

SNARE

System iNtrusion Analysis & Reporting Environment

Guide to Snare for Windows

INTERSECT
ALLIANCE

Documentation History

Version No.	Date	Edits	By whom
0.9	7 November 2003	First draft of the Guide to Snare for Windows.	George Cora
1	13 November 2003	Approved Version	George Cora
1.1	15 December 2003	Conversion of title graphics	Leigh Purdie
1.2	23 July 2004	Included remote control and other updates	George Cora
1.3	1 August 2004	Final version for 2.4 release	Leigh Purdie
2.0	2 April 2005	Minor rewording	George Cora
2.1	30 November 2005	Formatting changes and new versions	George Cora
2.2	12 December 2005	Minor formatting change	Leigh Purdie
2.3	28 April 2006	Included documentation for supported agents	George Cora
2.4	15 May 2006	Updated documentation on supported agents	David Mohr
2.5	10 August 2006	Removed GUI documentation and included new remote control features	David Mohr
2.6	26 October 2006	Included documentation for new USB features and updated graphics	David Mohr
2.7	16 August 2007	Updated documentation for new silent install and event exclusion options	David Mohr
2.8	4 June 2008	Updated supported features	David Mohr
2.9	1 July 2010	Updated graphics and feature information	David Mohr
4.0	9 June 2011	Updated documentation on new single installer. Documented new silent install feature. Updated document version to align with new agent.	David Mohr

© 1999-2011 Intersect Alliance Pty Ltd. All rights reserved worldwide.

Intersect Alliance Pty Ltd shall not be liable for errors contained herein or for direct, or indirect damages in connection with the use of this material. No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Intersect Alliance Pty Ltd. This does not include those documents and software developed under the terms of the open source General Public Licence, which covers the Snare agents and some other software.

The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance Pty Ltd. Other trademarks and trade names are marks' and names of their owners as may or may not be indicated. All trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

About this guide

This guide introduces you to the functionality of the Snare agent for Windows operating systems. The development of 'Snare for Windows' will allow event logs collected by the Windows operating system (including NT, 2000, 2003, XP, Vista, 2008 and Windows7), to be forwarded to a remote audit event collection facility. Snare for Windows will also allow a security administrator to fully remote control the application through a standard web browser if so desired.

Other guides that may be useful to read include:

- Snare Server User's Guide.
- Installation Guide to the Snare Server.
- Snare Server Troubleshooting Guide.
- The Snare Toolset - A White Paper.

Table of contents:

1 Introduction.....	4
2 Overview of the Snare Agents.....	5
3 Installing and running Snare.....	7
3.1 Wizard Install.....	7
3.2 Silent Install.....	13
3.3 Running Snare.....	14
4 Setting the audit configuration.....	15
4.1 Auditing control	15
5 Audit event viewer functions.....	21
6 Remote control and management functions.....	22
7 Retrieving user and group information.....	24
8 Snare Server.....	25
9 About Intersect Alliance.....	27
Appendix A - Event output format.....	28
Appendix B - Snare Windows registry configuration description.....	29
Appendix C - Objectives and security event IDs.....	32

1 Introduction



The team at Intersect Alliance have experience with auditing and intrusion detection on a wide range of platforms - Solaris, Windows NT/2000/2003/XP/Vista/2008/Windows7, Netware, Tru64, Linux, AIX, IRIX, even MVS (ACF2/RACF); and within a wide range of IT security in businesses such as National Security and Defence Agencies, Financial Service firms, Government Departments and Service Providers.

This background gives us a unique insight into how to effectively deploy host and network intrusion detection systems that support and enhance an organization's business goals.

The development of 'Snare for Windows' allows Windows event logs to be collected from Windows NT/2000/2003/XP/Vista/2008/Windows7, and forwarded to a remote audit event collection facility. Snare for Windows will also allow a security administrator to fully remote control and monitor the application through a standard web browser. Snare has been designed in such a way as to allow the remote control functions to be easily effected manually, or by an automated process, with built in security measures to guard against unauthorized changes.

Intersect Alliance are proud to release Snare for Windows under an open source license. Other Snare agents are also available under the terms of the GNU Public License, including Snare for Solaris, AIX, IRIX, Linux, IIS, Apache and many more. The overall project is called '**Snare**' - **System iNtrusion Analysis & Reporting Environment**. The '**Snare Server**' is a commercial release of software beneficial to organizations that wish to collect from a wide variety of Snare agents and appliances such as firewalls or routers.

Intersect Alliance welcomes and values your support, comments, and contributions. Our contact details are available from our contact page at www.intersectalliance.com.

2 Overview of the Snare Agents



Snare operates through the actions of a single component; the **SnareCore** service based application (*snarecore.exe*). The **SnareCore** service interfaces with the Windows event logging sub-system to read, filter and send event logs from the primary Application, System and Security event logs to a remote host. Please note that where available, the agent is also capable of reading, filtering and sending logs from the DNS Server, File Replication Service, DFS-Replication and Directory Service logs, as well as any Custom event log sources. In addition, on Windows 2000, 2003 and XP, **SnareCore** will collect USB connect and disconnect notifications.

Once gathered, the logs are then filtered according to a set of objectives chosen by the administrator, and passed over a network using the UDP or TCP protocol, to a remote server. *The Custom event log capability, TCP protocol capability and the ability to send events to multiple hosts is only available to users who have purchased the supported version of the agents. See Chapter 8 of this document for further details.* The **SnareCore** service can be remotely controlled and monitored using a standard web browser (see Figure 1a and Figure 1b for example screens).

The **SnareCore** service reads event log data from the core Windows event sources listed above, plus USB device notifications. **SnareCore** converts the binary/encoded event log record to a human-readable format. If a SYSLOG or Snare Server is being used to collect the event log records, the event records will be TAB delimited. This format, is further discussed in *Appendix A Event output format on page 28*. The net result is that a raw event, as processed by the SnareCore service may appear as follows:

Example:

```
Test_Host MSWinEventLog 0 Security 3027 Thu Jun 09 09:30:43 2011 593
Security Administrator User Success Audit LE5678WSP Detailed
Tracking A process has exited: Process ID: 656 User Name:
Administrator Domain: LE5678WSP Logon ID: (0x0,0x6C52)
```

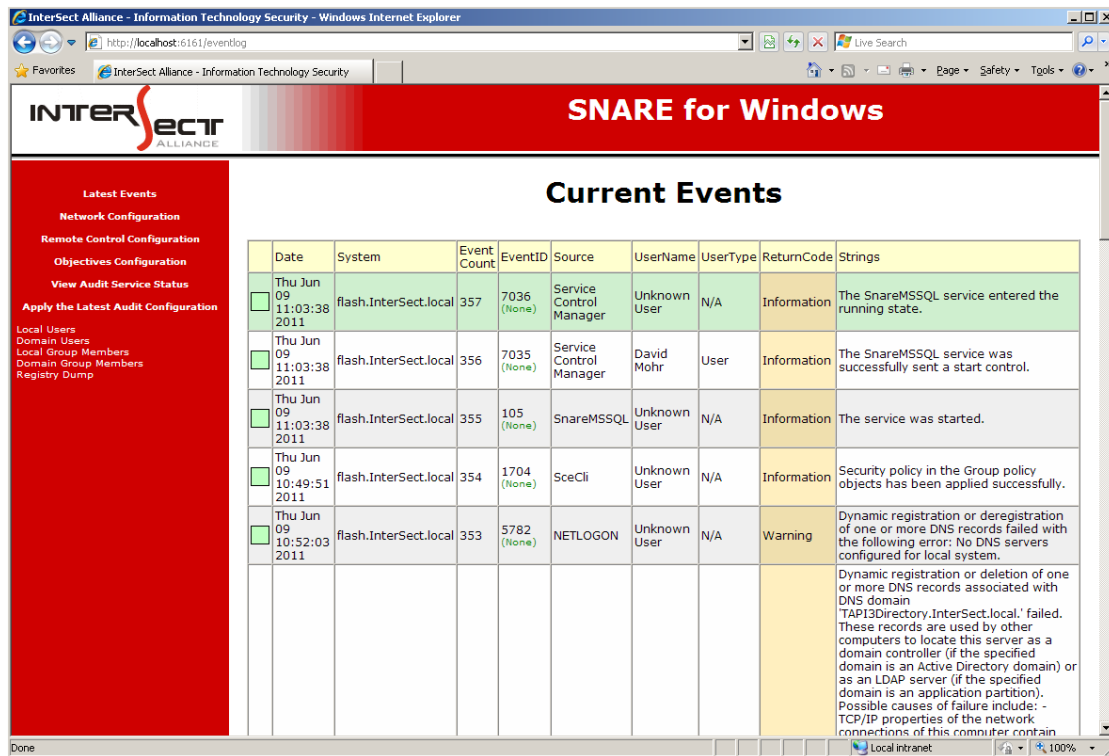


Figure 1a Main event window (Windows 2003)



Figure 1b Main event window (Windows Vista)

3 Installing and running Snare



Snare is provided as a single-file self-extracting archive, and has been designed with an installation wizard and advanced silent install options to allow for easy installation and configuration of all critical components. The self-extracting archive installs all components of Snare, including icons, changelog documentation, and the snarecore.exe binary. The snarecore.exe binary implements the “SnareCore” service, which is responsible for reading event log records, filtering the events according to the objectives, providing a web based remote control and monitoring interface and providing all the necessary logic to allow the binary to act as a service defined in any of the supported versions of Windows (including 64 bit versions).

