VISUAL
message center

Security Auditing with Tango/04 Products

Windows Platform

VMC-GEN

tango04 Computing Group

Solutions for Advancing People

Security Auditing with Tango/04 Products - Windows Platform

Copyright Notice

Document date: June 2011

Document version: 2.01

Product version: All products

Trademarks

Technical Support

For technical support visit our web site at www.tango04.com.

Tango/04 Computing Group S.L.
Avda. Meridiana 358, 5 A-B
Barcelona, 08027
Spain

Tel: +34 93 274 0051

Table of Contents

Table of Contents iii

Chapter 1

Introduction 1

Chapter 2

Activating the Audit 2

2.1. At Windows Server Level 2

2.2. At Sensitive File Level 6

Chapter 3

Controls 9

3.1. Access over the Communication Network 9

3.2. Eliminating Temporary Ffiles 9

3.3. Communicate the policies 10

3.4. Record of Incidences 11

3.5. Audited Events 11

3.5.1. Account logon events (start of interactive session) 11

3.5.2. Logon events (start of domain session) 12

3.5.3. Account management events 12

3.5.4. Object access events 13

3.5.5. System events 13

3.5.6. Audit privilege use and policy changes events 14

3.6. Backup Copies 14
3.7. Testing with Real Data 14
3.8. Recording Access 14

About Tango/04 Computing Group 15
Legal Notice 16

Chapter 1
Introduction

This document is intended as a reference for Windows platforms administrators when implementing controls for a security auditing project to comply with regulations like SOX, 21 CFR Part 11, HIPAA, CA SB 1386, LOPD, etc.

For each control, the document indicates what elements of the Operating System must be activated or configured and how. It also explains what Tango/04 Computing Group product recollects and processes the auditing data generated by the controls.

The information presented here does not replace the manuals of the different Tango/04 Computing Group products involved. The manuals contain detailed information regarding the configuration and use of each product.

Chapter 2
Activating the Audit

2.1 At Windows Server Level

On each Windows Server or PC containing sensitive data, enable the following auditing instructions of the operating system:

1. Audit account logon events (start of interactive session).
2. Audit logon events (start of domain session).
3. Audit account management.
4. Audit object access.
5. Audit privilege use.
6. Audit system events.
7. Audit policy changes.

Each audit setting can be enabled to generate events for correct attempts and error or failed attempts. The following table details the type of activation per server depending on the level of sensitive files they contain:

Audit Instructions	Level of sensitive files					
	Basic		Medium		High	
	Success	Failure	Success	Failure	Success	Failure
Audit account logon events		X		X	X	X
Audit logon to Start of domain session		X		X	X	X
Audit Account management	X	X	X	X	X	X
Audit Object Access		X		X	X	X
Audit privilege use		X		X	X	X
Audit system events	X	X	X	X	X	X

Audit policy changes	X	X	X	X	X	X

For servers that control a domain a number of additional controls exist for the events of the active directory.

The operating system sends the generated events to its security events log. These incidences are sent to a central database.

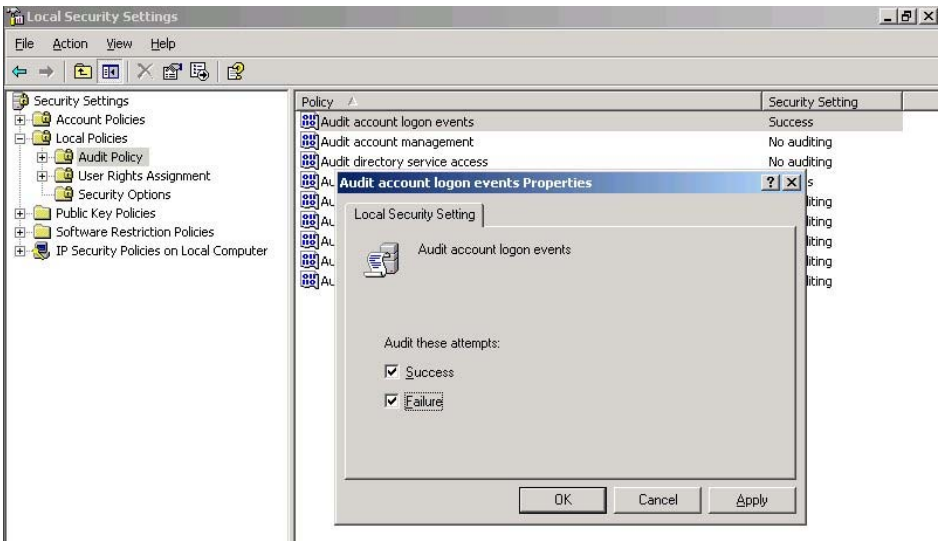

Figure 1 – Configuration for audit account logon events. (English language version - Windows 2000/ XP/2003)

