



Knowledge Base Article: Article 225

#### How to Backup and Restore NSI configuration

Date: March 11<sup>th</sup>, 2011

#### **Table of Contents**

Section 1: Backup your current configuration	2
A. Backup your License Certificates	2
B. Backup NSI Log Acquisition Configuration	2
C. Backup NSI Web Portal Configuration	3
D. Backup the database files	4
Section 2: Restore your configuration	5
A. Enter your License Certificate	5
B. Restore the WebPortal Configuration	7
C. Restore your custom NSI Log Sources Configuration	9
D. Restore the Scheduled Tasks 1	3
Section 3: Check your configuration	6
A. Log Acquisition 1	6
B. Log Insertion 1	7
C. Report Generation	20
D. Event Viewer	22

## www.clickndecide.com



#### Section 1: Backup your current configuration

#### A. Backup your License Certificates

 Save your NetReport license at: C:\Program Files\Click and DECiDE\NSI\\_license.cert (by default).

#### **B. Backup NSI Log Acquisition Configuration**

1. Start the Management Console: Start>All Programs>Click and DECiDE>Network Security Intelligence>Management Console.

Note: the default login/password is now admin/admin.

- 2. Navigate to Click and DECiDE/localhost (or NetReport/localhost for earlier version).
- 3. Click on Backup.

🚟 Click and DECiDE Management Console	e - [Console Root\Click and Decid	e\localhost][	IX				
🚡 Eile Action View Favorites Windo	w <u>H</u> elp	_16	1×1				
🗢 🔿 🙍 🖬 🛛 🖬							
	Port :	12343					
Click and Decide     I    I    I    I    I    I    I	Shared Secret :	•••••					
🛨 📜 Packages Server							
ULA	If your modify the above parar	neters, click here to reconnect to the configuration server using the new					
E Cog Vault	This will overw	rite recent XML configurations that have not been saved.					
🗄 🖏 Backups		Reconnect					
		e e e e e e e e e e e e e e e e e e e					
	<sup>∥</sup> Reload from	n Configuration Server 🛛 💌					
	Click here to restore the last configuration of the configuration server.						
	Reload						
		3					
	Backup the	Current Configuration 🥌					
	Click he	ere to save a backup of your current configuration.					
	A backup will be made and become available in the <b>Backups</b> branch.						
	Hackup						
	8						
			-				
Done							

- Save the new folder named YYYYMMDD-HHMM-user-vNNNN created in C:\Program Files\ Click and DECiDE\NSI\ConfigurationBackup (by default).
- 5. Close the Management Console.

## www.clickndecide.com



#### C. Backup NSI Web Portal Configuration

- 1. Start the Administration Manager: Start>All Programs>Click and DECiDE>Administration Manager.
- 2. Go to File>Backup Security Database...

	Click and DECiDE Administration Manager _ 🗖 🗙
File Edit View Tools Help	
Update Database Security         Check Database Security         Export Report         Backup Database Security         Import Windows Users and Group         Exit	S No item selected.
Data Sources & User Groups &	Users Menu 🕅 Authentications

- 3. Save the Security Database configuration into a .bck file.
- 4. Close Administration Manager.
- 5. Save your own Click and DECiDE BAI projects (\*.wfv files) created with Click and DECiDE Builder. We recommend to put these file in the **MyProject** folder located at: C:\Program Files\Click and DECiDE\BAI\Runtime Projects\My Projects (by default).
- 6. Save the external files (for example, the images) used by your own Click and DECiDE BAI projects. We recommend to put these file with the other image files in the Runtime\_projects folder located at: C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects (by default).
- 7. Save the standard reports and cubes (if applicable) respectively located in: C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects\enu (by default) and C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects\utilities (by default) and C:\Program Files\Click and DECiDE\BAl\Runtime\_Projects\cubes (by default).
- 8. Save your customized menus (if applicable): these are the \*.wmu files in the Runtime\_projects folder located at:

C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects (by default).





- Save the scheduled tasks configuration file d7tasks.xml located at: C:\Program Files\Click and DECiDE\BAI\d7tasks.xml (by default).
- Save your own script (if applicable) which are located in: C:\Program Files\Click and DECiDE\BAI\TaskScripts (by default).

#### **D. Backup the database files**

Whereas it does not concerns NSI Configuration we strongly recommend to regularly backup the netreport database. Please consult your Database Administrator for this task.







### Section 2: Restore your configuration

#### A. Enter your License Certificate

- 1. Launch the Log Source Configuration: Start>All Programs>Click and DECiDE>Network Security Intelligence>Management Console.
- 2. Click Settings... in the License Certificate section.