3.1 Wizard Install

Download the SnareForWindows-*{Version}*.exe file from the Intersect Alliance website (where *{Version}* is the most recent version of the file available).

Ensure you have administrator rights, double-click the SnareForWindows-*{Version}*.exe file. This is a self-extracting archive, and will not require WinZip or other programs.

You will be prompted with the following screens:

Welcome to the Snare Setup Wizard



This screen provides a brief overview of the product you are about to install.

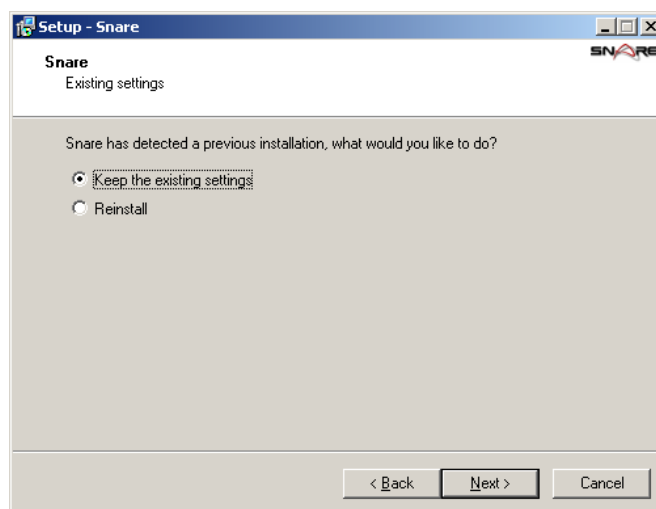
Where available, select “Next” to continue the installation, “Back” to return to the previous screen or “Cancel” to abort the installation.

License Page



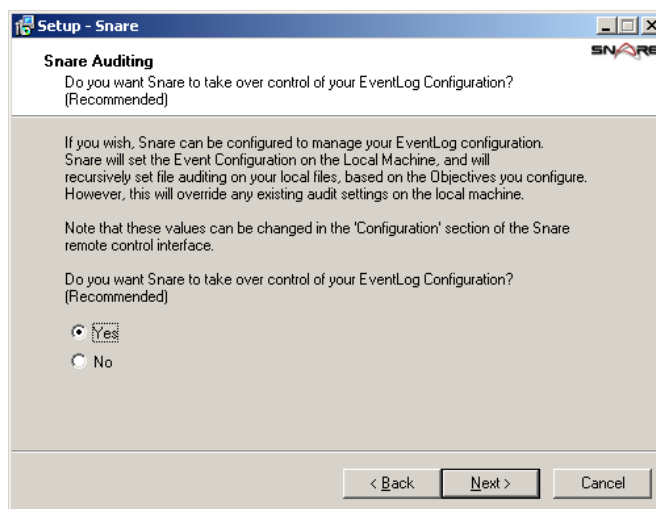
The License Page displays the End User License Agreement (EULA) for supported versions of the agent or the GNU General Public License (GPL) for the open source release. Please read the document carefully and if you accept the terms of the agreement, select “I accept the agreement” and the “Next” button will be enabled allowing the installation to continue.

Existing Install (Upgrade only)



If the Wizard detects a previous install of the Snare agent, you will be asked how to proceed. Selecting “Keep the existing settings” will leave the agent configuration intact and only update the Snare files. The Wizard will then skip directly to the Ready to Install screen. Selecting “Reinstall” will allow the configuration wizard to continue and replace your existing configuration with the values you input. Note that replacing the configuration does not happen immediately; it takes place after selecting the “Install” button on the Ready to Install screen.

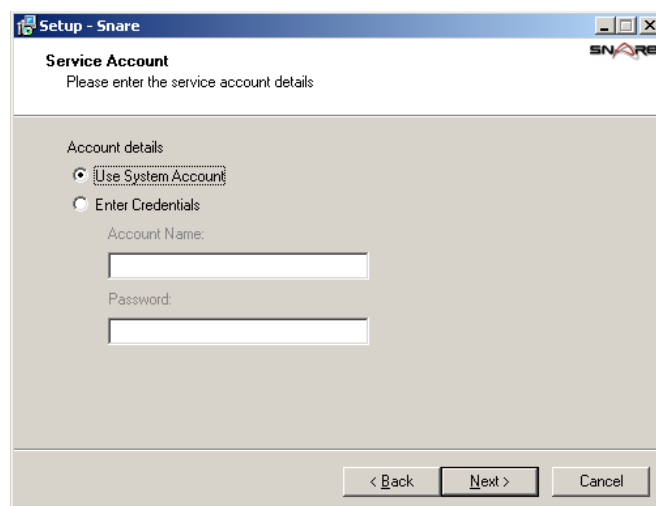
Auditing



The Snare agent has the ability to automatically configure the audit settings of the local machine to match the configured objectives. To enable this feature, select “Yes”.

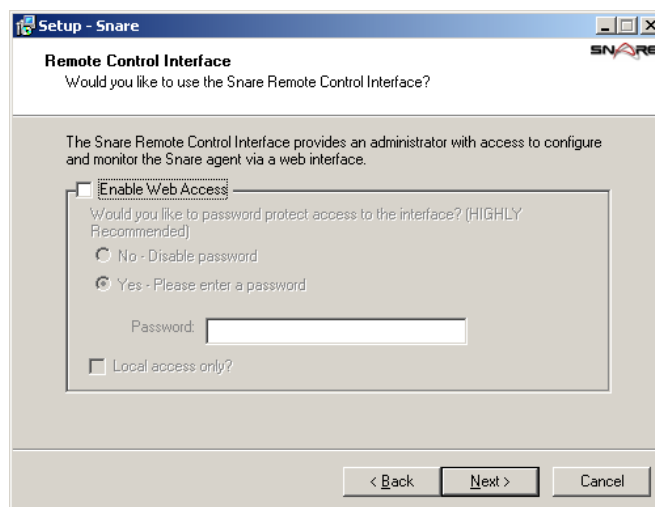
NB: VERY IMPORTANT: IF YOU DO NOT SELECT THIS OPTION AND/OR THE WINDOWS ACTIVE DOMAIN GROUP POLICIES OVERWRITE THE AUDIT SETTINGS, THEN YOU WILL NEED TO MANUALLY ENSURE THAT THE WINDOWS AUDIT SETTINGS MATCH YOUR DESIRED OBJECTIVE CONFIGURATION.

Service Account



The Snare agent requires a service account to operate. The default option is to use the in-built SYSTEM account.

Remote Control Interface



This screen provides a means to configure the Snare Agent's web interface for first time use.

Select from the following options to configure the *Snare* web interface:

- “Enable Web Access”

Select this option to enable the web interface. If this option is NOT selected, all configuration changes will need to be made by directly modifying registry settings and the service will need to be restarted for any changes to take effect.

- “No - Disable password”

The web interface will operate without a password, allowing unauthenticated access to the configuration options.

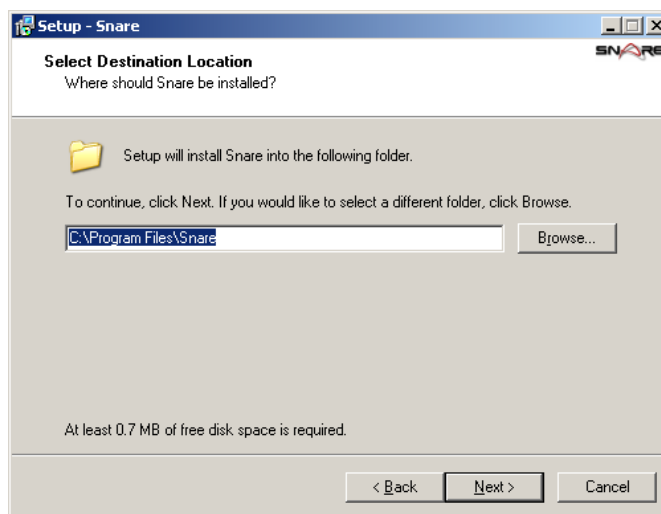
- “Yes - Please enter a password”

A user/password combination will be required to access the web interface. The user is always “snare” and the password will be set to text supplied in the “Password” field.

- “Local access only?”

Selecting “Local access only” will configure the web interface to restrict access to local users only. Remote users will be unable to contact the web interface.

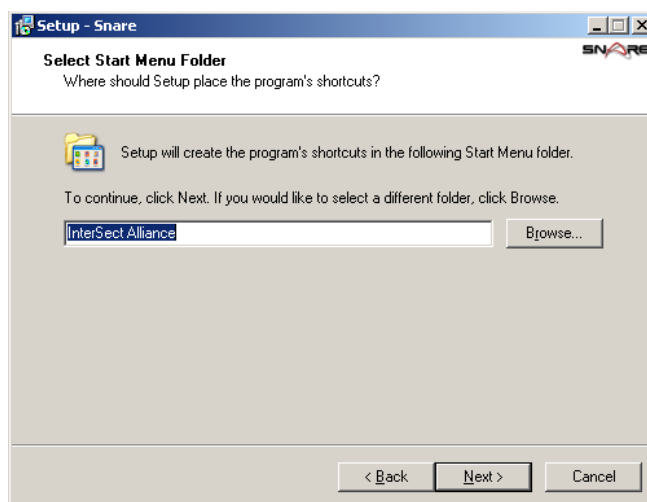
Select Destination Location



This screen provides a means to select the folder where the Snare Agent will be installed. If the folder name specified does not exist, it will be created. It is important that this folder has at least enough space available to install the agent.

