Click&DECiDE
Le Décisionnel Polyvalent

NSI TRAINING BOOK

Part 1: Log Source 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 7
1. Product Overview 8
1.1. Product Range 8
1.1.1. Click&DECiDE NSI Professional Package 8
1.1.2. Click&DECiDE NSI Enterprise Package 8
1.1.3. Click&DECiDE BAI Express Edition 8
1.1.4. Click&DECiDE BAI Standard Edition 8
1.1.5. Click&DECiDE BAI Professional Edition 9
1.1.6. Click&DECiDE BAI Enterprise Edition 9
1.1.7. Product Modules 10
1.2. Architecture 11
1.3. Advanced Installation Architectures 13
1.4. Hardware System Requirements 14
1.5. Software System Requirements 14
2. Install Click & DECiDE - NSI 16
2.1. Turning on the Required IIS Features 16
2.2. Download and install the Framework .NET 3.5 SP1 16
2.3. Download and extract the Click&DECiDE NSI setup 17
2.4. The Click and DECiDE - NSI Installation Wizard 18
2.5. Suggestions for Practice: 21
3. Working with Click&DECiDE NSI Log Source Configuration 22
3.1. Selecting a License Certificate 22
3.2. Working with the Log Source Configuration Screen 24
3.2.1. Device Type Installed 25
3.2.2. Network 25
3.2.3. Database 26
3.2.4. Scheduled Tasks 26
3.2.5. Web Portal 26
3.2.6. Log Archive 27
3.2.7. License Certificate 27
3.2.8. Enabling the Description… button 29
3.2.9. Working with Undefined Settings 30

3.3. Working with Device Settings 30
3.3.1. Add Device 30
3.3.2. Suggestions for Practice 31
3.3.3. Log File Acquisition Settings 32
3.3.4. Suggestions for Practice 33
3.3.5. Log Acquisition and Treatment Settings 34
3.3.6. Suggestions for Practice 36
3.4. Working with Network Settings 37
3.4.1. Network Connection Settings 37
3.4.2. Network Change 38
3.4.3. Suggestions for Practice 39
3.5. Working with Database Settings 39
3.5.1. Database Connection Settings 40
3.5.2. Click&DECiDE NSI Login 41
3.5.3. Database Update Settings 42
3.5.4. Database Time Zone Settings 43
3.5.5. Suggestions for Practice 44
3.6. Working with Scheduled Task Settings 44
3.6.1. Scheduling 45
3.6.2. Purge Settings 45
3.6.3. Suggestions for Practice 46
3.7. Working with Web Portal Settings 46
3.7.1. Web Portal Authentication Mode 46
3.7.2. Mail Server Settings 47
3.7.3. Mail Action Settings 47
3.7.4. Suggestions for Practice 48
3.8. Working with Log Archive Settings 48
3.8.1. Log Archive Settings 48
3.8.2. Suggestions for Practice 52
3.8.3. Add Device Logs to Archive 53
3.8.4. Transfer Archive File Settings 55
3.8.5. Suggestions for Practice 56
3.9. Updating Log Source Configuration Settings 56
3.9.1. Suggestions for Practice 58
3.10. Suggestions for Practice 59

Table of Figures

Figure 1 - Process Architecture 11
Figure 2 - Appliance #1 Architecture 13
Figure 3 - Licence Email sample 17
Figure 4 - Save File Installation path....17
Figure 5 - File extraction process....18
Figure 6 - Click&DECiDE Welcome Screen 18
Figure 7 - Click&DECiDE Licence Agreement....19
Figure 8 - Installation destination folder....19
Figure 9 - Installation type selection....20
Figure 10 - Installation wizard end with success....20
Figure 11 - Installation reboot 21
Figure 12 - Empty Licence Box 22
Figure 13 - Insert a Valide Click&DECiDE Licence 23
Figure 14 - Main log Source Configuration Screen....24
Figure 15 - Device Type Configuration 25
Figure 16 - Network Configuration....25
Figure 17 - Database Configuration 26
Figure 18 - Scheduled Tasks Configuration....26
Figure 19 - Web Portal Configuration 26
Figure 20 - Log Archive Configuration 27
Figure 21 - License Certificate Configuration 27
Figure 22 - Valid License Sample....28
Figure 23 - Invalid License message....29
Figure 24 - Adding devices in Click&DECiDE 30
Figure 25 - Practice : select Fortinet UTM device 31
Figure 26 - Practice : Configure Fortinet UTM Device 31
Figure 27 - Log File Acquisition Settings 32
Figure 28 - Log Source configuration, Flat File or Syslog 32
Figure 29 - Log Time Zone Settings....33
Figure 30 - Log Acquisition and Treatment Settings....34
Figure 31 - Log Acquisition Configuration....35
Figure 32 - Flat File device properties 35
Figure 33 - Syslog device properties 35
Figure 34 - Log Treatment Configuration 36
Figure 35 - Network Connection Configuration 37
Figure 36 - Network Connection Change....38
Figure 37 - Database Settings 39

Figure 38 - Database Connection Settings....................40
Figure 39 - Connection to the Local Database....................41
Figure 40 - Connection to the Remote Database....................41
Figure 41 - Database Connection test message....................42
Figure 42 - Database Update Settings....................42
Figure 43 - Database Time Zone Settings....................43
Figure 44 - Scheduled Task Settings....................44
Figure 45 - Consolidation, Aggregation, Purge and Report Tasks Settings....................45
Figure 46 - Purge Settings....................45
Figure 47 - Web Portal Settings....................46
Figure 48 - Web Portal Authentication Mode....................46
Figure 49 - Mail Server Settings....................47
Figure 50 - Mail Action Settings....................47
Figure 51 - Log Archive Settings....................49
Figure 52 - Log Storage Settings....................49
Figure 53 - Log Vault General Settings....................50
Figure 54 - Device Log File Archive Settings....................51
Figure 55 - Practice: Log Treatment Archive selection....................52
Figure 56 - Add Device Logs to Archive....................53
Figure 57 - General Archive File Setting....................54
Figure 58 - Security Archive File Setting....................54
Figure 59 - Transfer Archive Files....................55
Figure 60 - Transfer Archive File Settings....................55
Figure 61 - Updating Log Source Configuration Settings....................57
Figure 62 - Log Source Configuration Update overwrite previous settings....................57
Figure 63 - Log Source Configuration Update process bar....................58
Figure 64 - Configuration Updated....................58

Course Goals

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

1. Product Overview

1.1. Product Range

In this manual, we are going to present Click&DECiDE NSI product line.

1.1.1. Click&DECiDE NSI Professional Package

Click&DECiDE NSI Professional collects disparate event logs from heterogeneous vendor from a standard supported device list. You can generate scheduled or dynamic categorized Dashboard reports. Click&DECiDE NSI Professional also provides advanced dynamic cross-tables or Cubes focused point-and-click data analysis from any angle. The archival module stores logs in native and enriched formats and securely archives them into a log vault to ensures secure legal long-term archival.

1.1.2. Click&DECiDE NSI Enterprise Package

Click&DECiDE NSI Enterprise collects disparate event logs from heterogeneous vendor from all types of devices; know in the standard supported device list as well as unknown log source, using our open regular expression engine. You can generate scheduled or dynamic categorized Dashboard reports. Click&DECiDE NSI Enterprise also provides advanced dynamic cross-tables or Cubes focused point-and-click data analysis from any angle. The archival module stores logs in native and enriched formats and securely archives them into a log vault to ensures secure legal long-term archival. The alerting and correlation engine allow users to set-up real time correlations and events alerts send by multiple mean (eMail, RSS feed, web parts information or alerts, SNMP traps, syslog…)

1.1.3. Click&DECiDE BAI Express Edition

Click&DECiDE BAI Express allow users to access any types of structured database, create ad Hoc Queries and ad hoc Reports, create OLAP Cube from all Database[1] and Interactive Dashboard. The execution of reports can be done on a local PC only. All output formats are available among PDF, Excel, HTML, XML and others.

1.1.4. Click&DECiDE BAI Standard Edition

Click&DECiDE BAI Standard allow users to access any types of structured database, create ad Hoc Queries and ad hoc Reports, create OLAP Cube from all Database and

[1] Click&DECiDE, any Edition, can access many data sources, using a native and direct access engine or using an ODBC interface.
Native Direct Access (SQL Server, Oracle, iSeries-AS/400 TCP/IP, DB2-UDB)
Access through ODBC Drivers (Excel, MySQL, Informix…)

Interactive Dashboard. Reports projects can be shared within Click&DECiDE BAI Standard users. All output formats are available among PDF, Excel, HTML, XML, Txt, CSV, Databases and others.

1.1.5. Click&DECiDE BAI Professional Edition

Click&DECiDE BAI Professional allow users to access any type of structured database, create ad Hoc Queries and ad hoc Reports, create OLAP Cube from all Database and Interactive Dashboard. Reports projects can be shared within Click&DECiDE BAI Professional users. All output formats are available among PDF, Excel, HTML, XML, Txt, CSV, Databases and others. Click&DECiDE BAI Professional users can access the information throw user’s profiled web portal to generate in real-time, or schedule reports, cube, and dashboard. The scheduled results can be delivered via email, RSS Feed, Web Parts or Share Point Web Parts and Web Queries.

1.1.6. Click&DECiDE BAI Enterprise Edition

Click&DECiDE BAI Enterprise allow users to access any type of structured database, create ad Hoc Queries and ad hoc Reports, create OLAP Cube from all Database and Interactive Dashboard. Reports projects can be shared within Click&DECiDE BAI Enterprise users. All output formats are available among PDF, Excel, HTML, XML, Txt, CSV, Databases and others. Click&DECiDE BAI Enterprise users can access the information via user’s profiled web portal to generate in real-time, or schedule reports, cube, and dashboard. The scheduled results can be delivered via email, RSS Feed, Web Parts or Share Point Web Parts and Web Queries. Profiling and Models can be applied to filter data delivery and report access only to the correct user. Also, Intelligence can be applied to Reports and alerting can be produced based on report and query results.

1.1.7. Product Modules

Features & Functions	BAI				NSI	
	Express Edition	Standard Edition	Professional Edition	Enterprise Edition	Professional Package	Enterprise Package
Acquisition / Aggregation / Maintenance						
Structured Data (access and insertion)						
MS SQLServer	✓	✓	✓	✓	✓	✓
Oracle, UDB & ODBC	✓	✓	✓	✓		
Other Data access (Excel, Analysis services)	✓	✓	✓	✓		
Unstructured Data (number of events per Day)						
Syslog, Flat File, WMI Acquisition (1)				✓	✓	✓
Other Acquisition (Radius, SNMP, LEA)					✓	✓
Data enrichment (LDAP, SQL, RDNS…)				✓	✓	✓
Event / Information filtering				✓		✓
Database Maintenance Scheduling				✓	✓	✓
Information Delivery via Desktop						
Creation & execution:						
Ad Hoc Queries and ad hoc Reports	✓	✓	✓	✓		
OLAP Cube file Creation from all Database	✓	✓	✓	✓		
Interactive Dashboard	✓	✓	✓	✓		
Execution of reports created by user only	✓					
Set of pre-defined packaged reports by default						
Delivery Method:						
Real Time	✓	✓	✓	✓		
Delivery Format:						
PDF, Microsoft & Others (Txt, CSV …)	✓	✓	✓	✓		
HTML, XML	✓	✓	✓	✓		
User Profile specific information delivery						
Modeling & Filtering				✓		
User Profile management:						
Windows, MS AD, LDAP, Radius			✓	✓		
Information Delivery via Web Portal						
Execution of pre-defined packaged reports:						
Ad Hoc Queries & Reports					✓	✓
OLAP Cubes					✓	✓
Delivery Method:						
Real Time & Scheduled			✓	✓	✓	✓
Automation			✓	✓		
Delivery Format:						
HTML, XML & PDF			✓	✓	✓	✓
Microsoft & Other (Txt, CSV …)			✓	✓		
RSS Feed or email, or via shortcuts			✓	✓		
Web Parts & Share Point Web Parts, Web Query			✓	✓		
User Profile specific information delivery						
Modeling & Filtering				✓		
User Profile management:						
Windows, MS AD, LDAP, Radius			✓	✓	✓	✓
Advanced Analysis, Correlation, Alerting, and Forensic						
Data Correlation:						
OLAP Cube Analysis	✓	✓	✓	✓	✓	✓
Interactive Reports (inc drill down)			✓	✓	✓	✓
Interactive Dashboard	✓	✓	✓	✓		✓
Real time alert correlation						✓
Forensic analysis:						
OLAP Cube Analysis	✓	✓	✓	✓	✓	✓
Interactive Reports (inc drill down)			✓	✓	✓	✓
Interactive Dashboard	✓	✓	✓	✓		
Combined criteria based alerting on KPI s						
RSS Feed or email, or through shortcuts				✓		
Web Parts				✓		
Other (Syslog, SNMP Trap…)				✓		
Archiving for audit, and regulatory compliance						
Unstructured data archiving in native format					✓	✓
Archive signature, compression and number					✓	✓
Archive replay					✓	✓
Powerful Toolkit						
Customization / Customized Report Model	✓	✓	✓	✓		
Skin Customization				✓		
Unstructured data universal parser						✓
Tabular data universal parser						✓

Table 1 - Product Module

1.2. Architecture

Let’s take a closer look at the architecture behind Click&DECiDE NSI’s solutions.

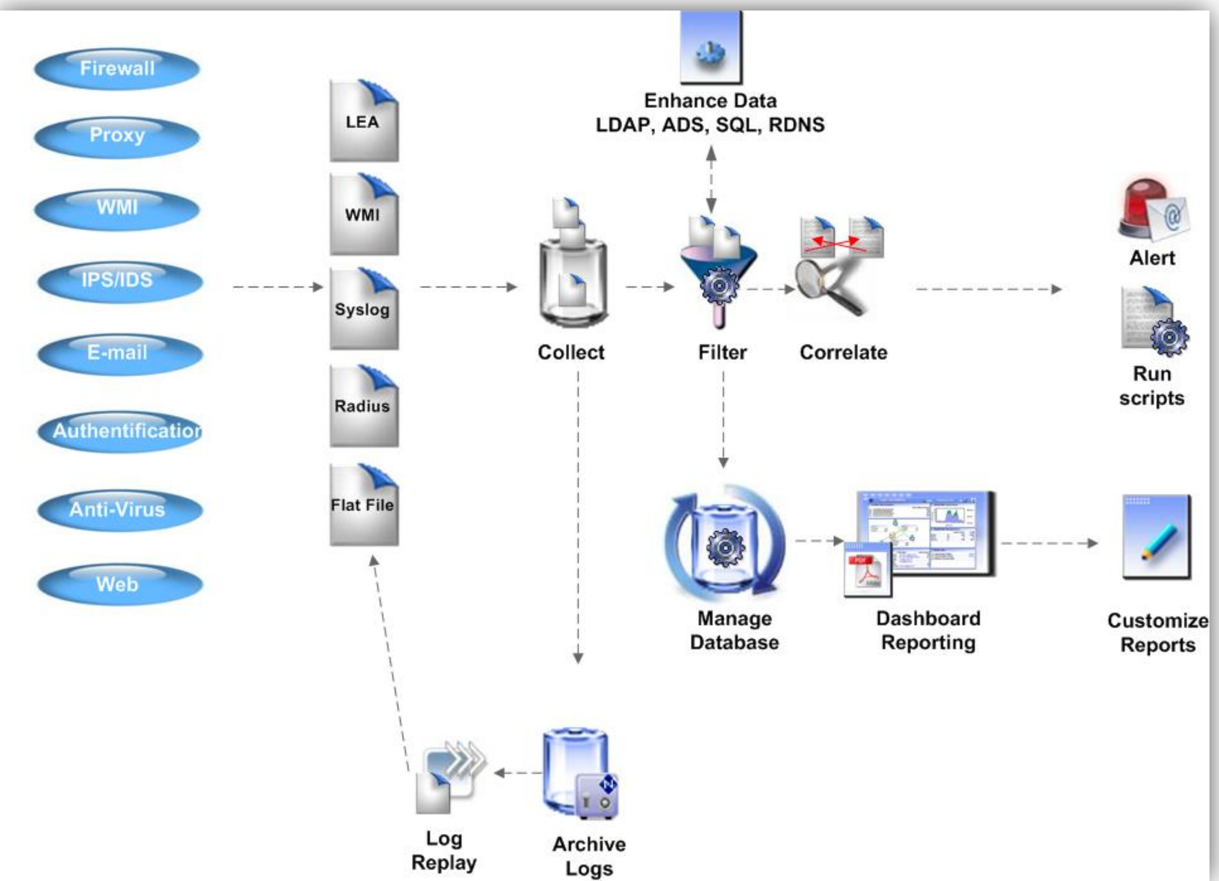


Figure 1 - Process Architecture

Step 1: Log Collection

- From Heterogeneous Devices
- We can note that Click&DECiDE NSI supports the following major device categories currently on the market: Firewall, Proxy, Microsoft WMI (Windows Management Instrumentation), IPS (Intrusion Prevention System), IDS (Intrusion Detection System), E-mail, Authentication, Content Filtering (Threats, Virus, Spam…), Web.
- With a Broad Range of Log Formats
- Click&DECiDE NSI collects disparate event data from all your heterogeneous devices. Event data is collected in the following formats: Check Point LEA, Microsoft WMI (Windows Management Instrumentation); Syslog, Radius, SNMP, SQL, ODBC, Flat File and CSV. Click&DECiDE NSI collects you log data in real-time 24/7.

Step 2: Log Archival

- The data collected is then stored via the Click&DECiDE NSI Log Archive module to ensure its integrity over the long-term.
- The data includes a digest, it is compressed and encrypted before being archived in the Log Vault.

