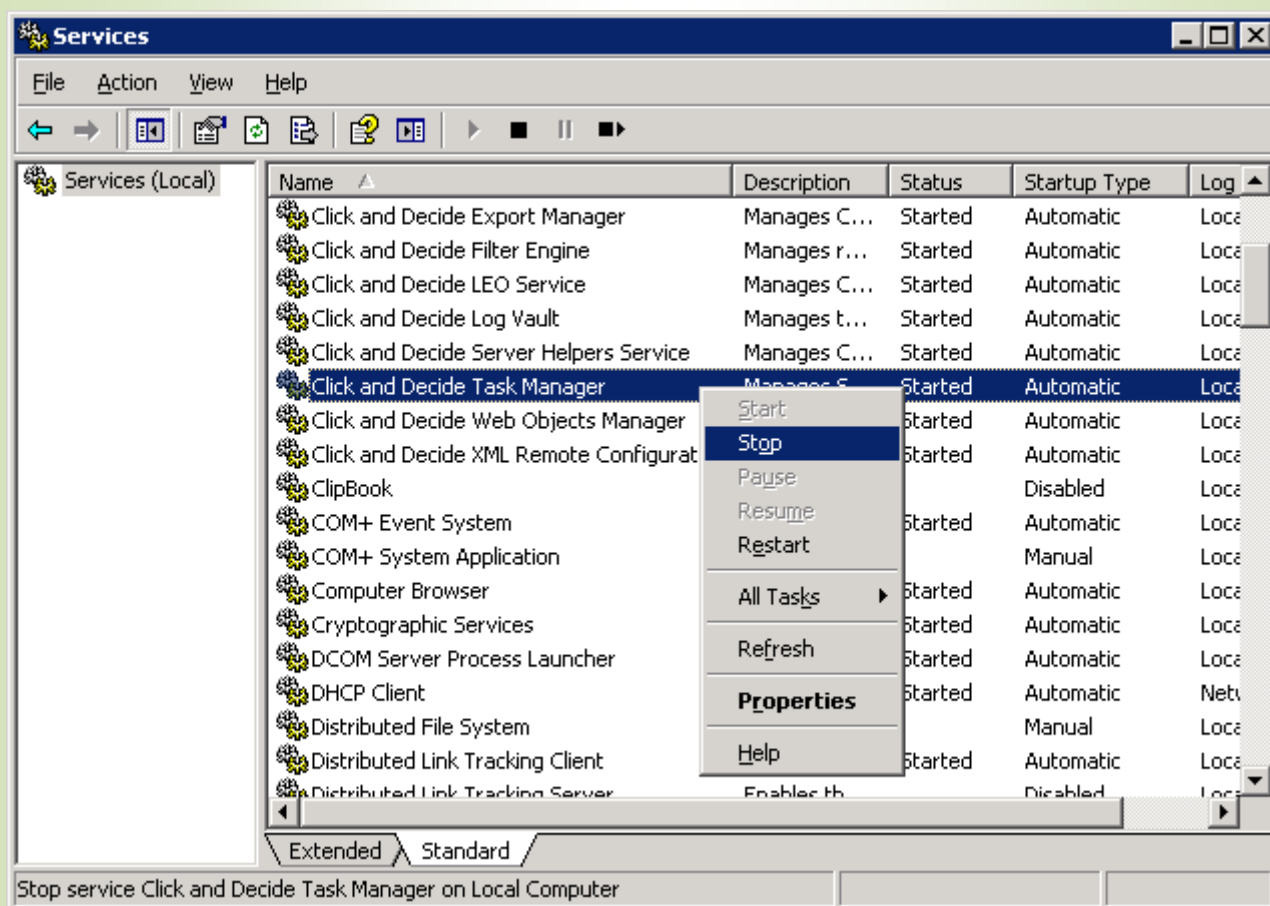


Figure 71 - Stopping Click&DECiDE Task Manager

4. Copy the d7tasks.xml file including any non-default Scheduled Dashboard generation tasks created via the Click&DECiDE Web Portal to the following directory:
C:\Program Files\NetReport\WebPortal\d7tasks.xml
5. Select **Start> Control Panel> Administrative Tools> Services**. The **Services console** appears.
6. Right-click the **Click&DECiDE Task Manager** service.