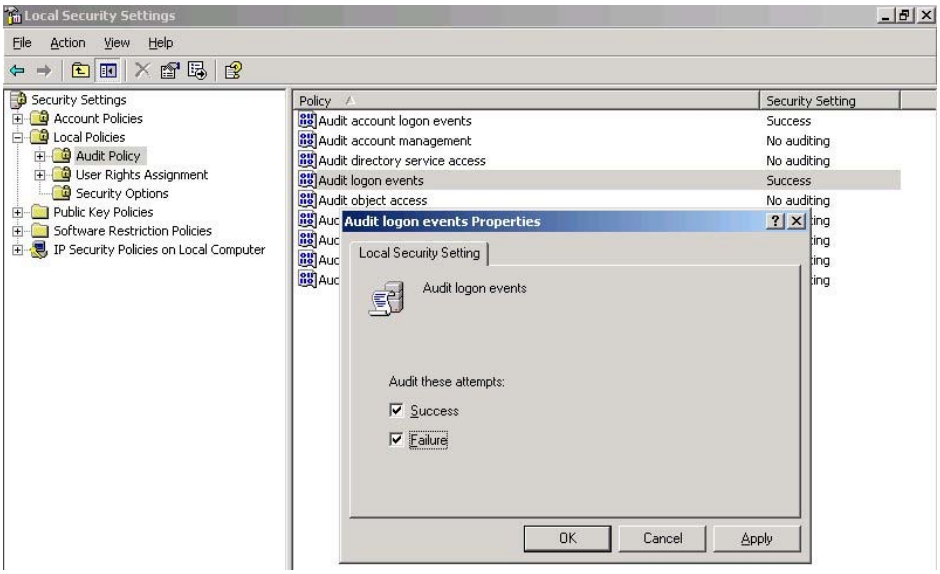

Figure 2 – Configuration for audit logon events. (English language version - Windows 2000/XP/2003)

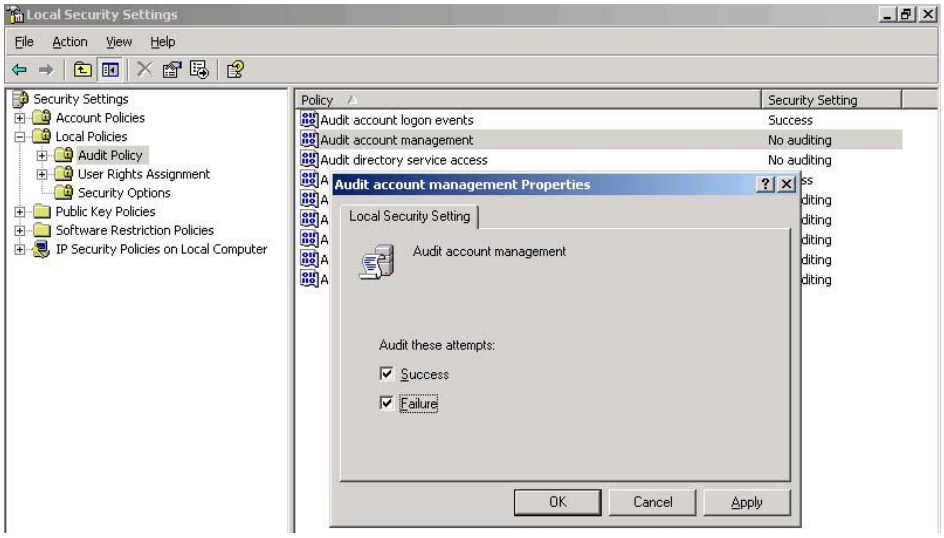

Figure 3 – Configuration for audit account management. (English language version - Windows 2000/ XP/2003)