Step 3: Log Filtering & Data Enhancement

- The Click&DECiDE NSI ULA (Universal Log Analyzer) Filter Engine standardizes filters and analyses the event data. Click&DECiDE NSI further enhances the data.
- Click&DECiDE NSI's Filter Engine guarantees flexibility and an ease of use while preserving its ability to be a powerful and precise tool for analysis.
- Each Click&DECiDE NSI Filter Engine enables you to insert several tens of millions of events in the database per day.

Step 4: Database Management

- Click&DECiDE NSI aggregates, consolidates and purges your security event data in the Click&DECiDE database thanks to its automated Database management tasks.
- Scheduled aggregation and purge features enable Click&DECiDE NSI to reduce the size of your database volume by 25. Intuitive drill-down to the information you need.

Step 5: Dashboard Creation

- Dashboard generation is automated and can easily be scheduled.
- Click&DECiDE NSIs dashboards enable real-time advanced integrated visual charting.
- The powerful drill-down features enable the user to go directly to the detailed information they need.
- The navigation features enable users to go to the sections they need and perform historical trending by navigating from day-to-day or month-to-month in a click.

Step 6: Customizing Reports

- Thanks to the Click&DECiDE NSI Tool Kit you can create Ad Hoc reports focusing on your company's look and feel and pinpointed to the alternative view you want to study.

Step 7: Correlation and Alerting

- Click&DECiDE NSI's correlation features enable you to rapidly detect violations and identify vulnerabilities.

- The Click&DECiDE NSI Alerting & Correlation Console provides you with real-time alerting and Zero Day protection.
- Click&DECiDE NSI centralizes displays and sends trusted alerts to your IT Staff in real-time via e-mail, pager and SNMP traps to help them quickly isolate and resolve potential threats and automate protection.

1.3. Advanced Installation Architectures

Several architecture can set-up depending on your network architecture or your log volume.

A classic architecture that can be used with Click&DECiDE NSI is the Appliance #1 architectures

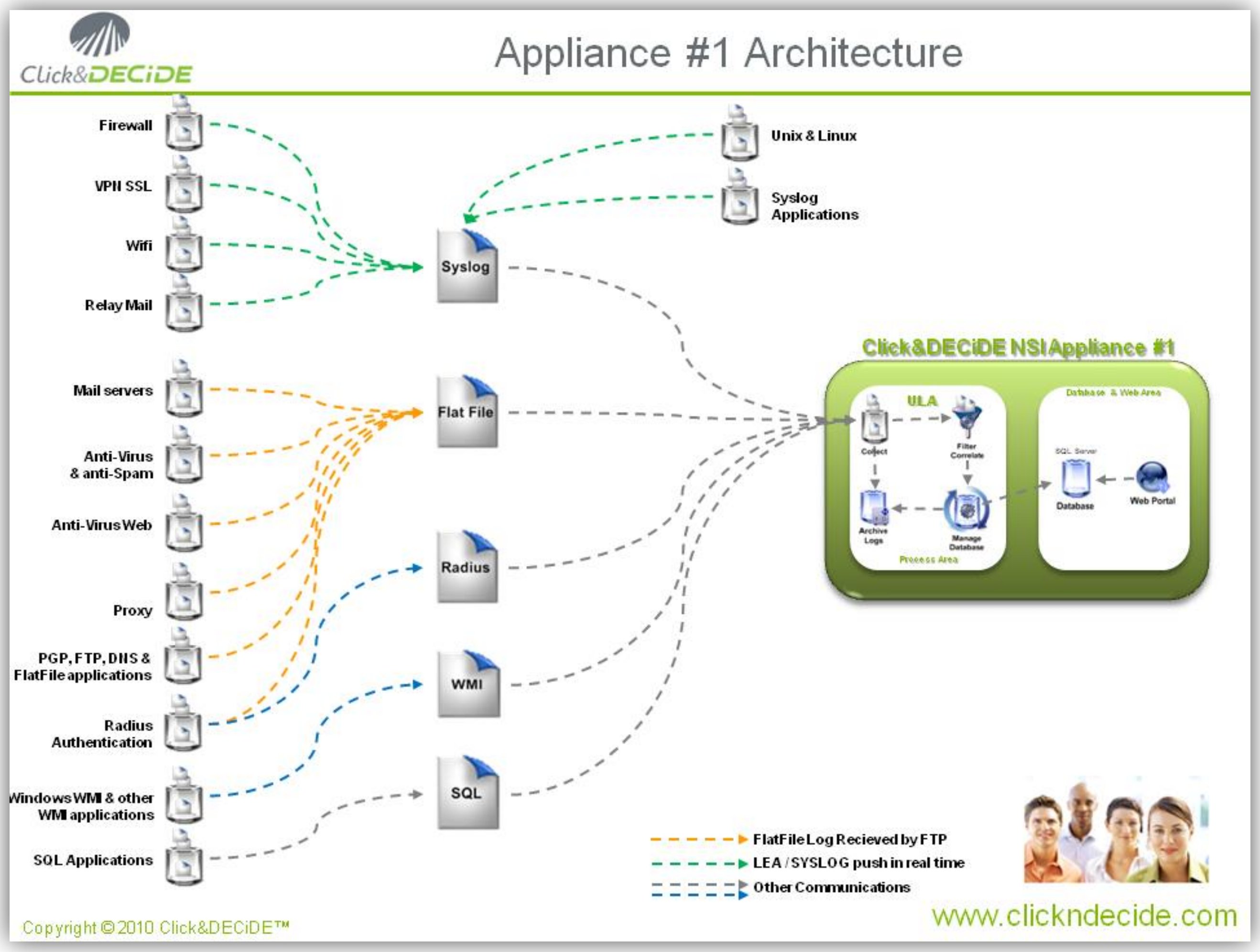


Figure 2 - Appliance #1 Architecture

For more architecture, please check our web site for the following document:
➔ ClicknDECiDE_NSI_Architecture_implementation

1.4. Hardware System Requirements

The minimum hardware configuration to run Click&DECiDE NSI is:

- Single Processor Dual Core.
- 2 Gb RAM.
- 80 Gb usable disk.

The recommended hardware configuration to run Click&DECiDE NSI is:

- Memory: 4 to 8 Go
- Processors: 1 to 2 quad cores CPUs
- Hard Disk: 300 Gb to 600 Gb usable space, 10k or 15k speed
- Raid: 1 or 5
- Disk Cache: High

1.5. Software System Requirements

The software environment expected is server type operating system.

Systems & Database:

- Windows ® 2003 (minimum SP2) 32bit
  - Microsoft SQL Server 2005 (SP3) 32bit
  - Microsoft SQL Express 2005
- Windows ® 2008 (minimum SP1) 32bit
  - Microsoft SQL Server 2008 (SP1) 32bit
  - Microsoft SQL Express 2008
- Windows ® 2008 (minimum SP1) 64bit
  - Microsoft SQL Server 2008 (SP1) 64bit

Note that if you use Microsoft SQL Express 2005/2008, you will be limited in concurrent access to the database and also in quantity of logs (less than 250.000 EPD [Event Per Day]).
We do not recommend Microsoft SQL Express for a production environment.

- Other Software requested:
  - Adobe Acrobat Reader (Minimum v7)
  - Internet Explorer 7.0 (Minimum SP1) or higher version of IE
  - IIS (Internet Information Service)
  - Framework .NET 3.5 (Minimum SP1)
  - IIS must be installed before .NET
  - *If not, or if you are not sure*, please run the following command for the .NET directory:
    - .NET Directory: C:\Windows\Microsoft.NET\Framework\v2.0.50727
    - Command to run: **aspnet_regiis –i**

2. Install Click & DECiDE - NSI

> **Note:** the operations described in this article require a full access to the computer. Be sure to be logged as an Administrator.

2.1. Turning on the Required IIS Features

IIS is a Windows feature, to launch the Turn Windows Features On or Off module please follow the steps below:

1. Select **Start> Control Panel**.
2. Click **Programs and Features**.
3. Click **Turn Windows Features On or Off**.
4. Select the following Internet Information Services features:
5. **Web Management Tools**
   a. **IIS Management Console**
   b. **IIS Management Scripts and Tools**
   c. **IIS Management Service**
6. **World Wide Web Services**
   a. **Applications Development Features**
      i. **ASP.NET**
      ii. **ASP**
   b. **Security**
      i. **Basic Authentication**
      ii. **Windows Authentication**
7. Click **OK**.

2.2. Download and install the Framework .NET 3.5 SP1

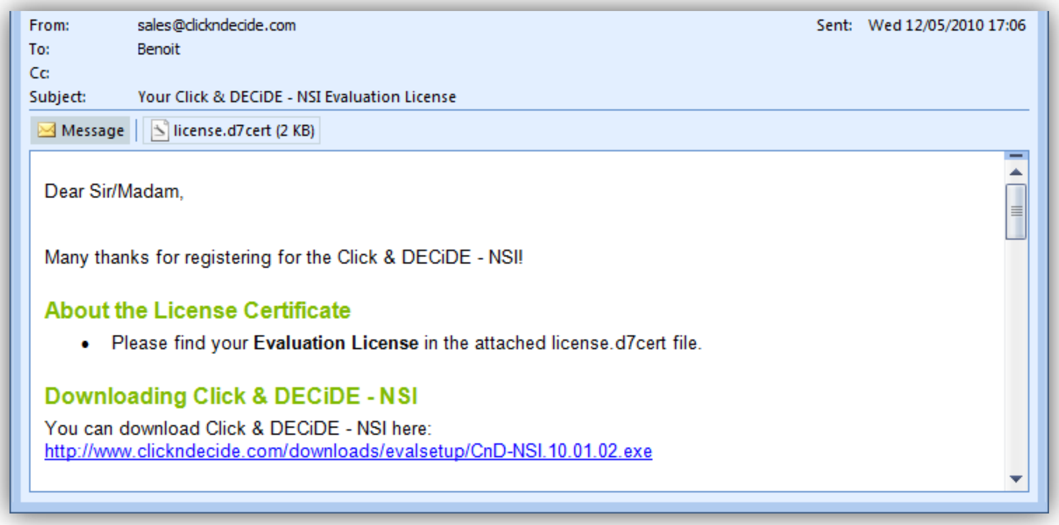
Click&DECiDE need the Framework .NET to work properly. We recommend you to install the latest version before installing Click&DECiDE. Follow the link and install the framework:

http://www.microsoft.com/downloads/details.aspx?familyid=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en

2.3. Download and extract the Click&DECiDE NSI setup

1. Check that you have downloaded the latest version of Click & DECiDE NSI. If you are not sure, please download the latest release of Click&DECiDE NSI from our web site:
   http://license.clickndecide.com/downloads/cndnsi_request.aspx

2. Download from the received email link, the latest release of Click&DECiDE.



From: sales@clickndecide.com
To: Benoit
Cc:
Subject: Your Click & DECiDE - NSI Evaluation License
Sent: Wed 12/05/2010 17:06

Dear Sir/Madam,

Many thanks for registering for the Click & DECiDE - NSI!

About the License Certificate

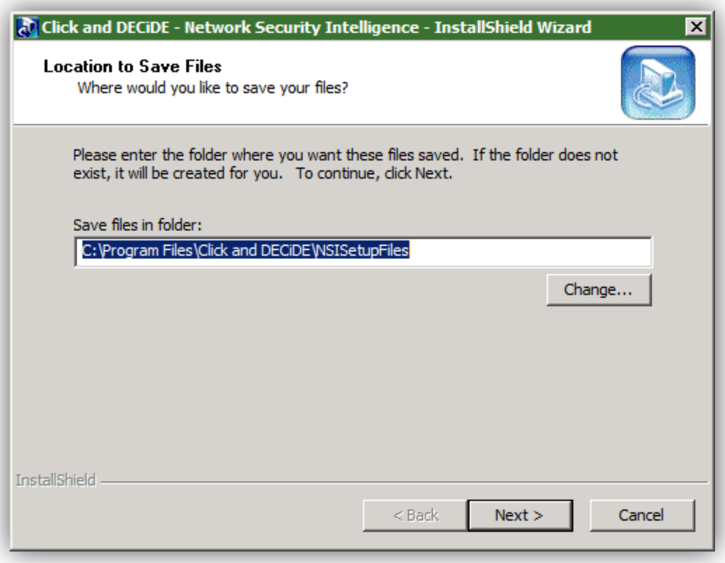
- Please find your **Evaluation License** in the attached license.d7cert file.

Downloading Click & DECiDE - NSI

You can download Click & DECiDE - NSI here:
http://www.clickndecide.com/downloads/evalsetup/CnD-NSI.10.01.02.exe

Figure 3 - Licence Email sample

3. Save the license file on the disk, if you are using this guide for an evaluation. Otherwise, save the license file received following your product order.
4. Choose where you want to extract the files required for the installation.



Click and DECiDE - Network Security Intelligence - InstallShield Wizard

Location to Save Files
Where would you like to save your files?

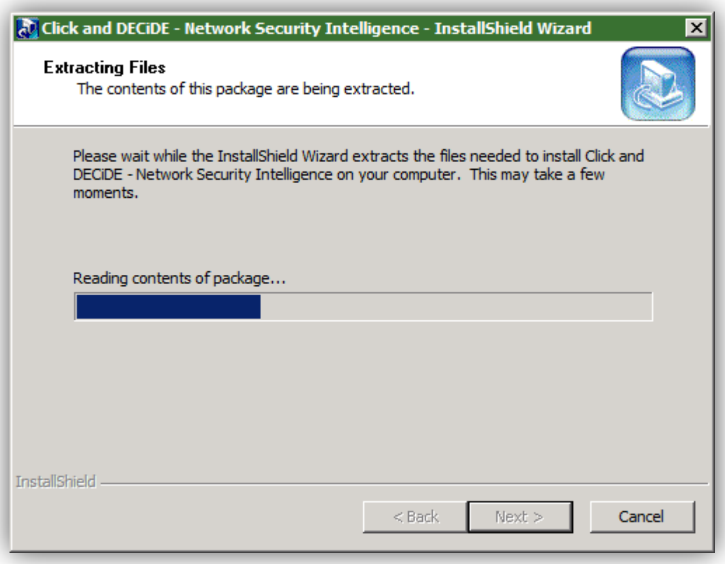
Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next.

Save files in folder:
C:\Program Files\Click and DECiDE\NSISetupFiles

Change...
InstallShield
< Back
Next >
Cancel

Figure 4 - Save File Installation path

5. Click **Next**.
6. Wait for the extraction to complete.



Click and DECiDE - Network Security Intelligence - InstallShield Wizard

Extracting Files

The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install Click and DECiDE - Network Security Intelligence on your computer. This may take a few moments.

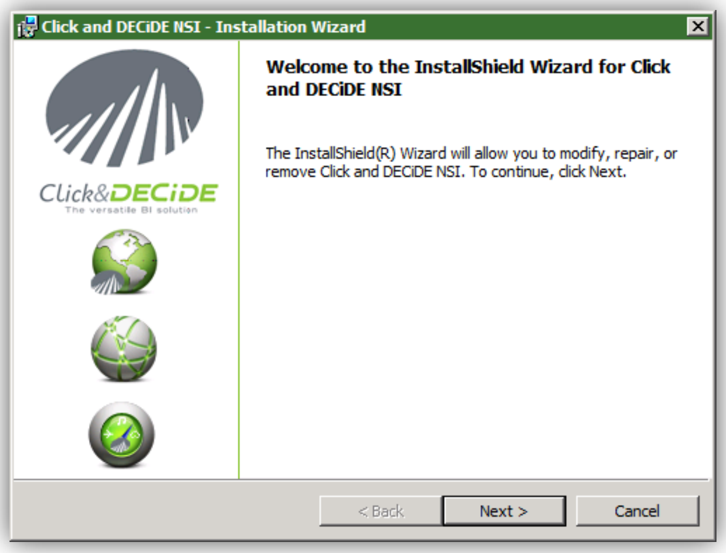
Reading contents of package...

Figure 5 - File extraction process

7. The Click and DECiDE - NSI Installation Wizard will launch.

2.4. The Click and DECiDE - NSI Installation Wizard

1. If you have any prerequisites, click **Install** to install them.



Click and DECiDE NSI - Installation Wizard

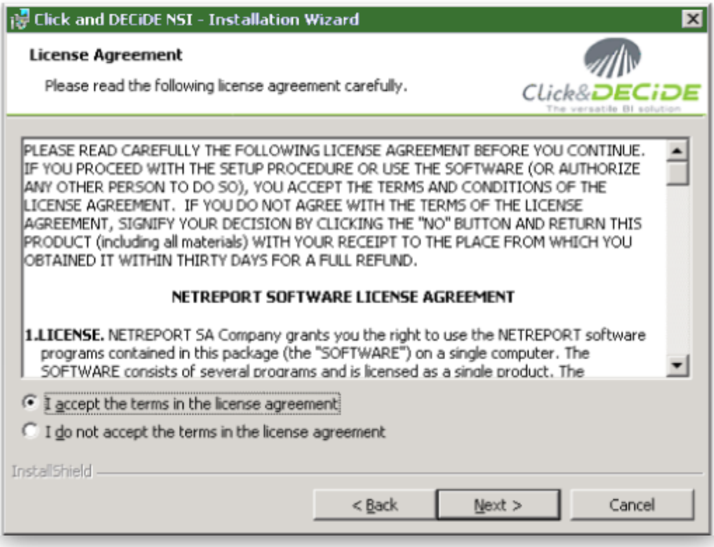
Welcome to the InstallShield Wizard for Click and DECiDE NSI

The InstallShield(R) Wizard will allow you to modify, repair, or remove Click and DECiDE NSI. To continue, click Next.