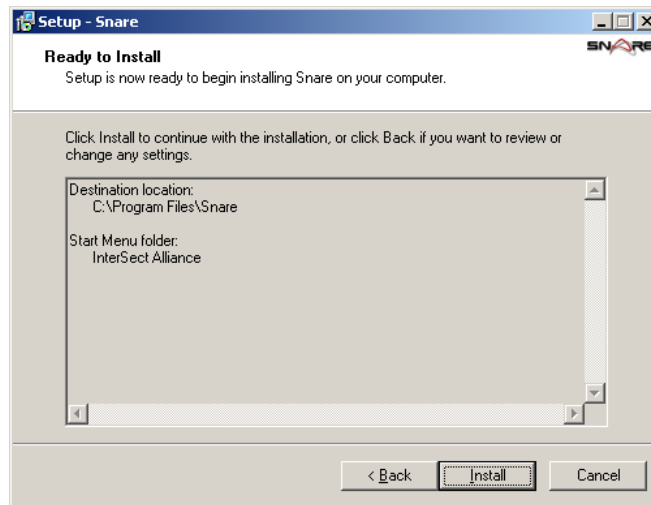
By default, the installation wizard will install Snare under the *Program Files* folder. If a different destination is desired, one may be selected via the “Browse” button, or by typing the full path name directly into the box.

Select Start Menu Folder



Select the program group within the *Start Menu* under which a shortcut to the Snare Agent's remote control interface will be created.

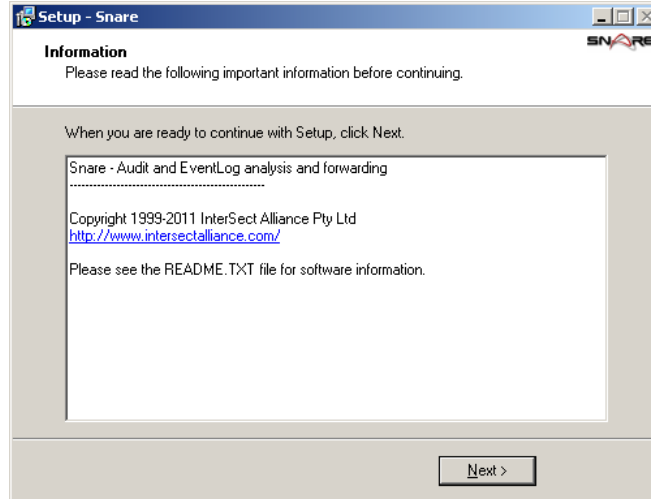
Ready to Install



This screen provides a final summary of the chosen installation options. If the options listed are incorrect, select the “Back” button to return to previous screens and change their configuration.

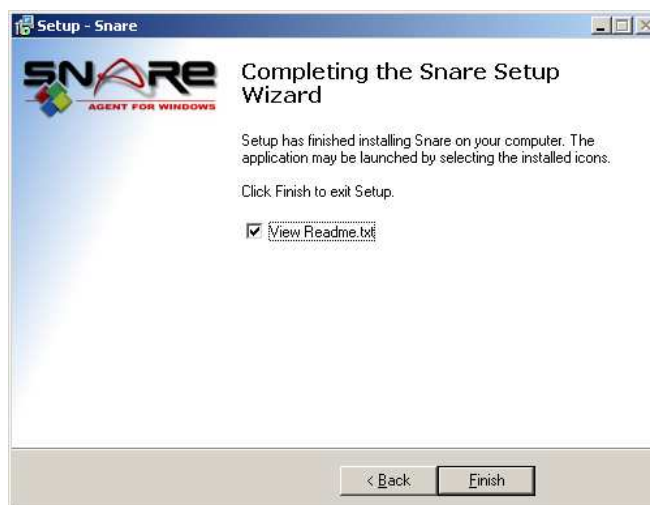
Select the “Install” button to proceed with the listed choices, or “Cancel” to abort the installation without making any changes. The “Back” button may be used to return to the previous screen.

Information



This screen provides basic copyright information and last minute documentation which may not be included within this manual.

Completing the Snare Setup Wizard



This is the final screen of the installation wizard. By default, a Readme.txt file will be opened after selecting “Finish”. Please review this readme for details of the changes made to the agent.

3.2 Silent Install

The silent install option is provided for system administrators wishing to automate the process of installing Snare for Windows.

Command line options

The Snare installer has a number of command line options to support silent, automated installations:

- **/VerySilent** - The Wizard will be hidden for the duration of the installation process. Any message boxes will still be displayed.
- **/SuppressMsgBoxes** - Any messages boxes will be dismissed with the default answer.
- **/Log="filename"** - Two log files will be create: *filename* and *filename.Snare.log*. The Wizard installation log will be written to *filename* and a detailed Snare installation log will be written to *filename.Snare.log*.
- **/LoadInf="INFfile"** - The *INFfile* is a template file produced by another Snare installation. It contains all the necessary information to complete the installation and configure the agent for normal operations. See below for more details on how to produce this file.
- **/SnarePass="ZPass"** - For security reasons, some parts of the *INFfile* are encrypted and require a decryption password. *ZPass* is an encrypted version of the decryption password and is produced as part of the *INFfile* procedure.
- **/Reinstall** - Tell the installer to overwrite any existing installation.
- **/Upgrade** - Tell the installer to upgrade the existing installation. If no existing installation is detected, the installer will abort. This option will only upgrade the Snare files, all configuration settings will remain untouched and the “LoadInf” file will be ignored.

Silent Install Setup Information File (INF)

To silently deploy a completely configured agent, the installer requires the help of a Setup Information File, also known as an INF file. To produce a working INF file, follow these steps:

1. Install the Snare agent using the Wizard.
2. Using the web interface (see chapter 3.3 below), configure the agent's Network and Remote Control settings.
3. Configure one or more objectives.
4. Ensure you have administrator rights, open a command prompt and browse to the directory where Snare is installed.
5. Run the following commands:
 - **SnareCore.exe -x**
Export the information and error messages, along with the INF file contents to the screen.
 - **SnareCore.exe -x "INFfile"**
Export the information and error messages to the screen and write the INF file contents to *INFfile* for use with the `/LoadInf` command line option.
6. Follow the prompts carefully and where required, enter the necessary password information for either the Service Account and/or the Sensitive Information encryption.
7. Note down the Installation Password. The `/SnarePass` command line option will accept this encrypted password and use it to decrypt the sensitive information in *INFfile*.

Silent Deployment

To install using the silent installer, ensure you have administrator rights, open a command prompt and browse to the directory where the setup program is stored. Using the `"/verysilent"` option, run the file:

```
SnareForWindows-{Version}.exe /verysilent /suppressmsgboxes /LoadInf="Settings.inf"
```

This will install the *Snare* application with the options specified in the Settings.INF file and will not display any pop-up windows. This option is suitable for packaging and non-interactive installations.

3.3 Running Snare

Upon installation of the Snare agent, an 'Intersect Alliance' menu item is available from the **All Programs** Windows menu. The Snare remote control launch menu is then available from **All Programs->Intersect Alliance->Snare for Windows**. If the menu launcher is not available, the Snare control interface may be accessed via a web browser from the local machine by visiting the URL <http://localhost:6161/>. If you previously configured a password, you will need this to log in, along with the username 'snare'.

For events to be passed to a remote host, the *SnareCore* service must be running. Ensure the *SnareCore* service is active by selecting the Services item in Control Panel on older Windows NT hosts or by selecting Services from the **Administrative Tools** or **Computer Management** menus. If Snare is not running, double click on the service name, then select **Automatic** from the Startup Type list so that the service is started automatically when the host is rebooted and then click the **Start** button. Click **OK** to save the settings.

4 Setting the audit configuration



The configurations for Snare are stored in the system registry. The registry is a common storage location of configuration parameters for Windows programs and other applications. The registry location contains all the details required by Snare to successfully execute. Failure to specify a correct configuration will not 'crash' the *SnareCore* service, but may result in selected events not being able to be read and the agent not working as specified.

Note manual editing of the registry location is possible, but care should be taken to ensure that it conforms to the required Snare format. Also, any use of the web based Remote Control Interface to modify selected configurations, will result in manual configuration changes being overwritten. Details on the configuration format for the registry can be viewed in *Appendix B - Snare Windows registry configuration description on page 29*.

The most effective and simplest way to configure the *SnareCore* service is to use the Snare web based Remote Control Interface. The audit configuration settings can be selected from the menu items on the left-hand side (see Figure 2).

4.1 Auditing control

The initial audit configuration parameters to consider are:

- The hostname, IP address and UDP port of the remote collection server. *Please note: The TCP protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased a Snare Server, through the supported agents. See Chapter 8 of this document for further details.*
- The requirement to incorporate a SYSLOG header. Snare Server users should only send events to UDP or TCP port 6161.
- Whether Snare is to automatically set the necessary audit parameters for effective auditing. Note it is recommended that the audit configuration parameters shown in Figure 2 are enabled. **NB: VERY IMPORTANT: IF YOU DO NOT SELECT THIS OPTION AND/OR THE WINDOWS ACTIVE DOMAIN GROUP POLICIES OVERWRITE THE AUDIT SETTINGS, THEN YOU WILL NEED TO MANUALLY ENSURE THAT THE WINDOWS AUDIT SETTINGS MATCH YOUR DESIRED OBJECTIVE CONFIGURATION.**
- The requirement to log events to a file (separate to the event viewer log files). Note that if this selection is made the log files must be managed, since Snare *will not* rotate or otherwise manage these files. **Failure to do so may result in a huge amount of disk space being taken up by this log file.**
- The checkbox titled '*Perform a scan of ALL objectives, and display the maximum criticality?*', if set, will scan through each defined objective, and save the highest criticality value encountered. The event will be sent with this criticality value. Turning off this option will send the event as soon as ONE match is detected, which may reduce the CPU usage of the Snare agent, but the criticality value may not be the highest possible value. Users of the 'Snare Server' software can safely choose to turn off this option, as the Snare Server does not use the Windows criticality value.
- If 'SYSLOG' is used, whether Snare is configured to use a static, or dynamic priority value. If 'Dynamic' is selected as the SYSLOG priority value, the priority sent to the remote SYSLOG server, will mirror the Snare 'criticality' value of the matched objective. (Note you may wish to ensure '*Perform a scan of ALL objectives, and display the maximum criticality?*' is also selected).