Click and I	DECiDE Configurator - License Certificate	×
	No License installed for Click and DECiDE.	<u> </u>
	Please contact your supplier to receive the appropriate license	
	certificate.	
		<u> </u>
	OK Cancel Change H	elo

3. Click Change...





4. Select the License Certificate we sent you for Click & DECiDE - NSI 10.1.2.

Click and [	DECiDE Configurator - License Certificate	×			
S 11	This Could a low a delivery data				
	I his Certificate was delivered to:				
	This License authorizes you to use version of:				
	Click and DECiDE - for NSI Enterprise				
	Business Application Intelligence Enterprise Edition v10.1				
	Builder 1 CAL user(s)				
	WebPortal 5 CAL user(s)				
	WebPortal 5 Concurrent user(s)(Client Access)				
	Scheduled Tasks Yes				
	Project Types NSI Projects (Execute only)				
	Maintenance Agreement Valid until 1/31/2011				
	Network & Security Intelligence				
	Daily Records 200000				
	Maintenance Agreement Valid until 1/31/2011				
	This Certificate will expire on:1/31/2011				
	Internal Use Only				
		-			
	UK Cancel <u>Ehange</u>	Help			





5. Click OK.

Device Type Installed	🚬 Cli	ck and DECiDE - for NSI Enterprise Configu	urator	×
Type       Number of Devices       Add         Click and DECIDE - for NSI Enterprise Configurator - Add Device       Image         Select the device type that you want to add.       Image         Device Type       Category         Aladdin eSale       Email Content Filtering         Aladdin eSale v5.2       Content Filtering         Check Point (Real Time)       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Cisco InoPort-C       Content Filtering: E-mail         Cisco InoPort-S       Proxy         Demo       Firewall         Demo       Firewall         OK       Cancel         UPHy All       Intrusion Prevention System; Web Site		wice Tune Installed		
Type       Number of Devices         Add       Change         Click and DECIDE - for NSI Enterprise Configurator - Add Device       Image: Change         Select the device type that you want to add.       Image: Change         Device Type       Category         Aladdin eSafe       Email Content Filtering         Aladdin eSafe       Content Filtering         Apache       Web Site         Apache       Web Site         Check Point [Real Time]       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Cisco IronPort-C       Content Filtering: E-mail         Cisco IronPort-S       Proxy         Clavister       Firewall         Demo       Firewall         Demo       Firewall         OK       Cancel         Leap       Image: Leap         Mail       Intrusion Prevention System         Demo       Firewall         Demo       Firewall         Demo       Firewall         OK       Cancel         Help       Image: Leap         OK       Canc				
Click and DECIDE - for NSI Enterprise Configurator - Add Device       Image: Imag		ype Number of Devices		<u>A</u> dd
Click and DECiDE - for NSI Enterprise Configurator - Add Device         Select the device type that you want to add.         Device Type       Category         Aladdin eSafe v5.2       Content Filtering         Apache       Web Site         AFKDON Network Security       Firewall; Proxy: Intrusion Prevention System         Blue Coat       Proxy: Content Filtering         Check Point Firewall (Command Line Flat File)       Firewall         Check Point Firewall (Dommand Line Flat File)       Firewall         Check Point Firewall (Command Line Flat File)       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Demo       Firewall         Demo       Firewall         Demo       Firewall         OK       Cancel         Uew ou update your current Click and DECIDE License Certificate.         Settings				
Click and DECIDE - for NSI Enterprise Configurator - Add Device         Select the device type that you want to add.         Device Type         Category         Aladdin eSafe         Aladdin eSafe         Content Filtering         Aladdin eSafe v5.2       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 (GUI Flat File)       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Cisco TonPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Clavister       Firewall         Demo       Firewall, Proxy: Intrusion Prevention System         Demy All       Intrusion Prevention System         OK       Cancel         Help       OK				<u>C</u> hange
Select the device type that you want to add.         Device Type       Category         Aladdin eSafe       Email 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 (GUI Flat File)       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Check Point Syslog UTM       Firewall         Check Point Syslog UTM       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Demo       Firewall         DK       Cancel		lick and DECiDE - for NSI Enterprise Confi	gurator - Add Device	×
Device Type       Category         Aladdin eSafe v5.2       Content Filtering         Apache       Web Site         ARKDON 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 Firewall (GUI Flat File)       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Demo       Firewall         Demo       Mathematical Addition         Demo       Mathematical Addition         Demo       Mathematical Addition         Demo       Mathematical Addition         Demo       Mathematical Addition <th></th> <th>Colores the device time thet was ment to odd</th> <th></th> <th>ļ</th>		Colores the device time thet was ment to odd		ļ
Device Type       Category         Aladdin eSafe v5.2       Content Filtering         Apache       Web Site         ARKDON 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 Firewall (GUI Flat File)       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Demo       Firewall         Demo       Matematic         Demo       Firewall         Demo       Matematic         Demo       Matematic         Demo       Matematic         Demo       Matematematic	Ľ	Select the device type that you want to add.		
Device Type       Category         Aladdin eSafe       E-mail Content Filtering         Aladdin eSafe v5.2       Content Filtering         Apache       Web Site         ARK00N 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 Systeg UTM       Firewall         Cisco Firewalls       Firewall         Cisco Firewalls       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Demo       Firewall         Demo       Firewall         Demo       Firewall; Proxy; Intrusion Prevention System         Demo       Firewall         OK       Cancel         Vel       Vel         View or update your current Click and DECiDE License Certificate.       Settings				h