Figure 6 - Click&DECiDE Welcome Screen

2. On the Welcome to Installshield Wizard for Click and DECiDE - NSI dialog, click **Next**.

3. On the License Agreement dialog, read the license agreement and select **I accept the terms in the license agreement to continue.**


Click and DECiDE NSI - Installation Wizard
License Agreement
Please read the following license agreement carefully.
Click&DECiDE
The versatile BI solution

PLEASE READ CAREFULLY THE FOLLOWING LICENSE AGREEMENT BEFORE YOU CONTINUE. IF YOU PROCEED WITH THE SETUP PROCEDURE OR USE THE SOFTWARE (OR AUTHORIZE ANY OTHER PERSON TO DO SO), YOU ACCEPT THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS OF THE LICENSE AGREEMENT, SIGNIFY YOUR DECISION BY CLICKING THE "NO" BUTTON AND RETURN THIS PRODUCT (including all materials) WITH YOUR RECEIPT TO THE PLACE FROM WHICH YOU OBTAINED IT WITHIN THIRTY DAYS FOR A FULL REFUND.

NETREPORT SOFTWARE LICENSE AGREEMENT

1.LICENSE. NETREPORT SA Company grants you the right to use the NETREPORT software programs contained in this package (the "SOFTWARE") on a single computer. The SOFTWARE consists of several programs and is licensed as a single product. The

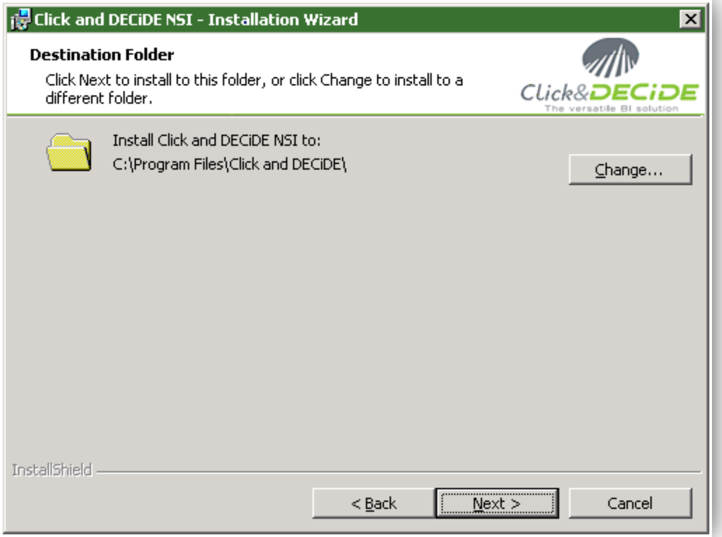
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Figure 7 - Click&DECiDE Licence Agreement

4. Click **Next**.
5. On the Destination Folder dialog, select a folder on a partition with enough hard disk space. See recommendations:

http://www.clickndecide.com/downloads/WebDoc/Support/ClicknDECiDE_NSI_Database_Archive_Disk_Size.zip

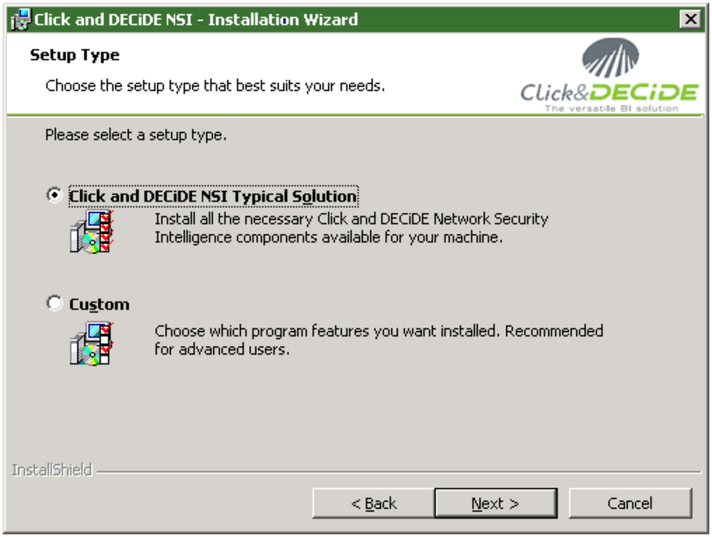


Click Next to install to this folder, or click Change to install to a different folder.

Install Click and DECiDE NSI to:
C:\Program Files\Click and DECiDE\

Figure 8 - Installation destination folder

6. Click Next.
7. On the Setup Type dialog, choose **Click and DECiDE NSI Typical Solution**.



Click and DECiDE NSI - Installation Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Click and DECiDE NSI Typical Solution**

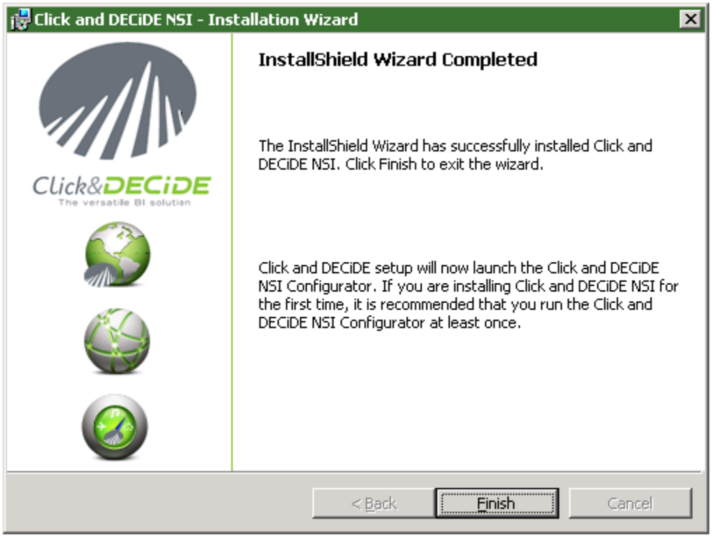
Install all the necessary Click and DECiDE Network Security Intelligence components available for your machine.

○ **Custom**

Choose which program features you want installed. Recommended for advanced users.

Figure 9 - Installation type selection

8. Click **Next**.
9. Click **Install**.
10. Wait for the installation to complete.
11. On the Installshield Wizard Completed dialog, Click **Finish**.



Click and DECiDE NSI - Installation Wizard

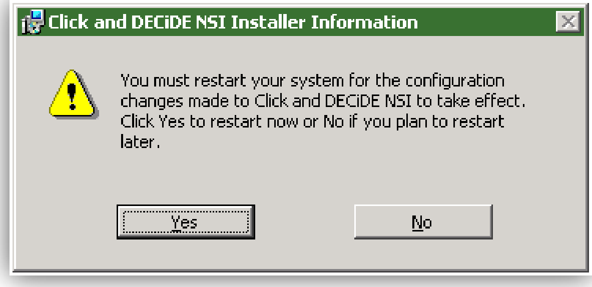
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Click and DECiDE NSI. Click Finish to exit the wizard.

Click and DECiDE setup will now launch the Click and DECiDE NSI Configurator. If you are installing Click and DECiDE NSI for the first time, it is recommended that you run the Click and DECiDE NSI Configurator at least once.

Figure 10 - Installation wizard end with success

12. The installation asks for a reboot. Save all your documents and close all your application and click **Yes**.



Click and DECiDE NSI Installer Information

You must restart your system for the configuration changes made to Click and DECiDE NSI to take effect. Click Yes to restart now or No if you plan to restart later.

Figure 11 - Installation reboot

Congratulation, the installation is now finished!

2.5. Suggestions for Practice:

Follow the chapter 2.4 to install Click&DECiDE NSI software.

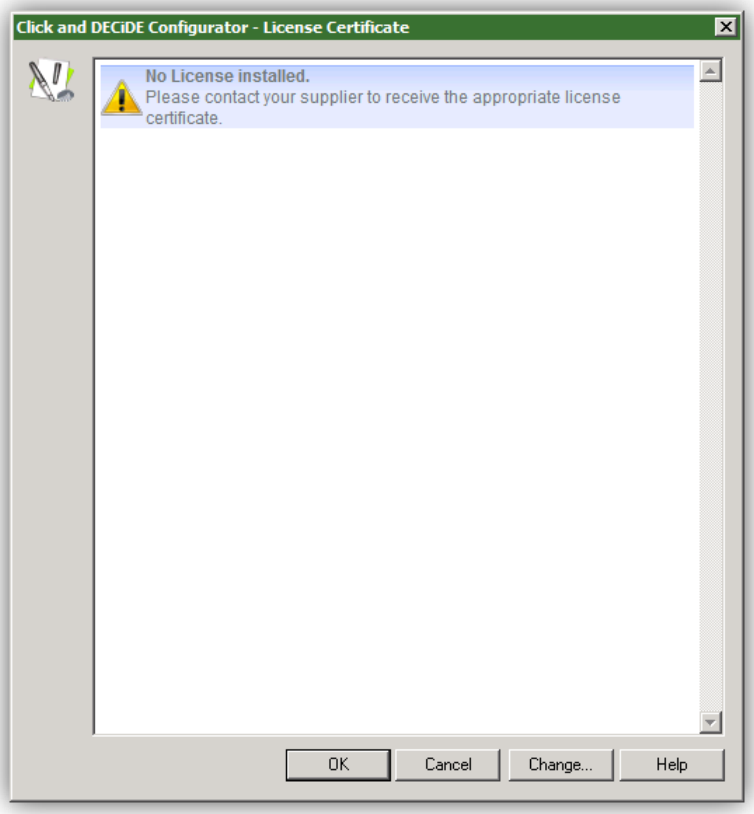
3. Working with Click&DECiDE NSI Log Source Configuration

If it is the first time you are configuring Click&DECiDE NSI then wait for the Click&DECiDE NSI Log Source Configuration to launch once you have completed the InstallShield Wizard.

Note that once you have configured Click&DECiDE NSI for the first time you can launch the Click&DECiDE NSI Log Source Configuration by selecting **Start> All Programs> Click and DECiDE> Network Security Intelligence> Log Source Configuration**.

3.1. Selecting a License Certificate

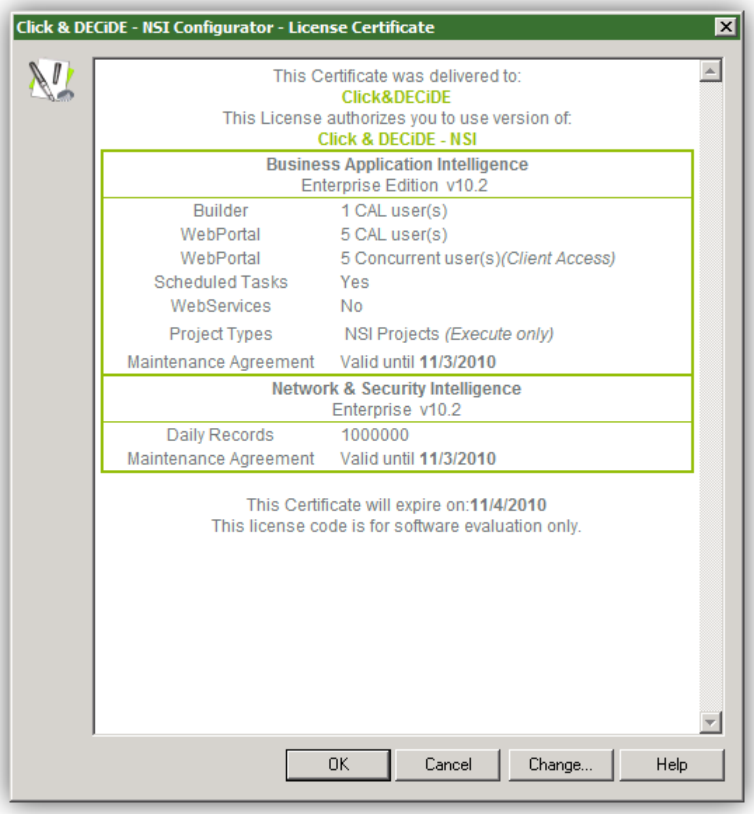
After rebooting your machine, the **Log Source Configuration** launches and asks for a License Certificate.



No License installed.
Please contact your supplier to receive the appropriate license certificate.

Figure 12 - Empty Licence Box

1. Click **Change…**
2. Select the License Certificate we sent you for Click&DECiDE NSI



Click & DECiDE - NSI Configurator - License Certificate

This Certificate was delivered to:
Click&DECiDE
This License authorizes you to use version of:
Click & DECiDE - NSI

Business Application Intelligence
Enterprise Edition v10.2

Builder	1 CAL user(s)
WebPortal	5 CAL user(s)
WebPortal	5 Concurrent user(s)*(Client Access)*
Scheduled Tasks	Yes
WebServices	No
Project Types	NSI Projects *(Execute only)*
Maintenance Agreement	Valid until **11/3/2010**

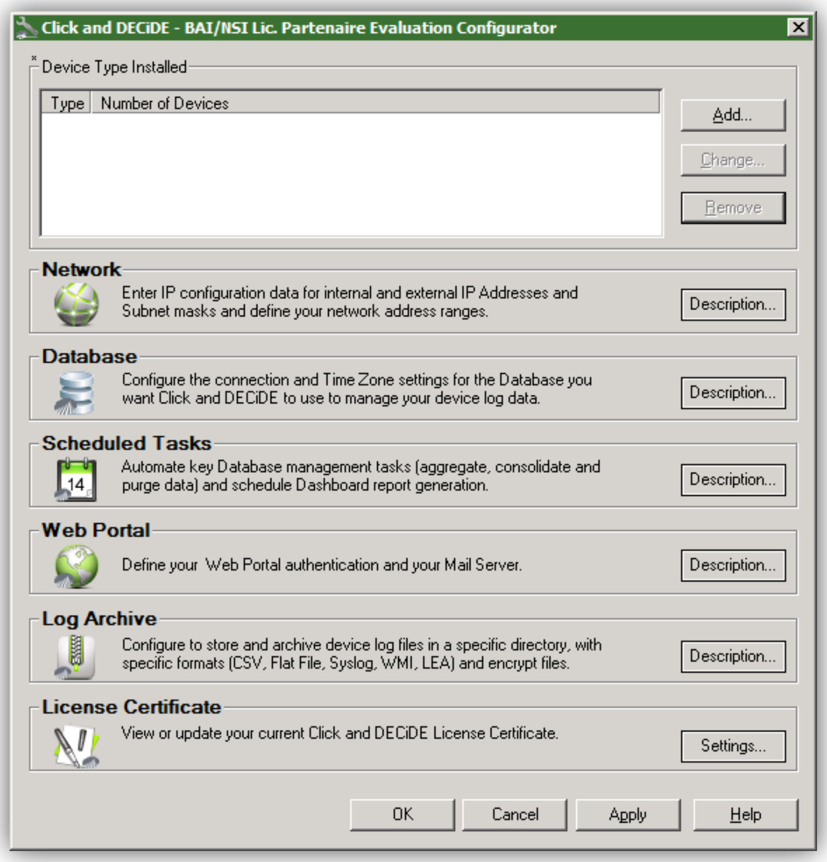
Network & Security Intelligence
Enterprise v10.2

Daily Records	1000000
Maintenance Agreement	Valid until **11/3/2010**

This Certificate will expire on:**11/4/2010**
This license code is for software evaluation only.

Figure 13 - Insert a Valide Click&DECiDE Licence

3.2. Working with the Log Source Configuration Screen



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator

Device Type Installed

Type	Number of Devices

Network

Enter IP configuration data for internal and external IP Addresses and Subnet masks and define your network address ranges.

Database

Configure the connection and Time Zone settings for the Database you want Click and DECiDE to use to manage your device log data.

Scheduled Tasks

Automate key Database management tasks (aggregate, consolidate and purge data) and schedule Dashboard report generation.

Web Portal

Define your Web Portal authentication and your Mail Server.

Log Archive

Configure to store and archive device log files in a specific directory, with specific formats (CSV, Flat File, Syslog, WMI, LEA) and encrypt files.

License Certificate

View or update your current Click and DECiDE License Certificate.

Figure 14 - Main log Source Configuration Screen

The Click&DECiDE NSI Log Source Configuration enables you to configure your device, network, database, scheduled tasks, Mail Server and Log Archive settings. The Log Source Configuration main page is divided into seven zones:

- Device Type Installed
- Network
- Database
- Scheduled Tasks
- WebPortal
- Log Archive
- License Certificate

3.2.1. Device Type Installed

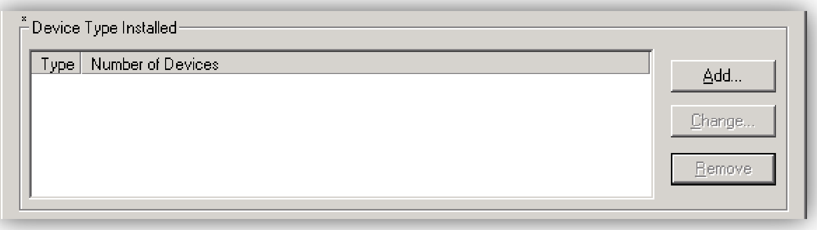


Figure 15 - Device Type Configuration

Enables you to add, change and remove devices.

Please note the following recommendations:

- Select at least one device in order to configure any of the other settings.
- Enable the **Generate Daily or Monthly Dashboard** check box in the **Log Treatment** zone for at least one device to configure Scheduled Tasks.
- Enable the **Archive Logs in Native Format and/or Archive Logs in Enriched CSV Format** to configure the Log Archive Settings. This ensures that both the Log generation for temporary Log Storage is enabled and that you have the possibility of selecting device logs to archive via Click&DECiDE NSI Log Vault.

Type: the type of third-party device.