- Note that the following options are only available to users who purchase a Snare Server. These are not part of the Open Source toolset. See Chapter 8 below for more details on the supported versions of the Snare agents.
 - Use UDP or TCP - Select the protocol you would like Snare to use when sending events. Using TCP will guarantee message delivery.
 - Event log cache size - Modify the default Windows event log size, allowing you to easily configure the desired cache size. Combined with the TCP, this option will allow the agent to cache messages if there is a network failure or the Snare Server is otherwise unavailable.
 - Encrypt Message - Encrypt messages between the agent and the Snare Server. This option requires matching Remote Access Passwords on both the agent and the Snare Server.
- USB auditing (Windows 2000, 2003 and XP only). To capture these events, you will need to activate USB auditing (see Figure 2) and then create a new objective to capture USB events. USB events will NOT be captured by default.

All of the aforementioned parameters are found in the **Network Configuration** window.

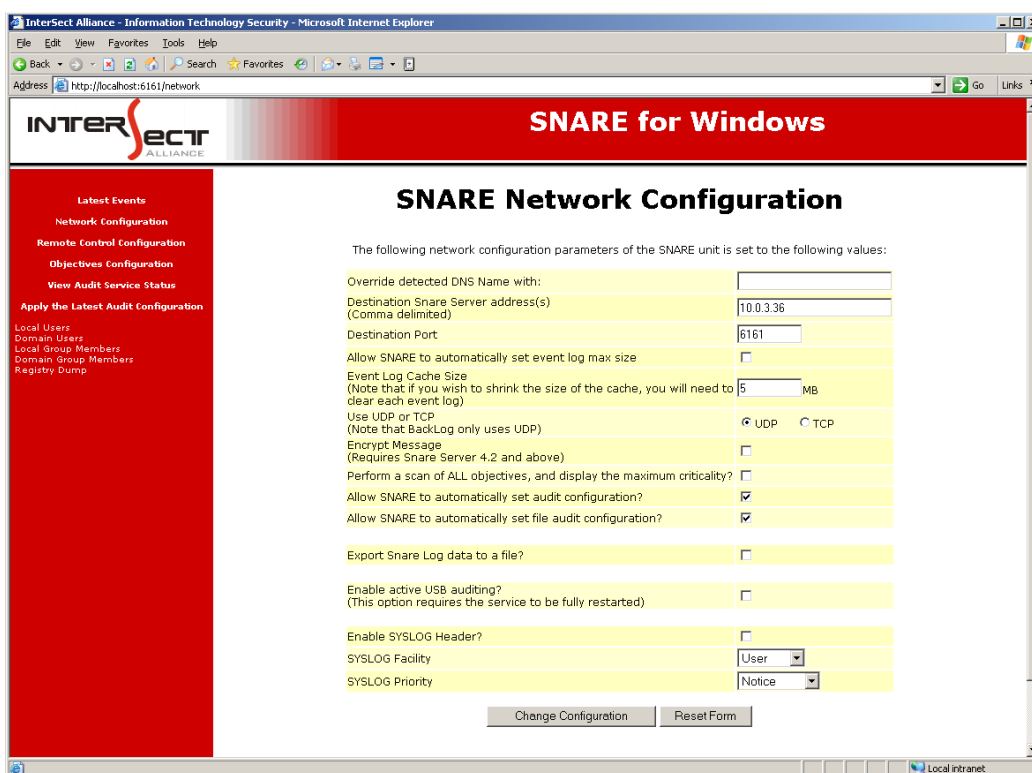


Figure 2 Network Configuration Window

The **Override detected DNS Name** field can be used to override the name that is given to the host when Windows is first installed. Unless a different name is required to be sent in the processed event log record, leave this field blank and the **SnareCore** service will use the default host name set during installation. Note that executing the command **hostname** on a command prompt window will display the current host name allocated to the host.

The SYSLOG function is a UNIX based service that allows for event records to be processed remotely, but has the requirement that the event records need to be in a specific format. This feature will allow the event log record to be formatted so as to be accepted by a SYSLOG server. In order to effectively audit events, there are a number of parameters which need to be automatically or manually set. These are:

- **Event Log Retention.** There is a risk in event auditing, that the Windows event logs may fill up. If this is the case, then no further events are able to be read and the auditing function effectively stops. If the **Automatically set audit configuration** checkbox has been set as shown in Figure 2, then Snare will set all the event logs to overwrite the logs as required. This will therefore prevent the event log sub-system from stopping. To prevent the agent from modifying the retention settings, use the *LeaveRetention* registry value defined in the Snare Windows registry configuration description on page 29.
- **Auditing of Categories.** If the **Automatically set audit configuration** checkbox has been set as shown in Figure 2 then the system will also select the required event log parameters to meet those objectives (see below) which have been set. This will alleviate any problems associated with ensuring that the correct audit event categories have been selected, based on those event IDs which are required to be filtered. This is also the most optimized setting in terms of system performance.

NB: VERY IMPORTANT: IF YOU DO NOT SELECT THIS OPTION AND/OR THE WINDOWS ACTIVE DOMAIN GROUP POLICIES OVERWRITE THE AUDIT SETTINGS, THEN YOU WILL NEED TO MANUALLY ENSURE THAT THE WINDOWS AUDIT SETTINGS MATCH YOUR DESIRED OBJECTIVE CONFIGURATION.

- **Setting of file system auditing.** In order for Windows to collect file accesses, not only must the correct audit category be selected, but also the correct file system parameters must also be set. The checkbox titled **Automatically set file system audit configuration**, as shown in Figure 2, will automatically set these parameters, based on the objectives which have been set. It is highly recommended that this checkbox be selected.

A major function of the Snare system is to filter events. This is accomplished via the advanced auditing 'objectives' capability. Any number of objectives may be specified and are displayed within the **Objective Configuration** window (Figure 3). These objective will be processed by the agent in the order they appear, that is, top to bottom. Please use the up and down arrows in the **Order** column to reorganize your objectives into the appropriate order. A listed objective may be viewed or modified within the **Create or Modify an Objective** window, as shown in Figure 4.



Figure 3 Objectives Configuration Window

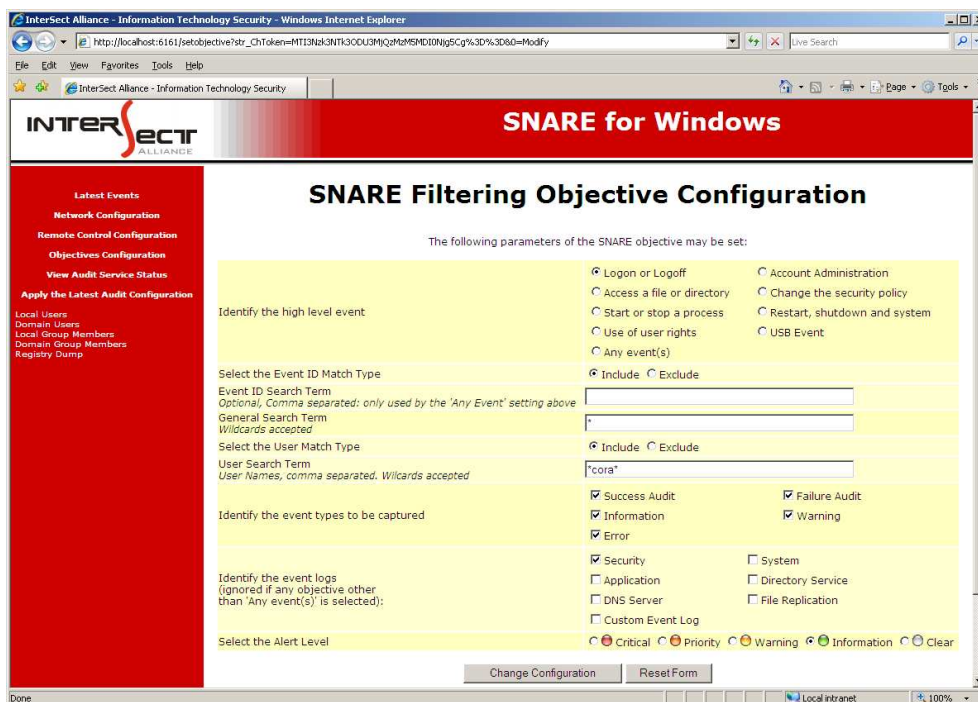


Figure 4 Create or Modify an Objective Window

Each of the objectives provides a high level of control over which events are selected and reported. Events are selected from a group of high level requirements and further refined using selected filters. Only **Windows Security Event Log** events are contained within the high level groups. Details on which Windows Event Log event IDs are used to generate the following objectives can be found in *Appendix C - Objectives and security event IDs on page 32*:

- Logon or Logoff.
- Access a file or directory.
- Start or stop a process.
- Use of user rights.
- Account administration.
- Change the security policy.
- Restart, shutdown and system.
- USB events
- Any event(s).