Aladdin eSafe       E-mail Content Filtering         Aladdin eSafe v5.2       Content Filtering         Apache       Web Site         Apache       Web Site         ARK00N Network Security       Firewall; Proxy: Intrusion Prevention System         Blue Coat       Proxy: Content Filtering         Check Point (Real Time)       Firewall         Check Point Firewall (GUI Flat File)       Firewall         Check Point Systog UTM       Firewall         Check Point Systog UTM       Firewall         Cisco Firewalls       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Clavister       Firewall         Demo       Eiternese Certificate         View or update your current Click and DECiDE License Certificate.       Settings		Device Type	Category	h
Aladdin eSale v5.2 Content Filtering Apache Web Site ARK00N 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 Systeg UTM Firewall Cisco Firewalls Firewall Cisco Firewalls Firewall Cisco IronPort-C Content Filtering; E-mail Cisco IronPort-S Proxy Clavister Firewall Demo Firewall; Proxy; Intrusion Prevention System Deny All Intrusion Prevention System; Web Site UCK Cancel Help View or update your current Click and DECIDE License Certificate. Settings		Aladdin eSafe	E-mail Content Filtering	
Apache web site ARK00N Network Security Firewall; Proxy; Intrusion Prevention System Blue Coat 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 Cisco IronPort-C Content Filtering; E-mail Cisco IronPort-S Proxy Clavister Firewall Demo Firewall Proxy; Intrusion Prevention System Deny All Intrusion Prevention System; Web Site	_	Aladdin eSafe v5.2	Content Filtering	
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 Check Point Syslog UTM Firewall Cisco Firewalls Proxy Cisco IronPort-C Content Filtering; E-mail Cisco IronPort-S Proxy Clavister Firewall Demo Firewall; Proxy: Intrusion Prevention System Deny All Intrusion Prevention System; Web Site		ARKOON Network Security	Firewall: Proxy: Intrusion Prevention System	
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 Check Point Syslog UTM Firewall Cisco IronPort-C Content Filtering; E-mail Cisco IronPort-S Proxy Clavister Firewall Demo Firewall; Proxy; Intrusion Prevention System Deny All Intrusion Prevention System; Web Site CK Cancel Help License Certificate View or update your current Click and DECiDE License Certificate. Settings		Blue Coat	Proxy; Content Filtering	
Check Point Firewall (GUI Flat File) Firewall Check Point Syslog UTM Firewall Check Point Syslog UTM Firewall Cisco Firewalls Firewall Cisco IronPort-C Content Filtering; E-mail Cisco IronPort-S Proxy Clavister Firewall Demo Firewall; Proxy; Intrusion Prevention System Demy All Intrusion Prevention System; Web Site Cisco Example Concel Help Cisco Forewall Demo Firewall; Proxy intrusion Prevention System Demy All Intrusion Prevention System; Web Site Cisco Example Concel Help Cisco Forewall; Proxy Cancel Help Cisco Settings		Check Point (Real Time)	Firewall	
Check Point Syslog UTM       Firewall         Cisco Firewalls       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Clavister       Firewall         Demo       Firewall; Proxy; Intrusion Prevention System         Demo       Firewall; Proxy; Intrusion Prevention System         Deny All       Intrusion Prevention System; Web Site         Image: Cancel Help       Image: Cancel Help         Image: Cancel View or update your current Click and DECiDE License Certificate.       Settings	<b>{</b>	Check Point Firewall (Command Line Flat File)	Firewall Firewall	
Cisco Firewalls       Firewall         Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Clavister       Firewall         Demo       Firewall; Proxy; Intrusion Prevention System         Deny All       Intrusion Prevention System; Web Site         Image: Certificate       Image: Certificate         Image: View or update your current Click and DECiDE License Certificate.       Settings		Check Point Syslog UTM	Firewall	h
Cisco IronPort-C       Content Filtering; E-mail         Cisco IronPort-S       Proxy         Clavister       Firewall         Demo       Firewall; Proxy; Intrusion Prevention System         Deny All       Intrusion Prevention System; Web Site         Image: Certificate       Image: Certificate         Image: View or update your current Click and DECiDE License Certificate.       Settings		Cisco Firewalls	Firewall	L L L L L L L L L L L L L L L L L L L
Clavister       Firewall         Demo       Firewall; Proxy; Intrusion Prevention System         Deny All       Intrusion Prevention System; Web Site         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system       Image: Control of the system         Image: Control of the system	_	Cisco IronPort-C	Content Filtering; E-mail	
Demo       Firewall; Proxy; Intrusion Prevention System         Demy All       Intrusion Prevention System; Web Site         Image: Certificate       Image: Certificate         Image: View or update your current Click and DECiDE License Certificate.       Settings	[]	Clavister	Firewall	
Deny All       Intrusion Prevention System; Web Site         OK       Cancel         Help         License Certificate         View or update your current Click and DECiDE License Certificate.         Settings		Demo	Firewall; Proxy; Intrusion Prevention System	n 📗
OK       Cancel       Help         License Certificate       View or update your current Click and DECiDE License Certificate.       Settings		Deny All	Intrusion Prevention System; Web Site	
OK       Cancel       Help         License Certificate       View or update your current Click and DECiDE License Certificate.       Settings		•		
License Certificate View or update your current Click and DECiDE License Certificate. Settings			OK Cancel	Help
License Certificate         View or update your current Click and DECiDE License Certificate.         Settings				
View or update your current Click and DECiDE License Certificate. Settings	Li	cense Certificate		
Settings		View or update your current Click and E	DECIDE License Certificate	
				Settings
OK L Cancel L Apply L Help L			OK Cancal Acolu	Help