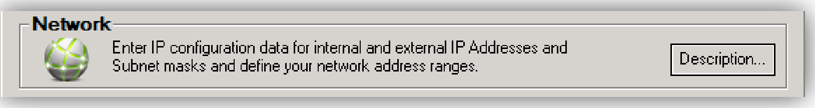
Number of Devices: the number of devices of this device type.

Add…: adds a device.

Change…: enables you to modify the settings you configured for a given device.

Remove: removes settings you configured via Click&DECiDE NSI for a device.

3.2.2. Network



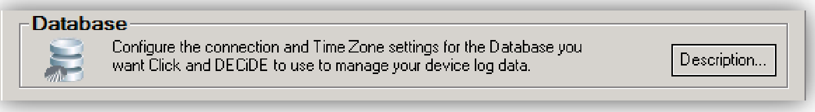
Enter IP configuration data for internal and external IP Addresses and Subnet masks and define your network address ranges.

Figure 16 - Network Configuration

Enables you to parameterize IP settings for internal and external IP addresses and Subnet masks and define your network address ranges. To configure Network settings:

- You must select at least one filter using RDNS Net Area in order to configure the Network settings, otherwise the **Description…** button will be displayed.
- Click **Settings…** to configure your Network settings.

3.2.3. Database



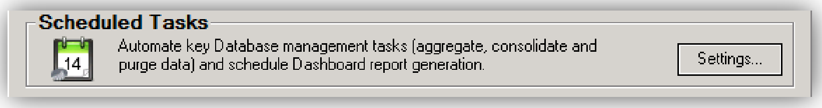
Configure the connection and Time Zone settings for the Database you want Click and DECiDE to use to manage your device log data.

Figure 17 - Database Configuration

Enables you to configure the database connection and time zone parameters for the Database (SQL or Oracle) that you want Click&DECiDE NSI to use to manage your device log data. To configure Database settings:

- Select a device from the **Device Type Installed** zone, click **Change…** and ensure the following option is selected for at least one device:
  - Generate Daily and Monthly Dashboards.
- Click **Settings…** to configure your Database settings.

3.2.4. Scheduled Tasks



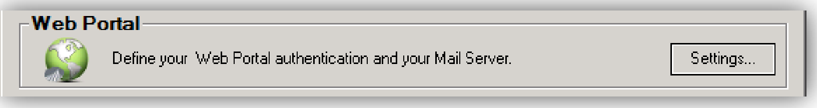
Automate key Database management tasks (aggregate, consolidate and purge data) and schedule Dashboard report generation.

Figure 18 - Scheduled Tasks Configuration

Enables you to automate the Consolidation, Aggregation, Purge and Report Tasks everyday at the time you wish.

- Click **Settings…** to configure your Scheduled Tasks settings and the database purge settings.

3.2.5. Web Portal



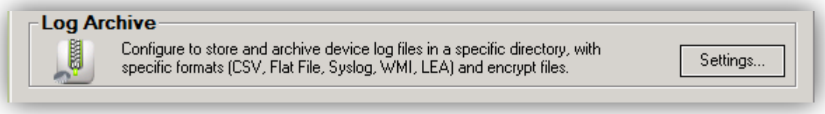
Define your Web Portal authentication and your Mail Server.

Figure 19 - Web Portal Configuration

Enables you to define the authentication method to access the web portal and the Mail Server along with the e-mail addresses you want Click&DECiDE NSI to use to send alerts. To configure the Web Portal settings:

- You must select a device from the **Device Type Installed** zone. Click **Add…** to add a device. Configure the settings you want for the device.
- Click **Settings…** to configure your Web Portal settings.

3.2.6. Log Archive



Log Archive

Configure to store and archive device log files in a specific directory, with specific formats (CSV, Flat File, Syslog, WMI, LEA) and encrypt files.

Figure 20 - Log Archive Configuration

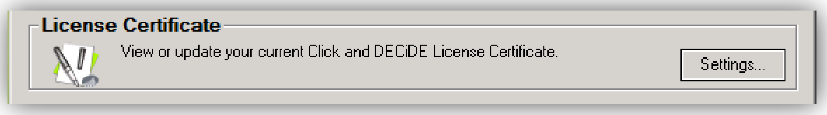
Click&DECiDE NSI Log Archive includes two components, Click&DECiDE NSI Log Storage and Click&DECiDE NSI Log Vault:

- **Click&DECiDE NSI Log Storage:** generates files in Native and/or Enriched CSV format for temporary storage before they are archived by Click&DECiDE NSI Log Vault.
- **Click&DECiDE NSI Log Vault:** generate a digest (to verify data integrity), compresses and encrypts logs for long-term archival. Archived logs can be moved via local copy or FTP transfer.

Click&DECiDE NSI Log Archive therefore enables you to store and archive device log files in a specific directory, with specific formats (CSV (i.e. Comma Separated Values), Flat File, Syslog, WMI, LEA) and encrypt files. To configure Click&DECiDE NSI Log Archive Settings:

- You must select either a device with flat file format logs or the following Log Treatment for at least one device:
  - Archive Logs in Native Format
  - Archive Logs in Enriched CSV Format
- Click **Settings...** to configure your Click&DECiDE NSI Log Archive settings.

3.2.7. License Certificate



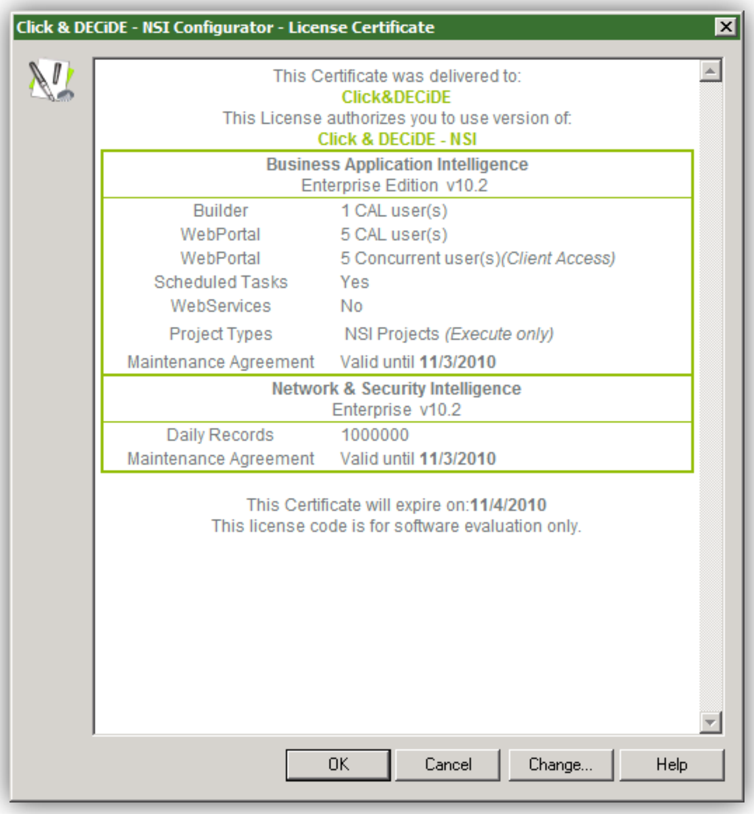
License Certificate

View or update your current Click and DECiDE License Certificate.

Figure 21 - License Certificate Configuration

The Click&DECiDE NSI Log Source Configuration checks the existence and validity of the License Certificate when it loads. If your License Certificate is valid the Click&DECiDE NSI Log Source Configuration will display the **Settings…** button in the **License Certificate** zone at the base of the Click&DECiDE NSI Log Source Configuration main screen.

If you click **Settings…** you will see the following **License Certificate** dialog box with the information concerning your specific License Certificate.



This Certificate was delivered to:
Click&DECiDE
This License authorizes you to use version of:
Click & DECiDE - NSI

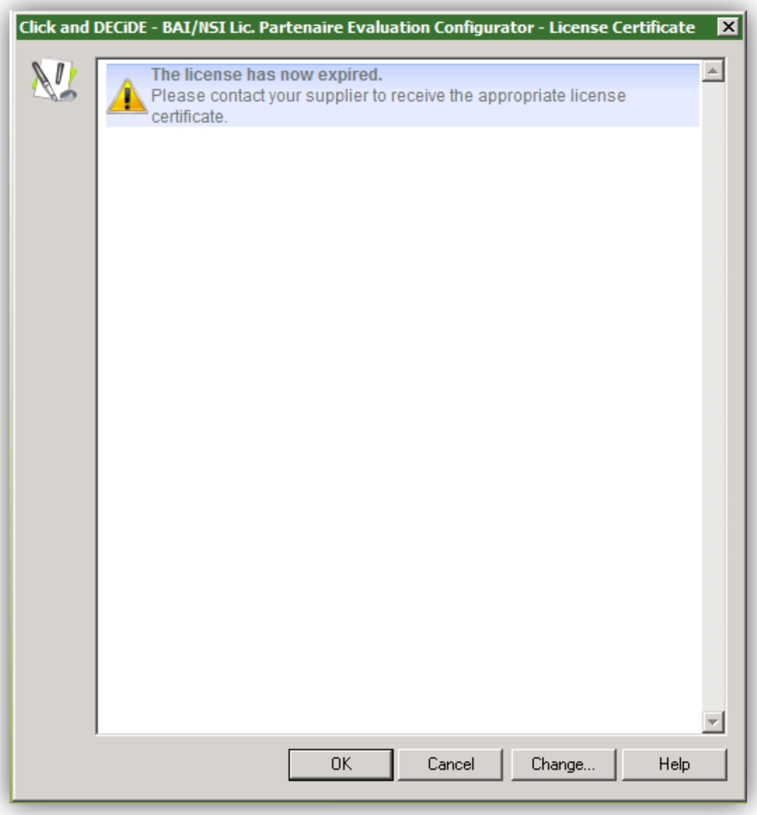
Business Application Intelligence Enterprise Edition v10.2	
Builder	1 CAL user(s)
WebPortal	5 CAL user(s)
WebPortal	5 Concurrent user(s)*(Client Access)*
Scheduled Tasks	Yes
WebServices	No
Project Types	NSI Projects *(Execute only)*
Maintenance Agreement	Valid until **11/3/2010**

Network & Security Intelligence Enterprise v10.2	
Daily Records	1000000
Maintenance Agreement	Valid until **11/3/2010**

This Certificate will expire on:**11/4/2010**
This license code is for software evaluation only.

Figure 22 - Valid License Sample

If your License Certificate is invalid the Log Source Configuration will display the following message:



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - License Certificate

The license has now expired.
Please contact your supplier to receive the appropriate license certificate.

Figure 23 - Invalid License message

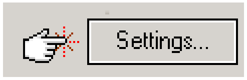
You must change your License Certificate. If you need a new License Certificate, please contact Click&DECiDE NSI's Sales team: sales@clickndecide.com

To change your License Certificate, click **Change…** and select the valid licence.d7cert file. Click **Open** and then **OK**.

3.2.8. Enabling the Description… button

- If a **Description…** button appears to the right of one of the Log Source Configuration zones, this indicates that you must do one or more of the following:
- Add a device, if you have not selected any devices.
- Select the Generate Daily and Monthly Dashboards check box in the Device Configuration Log Treatment zone.
- Select the Archive Logs in Native Format and/or Select Log in Enriched CSV Format check boxes in the Device Configuration Log Treatment zone.

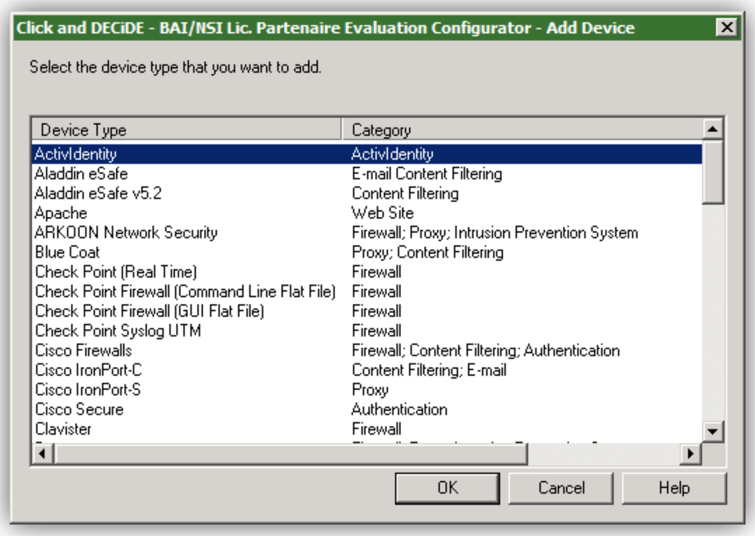
3.2.9. Working with Undefined Settings



Each time you see a hand icon next to **Settings…** this indicates that you have not yet parameterized these settings. You must click the button and configure the settings you want. Once this has been done the hand icon will disappear.

3.3. Working with Device Settings

3.3.1. Add Device


Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Add Device
OK
Cancel
Help

Select the device type that you want to add.

Device Type	Category
ActivIdentity	ActivIdentity
Aladdin eSafe	E-mail Content Filtering
Aladdin eSafe v5.2	Content Filtering
Apache	Web Site
ARKOON Network Security	Firewall; Proxy; Intrusion Prevention System
Blue Coat	Proxy; Content Filtering
Check Point (Real Time)	Firewall
Check Point Firewall (Command Line Flat File)	Firewall
Check Point Firewall (GUI Flat File)	Firewall
Check Point Syslog UTM	Firewall
Cisco Firewalls	Firewall; Content Filtering; Authentication
Cisco IronPort-C	Content Filtering; E-mail
Cisco IronPort-S	Proxy
Cisco Secure	Authentication
Clavister	Firewall

Figure 24 - Adding devices in Click&DECiDE

Device Type: the type of device you want to add. Scroll to select the device type you want to add. Click&DECiDE NSI presents the device types supported along with the device category.

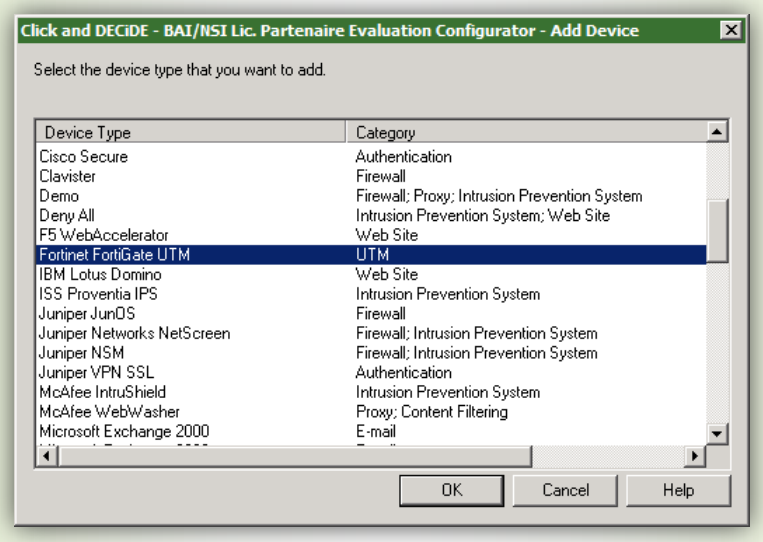
Category: Click&DECiDE NSI lists the following categories:

- Authentication
- Content Filtering
- E-mail
- Firewall
- Intrusion Prevention System (IPS)
- Proxy
- Router & Switches
- UTM
- Web Site
- WMI

Note: the devices that belong to several categories, for example Cisco Firewalls (which belongs to the Firewall, Content Filtering and Authentication categories), ARKOON Network Security (which belongs to the Firewall, Proxy and IPS categories). The following devices do not belong to the standard categories listed above: ActivIdentity, Radius, TrendMicro (some versions) and a few others.

3.3.2. Suggestions for Practice

1. Select **Fortinet FortiGate UTM** from the list.



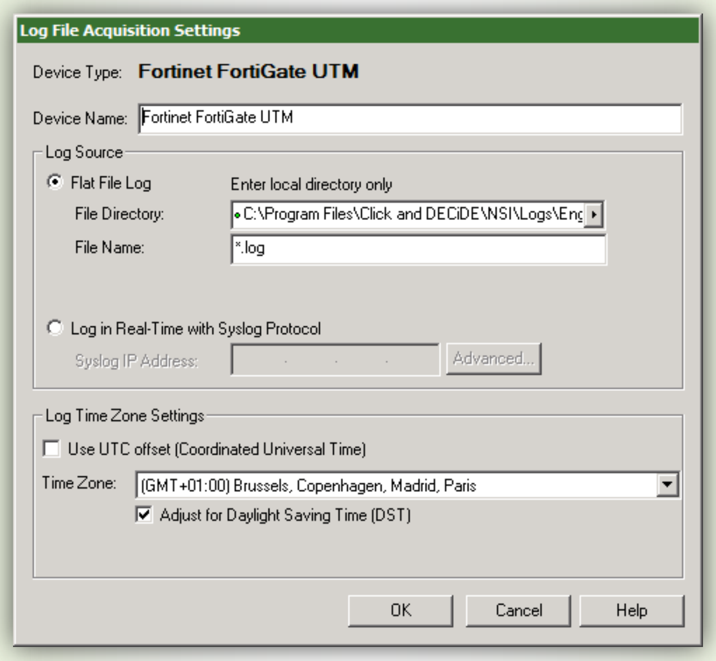
Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Add Device

Select the device type that you want to add.