Note that the groups above are provided to service the most common security objectives that are likely to be encountered. If other event types are required, then the **Any event(s)** objective will allow fully tailored objectives to be set. From each of these groups, a level of importance can be applied. These criticality levels are **critical**, **priority**, **warning**, **information** and **clear**. These security levels are provided to enable the Snare user to map audit events to their most pressing business security objectives and to quickly identify the criticality of an event via the coloured buttons on the Snare remote control interface, as shown in Figure 4.

The following filters can be applied to incoming audit events:

- Filter on the **EventID Match Type** field
This allows the user to select whether to include or exclude messages that match this objective. If an objective is set to 'Exclude', matching event logs will be immediately discarded. Please note, objectives are processed from the top of the list to bottom, so it is important to place any Exclude objectives at the top of the list to ensure unwanted events are discarded. Also ensure the **Perform a scan of ALL objectives** configuration option is disabled in the **Network Configuration** window.
- Filter on the **EventID Search Term** field
Each event contains a unique number known as the **Event ID**. If the high level event **Any event(s)** is selected, then the user is able to filter on the EventID field. If multiple events are required, the user may enter the event IDs as a comma separated string. **Example: 562,457,897**. Using the wildcard character '*' will select all events. Use the wildcard with caution since ALL events will be collected and passed to the remote host. For all other high level events, this field is ignored and automatically managed by the agent.

- **General Search field**

This allows the user to further refine a search based on the event record payload. For most high level events, this option will search all the fields of an event record, except the header. There is NO need to use the wildcard character at the start or end of this field as it is automatically added to the search term when the objective is saved. The exception to this rule is when the **Access a file or directory** high level event is selected and the **Automatically set file audit configuration** option is enabled. In this situation, the **General Search** field is used to identify the file or directory that requires auditing

Example: To monitor for a file being opened for reading, the objective **Access a file or directory** would be selected and the actual directory would be entered into this field as follows: **C:\Example**. The agent will then recursively apply auditing to the destination folder, ensuring that any files or directories below **C:\Example** would be subject to audit and trapped.

Tip: If setting a file search parameter, it is important that the **FULLY QUALIFIED** directory name is entered so that the Snare system can set the appropriate auditing. **Example:** **C:\TEMP\SECRET*** will work, but **SECRET*** will not.

- **Filter on User**

An event record may be selected or discarded based on a userid, or partial match of a userid. If no users are entered AND the **Include Search Term Users** radio button has been selected, then ALL users will be audited. If a term is entered in this field, then an event record will be trapped or discarded based on a valid match and whether the **Include** or **Exclude** radio buttons have been selected. There is no need to use the wildcard character at the start and end of this field as it is automatically added when the objective is saved. Multiple users may be entered using a comma separated list.

- **Event Type**

Windows allows for five different audit event types, namely **Success Audit**, **Failure Audit**, **Information**, **Warning** and **Error**. If it is unclear which type of event is required, then selecting all of the check boxes will ensure that no events are lost. Note if no checkboxes are selected, then NO events will be trapped.

- **Event Logs**

Windows collects logs from a number of event log sources. On Windows Servers, all six primary event logs may be found, however on Workstation installations only three of these event logs (Security, System and Application) are available. *The Custom event log capability is only available to those users that have purchased a Snare Server, through the supported agents. See Chapter 8 of this document for further details.* If in doubt, there will be no harm done in selecting all event log types, except that **SnareCore** will now read from, and attempt to filter, from all the selected event logs and this will have some slight negative performance impact. Please note, if any high level event except for **Any event(s)** is selected, then this item is ignored as it is set automatically by the high level event.

Once the above settings have been finalized, click **OK** to save the configuration to the registry. To ensure the **SnareCore** service has received the new configuration, the **SnareCore** service **MUST** be restarted via the **Windows Services control panel** or via the **Apply the latest audit configuration** menu item in the remote control interface.

5 Audit event viewer functions

Events collected by the agent that meet the filtering requirements as per the **Audit Configuration**, will be displayed in the 'Latest Events' window (as shown in Figure 5). This display is NOT a display from the event log file, but rather a temporary display from a **shared memory** connection between the Snare remote control interface and the **SnareCore** service. This list will be empty if the agent has not yet found any matching events or if there has been a network problem and the agent has temporarily suspended event processing. A key feature of the **SnareCore** service is that events are not stored locally on the host (except for events stored natively in the Windows event log), but rather sent out over the network to one or more remote hosts. *Please note: The TCP protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased a Snare Server, through the supported agents. See Chapter 8 of this document for further details.*

A summary version of the events is displayed on the 'Latest Events' window. The 'Latest Events' window is restricted to a list of 20 entries and cannot be cleared, except by restarting the agent. The window will automatically refresh every 30 seconds.

Date	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
Thu Jul 01 17:55:31 2010	flash.Intersect.local	740	1704 (None)	SecCli	Unknown User	N/A	Information	Security policy in the Group policy objects has been applied successfully.
Thu Jul 01 17:55:31 2010	flash.Intersect.local	739	643 (Account Management)	Security	SYSTEM	User	Success Audit	Domain Policy Changed: Password Policy modified Domain Name: INTERSECT Domain ID: %S-1-5-21-4225700407-1522440742-3458925109} Caller User Name: FLASHS Caller Domain: INTERSECT Caller Logon ID: (0x0,0x3E7) Privileges: - Changed Attributes: Min. Password Age: - Max. Password Age: 529600 Force Logoff: - Lockout Threshold: - Lockout Observation Window: - Lockout Duration: - Password Properties: - Min. Password Length: - Password History Length: 20 Machine Account Quota: - Mixed Domain Mode: - Domain Behavior Version: - OEM Information: -
Thu Jul 01 17:55:00 2010	flash.Intersect.local	738	612 (Policy Change)	Security	SYSTEM	User	Success Audit	Audit Policy Change: New Policy: Success Failure - - Logon/Logoff - - Object Access - - Privilege Use + + Account Management + + Policy Change + + System - - Detailed Tracking + - Directory Service Access - - Account Logon Changed By: User Name: FLASHS Domain Name: INTERSECT Logon ID: (0x0,0x3E7)
Thu Jul 01 17:55:00 2010	flash.Intersect.local	737	612 (Policy Change)	Security	SYSTEM	User	Success Audit	Audit Policy Change: New Policy: Success Failure - - Logon/Logoff - - Object Access - - Privilege Use + + Account Management + + Policy Change + + System - - Detailed

Figure 5 Latest Events Window

6 Remote control and management functions

The *SnareCore* service is a separate, standalone component of the Snare system, as described in 2 *Overview of the Snare Agents on page 5*. The Snare remote control interface can be used to interact with a number of aspects of its operation. Primarily, the interface is used to develop and set the audit, network and objectives configuration, as described in the previous sections, however, options are available to manage the *SnareCore* service.

The *SnareCore* service can be reloaded directly from the menu item **Apply the latest audit configuration**. This will instruct the *SnareCore* service to re-read all the configuration settings, clear the buffers and essentially restart the service. This function is useful to apply any saved changes that have been made to the audit configuration. The user can therefore select when to activate a new configuration by selecting this menu item. Please note, this option does not restart the Windows service, but instead performs all the operations as if the service had been restarted.

The *SnareCore* service status can be viewed by selecting the **View Audit Service Status** menu item as shown in Figure 6. This will display whether the *SnareCore* service is active as well as information relating to the architecture of the machine and the running binary file.

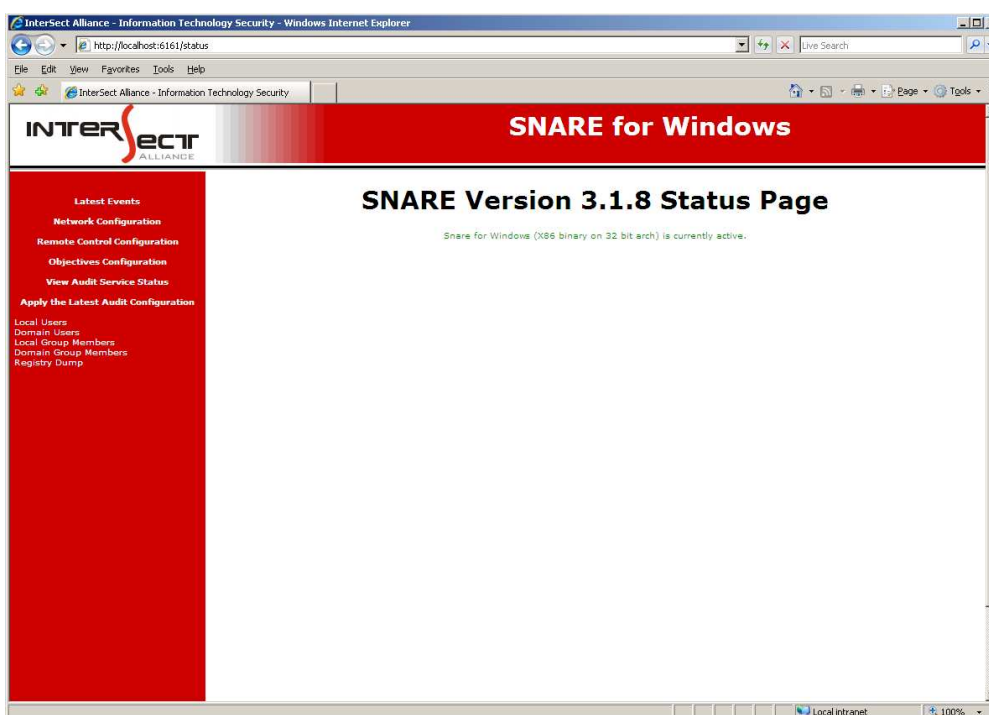


Figure 6 Audit Status Window

A significant function of the **SnareCore** service is its ability to be remote controlled. This facility has been incorporated to allow all the functions previously available through the front end Snare tool, to be available through a standard web browser. The **SnareCore** service employs a custom designed web server to allow configuration through a browser, or via an automated custom designed tool. The parameters which may be set for remote control operation are shown in Figure 7 and discussed in detail below:

- **IP Address allowed to remote control Snare.** Remote control actions may be limited to a given host. This host, entered as an IP address in this field, will only allow remote connections to be effected from the stated IP address. Note that access control based on source IP address is prone to spoofing, and should be considered as a security measure used in conjunction with other countermeasures.
- **Password to allow remote control of Snare.** A password may be set so that only authorised individuals may access the remote control functions. If accessing the remote control functions through a browser or custom designed tool, note that the userid is 'snare', and the password is whatever has been set through this setting. Note that this password is stored in an encrypted form in the registry, using the MD5 hashing algorithm.
- **Web Server Port.** Normally, a web server operates on port 80. If this is the case, then a user need only type the address into the browser to access the site. If however, a web server is operating on port (say) 6161, then the user needs to type **http://mysite.com:6161** to reach the web server. The default **SnareCore** web server port (6161) may be changed using this setting, if it conflicts with an established web server. However, care should be taken to note the new server port, as it will need to be placed in the URL needed to access the Snare agent.
- **Allow remote control of Snare agent.** Although previously available through the remote control interface, additional programs are now included with the agent to restore or disable remote access. This option is also configurable at the time of installation. Enabling this option will allow the Snare agent to be remote controlled by a remote host. This host may be independent from the (say) Snare Server. If the remote control feature is unselected, it may only be turned on by enabling the correct registry key on the hosted PC which the Snare agent has been installed.

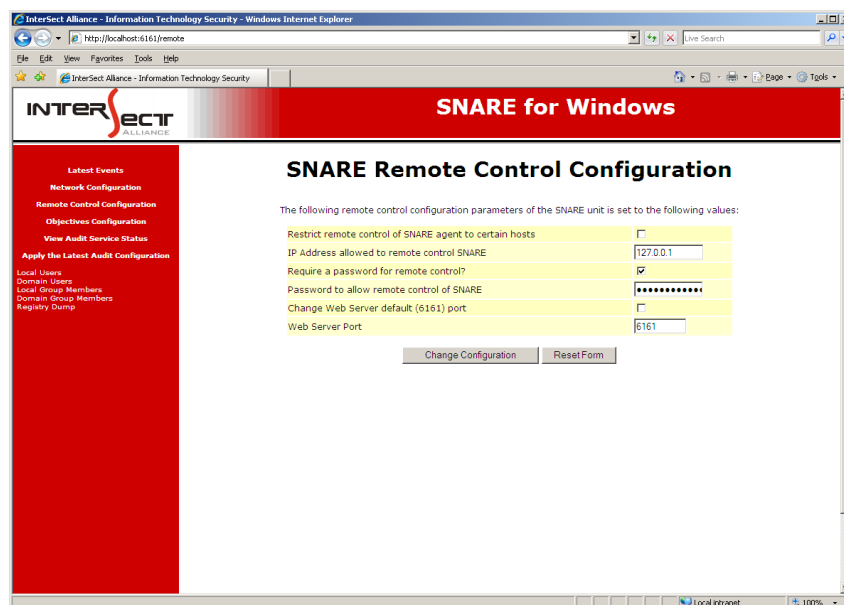


Figure 7 Remote Control Window

7 Retrieving user and group information

The *SnareCore* service also has the ability to retrieve local and domain users, groups and group membership from accounts local to the host that is running the agent and from the domain for which it is a member (if any). The host that is running the Snare agent must be a member of the domain, and have the ability to read user and group information, for the 'domain users/group' feature to work.

This feature is available through the remote control web page and can be accessed through any standard web browser. The menu structure on the remote web pages (as shown in Figure 7) shows the selections:

- 'Local Users'
- 'Local Groups'
- 'Local Group Members'
- 'Domain Group Members'
- 'Registry Dump'

Selecting any of these items will then display the relevant details. For example, Figure 8 below shows the output of selecting 'Local Users'. The output from these commands has been designed with no HTML markup to assist automated services, such as the Snare Server, to interrogate the users, groups and group membership.

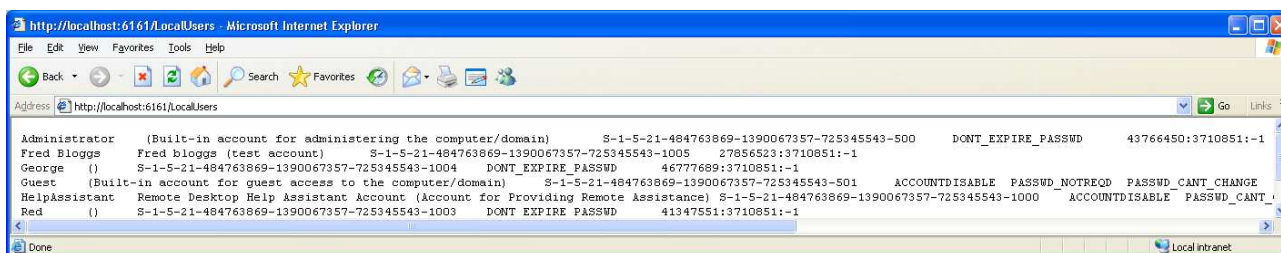


Figure 8 Output of 'Local Users'

In the case of 'Local Users' or 'Domain Users', the output shows a number of tab delimited entries, per line. These entries should be interpreted as follows:

Username; Description; SID; Attributes; Settings; These attributes include items such as Don't expire the password (token will be: DONT_EXPIRE_PASSWD); Account Disabled (token will be: ACCOUNTDISABLE); No Password (token will be: PASSWD_NOTREQD). The settings are "Password age in seconds since last reset : Maximum password age in seconds : Account Expiry as seconds elapsed since 00:00:00 1 January, 1970 (-1 means the account will not expire)".

The first three entries of username, description and SID will be displayed as a tab delimited list. The remaining tokens will only be shown if they exist in relation to a particular account. The settings will always appear at the end of each line.

In the case of Group Memberships, the attributes displayed are **Groupname; GID; Group Members**. The group member list will be shown when selecting the 'Local Group Members' or 'Domain Group Members' menu item from the remote control web page. Additionally, the group members will be displayed as a comma separated list of usernames. As stated previously, the 'Domain Group Members' and associated membership displayed via the web browser will only be displayed if the host that is running the Snare agent is a member of a Windows domain.

8 Snare Server



The Snare Server collects events and logs from a variety of operating systems, applications and appliances including, but not limited to: Windows NT/2000/XP/2003/Vista/2008/Windows7, Solaris, AIX, Irix, Linux, Tru64, ACF2, RACF, CISCO Routers, CISCO PIX Firewall, CyberGuard Firewall, Checkpoint Firewall1, Gauntlet Firewall, Netgear Firewall, IPTables Firewall, Microsoft ISA Server, Microsoft IIS Server, Lotus Notes, Microsoft Proxy Server, Apache, Squid, Snort Network Intrusion Detection Sensors, IBM SOCKS Server, and Generic Syslog Data of any variety.

In addition to the above, the benefits of purchasing the Snare Server include:

- Official support mechanism for the Snare open source agents. Note that official Snare agent support is not offered through *any* other channels.
- All future Snare Server versions and upgrades included as part of an annual maintenance fee.
- Ability to collect any arbitrary log data, either via UDP or TCP protocols.
- Proven technology that works seamlessly with the Snare agents.
- Snare reflector technology that allows for all collected events to be sent, in real time, to a standby/backup Snare Server.
- Ability to continuously collect large numbers of events. Snare Server collection rates exceed 60,000 events per minute using a low end, workstation class, Intel based PC on a 100Mbps network.
- Ability to drill down from top level reports. This reduces the amount of data “clutter” and allows a system administrator to fine tune the reporting objectives.
- Ability to create “cloned” objectives that allow very specific reporting against any collection profile. These reports, along with all Snare Server objectives, may be scheduled and emailed to designated staff.
- The Snare Server uses extensive discriminators for each objective, allowing system administrators to finely tune reporting based on inclusion or exclusion of certain parameters.
- Very simple, single CD installation for those users not requiring a hardware based appliance.

The Snare Server uses a hardened version of the Linux operating system base for stability and its ability to use a myriad of stable and functional open source tools. A Snare Server user, however need not be concerned with managing a Linux server. The Snare Server, once installed, is a fully contained appliance, and does not require any system administrator level maintenance. The Snare Server will operate on commonly available Intel based PCs, with hardware specifications shown on the next page.

There are supported versions of the Snare agents which are only available through the purchase of a Snare Server. Functionality includes, but is not limited to, the ability to collect records from Custom event log sources, the ability to send events via TCP as well as UDP and the ability to send events to many destinations, not just one host.