- 6. Click Cancel.
- 7. Click Cancel and exit the Log Source Configuration.

#### **B. Restore the WebPortal Configuration**

- Restore your own Click and DECiDE BAI projects (\*.wfv files) created with Click and DECiDE Builder (see Section 1.C.5). We recommend to put these file in the MyProject folder located at: C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects\My Projects (by default).
- Restore the external files (for example, the images) used by your own Click and DECiDE BAI projects (see Section 1.C.6). We recommend to put these file with the other image files in the Runtime\_projects folder located at:

C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects (by default).





**Note:** Do not replace any existing files. Complete the guide first and then modify the files you think are appropriate.

- Restore the standard reports and cube (see Section 1.C.7) located in: C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects\enu (by default) and C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects\utilities (by default) and C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects\cubes (by default).
- 4. Restore your customized menus (see Section 1.C.8) in the **Runtime\_projects** folder located at: C:\Program Files\Click and DECiDE\BAI\Runtime\_Projects (by default).

**Note:** Do not replace any existing menu. Complete the guide first and then modify the menu with the **Menu** editor.

- 5. Locate the Security Database backup file (.bck) from Section 1.C.3 on your hard drive.
- 6. Double click on the file. Administration Manager asks if you want to restore the Security Database.
  Click and DECiDE Administration Manager



7. Click Yes.





8. Click Update Security icon

	Click and DECiDE Administration Man	iger	_ = X
EFile Edit View	Tools Help		
	이 [1] [2] [2] [2] [2] [2] [2] [2] [2] [2] [2		
Mel 👩 Update Seco	urity		
Me Update Securi	ity Path	Name:	Muldenu
	%NetReport_Directory%(NetReport.wmu	ritanio.	Imymenu
	%NetReport_Directory%(NetReport Utilities.wmu	Datks	%NetBeport Directory
	%NetReport_Directory%(NetReport Static, who	Fain.	
	%NetReport_Directory%(NetReport Alerts.wmu		
a summer in	%NetReport_Directory%(MyMend.Wind		
•		•	
🧻 Data Sources 🛛 🎎	User Groups 🤱 Users 🗮 Menu 💡 Authentications		
Update Security			CAPS NUM SCRL

- 9. Click OK.
- 10. Close Administration Manager.