Device Type	Category
Cisco Secure	Authentication
Clavister	Firewall
Demo	Firewall; Proxy; Intrusion Prevention System
Deny All	Intrusion Prevention System; Web Site
F5 WebAccelerator	Web Site
Fortinet FortiGate UTM	UTM
IBM Lotus Domino	Web Site
ISS Proventia IPS	Intrusion Prevention System
Juniper JunOS	Firewall
Juniper Networks NetScreen	Firewall; Intrusion Prevention System
Juniper NSM	Firewall; Intrusion Prevention System
Juniper VPN SSL	Authentication
McAfee IntruShield	Intrusion Prevention System
McAfee WebWasher	Proxy; Content Filtering
Microsoft Exchange 2000	E-mail

Figure 25 - Practice : select Fortinet UTM device

2. Click **OK**. The Log File Acquisition Settings dialog box appears.



Log File Acquisition Settings

Device Type: **Fortinet FortiGate UTM**

Device Name: Fortinet FortiGate UTM

Log Source

● Flat File Log — Enter local directory only

File Directory: C:\Program Files\Click and DECiDE\NSI\Logs\Eng

File Name: *.log

○ Log in Real-Time with Syslog Protocol

Syslog IP Address: . . .

Log Time Zone Settings

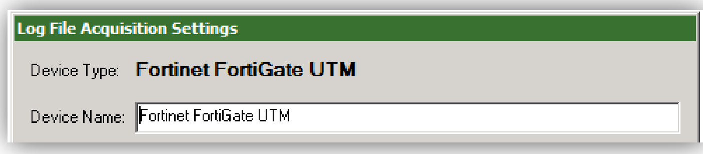
□ Use UTC offset (Coordinated Universal Time)

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

☑ Adjust for Daylight Saving Time (DST)

Figure 26 - Practice : Configure Fortinet UTM Device

3.3.3. Log File Acquisition Settings



Log File Acquisition Settings

Device Type: Fortinet FortiGate UTM

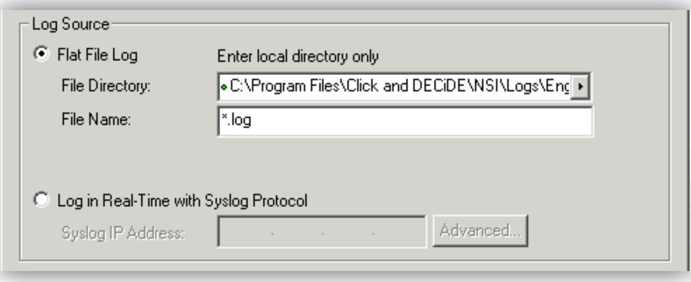
Device Name: Fortinet FortiGate UTM

Figure 27 - Log File Acquisition Settings

Device Type: default type of third-party device.

Device Name: the name you want to use for this device. For example, **Fortinet FortiGate UTM - Paris** (where you could add another **Fortinet FortiGate UTM** device with the Device Name, **Fortinet FortiGate UTM - London**).

Log Source:



Log Source

● Flat File Log

Enter local directory only

File Directory: C:\Program Files\Click and DECiDE\NSI\Logs\Eng

File Name: *.log

○ Log in Real-Time with Syslog Protocol

Syslog IP Address: . . .

Figure 28 - Log Source configuration, Flat File or Syslog

Define the log source that you want Click&DECiDE NSI to scan for log files.

Flat File Log: the default log format.

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

> The default File Directory is for demonstration only. For production, it is strongly recommended to use a directory on a different drive than the one where NSI is installed.

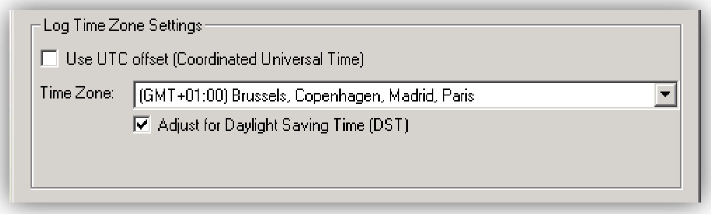
File Name: the default file name for your logs.

Log in Real-Time with Syslog Protocol: for logs with Syslog Protocol.

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

Advanced...: click here to configure advanced Syslog settings. The **Advanced Syslog Settings** dialog box appears and enables you to parameterize the Facility, Severity, Hostname and Process name for the IP Address you enter in the Syslog IP Address field.

Log Time Zone Settings



Log Time Zone Settings

□ Use UTC offset (Coordinated Universal Time)

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

☑ Adjust for Daylight Saving Time (DST)

Figure 29 - Log Time Zone Settings

Click&DECiDE NSI 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 NSI 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 NSI will simply leave the time data in UTC.

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 NSI 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.

Use UTC offset (Coordinated Universal Time): for Click&DECiDE NSI 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 where your device is physically located, ignore that option if your device is configured for Coordinated Universal Time.

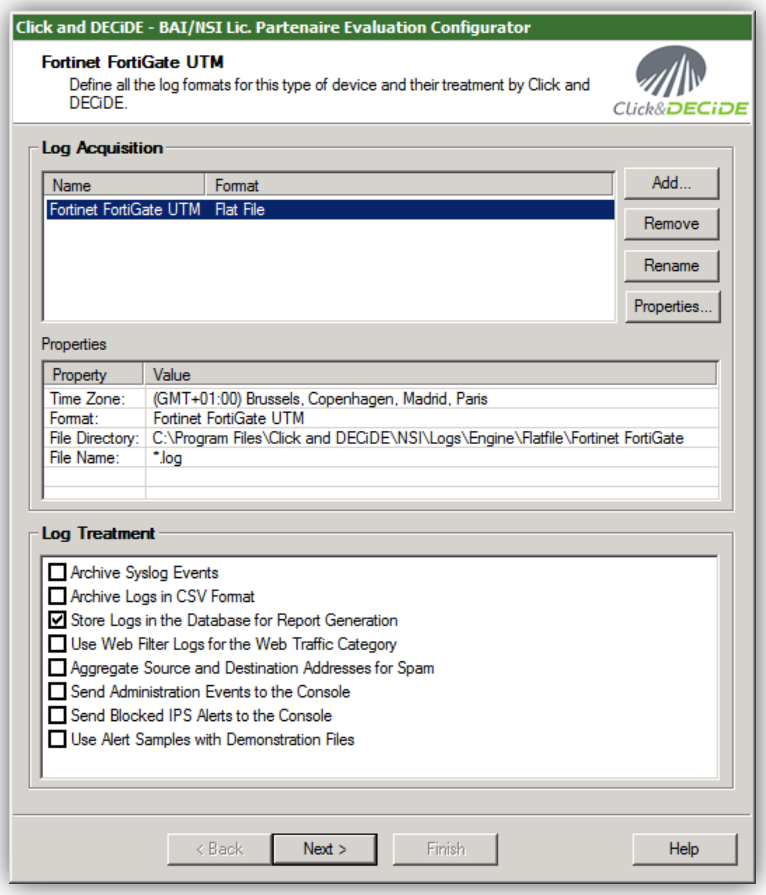
Adjust for Daylight Saving Time (DST): select this check box if the Date/Time parameters of your device are configured to adjust for Daylight Saving Time (DST). That is, where clocks are set one hour or more ahead of standard time to provide more daylight at the end of the working day during late spring,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

3.3.4. Suggestions for Practice

1. Enter the **Device Name**.
2. Select the **File Directory** you want Click&DECiDE NSI to scan for log files. Click the arrow to browse and select the appropriate directory.

3. Enter the **File Name** of your logs.
4. Select the appropriate **Time Zone**.
5. Select the **Adjust for Daylight Saving Time (DST)** check box if appropriate.
6. Click **OK**.

3.3.5. Log Acquisition and Treatment Settings



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator

Fortinet FortiGate UTM

Define all the log formats for this type of device and their treatment by Click and DECiDE.

Log Acquisition

Name	Format
Fortinet FortiGate UTM	Flat File

Properties

Property	Value
Time Zone:	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
Format:	Fortinet FortiGate UTM
File Directory:	C:\Program Files\Click and DECiDE\NSI\Logs\Engine\Flatfile\Fortinet FortiGate
File Name:	*.log

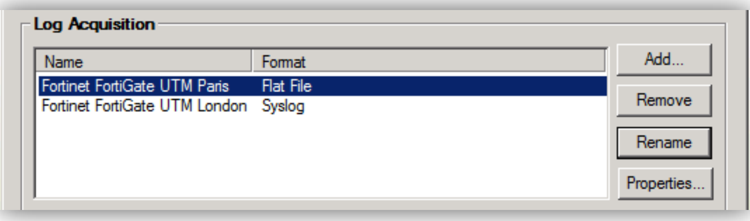
Log Treatment

- ☐ Archive Syslog Events
- ☐ Archive Logs in CSV Format
- ☑ Store Logs in the Database for Report Generation
- ☐ Use Web Filter Logs for the Web Traffic Category
- ☐ Aggregate Source and Destination Addresses for Spam
- ☐ Send Administration Events to the Console
- ☐ Send Blocked IPS Alerts to the Console
- ☐ Use Alert Samples with Demonstration Files

Figure 30 - Log Acquisition and Treatment Settings

The **Device Log Acquisition and Log Treatment** dialog box defines all the log formats (for example, Flat File and Syslog) for the device type along with their treatment by Click&DECiDE NSI. If you have many of the same device type, simply click **Add…** for each device of this type which you want to configure for Click&DECiDE NSI.

3.3.5.1. Log Acquisition



Name	Format
Fortinet FortiGate UTM Paris	Flat File
Fortinet FortiGate UTM London	Syslog

Figure 31 - Log Acquisition Configuration

Name: the Name you specified for the device. For example, you can write **Fortinet FortiGate UTM - Paris**.

Format: the log format (for example, Flat File, Syslog).

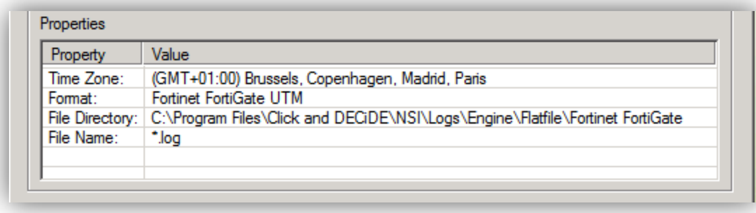
Add…: adds a device of the same device type. The Device Log Acquisition Settings dialog appears and you can configure the settings you want for the additional device.

Remove: removes a device from the list.

Rename: modifies the Name you specified for the device.

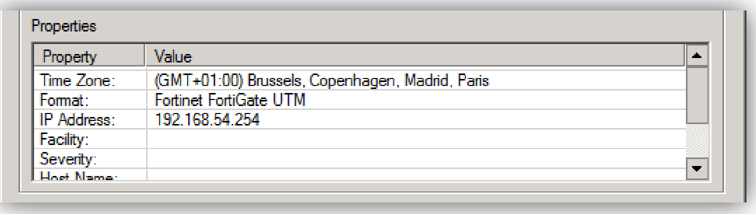
Properties…: displays the properties you selected for the device in the Device **Log Acquisition Settings** dialog box.

3.3.5.2. Properties



Property	Value
Time Zone:	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
Format:	Fortinet FortiGate UTM
File Directory:	C:\Program Files\Click and DECiDE\NSI\Logs\Engine\Flatfile\Fortinet FortiGate
File Name:	*.log

Figure 32 - Flat File device properties



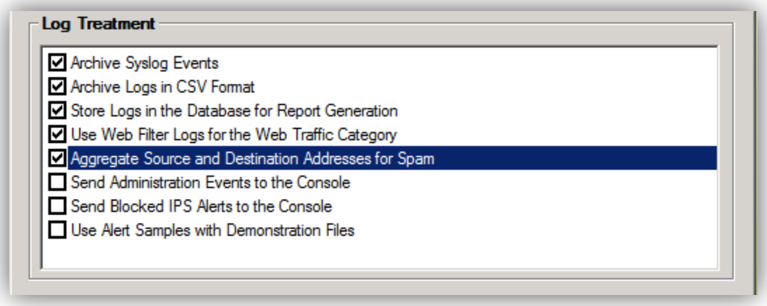
Property	Value
Time Zone:	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
Format:	Fortinet FortiGate UTM
IP Address:	192.168.54.254
Facility:	
Severity:	
Host Name:	

Figure 33 - Syslog device properties

Property: the parameter you configured in the Device **Log Acquisition Settings** dialog box (click Properties… to display this dialog box).

Value: the value you specified in the Device **Log Acquisition Settings** dialog box (click Properties… to display this dialog box).

3.3.5.3. Log Treatment



Log Treatment

☑ Archive Syslog Events
☑ Archive Logs in CSV Format
☑ Store Logs in the Database for Report Generation
☑ Use Web Filter Logs for the Web Traffic Category
☑ Aggregate Source and Destination Addresses for Spam
□ Send Administration Events to the Console
□ Send Blocked IPS Alerts to the Console
□ Use Alert Samples with Demonstration Files

Figure 34 - Log Treatment Configuration

Archive Syslog Events: This enables the preparation of the Syslog flat file archive. The Syslog flat file archive is mainly used for legal and regulation proof request. However, you must go to the Log Archive Settings dialog box and configure the Log Archive settings and add the device logs you want to archive via Log Vault for Click&DECiDE NSI to archive your logs.

Archive logs in CSV format: This enables the preparation of the Comma Separated Values flat file archive. The CSV flat file archive is mainly used for direct long term investigation as it is the exact copy of the enriched time contextualized version of the log. However, you must go to the Log Archive Settings dialog box and configure the Log Archive settings and add the device logs you want to archive via Log Vault for Click&DECiDE NSI to archive your logs.

Store Logs in the Database for Report Generation: stores logs in the “netreport” database to enable the creation of the Click&DECiDE NSI Daily Dashboards and Monthly Dashboards. This option must be selected if you want to create dashboard reports.

On some devices, you may have log treatment options specialized on the selected device. For example, the fact that you should **Aggregate Spam**, **Ignore Rejected Anonymous user**.

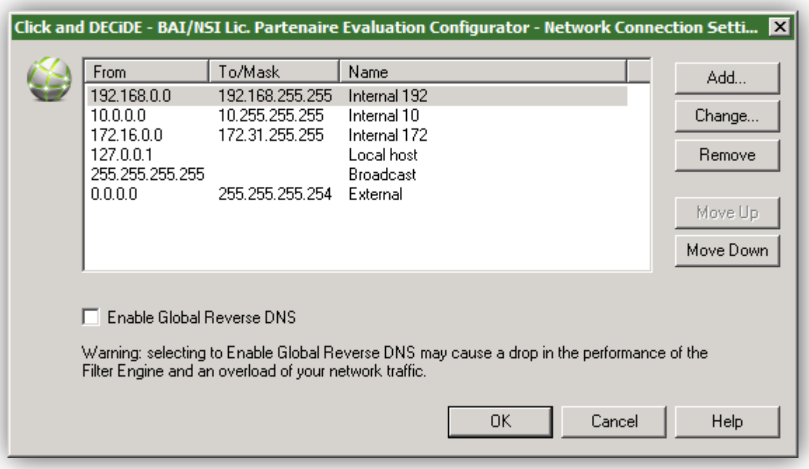
3.3.6. Suggestions for Practice

1. Note the Time Zone, Format, File Directory and File Name you defined for this device.
2. Select the **Archive logs in Enriched CSV format** check box.
3. Select the **Use Web Filter Logs for the Web Traffic Category**
4. Select the **Aggregate Sources and Destination addresses for Spam**
5. Click **Finish**.

3.4. Working with Network Settings

3.4.1. Network Connection Settings

The **Network Connection Settings** dialog box is proposed if you chose to configure one or more devices. The data collected here will configure the RNDS Net Area initialization defined for Click&DECiDE NSI Enterprise.



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Network Connection Setti...

From	To/Mask	Name
192.168.0.0	192.168.255.255	Internal 192
10.0.0.0	10.255.255.255	Internal 10
172.16.0.0	172.31.255.255	Internal 172
127.0.0.1		Local host
255.255.255.255		Broadcast
0.0.0.0	255.255.255.254	External

☐ Enable Global Reverse DNS

Warning: selecting to Enable Global Reverse DNS may cause a drop in the performance of the Filter Engine and an overload of your network traffic.

Figure 35 - Network Connection Configuration

From: IP Address.

To/Mask: IP Address or Network Mask.

Name: enter a Name for the range of addresses in the Name column. This name will allow you to distinguish between two zones of the same type but with different attributions (engineering department, sales department and so on) or two zones that are located in different places (Paris, London and so on).

Internal: Addresses that are part of your network.

External: Addresses that are external to your network.

Broadcast: The broadcast address is the address network broadcasts are sent to. It is the "255" (255 being the total of an 8 bit binary number of all 1's, given a subnet it would be a smaller number, depending on how many bits were given to it) of the network range. Using the /28 above, and using the same method to determine that our address range is .160-.175, we know that our broadcast address is .175 - because .175 is the LAST address in our range.

DMZ: Addresses that are part of your demilitarized zone.

Add: inserts a new row in the table via the Network Change dialog box.

Change: modifies the row you selected via the Network Change dialog box.

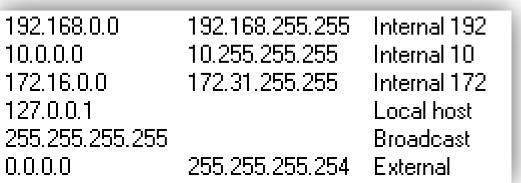
Remove: removes the row from the table.

Move Up: moves the row up a row.

Move Down: moves the row down a row.

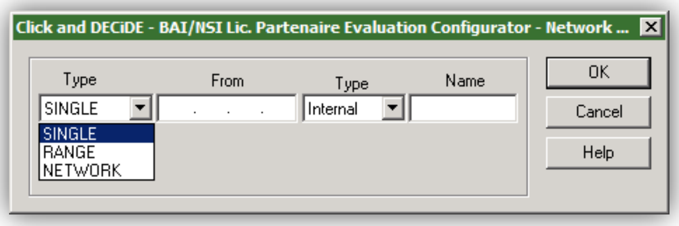
Enable Global Reverse DNS: enables the translation of IP addresses to domain name using Reverse DNS queries. Selecting this option may lead to a drop in the Click&DECiDE NSI Engine's performance and a network traffic overload.