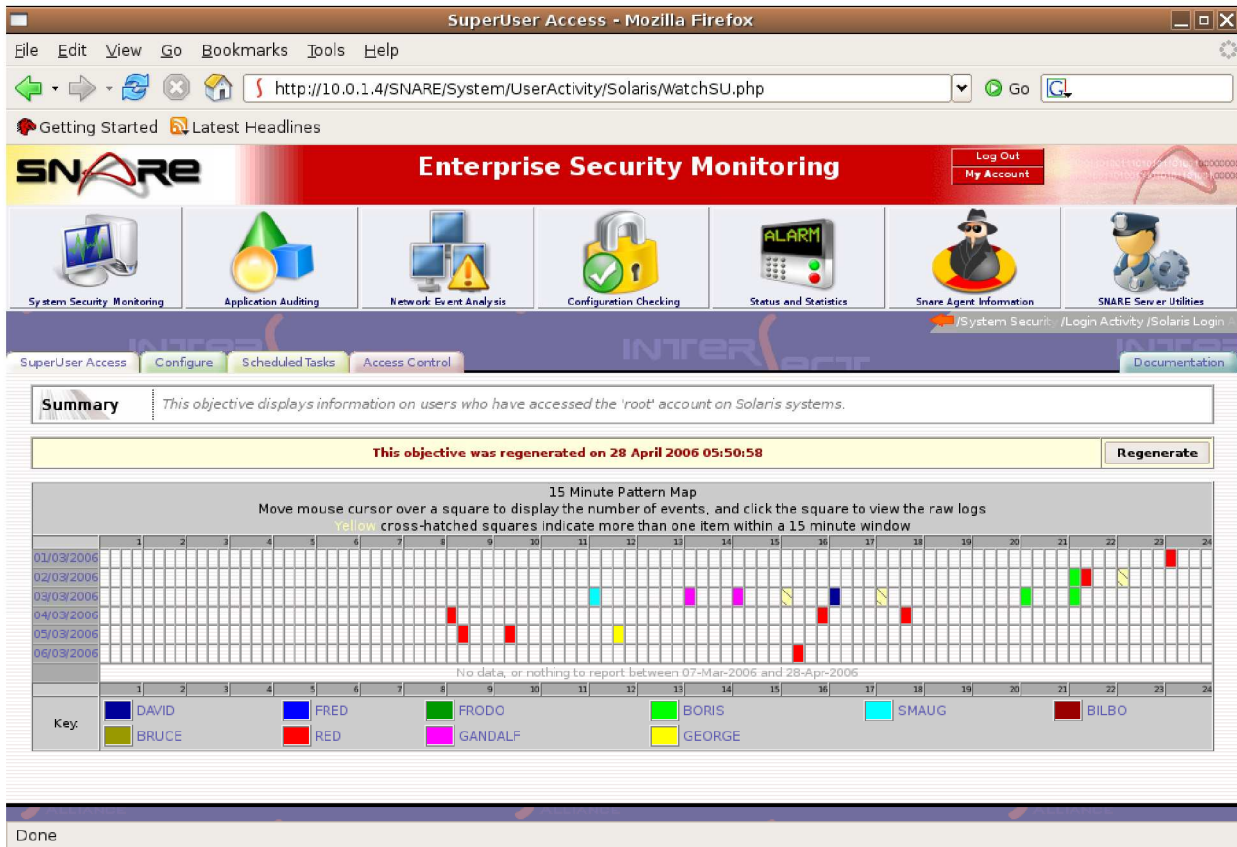


Figure 9 Screen shot from the Snare Server

9 About Intersect Alliance



Intersect Alliance is a team of leading information technology security specialists. In particular, Intersect Alliance are noted leaders in key aspects of IT Security, including host intrusion detection. Our solutions have and continue to be used in the most sensitive areas of Government and business sectors.

The Intersect Alliance business strategy includes demonstrating our commitment and expertise in IT security by releasing open source products such as Snare, and the proprietary Snare Server. Intersect Alliance intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.

Visit the Intersect Alliance website for more information at www.intersectalliance.com.

Appendix A - Event output format

The *SnareCore* service reads data from the Windows operating system via the Event Logs. It converts the binary audit data into text format, and separates information out into a series of TAB delimited tokens. The token delimiter may not be specified as something other than TAB. A 'token' is simply data, such as 'date' or 'user'. Groups of tab separated tokens make up an audit event, which may look something like this, depending on whether the *SnareCore* service has SYSLOG header functionality active.

Example:

```
Test_Host MSWinEventLog 0 Security 3027 Tue Jun 29 20:30:43 2010 593 Security
Administrator User Success Audit LE5678WSP Detailed Tracking A process has
exited: Process ID: 656 User Name: Administrator Domain: LE5678WSP
Logon ID: (0x0,0x6C52)
```

The format of the event log record is as follows:

1. **Hostname** (the assigned hostname of the machine or the override value entered using the Snare front).
2. **Event Log Type**. Fixed value of 'MSWinEventLog'.
3. **Criticality**. This is determined by the Alert level given to the objective by the user and is a number between 0 and 4, as detailed in the registry settings in Appendix B.
4. **SourceName**. This is the Windows Event Log from which the event record was derived. In the above example, the event record was derived from the 'security' event log.
5. **Snare Event Counter**. Based on the internal Snare event counter. Rotates at 'MAXDWORD'.
6. **DateTime**. This is the date time stamp of the event record.
7. **EventID**. This is the Windows Event ID.
8. **SourceName**. This is the Windows Event Log from which the event record was derived. In the above example, the event record was derived from the 'security' event log.
9. **UserName**. This is the Window's user name.
10. **SIDType**. This is the type of SID used. In the above example, it is a 'user' SID, but it may also be a 'computer' or other type of SID.
11. **EventLogType**. This can be anyone of 'Success Audit', 'Failure Audit', 'Error', 'Information', or 'Warning'.
12. **ComputerName**. This is the Windows computer name.
13. **CategoryString**. This is the category of audit event, as detailed by the Windows event logging system.
14. **DataString**. This contains the data strings.
15. **ExpandedString**. This contains the expanded data strings.
16. **MD5 Checksum** (optional). An md5 checksum of the event can optionally be included with each event sent over the network by the Snare for Windows agent. Note that the application that evaluates each record will need to strip the final delimiter, plus the checksum, prior to evaluating the event.

Appendix B - Snare Windows registry configuration description

Details on the audit configuration are discussed in the **Audit Configuration** section. The purpose of this section is to discuss the makeup of the configuration items in the registry. The Snare configuration registry key is located at **HKEY_LOCAL_MACHINE\SOFTWARE\Intersect Alliance\AuditService** and this location may not be changed. If the configuration key does not exist, the **SnareCore** service will create it during installation, but will not actively audit events until a correctly formatted objective(s) is present.

Snare can be configured in several different ways, namely:

- Via the remote control interface (Recommended).
- By manually editing the configuration items in the registry (NOT Recommended).

The format of the audit configuration registry subkeys is discussed below.

[Config]	This subkey stores the delimiter and clientname values.
CritAudit	This value is of type REG_DWORD, and determines whether Snare will only send an event for the highest criticality match
FileExport	This value is of type REG_DWORD, and determines whether Snare will write a log file to the system32 path. USE WITH CARE!!
Delimiter	This is of type REG_SZ and stores the field delimiting character, ONLY if syslog header has been selected. If more than one char, only first char will be used. If none set, then TAB will be used. This is a HIDDEN field, and only available to those users that wish to set a different delimiter when using the SYSLOG header. This selection option will not be found in the Snare front end or the web pages.
Clientname	This is the Hostname of the client and is of type REG_SZ. If no value has been set, "hostname" command output will be displayed. Must be no more than 100 chars, otherwise will truncate.
Audit	This value is of type REG_DWORD, and determines whether Snare is to automatically set the system audit configuration. Set this value to 0 for no, or 1 for Yes. Will default to TRUE (1) if not set. The audit configuration includes selecting the audit categories and the retention policy on ALL event log files.
FileAudit	This value is of type REG_DWORD, and determines whether Snare is to automatically set the file system audit configuration. Set this value to 0 for no, or 1 for Yes. Will default to TRUE (1) if not set.
Checksum	This value is of type REG_DWORD, and determines whether Snare is includes an MD5 Checksum of the contents of each audit record, with the record in question. Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set. Note that the checking application will need to strip the final delimiter, plus the MD5 Checksum, from the record before evaluating the record against the checksum.
EnableUSB	This value is of type REG_DWORD, and determines whether Snare should actively capture USB auditing events (2000/2003/XP only). Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set.
LeaveRetention	This value is of type REG_DWORD and determines whether Snare should leave the existing Log Retention settings as they are on each event log. Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set.

[Objective]	This subkey stores all the filtering objectives.
Objective# (where # is a serial number)	<p>This section describes the format of the objectives. Objectives are of type REG_SZ, of no greater than 1060 chars, and is composed of the following string (the figures in the brackets represent the maximum size of the strings that can be entered):</p> <p>Criticality(DWORD);Event Type (DWORD);Event Log Type(DWORD);EventID Match [256];General Match[512];UserMatchType(DWORD);User Match[256];EventIDMatchType(DWORD)</p> <p>Criticality - an integer between 0 and 4 that indicates the severity of the event. Critical = 4, Priority = 3, Warning = 2, Information = 1, Clear = 0</p> <p>User Match Type: =0 (Include users that match user search term type; =1 for Exclude)</p> <p>EventID Match Type: =0 (Include events that match the entire objective; =1 for Exclude)</p> <p>Event Type: Success = 16, Failure = 8, Error = 4, Information = 2, Warning = 1. (These values are checkboxes, hence the sum of the selected values is recorded).</p> <p>Event Log Type: Custom = 64, Security = 32, System = 16, Application = 8, Directory Service = 4, DNS Server = 2, File Replication = 1. (These values are checkboxes, hence the sum of the selected values is recorded).</p> <p>The match terms (EventID Match, General Match and User Match) are the filter expressions and are defined to be any value (except TAB) which includes DOS wildcard characters. Note that these are NOT regular expressions.</p> <p>NOTE: Semicolons are actually "TAB" characters.</p>
[Network]	This subkey stores the general network configurations.
Destination	This sub key is of type REG_SZ and is a comma separated list of destinations, which should be a maximum of 100 characters each. It details the IP address or hostname which the event records will be sent (NB: multiple hosts only available in supported agent).
DestPort	This value is of type REG_DWORD, and determines the Destination Port number. This value must be in 1-65535 range. Will default to 514 if a SYSLOG header has been specified.
Syslog	This value is of type REG_DWORD, and determines whether a SYSLOG header will be added to the event record. Set this value to 0 for no SYSLOG header. Will default to TRUE (1) if not set.
SyslogDest	This value is of type REG_DWORD, and determines the SYSLOG Class and Criticality. This value will default to 13 if not set, or out of bounds.
SocketType	This value is of type REG_DWORD, and determines the protocol used (0 for UDP, 1 for TCP). This feature only appears in supported agents.