#### C. Restore your custom NSI Log Sources Configuration

- 1. Copy the YYYYMMDD-HHMM-user-vNNNN folder (see Section 1.B.4) to the folder: C:\Program Files\Click and DECiDE\NSI\ConfigurationBackup
- 2. Open the Management Console: Start>All Programs>Click and DECiDE>Network Security Intelligence>Management Console.

Note: the default login/password is now admin/admin.





3. Navigate to Click and DECiDE/localhost/Backups/User Backup YYYY-MM-DD HH:MM v.NN.NN (or NetReport/localhost/Backups/User Backup YYYY-MM-DD HH:MM v.NN.NN for earlier version).



4. Click Restore.



5. Click Yes.



6. Click OK.

Contact us: E-mail: <u>sales@clickndecide.com</u> Tel: +33 (0)6 71 99 86 60 Sales Offices: 98, route de la Reine - 92100 Boulogne-Bt, France. To contact your nearest Click&DECiDE partner, <u>click here</u>.





- 7. Navigate to Click and DECiDE/localhost/ULA (or NetReport/localhost/ULA for earlier version).
- 8. Click Apply Changes.



9. Navigate to Click and DECiDE/localhost/Log Vault (or NetReport/localhost/Log Vault for earlier version).





10. Click Apply Changes.



- 11. Open the **Click and DECiDE/localhost/Agents** (or **NetReport/localhost/Agents** for earlier version) sub-tree.
- 12. Navigate to a node with an asterix (\*).





13. Click Apply Changes.

🚟 Click and DECiDE Management Console	- [Console Root\Click and Decide\localhost\Agents\Flat File Parser*]	_ 🗆 🗙
🔚 Eile Action View Favorites Window	· Help	_ 8 ×
🔶 🔿 🔁 📊 🛛 🖬		
Console Root  Click and Decide  Click and Decide  Click and Decide  Click and Click a	Flat File Ag	ent
I statistics between I statistics between	>Click and Decide/localhost/Agents/Flat File	Parser<
☐ 🍫 Agents ① ① ② Check Point (Real Time)*	≣Flat File Spies	
🕀 🛃 Event Scheduler*	Current Spied Director	y List
	The files matching <b>*.log</b> ' of the directory <b>'C:\Program Files (x86)\Click and DECiDE\NSI\Logs\Engine\Flatfile\Fortinet FortiGate</b> ' are spied.	Edit
	Follow this link in order to add a new spied directory or to manage list.	*
🕀 📑 Log Vault		8
➡ Wizard Backup 2011-03-11 ₩ Wizard Backup 2011-03-11	#Applying Changes	
⊞ 👸 User Backup 2011-03-11 17	Click here to save all your changes for the flat file agent. All the changes you have made locally will be sent to the flat file agent.	
	Apply Changes	
	₿Agent Status	
	Stop Running Agent is running.	¢
K		
Done	·	

- 14. Repeat step 12. and 13. for every agent with an asterix (\*).
- 15. Close the Mangement Console.

#### **D. Restore the Scheduled Tasks**

#### For version 11 and later:

- 1. Open Web Portal: Start>All Programs>Click and DECiDE>Web Portal.
- 2. Click the Scheduled Tasks & Tasks tab.
- 3. Click 🌺.
- 4. Click Continue.
- 5. Click Browse....
- 6. Select the scheduled tasks configuration file d7tasks.xml (see Section 1.C.9) you have backed up.
- 7. Click Open.
- 8. Click Import.





#### For earlier version:

- 1. Open the Services Management Console: Start>Administrative Tools>Services
- 2. Right click on Click and DECiDE Task Manager and select Stop