Note: The Network Connection Settings work in first match order. Give particular attention to the order of your Network Connection Settings. We advise you to always leave the last 6 lines to be sure to identify all possible internal IP's that may be encountered in your network, and to add all new networks on top of those 6 lines.



192.168.0.0	192.168.255.255	Internal 192
10.0.0.0	10.255.255.255	Internal 10
172.16.0.0	172.31.255.255	Internal 172
127.0.0.1		Local host
255.255.255.255		Broadcast
0.0.0.0	255.255.255.254	External

3.4.2. Network Change



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Network ...

Type: SINGLE; From: . . . ; Type: Internal; Name:

Figure 36 - Network Connection Change

- Type:
    - **Single:** a single IP Address.
    - **Range:** a range of IP Addresses.
    - **Network:** a range that defines a network. From and to a Mask.
- **From:** an IP Address.

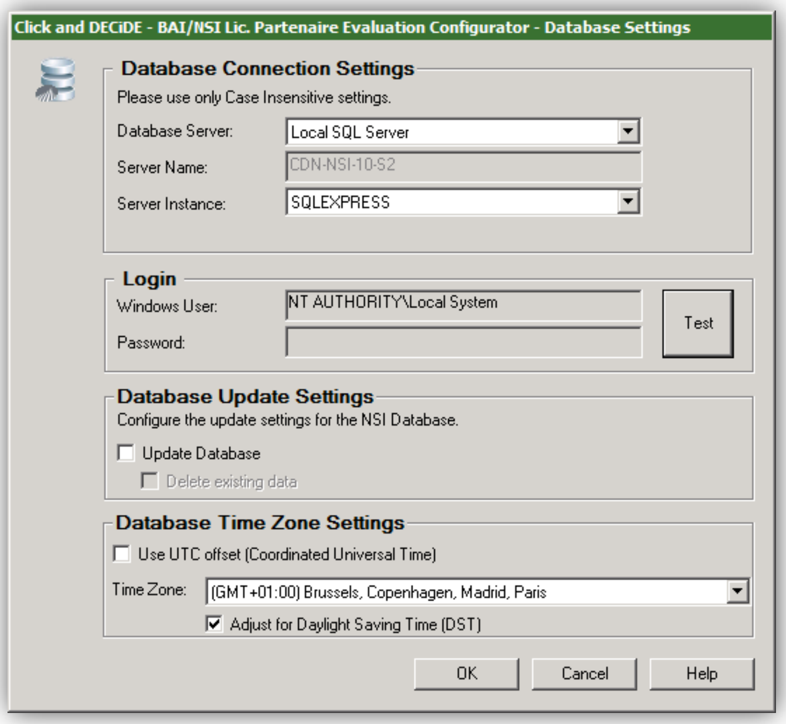
- **To/Mask:** to an IP Address or a Network Mask. A network mask determines which portion of an IP address identifies the network and which portion identifies the host
- Type:
  - **Internal:** Addresses that are part of your network.
  - **DMZ:** Addresses that are part of your demilitarized zone.
- **Name**: enter a Name for the range of addresses in the Name column. This name will allow you to distinguish between two zones of the same type but with different attributions (engineering department, sales department and so on) or two zones that are located in different places (Paris, London and so on).

Note: the size of the Network Connection Settings text field is limited to 15 characters, including “DMZ_” or “Internal_”. Try to limit your text to 5 characters of internal networks.

3.4.3. Suggestions for Practice

1. Click **Add… and** add :
   a. A single DMZ web server at IP 194.206.126.204 on line 1 position
   b. A public DMZ network 192.168.2.0 / 255.255.255.0 on line 2 position

3.5. Working with Database Settings



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Database Settings

Database Connection Settings

Please use only Case Insensitive settings.

Database Server: Local SQL Server

Server Name: CDN-NSI-10-S2

Server Instance: SQLEXPRESS

Login

Windows User: NT AUTHORITY\Local System

Password:

Database Update Settings

Configure the update settings for the NSI Database.

☐ Update Database

☐ 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)

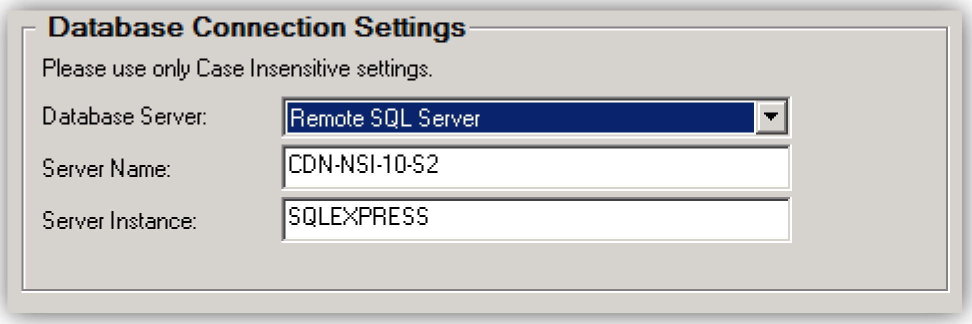
Figure 37 - Database Settings

The **Database Settings** dialog box configures the connection and Time Zone Settings for the Database you want Click&DECiDE NSI to use to manage your device log data.

3.5.1. Database Connection Settings

To analyze logs, Click&DECiDE NSI inserts the data collected into a database name “netreport”. This database must be queried via the network to enable reports to be generated via the Click&DECiDE NSI Web Portal. These two connections to a database are made via two data sources. These two data sources both point towards the same database however, the second source is secured for querying through the Internet while the first source is not, to enable data to be inserted. The Database Settings dialog box's purpose is to collect the necessary information to create these data sources.

> **Note:** check again your system requirements (Chapter 1.5) for the available database.



Database Connection Settings

Please use only Case Insensitive settings.

Database Server: Remote SQL Server

Server Name: CDN-NSI-10-S2

Server Instance: SQLEXPRESS

Figure 38 - Database Connection Settings

Database Server: select if you want to use a database that you already have access to or a remote one.

> Note; If no local SQL Database is available, the system will propose to install an SQL Express Database for test purposes.

Server Name: enter your remote IP or server name

Server Instance: enter your server instance name

3.5.2. Click&DECiDE NSI Login

3.5.2.1. Local Database

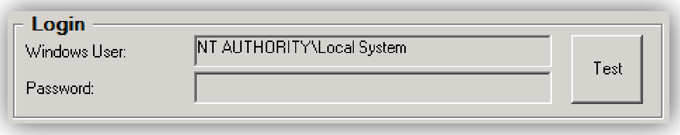


Figure 39 - Connection to the Local Database

When using a local database, Click&DECiDE NSI Engine uses the Local System account to connect to the database. The “netreport” database and tables are created by the Click&DECiDE NSI Log Source Configuration using the user you are logged on.

3.5.2.1. Remote Database

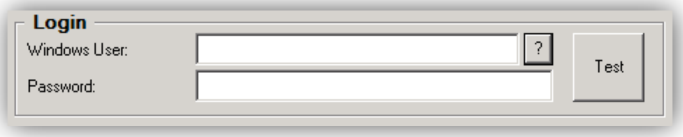


Figure 40 - Connection to the Remote Database

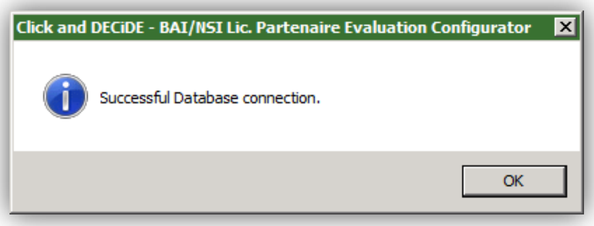
When using a remote database, Click&DECiDE NSI uses a remote authorized account to connect to the database and creates the required tables. Please contact your system administrator to get an authorized account.

Please consult our FAQ for more information:
http://www.clickndecide.com/downloads/WebDoc/CnDRnD/KBA/KBA200_How_to_Connect_to_Remote_SQL_Server.pdf

Windows User: Enter the user ID of a Windows account that can connect to the remote database.

Password: Enter the password of a Windows account that can connect to the remote database.

Test: Click in order to validate your database configuration before proceeding further. The Successful Database connection message appears.

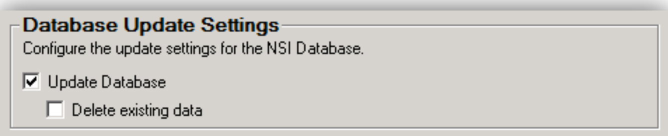


Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator

Successful Database connection.

Figure 41 - Database Connection test message

3.5.3. Database Update Settings



Database Update Settings

Configure the update settings for the NSI Database.

☑ Update Database

☐ Delete existing data

Figure 42 - Database Update Settings

The first time you launch the Log Source Configuration the “netreport” database is fully updated. The second time you launch the Log Source Configuration the “netreport” database is not updated. You must select the **Update Database** check box under **Database Update Settings** in the **Database Settings** dialog box each time you set parameters via the Log Source Configuration for the “netreport” database to be updated.

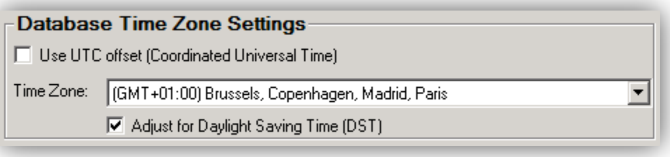
> **Note:** you must run the Log Source Configuration update at least once for the Database Update Settings to be freely configurable. The first time you install Click&DECiDE NSI, the Log Source Configuration selects the Update Database check box by default, since the netreport database must be updated to use Click&DECiDE NSI.

Update Database: update the “netreport” database.

Delete existing data: this will drop and re-create all tables in the “netreport” database (if it is the first time you install Click&DECiDE NSI) wiping all data from the database.

> **Warning:** if you select the **Delete existing data** check box, Click&DECiDE recommend that you save existing data in the database tables.

3.5.4. Database Time Zone Settings



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)

Figure 43 - Database Time Zone Settings

Click&DECiDE NSI collects your security device logs and converts them from their specific Time Zone into Coordinated Universal Time (UTC) before they are analyzed. However, if you want the logs that Click&DECiDE NSI saves to the Click&DECiDE NSI database to:

Either:

Be left in Coordinated Universal Time (UTC)

Or to

Be converted to a specific Time Zone with or without the application of the Daylight Saving Time (DST) adjustment.

You must enter these values under Database Time Zone Settings.

Use UTC offset (Coordinated Universal Time): for Click&DECiDE NSI to correctly treat your logs, and leave them in UTC when they are saved in the Click&DECiDE NSI database, you must select to use the UTC (Coordinated Universal Time) offset.

The international time standard (formerly Greenwich Mean Time, or GMT). An acronym for Coordinated Universal Time, is a time scale that joins Greenwich Mean Time (GMT), which is based solely on the Earth's inconsistent rotation rate, with highly accurate atomic time. When atomic time and Earth time approach a one second difference, a leap second is added into UTC. Zero hours UTC is midnight in Greenwich, England, which is located at 0 degrees longitude. Everything east of Greenwich (up to 180 degrees) is later in time; everything west is earlier. There are 42 time authorities around the world that are constantly synchronizing with each other. In the U.S., the time authorities are located at the U.S. Naval Observatory (USNO) and the National Institute of Standards & Technology (NIST).

Time Zone: for Click&DECiDE NSI to correctly convert the date/time values in your logs from UTC to a specific Time Zone when they are saved in the Click&DECiDE NSI database, you must select the appropriate Time Zone in the Time Zone drop-down list.

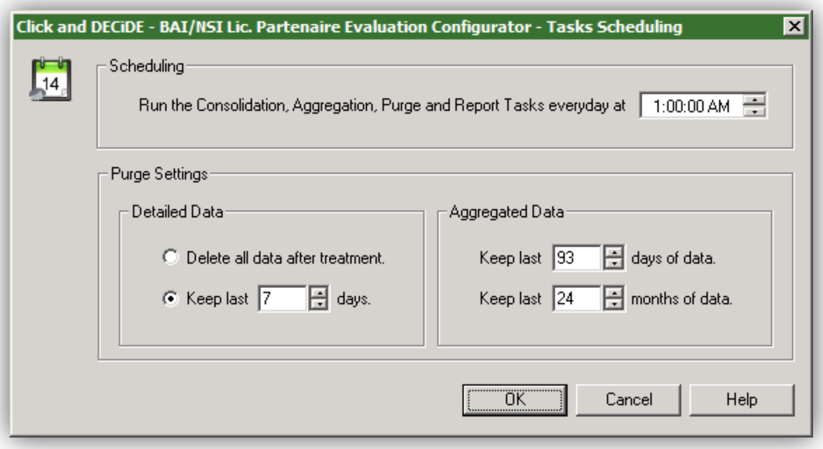
Indicates the local time zone in relation to Greenwich Mean Time (GMT). Part of the Earth surface where the same time is adopted by convention. Ideally, it is an area bounded between two meridians spaced by 15 degrees of longitude. Practically, for administrative and political reasons, it is often bounded by state borders that better approximate the two meridians.

Adjust for Daylight Saving Time (DST): select this option for Click&DECiDE NSI to correctly convert the date/time values in your logs from UTC to a Time Zone with the Daylight Saving Time (DST) adjustment and save them in the Click&DECiDE NSI database. Daylight Saving Time (or Summer Time as it is called in many countries) is a way of getting more out of the summer days by advancing the clocks by one hour during the summer. Then, the sun will appear to rise one hour later in the morning, at the benefit of one hour longer evenings. The sunset and sunrise are one hour later than during normal time. To make DST work, the clocks must be adjusted one hour ahead when DST begins (during spring), and adjusted back one hour to standard time every autumn. There are many countries who observe DST, and many who do not. During the following months: March/April-September/October, the countries on the northern hemisphere have their summer and may observe DST, while the countries in the southern hemisphere have their winter. During the rest of the year (September/October-March/April) is the opposite: Winter on the northern hemisphere, summer in the southern hemisphere.

3.5.5. Suggestions for Practice

1. Install SQLEXPRESS if you have no local database
2. Check your **Server Name**. and **Server Instance**
3. **Test** you database access
4. Select the appropriate **Time Zone**.
5. Click **OK**.

3.6. Working with Scheduled Task Settings



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Tasks Scheduling

Scheduling

Run the Consolidation, Aggregation, Purge and Report Tasks everyday at 1:00:00 AM

Purge Settings

Detailed Data

○ Delete all data after treatment.

● Keep last 7 days.

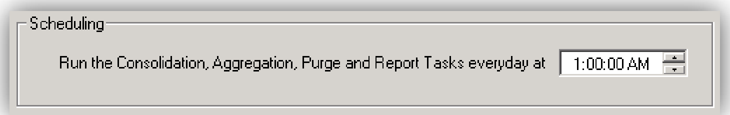
Aggregated Data

Keep last 93 days of data.

Keep last 24 months of data.

Figure 44 - Scheduled Task Settings

3.6.1. Scheduling



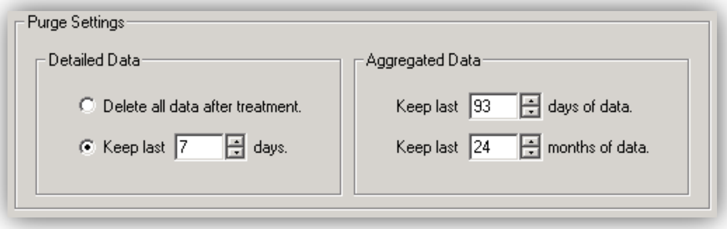
Scheduling

Run the Consolidation, Aggregation, Purge and Report Tasks everyday at 1:00:00 AM

Figure 45 - Consolidation, Aggregation, Purge and Report Tasks Settings

Run the Consolidation, Aggregation, Purge and Report Tasks everyday at: the time which the Consolidation, Aggregation, Purge and Report Task will be performed at.

3.6.2. Purge Settings



Purge Settings

Detailed Data

○ Delete all data after treatment.

● Keep last 7 days.

Aggregated Data

Keep last 93 days of data.

Keep last 24 months of data.

Figure 46 - Purge Settings

Detailed Data:

> Detailed data is used for forensics analysis. The less day you keep, the less you will be able to backtrack a specific event.

Delete all data after treatment: purges the detailed data from the detailed data table once it has been aggregated.

Keep last n days: select the number of days of detailed data that you selected to keep in the database. Please note that this is from the last data date and not necessarily from the current day (i.e. today). The Data recorded preceding the period of days you selected to keep will be purged.

Aggregated Data:

> Aggregated data is used for daily and monthly dashboards.

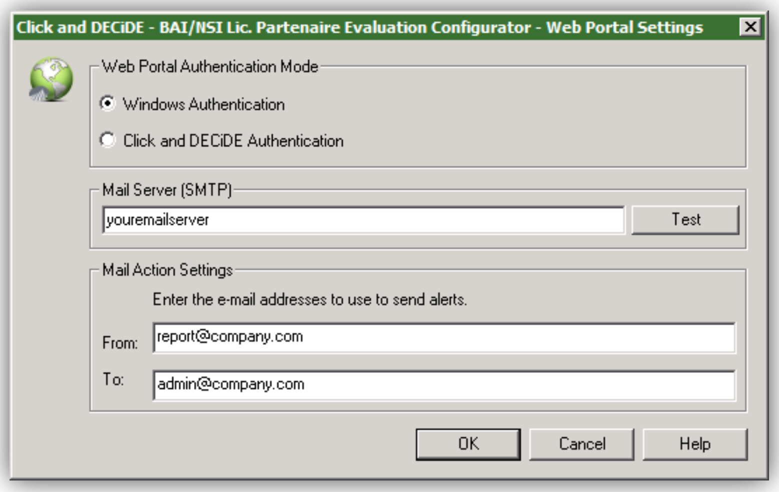
Keep last n Days of Data: keep the last n days of data in the table containing the database data aggregated by day. The data preceding the last days selected will be purged from the table containing the data aggregated by day. Please note that this is from the last data date and not necessarily from the current day (i.e. today).