7. Select **Start** in the context menu

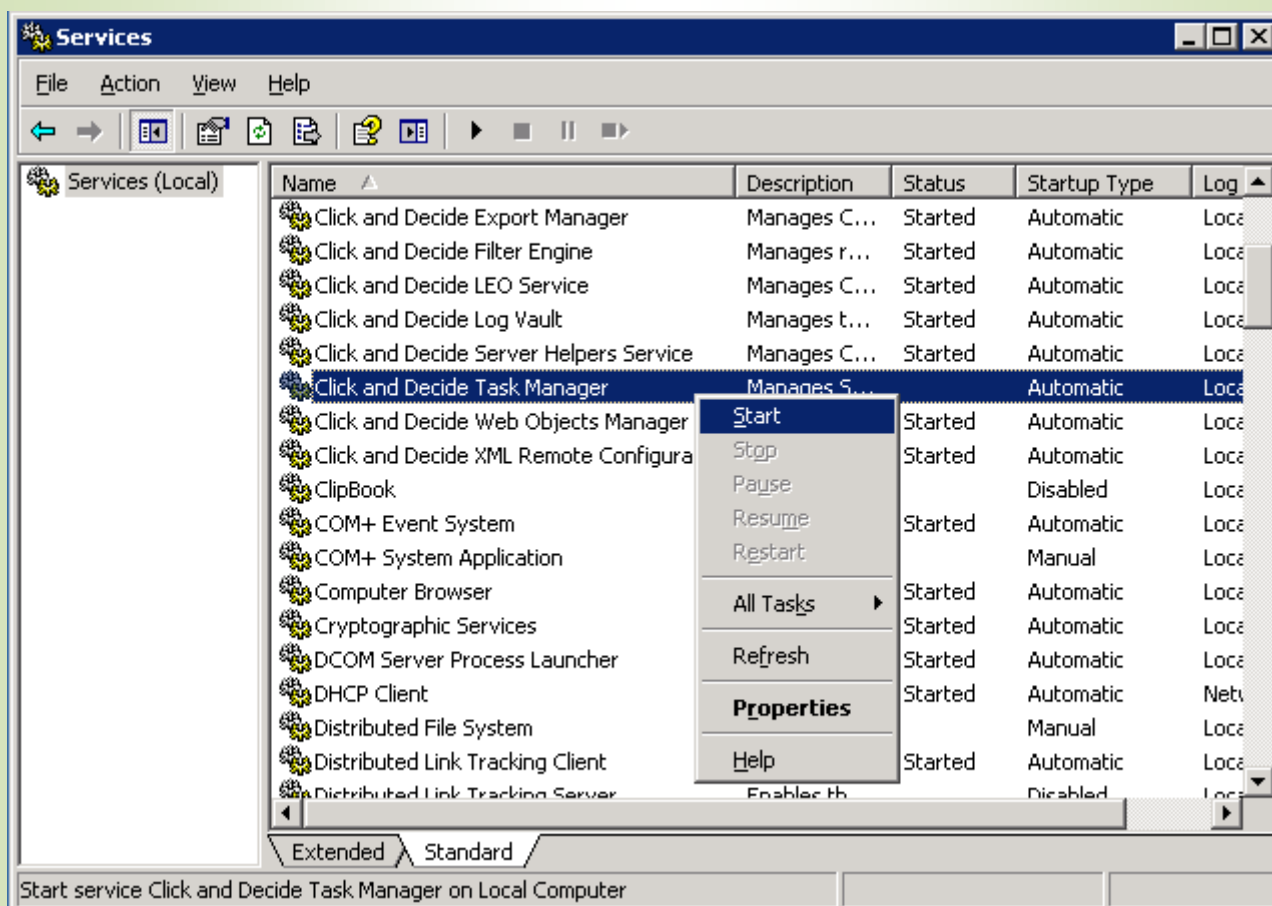


Figure 72 - Starting Click&DECiDE Task Manager

7.2.1.7. Task 7: Restoring Log Archive Files and Non-Default Report Files

1. Copy any non-default *.wfv files to the following directory:
C:\Program Files\NetReport\WebPortal\Runtime_Projects\enu
2. Copy the archive files to the following directory:
C:\NetReportArchives





8. Troubleshooting

Please Consult our NSI Troubleshooting Guide.





Reference Material

Please note the following related information:

Web Site

<http://www.clickndecide.com>





Contacting **Click&DECiDE**

For Technical Support, please contact us:

By e-mail at: support@netreport.fr

By Telephone on: +33 (0)46 784 4800

By Fax on: +33 (0)46 784 4811

By post at: Click&DECiDE Headquarters,
130 rue Baptistou,
ZAE Nord,
34980 Saint Gély du Fesc,
FRANCE

For Sales Enquiries, please contact us:

By e-mail at: sales@netreport.fr

By Telephone on: +33 (0)1 70 80 97 46

By post at: Click&DECiDE Sales Offices,
3ème Etage,
98 route de la Reine,
92100 BOULOGNE,
FRANCE





© 2009 Click&DECiDE SAS. All rights reserved Click&DECiDE. Net Report, DataSet Report, DataSet Vision, Click&DECiDE and other DataSet products and services as well as their respective logos are trademarks or registered trademarks of Click&DECiDE SAS. All other company names, products and services used herein are trademarks or registered trademarks of their respective owners. The information published herein is subject to change without notice. This publication is for informational purposes only, without representation or warranty of any kind, and Click&DECiDE SAS shall not be liable for errors or omissions with respect to this publication. The only warranties for Click&DECiDE products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting any additional warranty.