🔍 Services							
File Action View Help							
🤹 Services (Local) 🛛 🔺	Description	Status	Startup Type	Log On As	<b>•</b>		
Application Experience	Processes		Manual	Local System			
Application Host Helper Service	Provides a	Started	Automatic	Local System			
Application Identity	Determines		Manual	Local Service			
Application Information	Facilitates		Manual	Local System			
Application Layer Gateway Service	Provides s		Manual	Local Service			
Application Management	Processes i		Manual	Local System			
ASP.NET State Service	Provides s		Manual	Network S			
Background Intelligent Transfer Service	Transfers f		Manual	Local System			
🔍 Base Filtering Engine	The Base F	Started	Automatic	Local Service			
Certificate Propagation	Copies use	Started	Manual	Local System			
Click and Decide Connect Service	Provides re	Started	Automatic	Local System			
Click and Decide Export Manager	Manages C	Started	Automatic	Local System			
Click and Decide Filter Engine	Manages r	Started	Automatic	Local System			
Click and Decide LEO Service	Manages C	Started	Automatic	Local System			
Click and Decide Log Vault	Manages t	Started	Automatic	Local System			
Click and Decide Server Helpers Service	Manages C	Started	Automatic	Local System			
Click and Decide Task Manager	Manages S	Started	Automatic	Local System			
Click and Decide Web Objects M	Manages C	Started	Automatic	Local System			
Click and Decide XML Remote Co	Provides s	Started	Automatic	Local System			
CNG Key Isolation	The CNG k		Manual	Local System			
COM+ Event System	Supports S	Started	Automatic	Local Service			
COM+ System Application	_ Manages t		Manual	Local System			
Computer Browser All Tasks	Maintains a		Disabled	Local System			
Credential Manager	Provides s		Manual	Local System			
Cryptographic Services	Provides fo	Started	Automatic	Network S			
DCOM Server Process Launcher Properties	The DCOM	Started	Automatic	Local System			
Desktop Window Manager Sessi Heln	Provides D	Started	Automatic	Local System	-		
Extended Standard							
Stop service Click and Decide Task Manager on Local Computer							

 Restore the scheduled tasks configuration file d7tasks.xml (see Section 1.C.9) located in: C:\Program Files\Click and DECiDE\BAI (by default).





4. In the Services Management Console, right click on Click and DECiDE Task Manager and select Start.

🗘 Services							
File Action View Help							
🔍 Services (Local)	Name 🔺	De	scription	Status	Startup Type	Log On As	<b>•</b>
	Application Experience	Pro	ocesses		Manual	Local System	
	Application Host Helper Service	Pro	ovides a	Started	Automatic	Local System	
	Application Identity	De	etermines		Manual	Local Service	
	Application Information	Fa	cilitates		Manual	Local System	
	Application Layer Gateway Service	Pro	ovides s		Manual	Local Service	
	Application Management	Pro	ocesses i		Manual	Local System	
	ASP.NET State Service	Pro	ovides s		Manual	Network S	
	Background Intelligent Transfer Service	Tra	ansfers f		Manual	Local System	
	Base Filtering Engine	Th	e Base F	Started	Automatic	Local Service	
	Certificate Propagation	Co	pies use	Started	Manual	Local System	
	Click and Decide Connect Service	Pro	ovides re	Started	Automatic	Local System	
	Click and Decide Export Manager	Ma	anages C	Started	Automatic	Local System	
	Click and Decide Filter Engine	Ma	anages r	Started	Automatic	Local System	
	Click and Decide LEO Service	Ma	anages C	Started	Automatic	Local System	
	Click and Decide Log Vault	Ma	anages t	Started	Automatic	Local System	
	Click and Decide Server Helpers Service	Ma	anages C	Started	Automatic	Local System	
	Click and Decide Task Manager	Start	es S		Automatic	Local System	
	Click and Decide Web Objects Manager	Ston	es C	Started	Automatic	Local System	
	Click and Decide XML Remote Configurati	Pause	es s	Started	Automatic	Local System	
	CNG Key Isolation	Resume	JG k		Manual	Local System	
	COM+ Event System	Restart	ts S	Started	Automatic	Local Service	
	COM+ System Application		es t		Manual	Local System	
	Computer Browser	All Tasks	🕨 ins a		Disabled	Local System	
	Credential Manager	Refresh	es s		Manual	Local System	
	Cryptographic Services	Ronosh	es fo	Started	Automatic	Network S	
	COM Server Process Launcher	Properties	:OM	Started	Automatic	Local System	
	Sestop Window Manager Session Manager	Help	es D	Started	Automatic	Local System	-
$\$ Extended $\lambda$ Standard /							
Start service Click and Decide Task Manager on Local Computer							

5. Close the **Services** Management Console.







### **Section 3: Check your configuration**

#### A. Log Acquisition

- 1. Start the log treatment.
- 2. Open the Performance Counters: Start>Administrative Tools>Performance.
- 3. Click the + in the toolbar.
- 4. Select the **NetReport Filter Engine** Performance object and select **All counters**.

Add Counters	? ×
<ul> <li>Use local computer counters</li> <li>Select counters from computer: \\RR0-W2003-32         \\\\RR0-W2003-32         \\\\\RR0-W2003-32         \\\\\\\RR0-W2003-32         \\\\\\\\\\\\\\\\\\\\\\\\\\\\\</li></ul>	<b>T</b>
Performance <u>o</u> bject:	
NetReport Filter Engine	
All counters	C <u>A</u> ll instances
C Select counters from list:	Select instances from list:
# nelf processed # of nelf in error queue # of nelff in queue Rate of nelff processed	NetReport Filter Engine
A <u>d</u> d <u>E</u> xplain	
	<u>C</u> lose

- 5. Click Add.
- 6. Click Close.