Keep last n Months of Data: keep the last n months of data in the table containing the database data aggregated by month. The data preceding the last months selected will be purged from the table containing the data aggregated by month. Please note that this is from the last data date and not necessarily from the current day (i.e. today).

3.6.3. Suggestions for Practice

1. Open the **Tasks Scheduling** dialog box.
2. Select to keep the last 31 days of detailed data.
3. Select to keep the last 93 days of aggregated data.
4. Select to keep the last 24 months of aggregated data.
5. Click **OK**.

3.7. Working with Web Portal Settings



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Web Portal Settings

Web Portal Authentication Mode

● Windows Authentication

○ Click and DECiDE Authentication

Mail Server (SMTP)

youremailserver

Mail Action Settings

Enter the e-mail addresses to use to send alerts.

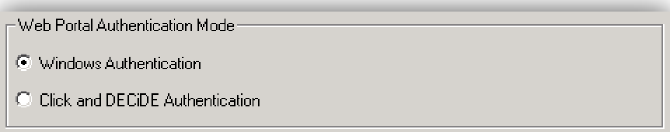
From: report@company.com

To: admin@company.com

Figure 47 - Web Portal Settings

3.7.1. Web Portal Authentication Mode

The Web Portal Authentication Mode Settings dialog box enables you to setup the method used by users to log in Click&DECiDE Web Portal.



Web Portal Authentication Mode

● Windows Authentication

○ Click and DECiDE Authentication

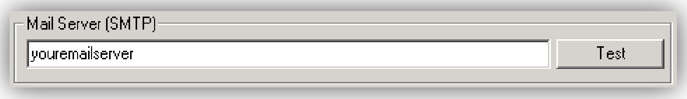
Figure 48 - Web Portal Authentication Mode

Windows Authentication: With this option selected, the user authentication scheme will came directly from the Windows session opened by the user using the Internet Explorer transport layer. A user identified in a common group in the Active Directory and in Click&DECiDE will get automatically the Click&DECiDE usage right of his group.

Click and DECiDE Authentication: With this option selected, the user, and their rights inside Click&DECiDE depends on the effective rights given in the **Administration Manager** program.

3.7.2. Mail Server Settings

The Mail Server Settings dialog box enables you to set the Mail Server you want to send e-mail messages and the e-mail addresses you want to use for Click&DECiDE NSI alerts.



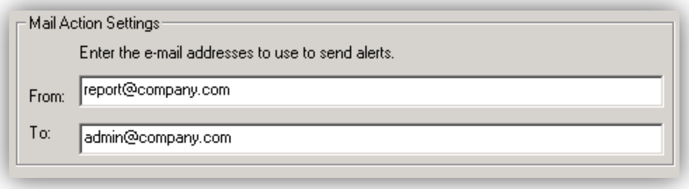
Mail Server (SMTP)

yourmailserver

Figure 49 - Mail Server Settings

Mail Server (SMTP): Enter the name of the SMTP server for the company in the Mail Server (SMTP) field. Click&DECiDE NSI will use this to send the reports generated by the Report Scheduler by e-mail for example. Click Test. This verifies that the name of the SMTP Server correctly entered.

3.7.3. Mail Action Settings



Mail Action Settings

Enter the e-mail addresses to use to send alerts.

From: report@company.com

To: admin@company.com

Figure 50 - Mail Action Settings

From: Enter the address which you want to send e-mails from via Click&DECiDE NSI in the From field.

To: Enter the address which you want to send e-mails to via Click&DECiDE NSI in the To field.

Note: if you have a Click&DECiDE license limited by the number of lines or the volume of events, please ensure you that you have correctly fill the Mail Server Settings and the Mail Action Settings as they are mandatory to receive alerts when the license limit is reached (100%), or almost reached (90%)

3.7.4. Suggestions for Practice

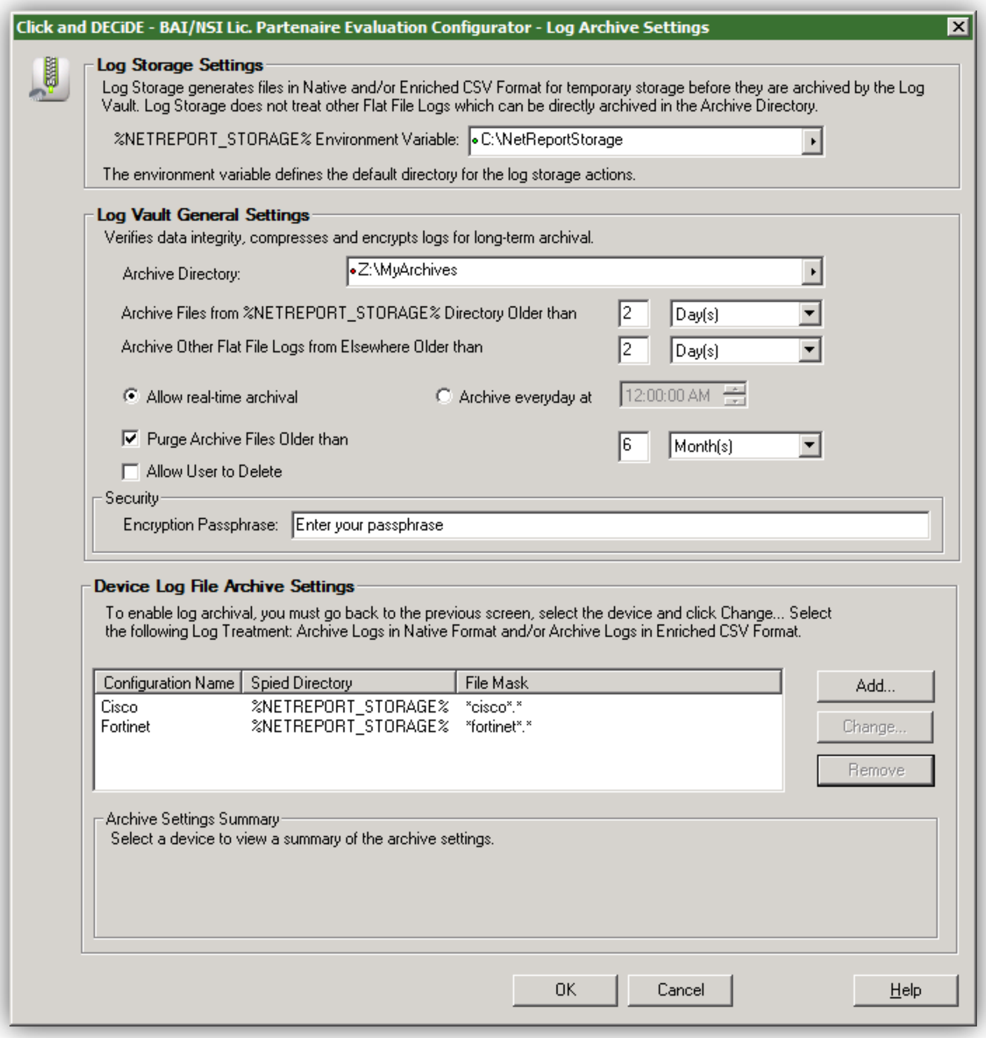
1. Enter the name of the SMTP server for your company in the **Mail Server** field.
2. Click **Test**. This verifies that the name of the SMTP Server correctly entered.
3. Enter the e-mail addresses you want to use to when Click&DECiDE NSI e-mail alerts are sent.
4. Click **OK**.

3.8. Working with Log Archive Settings

3.8.1. Log Archive Settings

Click&DECiDE NSI Log Archive includes two components, Click&DECiDE NSI Log Storage and Click&DECiDE NSI Log Vault:

- **Click&DECiDE NSI Log Storage:** generates files in Native and/or Enriched CSV format for temporary storage before they are archived by Click&DECiDE NSI Log Vault. Please note that other Flat File logs are not treated by Click&DECiDE NSI Log Storage, instead Click&DECiDE NSI Log Archive scans the spied directory you specified for your other Flat File logs, if you select to archive Flat File logs, then the logs will be transferred from the spied directory to the NetReportArchive directory
- **Click&DECiDE NSI Log Vault:** generates a digest (to verify data integrity), compresses and encrypts logs for long-term archival.



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Log Archive Settings

Log Storage Settings

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

%NETREPORT_STORAGE% Environment Variable: C:\NetReportStorage

The environment variable defines the default directory for the log storage actions.

Log Vault General Settings

Verifies data integrity, compresses and encrypts logs for long-term archival.

Archive Directory: Z:\MyArchives

Archive Files from %NETREPORT_STORAGE% Directory Older than 2 Day(s)

Archive Other Flat File Logs from Elsewhere Older than 2 Day(s)

● Allow real-time archival ○ Archive everyday at 12:00:00 AM

☑ Purge Archive Files Older than 6 Month(s)

□ Allow User to Delete

Security

Encryption Passphrase: Enter your passphrase

Device Log File Archive Settings

To enable log archival, you must go back to the previous screen, select the device and click Change... Select the following Log Treatment: Archive Logs in Native Format and/or Archive Logs in Enriched CSV Format.

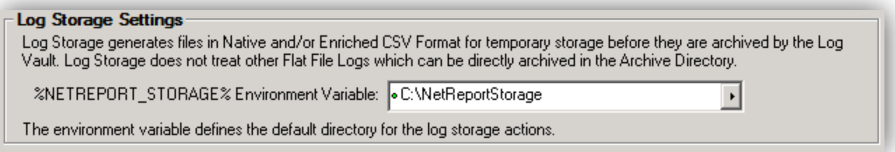
Configuration Name	Spied Directory	File Mask
Cisco	%NETREPORT_STORAGE%	*cisco*.*
Fortinet	%NETREPORT_STORAGE%	*fortinet*.*

Archive Settings Summary

Select a device to view a summary of the archive settings.

Figure 51 - Log Archive Settings

3.8.1.1. Log Storage Settings



Log Storage Settings

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

%NETREPORT_STORAGE% Environment Variable: C:\NetReportStorage

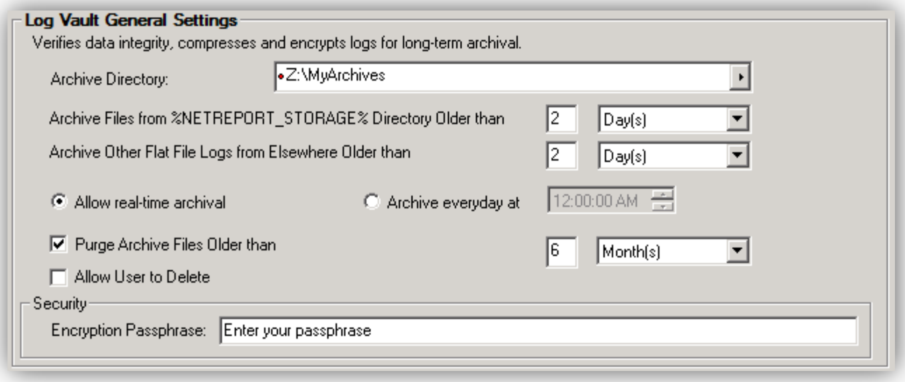
The environment variable defines the default directory for the log storage actions.

Figure 52 - Log Storage Settings

Log Storage Settings: the environment variable which defines the default directory where Click&DECiDE NSI temporarily stores the Native or Enriched CSV format log files that were generated for temporary storage before they are archived by Click&DECiDE NSI Log Vault.

Select a drive where you will have enough disk size to store the numbers of days you will ask to keep online on the **Log Vault General Settings.** It is recommended to select another drive than the one where Click&DECiDE NSI is installed.

3.8.1.2. Log Vault General Settings



Log Vault General Settings

Verifies data integrity, compresses and encrypts logs for long-term archival.

Archive Directory: •Z:\MyArchives

Archive Files from %NETREPORT_STORAGE% Directory Older than 2 Day(s)

Archive Other Flat File Logs from Elsewhere Older than 2 Day(s)

● Allow real-time archival ○ Archive everyday at 12:00:00 AM

☑ Purge Archive Files Older than 6 Month(s)

☐ Allow User to Delete

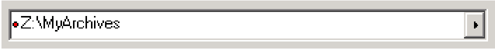
Security

Encryption Passphrase: Enter your passphrase

Figure 53 - Log Vault General Settings

Log Vault General Settings: generates a digest (to verify data integrity), compresses files and encrypts logs for long-term archival.

Archive Directory: the directory where Click&DECiDE NSI Log Vault archives your files for long-term storage. When a directory is not created and need to be created, a red dot is visible in front of the path has shown here



•Z:\MyArchives

Click&DECiDE NSI recommends that you store your log storage files on a separate disk from the disk which Click&DECiDE NSI is installed on.

Archive Files from %NETREPORT_STORAGE% Directory Older than: the frequency with which you wish the Log Vault to archive your files in minutes, hours, days or weeks. For example, if you select 2 Days, then all files that are older than 2 days will be archived in the Archive Directory you specified. Note that the default value for this field is 2 Days.

Archive Other Flat File Logs from Elsewhere Older than: the frequency with which you wish the Log Vault to archive your files in days or weeks. For example, if you select 2 Days, then all files that are older than 2 days will be archived in the Archive Directory you specified. Note that the default value for this field is 2 Days.

Allow real-time archival: the Log Vault archives your files in real time, with a directory check once a minute.

Archive everyday at: the Log Vault archives your files everyday at the time you select in the spin box.

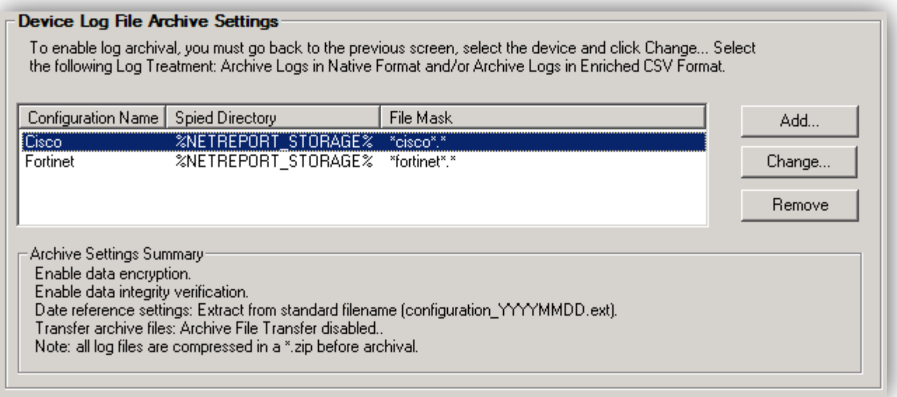
Purge Archives Files Older than: enables you to purge files that are older than a certain number of years. Note that the default value for this field is 6 month.

> Note: in many countries, it is recommended to keep one year of logs for the internet access

Allow user to delete: when this option is selected, the user can use the Click&DECiDE Management Console and delete archive log files. By default this check box is left clear.

Encryption Passphrase: Enter your Encryption Passphrase: A passphrase is 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.

3.8.1.3. Device Log File Archive Settings



Device Log File Archive Settings

To enable log archival, you must go back to the previous screen, select the device and click Change... Select the following Log Treatment: Archive Logs in Native Format and/or Archive Logs in Enriched CSV Format.

Configuration Name	Spied Directory	File Mask
Cisco	%NETREPORT_STORAGE%	*cisco*.*
Fortinet	%NETREPORT_STORAGE%	*fortinet*.*

Archive Settings Summary

Enable data encryption.
Enable data integrity verification.
Date reference settings: Extract from standard filename (configuration_YYYYMMDD.ext).
Transfer archive files: Archive File Transfer disabled..
Note: all log files are compressed in a *.zip before archival.

Figure 54 - Device Log File Archive Settings

Device Log File Archive Settings: the archive settings for flat files or devices for which you enabled the following Log Treatment:

- Archive logs in Native Format,
- Archive Logs in Enriched CSV Format

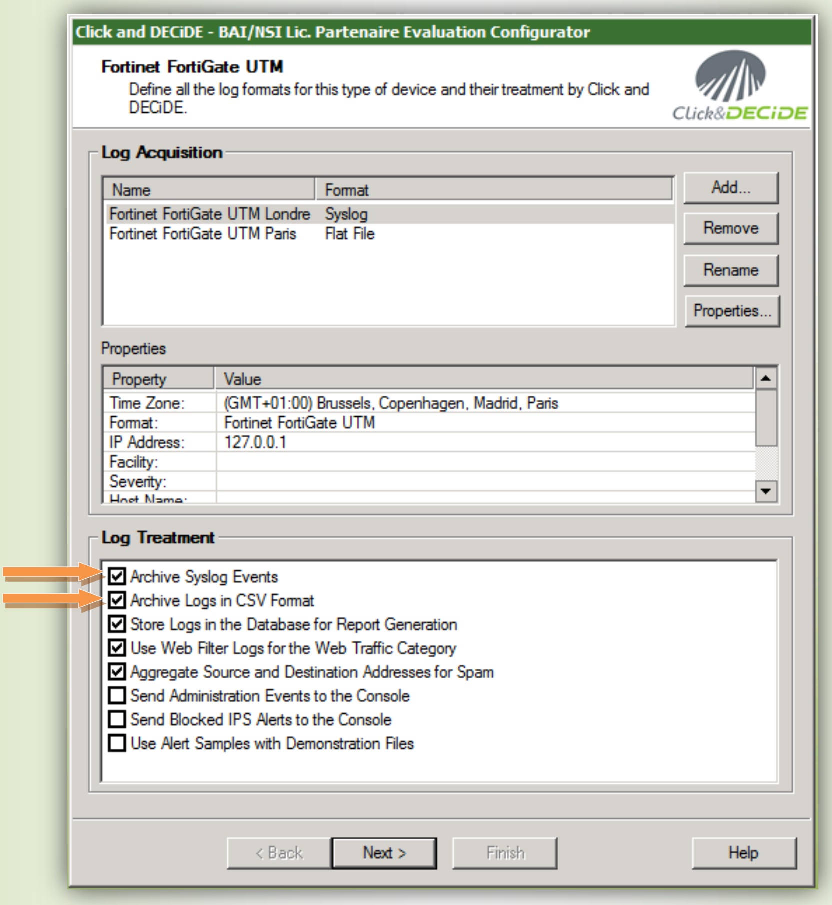
Select **Add** to create a new archive configuration, **Change** to edit an existing one, or **Remove** to suppress it.