EncryptMsg	This value is of type REG_DWORD, and determines if encryption should be used (0 for No, 1 for Yes). This feature only appears in supported agents.
CacheSizeSet	This value is of type REG_DWORD, and determines if the agent should set the Windows Event Log size (0 for No, 1 for Yes). This feature only appears in supported agents.
CacheSizeM	This value is of type REG_DWORD, and determines the size of the Windows Event Log (if CacheSizeSet is 1). The value must be between 1 and 1024. This feature only appears in supported agents.
[Remote]	This subkey stores all the remote control parameters.
Allow	"Allow" is of type REG_DWORD, and set to either 0 or 1 to allow remote control. If not set or out of bounds, will default to 0/NO (ie; not able to be remote controlled).
WebPort	This value is the web server port, if it has been set to something other than port 6161. It is of type REG_DWORD. If not set or out of bounds, it will default to port 6161.
WebPortChange	This value is of type REG_DWORD, and set to either 0 or 1 to signal whether the web port should be changed or not. 0 = no change.
Restrict	This value is of type REG_DWORD, and set to either 0 or 1 to signal whether the remote users should be restricted via IP address or not. 0 = no restrictions.
RestrictIP	This is of type REG_SZ and is the IP address set from above.
AccessKey	This value is of type REG_DWORD and is used to determine whether a password is required to access the remote control functions. It is set to either 0 or 1, with 0 signifying no password is required.
AccessKeySet	This is of type REG_SZ, and stores the actual password to be used, in encrypted format.

Appendix C - Objectives and security event IDs

The Snare application has a number of built in Objectives. These Objectives have been designed to 'trap' certain Security Log event IDs and enable the user to create some of the more common objectives without having to know which event IDs they require. For each high level event, the Windows 2000/XP/2003 event IDs will be listed in **blue** and the Vista/2008/Windows7 event IDs will be listed in **green**. As a rule of thumb, to find the equivalent 2000/XP/2003 event ID on a newer Windows operating system, just add 4096.

- **Logon of Logoff.**
 - 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 551, 552, 672, 673, 674, 675, 676, 677, 678, 680, 681, 682, 683
 - 4624, 4625, 4626, 4627, 4628, 4629, 4630, 4631, 4632, 4633, 4634, 4635, 4636, 4637, 4638, 4639, 4640, 4641, 4642, 4643, 4647, 4648, 4768, 4769, 4770, 4771, 4772, 4773, 4774, 4776, 4777, 4778, 4779, 4800, 4801, 4802, 4803
- **Access a file or directory.**
 - 560, 561, 562, 563, 564, 565, 566, 567, 594, 595
 - 4656, 4657, 4658, 4659, 4660, 4661, 4662, 4663, 4690, 4691
- **Start or stop a process.**
 - 592, 593, 594, 595
 - 4688, 4689, 4690, 4691
- **Use of user rights.**
 - 576, 577, 578, 608, 609
 - 4672, 4673, 4674, 4704, 4705
- **Account administration.**
 - 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671
 - 4720, 4721, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4736, 4737, 4738, 4739, 4740, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4763, 4764, 4765, 4766, 4767
- **Change the security policy.**
 - 516, 517, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 620, 643
 - 4612, 4613, 4704, 4705, 4706, 4707, 4708, 4709, 4710, 4711, 4712, 4713, 4714, 4716, 4719, 4739
- **Restart, shutdown and system.**
 - 512, 513
 - 4608, 4609
- **USB Events.**
 - 134,135
- **Filtering Events.**
 - 5152, 5153, 5154, 5155, 5156, 5157, 5158, 5159, 5447

Note some of the above events will only be generated on Windows 2000 hosts. The above events will be generated by turning on selected audit categories, on the Windows audit sub-system. The following paragraphs detail the Snare for Windows event IDs and the categories to which they belong.

Audit Privilege Use (Success and Failure) will generate:

576;Special privileges assigned to new logon
577;Privileged Service Called
578;Privileged object operation

Audit Process Tracking (Success and Failure) will generate:

592;A new process has been created
593;A process has exited
594;A handle to an object has been duplicated
595;Indirect access to an object has been obtained

Audit System Events (Success and Failure) will generate:

512;Windows NT is starting up
513;Windows NT is shutting down
514;An authentication package has been loaded
515;A trusted logon process has registered
516;Loss of some audits;
517;The audit log was cleared
518;A notification package has been loaded

Audit Logon Events (Success and Failure) will generate:

528;A user successfully logged on to a computer
529;The logon attempt was made with an unknown user name or bad password
530;The user account tried to log on outside of the allowed time
531;A logon attempt was made using a disabled account
532;A logon attempt was made using an expired account
533;The user is not allowed to log on at this computer
534;The user attempted to log on with a logon type that is not allowed
535;The password for the specified account has expired
536;The Net Logon service is not active
537;The logon attempt failed for other reasons
538;A user logged off
539;The account was locked out at the time the logon attempt was made
540;Successful Network Logon
541;IPSec security association established
542;IPSec security association ended
543;IPSec security association ended
544;IPSec security association establishment failed
545;IPSec peer authentication failed
546;IPSec security association establishment failed
547;IPSec security association negotiation failed
682;A user has reconnected to a disconnected Terminal Services session
683;A user disconnected a Terminal Services session without logging off

Audit Account Logon Events (Success and Failure) will generate:

- 672;An authentication service (AS) ticket was successfully issued and validated
- 673;A ticket granting service (TGS) ticket was granted
- 674;A security principal renewed an AS ticket or TGS ticket
- 675;Pre-authentication failed
- 676;Authentication Ticket Request Failed
- 677;A TGS ticket was not granted
- 678;An account was successfully mapped to a domain account
- 680;Identifies the account used for the successful logon attempt
- 681;A domain account log on was attempted
- 682;A user has reconnected to a disconnected Terminal Services session
- 683;A user disconnected a Terminal Services session without logging off

Audit Account Management Events (Success and Failure) will generate:

624;User Account Created
625;User Account Type Change
626;User Account Enabled
627;Password Change Attempted
628;User Account Password Set
629;User Account Disabled
630;User Account Deleted
631;Security Enabled Global Group Created
632;Security Enabled Global Group Member Added
633;Security Enabled Global Group Member Removed
634;Security Enabled Global Group Deleted
635;Security Disabled Local Group Created
636;Security Enabled Local Group Member Added
637;Security Enabled Local Group Member Removed
638;Security Enabled Local Group Deleted
639;Security Enabled Local Group Changed
640;General Account Database Change
641;Security Enabled Global Group Changed
642;User Account Changed
643;Domain Policy Changed
644;User Account Locked Out
645;Computer object added
646;Computer object changed
647;Computer object deleted
648;Security Disabled Local Group Created
649;Security Disabled Local Group Changed
650;Security Disabled Local Group Member Added
651;Security Disabled Local Group Member Removed
652;Security Disabled Local Group Deleted
653;Security Disabled Global Group Created
654;Security Disabled Global Group Changed
655;Security Disabled Global Group Member Added
656;Security Disabled Global Group Member Removed
657;Security Disabled Global Group Deleted
658;Security Enabled Universal Group Created
659;Security Enabled Universal Group Changed
660;Security Enabled Universal Group Member Added
661;Security Enabled Universal Group Member Removed
662;Security Enabled Universal Group Deleted
663;Security Disabled Universal Group Created
664;Security Disabled Universal Group Changed
665;Security Disabled Universal Group Member Added
666;Security Disabled Universal Group Member Removed
667;Security Disabled Universal Group Deleted
668;Group Type Changed
669;Add SID History (Success)
670;Add SID History (Failure)

Audit Object Access (Success and Failure) will generate:

560;Access was granted to an already existing object
561;A handle to an object was allocated
562;A handle to an object was closed
563;An attempt was made to open an object with the intent to delete it
564;A protected object was deleted
565;Access was granted to an already existing object type
566;Object Operation
608;A user right was assigned

Audit Policy Change (Success and Failure) will generate:

609;A user right was removed
610;A trust relationship with another domain was created
611;A trust relationship with another domain was removed
612;An audit policy was changed
613;IPSec policy agent started
614;IPSec policy agent disabled
615;IPSec policy changed
616;IPSec policy agent encountered a potentially serious failure
617;Kerberos policy changed
618;Encrypted data recovery policy changed
620;Trusted domain information modified
768;A collision was detected between a namespace element in two forests

Audit Directory Service Access (Success and Failure) will generate:

565;Information about accessed objects in AD