7. Check that you don't have any nelrf (Click&DECiDE events) in the error queue.



**Note:** the engine queues are stored in the folder **C:\Program Files\Click and DECiDE\NSI\Error agent Storage**. You can modify the destination of these files by changing the registry value: **HKEY\_LOCAL\_MACHINE\SOFTWARE\NetReport\MC\Agents\Error\StoragePath**.

You have to restart the Click & DECiDE Filter Engine service after any change

#### **B. Log Insertion**

- 1. Open Web Portal: Start>All Programs>Click and DECiDE>Web Portal.
- 2. Navigate to NSI Utilities/Database Status.





3. Open the project for the category of the log you have acquired. For example: **Firewall Statistics Utilities**.

🕼 Click and DECiDE Web Portal - Menus - Windows Internet Explorer						
Solution that the second secon	Menu.aspx 💌 😒 🍫 🗙	lo Bing	<b>₽</b> -			
A Favorites Click and DECIDE Web Portal - Menus						
M Click	& <b>DECiDE</b>					
Web Server Configuration	Firewall Statistics Utilities	Size Modification	Creation			
Menus	💷 <u>1 - Selected Record Details</u>	0 1/21/2010 5:14:15 PM	1 9/2/2004 10:43:08 AM			
🗆 🚞 NSI Utilities	💷 <u>2 - Number of Records in the Firewall Tables</u>	0 1/21/2010 5:20:02 PM	1 9/2/2004 10:43:08 AM			
🖃 🚘 Database Status	💷 <u>3 - Address Definition Management</u>	0 1/21/2010 4:07:29 PM	1 9/2/2004 10:43:08 AM			
Firewall Statistics Utilities	🕼 <u>4 - Firewall Aggregation Process Status</u>	0 4/28/2010 4:57:31 PM	1 9/2/2004 10:43:08 AM			
Proxy Statistics Utilities						
🗉 🚞 NSI Alert Management						
Scheduled Tasks & Tasks Web Part Configuration						
Content Builder						
Web Server Administration						

4. Open the report **2 - Number of Records in the Firewall Tables**.





5. Enter the time interval corresponding to the date of your logs. For example, if you are parsing logs from 10 days ago, enter 10 in the first text box.

🖉 Click and DECiDE Web Portal - Menu	s - Windows Internet Explorer	
Solution v localhost/dvweb/	Menu.aspx 🔄 🗟 😽 🗙 📴 Bing	<b>₽</b> -
🔶 Favorites 🛛 🏀 Click and DECIDE Web	Portal - Menus	
M Click	& <b>DECiDE</b>	
Web Server Configuration	🚮 🗐 📚 🛛 Parameters 🚽 Result 🚽 Both	
Menus         Image: Status         Image:	2 - Number of Records in the Firewall Tables From: Today - X days To: Today - Y days Start time: S/6/2009 12:00:00 AM Stop time: S/6/2010 11:59:59 PM Firewall? (Ignore for all): IGNORE Output Format: PDF Run	

6. Click Run.



Contact us: E-mail: <u>sales@clickndecide.com</u> Tel: +33 (0)6 71 99 86 60 Sales Offices: 98, route de la Reine - 92100 Boulogne-Bt, France. To contact your nearest Click&DECiDE partner, <u>click here</u>.

# www.clickndecide.com





7. Check that logs are inserted into the rawdata table.

#### **C.** Report Generation

- 1. Open the Scheduled Tasks panel: Start>Control Panel>Scheduled Tasks.
- 2. Right Click on Click and DECiDE Scheduled Dashboards and select Run.