3.8.2. Suggestions for Practice

Step 1: Enabling Log Storage

To configure Click&DECiDE NSI Log Archive:

1. Select either a device with Flat File format logs or the following Log treatment for at least one device:
   a. Archive in Syslog Events
   b. Archive in CSV Format.



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator

Fortinet FortiGate UTM

Define all the log formats for this type of device and their treatment by Click and DECiDE.

Log Acquisition

Name	Format
Fortinet FortiGate UTM Londre	Syslog
Fortinet FortiGate UTM Paris	Flat File

Properties

Property	Value
Time Zone:	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
Format:	Fortinet FortiGate UTM
IP Address:	127.0.0.1
Facility:	
Severity:	
Host Name:	

Log Treatment

- ☑ Archive Syslog Events
- ☑ Archive Logs in CSV Format
- ☑ Store Logs in the Database for Report Generation
- ☑ Use Web Filter Logs for the Web Traffic Category
- ☑ Aggregate Source and Destination Addresses for Spam
- ☐ Send Administration Events to the Console
- ☐ Send Blocked IPS Alerts to the Console
- ☐ Use Alert Samples with Demonstration Files

Figure 55 - Practice: Log Treatment Archive selection

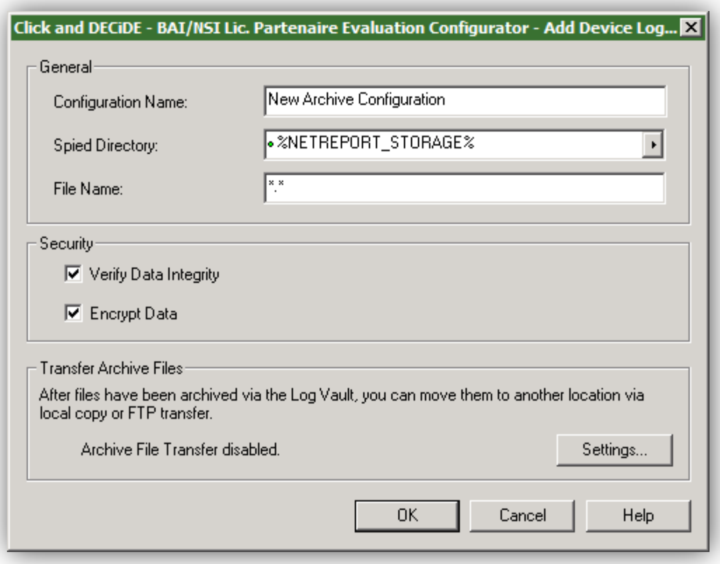
2. Click **Next** or/then **Finish**.
3. Click the **Settings…** button to the right of the Log Archive zone in the main Log Source Configuration screen.

Step 2: Adding Device Log Files' Archival

1. Enter the **Log Storage Settings** to define the default directory used for Click&DECiDE NSI log storage actions (such as archive logs in Native format).
2. Enter the **Log Vault Archive directory** the directory where Click&DECiDE NSI Log Vault archives your files for long-term storage.
3. Enter the **Archive Files from %NETREPORT_STORAGE% Directory Older than** settings. Select the frequency with which you wish the Log Vault to archive your files. 2 days is a good number.
4. Enter the **Archive Other Flat File Logs from Elsewhere Older** than settings. Select the frequency with which you wish the Log Vault to archive your files in days or weeks. 2 days is a good number.
5. Select either to
   a. **Allow real-time archival:** the Log Vault archives your files once a minute.
   b. **Archive everyday at:** the Log Vault archives your files everyday at the time you select in the spin box.
6. Enter the **Purge Archives Older than** settings. 12 month for example.
7. Check that the **Allow User to Delete Archives** check box is not selected.
8. Enter your **Encryption Passphrase**: enter your passphrase.
9. Click **Add…** under Device Log File Archive Settings.

3.8.3. Add Device Logs to Archive

The **Add Device Logs to Archive** dialog box shows the following settings:



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Add Device Log...

General

Configuration Name: New Archive Configuration

Spied Directory: %NETREPORT_STORAGE%

File Name: *.*

Security

☑ Verify Data Integrity

☑ Encrypt Data

Transfer Archive Files

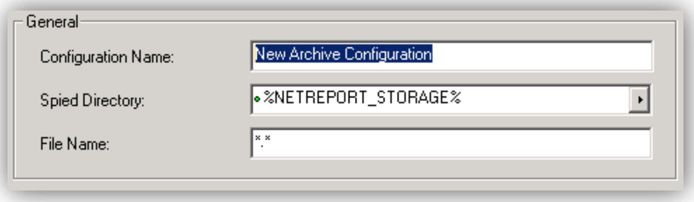
After files have been archived via the Log Vault, you can move them to another location via local copy or FTP transfer.

Archive File Transfer disabled.

Figure 56 - Add Device Logs to Archive

3.8.3.1. General Archive File Setting

General: the settings you configured for the device via the Device Type Log Acquisition and Log Treatment dialog box.



General

Configuration Name: New Archive Configuration

Spied Directory: %NETREPORT_STORAGE%

File Name: *.*

Figure 57 - General Archive File Setting

Configuration Name: Specify the name of the configuration. This name will be used as the main sub-directory where the file will be archived under.

Spied Directory: specify which directory you will monitor to archive files. By default, it is the **Log Storage** environment variable**:** %NETREPORT_STORAGE%

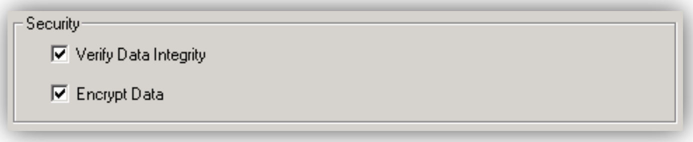
> **Note:** if you want to archive flat files, enter the flat file spied directory of your choice.

File Name: specify the characters sequence that will match the file name, like *juniper*.* or *cisco*.csv .

> **Note:** if you leave *.*, you will have a catch all sequence and all files will be archived under the chosen configuration name.

3.8.3.2. Security Archive File Setting

Security: the data integrity and encryption options.



Security

☑ Verify Data Integrity

☑ Encrypt Data

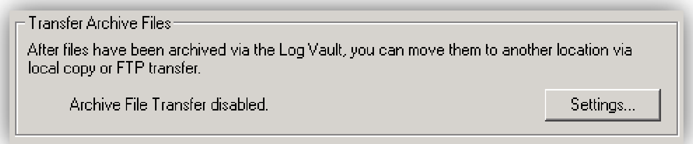
Figure 58 - Security Archive File Setting

Verify Data Integrity. this creates the message digest with the algorithm SHA-512.

Encrypt Data. this encrypts the files you archive with Click&DECiDE NSI Log Vault with the encryption algorithm AES-128.

Note: archives are compressed using the ZIP format.

3.8.3.3. Transfer Archive Files



Transfer Archive Files

After files have been archived via the Log Vault, you can move them to another location via local copy or FTP transfer.

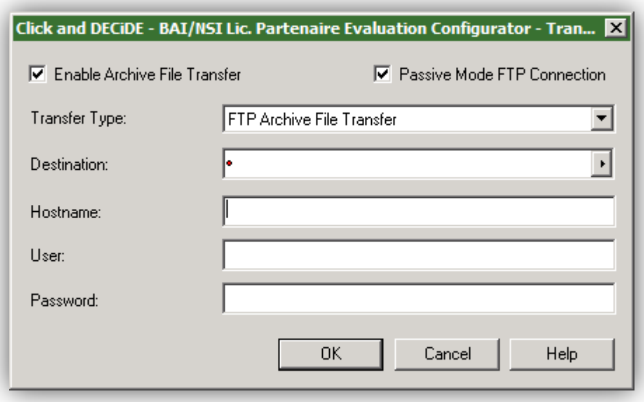
Archive File Transfer disabled.

Figure 59 - Transfer Archive Files

Transfer Archive Files: after device log files have been archived, you can move the archive files to another location via local copy or FTP transfer.

Note: once an archive file has been transferred, it is deleted from the Click&DECiDE Log Vault directory. A .nfo file still remains to keep track of the archives

3.8.4. Transfer Archive File Settings



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Tran...

☑ Enable Archive File Transfer ☑ Passive Mode FTP Connection

Transfer Type: FTP Archive File Transfer

Destination:

Hostname:

User:

Password:

Figure 60 - Transfer Archive File Settings

Move files that have already been archived via Click&DECiDE NSI Log Vault to another location via local copy or FTP transfer.

Enable Archive File Transfer: enables the Transfer Archive Files settings.

Passive Mode FTP Connection: enables Passive FTP connection. To enable Active Mode FTP Connection, simply clear this check box.

Transfer Type: either FTP Archive File Transfer or Local Archive File Transfer.

3.8.4.1. FTP Archive File Transfer

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

Destination: path to the destination folder on the FTP server.

Hostname: FTP Address of your server.

User: FTP User Name.

Password: FTP Password.

3.8.4.2. Local Archive File Transfer

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

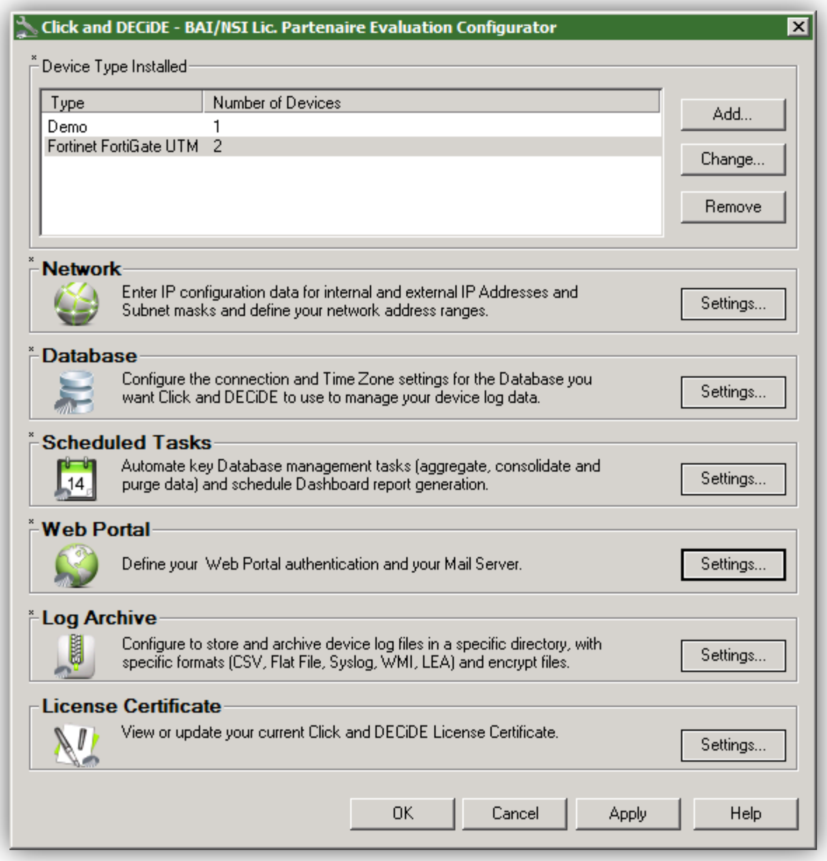
Destination: the directory where you want the files to be transferred to.

3.8.5. Suggestions for Practice

1. Select the Device whose logs you want to archive from the Device list.
2. Enter the **Spied Directory** which Click&DECiDE NSI Log Vault spies on.
3. Note the **File Name model**
4. Select whether you want to **Verify Data Integrity**.
5. Select whether you want to Encrypt Data.

3.9. Updating Log Source Configuration Settings

When you have finished the definition of your settings in the Click&DECiDE NSI Log Source Configuration, click **OK** or **Apply** to update your configuration settings.



Type	Number of Devices
Demo	1
Fortinet FortiGate UTM	2

* **Network**

Enter IP configuration data for internal and external IP Addresses and Subnet masks and define your network address ranges.

* **Database**

Configure the connection and Time Zone settings for the Database you want Click and DECiDE to use to manage your device log data.

* **Scheduled Tasks**

Automate key Database management tasks (aggregate, consolidate and purge data) and schedule Dashboard report generation.

* **Web Portal**

Define your Web Portal authentication and your Mail Server.

* **Log Archive**

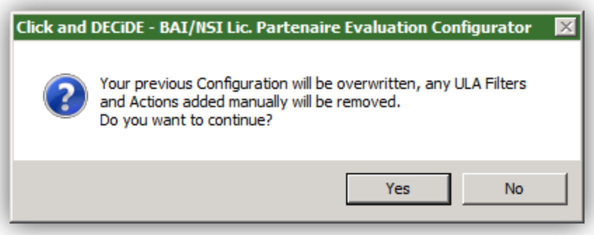
Configure to store and archive device log files in a specific directory, with specific formats (CSV, Flat File, Syslog, WMI, LEA) and encrypt files.

License Certificate

View or update your current Click and DECiDE License Certificate.

Figure 61 - Updating Log Source Configuration Settings

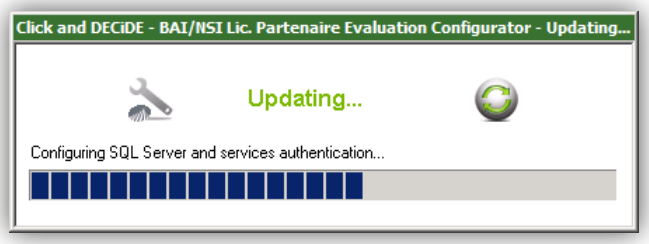
You need to update your configuration if you have a ***** sign in front of the Log Source Configuration menu.


Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator
Yes
No

Your previous Configuration will be overwritten, any ULA Filters and Actions added manually will be removed.
Do you want to continue?

Figure 62 - Log Source Configuration Update overwrite previous settings

Note: each time you update your setting with the Log Source Configuration program, a backup of the previous configuration is made.



Click and DECiDE - BAI/NSI Lic. Partenaire Evaluation Configurator - Updating...

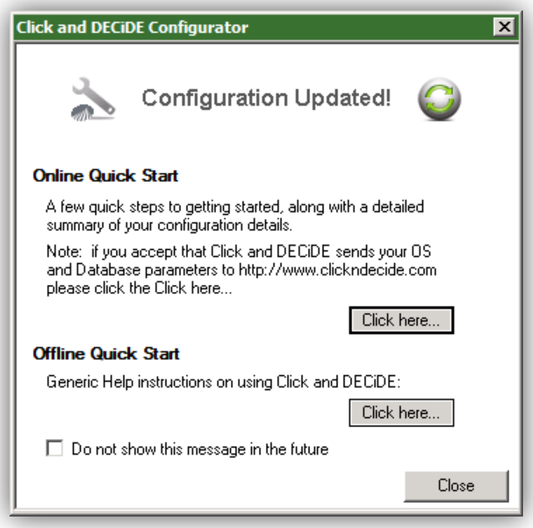
Updating...

Configuring SQL Server and services authentication...

Figure 63 - Log Source Configuration Update process bar

A process bar is shown during the Log Source Configuration Update process. If you made an update database action, a second bar will be shown during the update database process.

Note: all standard configuration and standard reporting project are reinstalled during the process.



Click and DECiDE Configurator

Configuration Updated!

Online Quick Start

A few quick steps to getting started, along with a detailed summary of your configuration details.

Note: if you accept that Click and DECiDE sends your OS and Database parameters to http://www.clickndecide.com please click the Click here...

Offline Quick Start

Generic Help instructions on using Click and DECiDE:

Figure 64 - Configuration Updated

3.9.1. Suggestions for Practice

1. Complete the configuration of your settings for Click&DECiDE NSI in the Click&DECiDE NSI Log Source Configuration.
2. Click either **Apply** or **OK** at the base of the Click&DECiDE NSI Log Source Configuration main screen. The **Your previous configuration will be overwritten** dialog box appears.
3. Click **Yes** if you want your previous configuration to be overwritten. The **Updating…** progress bar appears.

4. Wait for the update to finish. The **Configuration Updated** dialog box appears.
5. Click **Click here…** next to either the **Online**.
6. Note the details concerning your configuration.
7. Follow the key steps to getting started and view a detailed summary of your configuration details.
8. Click **Close**.

3.10. Suggestions for Practice

1. Using the Click & DECiDE Quick Installation Guide, work the Demo scenario
    a. Demo device installation
    b. Demo report generation
    c. Demo report analysis
    d. Demo cube generation
    e. Demo Cube manipulation