🔮 Scheduled Tasks							
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools Adva <u>n</u> ced <u>H</u> elp						2	
🕝 Back 👻 🕤 🖌 🏂 Search 🌔 Folders 🛛 🙀 🎯 🗙 🍤 🛄 🗸							
Address 🖆 Scheduled Tasks 🔹 🎅 Go							
Name 🔺		Schedule	Next Run Time	Last Ru	Status	Last Result	
Add Scheduled Task							
Click and DECIDE NSI Scheduled	Run	10 AM	1:00:00 AM	Never		0×0	
Burge Alerts Tables	End Task	:3 AM	1:23:00 AM	Never		0×0	
🛛 👧 SQL Firewall Alert		ed ed	Disabled	Never		0×0	
	Cut						
	Сору						
	<u>D</u> elete						
	Rena <u>m</u> e						
	P <u>r</u> operti	es					
-							







3. Wait for the task to complete (it may take some time depending on the volume of your logs).

睂 Scheduled Tasks							
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools Adva <u>n</u> ced <u>H</u> elp							
🕝 Back 🔻 🕥 👻 🏂 Search 🌔 Folders 🛛 🙀 🎯 🗙 🏹 🛄 🗸							
Address 🙆 Scheduled Tasks							
Name 🔺	Schedule	Next Run Time	Last Ru	Status	Last Result		
🖸 Add Scheduled Task							
Click and DECiDE NSI Scheduled Dashboards	At 1:00 AM	1:00:00 AM	5:01:41	Running	0×0		
👸 Purge Alerts Tables	At 1:23 AM	1:23:00 AM	Never		0×0		
🛜 SQL Firewall Alert	Disabled	Disabled	Never		0×0		
•					Þ		

- 4. Return to **Web Portal** (see Section 5.B).
- 5. Navigate to NSI Reports and Analysis/Published Report.





6. Select the category of the log you have acquired. For example: Firewall.

🖉 Click and DECiDE Web Portal - Menu	s - Windows Internet Explorer		
🚱 🗢 🙋 http://localhost/dvweb/	Menu.aspx	🖌 🗟 👉 🗙 📴 Bing	
🔆 Favorites 🛛 🄏 Click and DECiDE Web	Portal - Menus		
Clicka	& <b>DECil</b>	DE	
Web Server Configuration	Firewall	Size Modification	Creation
Menus	🔁 <u>Firewall Daily 100505</u>	164,630 5/6/2010 5:02:25 PM	1 5/6/2010 5:02:23 PM
Contraction of the second			
Proxy			
🚘 Dynamic Reports			
🚘 Forensic Analysis			
🚔 My Projects			
🖃 🗮 NSI Utilities			
🖃 🚞 Database Status			
Firewall Statistics Utilities			
Click and DECIDE Audit			
Proxy Statistics Utilities			
Si Alert Management			
Web Part Configuration			
Content Builder			
Web Server Administration			
1			

7. Check that a report has been generated. If you have inserted yesterday's logs, the reports should contain some data.

#### **D. Event Viewer**

1. Open the Event Viewer: Start>Administrative Tools>Event Viewer.







2. Select the Application event log.

😽 Event Viewer				_			
<u>File Action View H</u> elp							
	) 😫 💵						
Event Viewer (Local)	Application 1,739 event(s)						
Application     Security     System     Interpet Explorer	Туре	Date	Time	Source	Cat 🔺		
	Information	5/6/2010	4:39:09 PM	MSSQL\$SQLEXPRESS	(2)		
	Information	5/6/2010	4:16:39 PM	MSSQL\$SQLEXPRESS	(2)		
	Warning	5/6/2010	4:14:31 PM	Perflib	Nor		
	Warning	5/6/2010	4:14:31 PM	Perflib	Nor		
	Warning	5/6/2010	4:14:30 PM	Perflib	Nor		
	Information	5/6/2010	3:01:02 PM	Click and DECiDE Syslog Agent	Nor		
	Information	5/6/2010	3:01:02 PM	Click and DECiDE Syslog Agent	Nor		
	Information	5/6/2010	3:01:02 PM	Click and DECiDE Syslog Agent	Nor		
	Information	5/6/2010	3:01:02 PM	Click and DECiDE Syslog Agent	Nor		
	Information	5/6/2010	3:00:57 PM	Click and DECiDE Flat File Ag	Nor		
	Information	5/6/2010	3:00:57 PM	Click and DECiDE Flat File Ag	Nor		
	Information	5/6/2010	3:00:57 PM	Click and DECiDE Flat File Ag	Nor		
	Information	5/6/2010	3:00:57 PM	Click and DECiDE Flat File Ag	Nor		
	Warning	5/6/2010	2:52:21 PM	Click and DECiDE NSI Engine	Nor		
	Information	5/6/2010	2:52:21 PM	Click and DECiDE NSI Engine	Nor		
	🚹 Warning	5/6/2010	2:52:21 PM	Click and DECiDE NSI Engine	Nor		
	Information	5/6/2010	2:52:21 PM	Click and DECIDE NSI Engine	Nor 🗸 I		
	1	El closes	0.50.04.000				

3. Check that there are no error from a Click and DECiDE process.