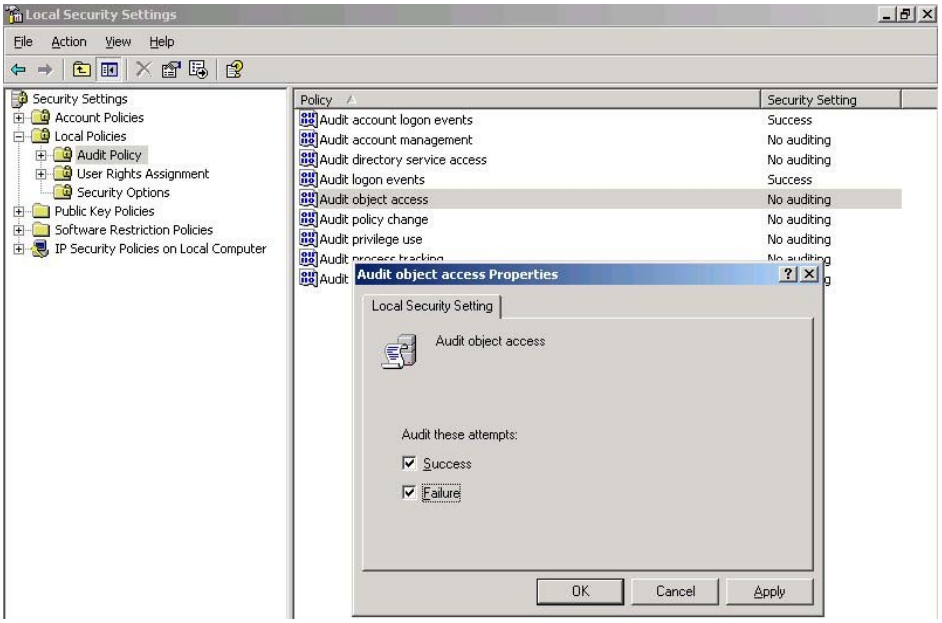

Figure 4 – Configuration for audit objects access. (English language version - Windows 2000/XP/ 2003)

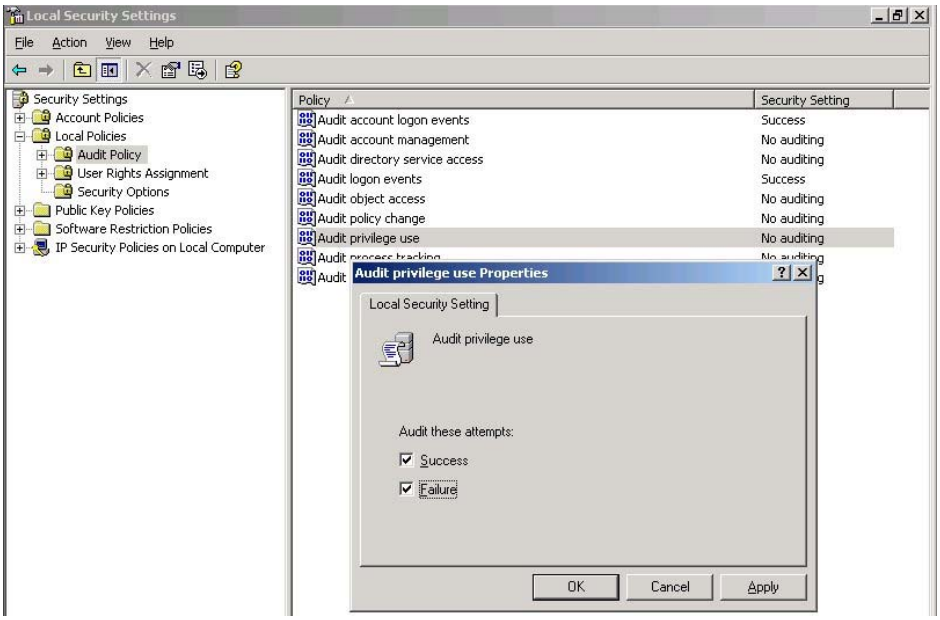

Figure 5 – Configuration for audit privilege use (English language version - Windows 2000/XP/2003)

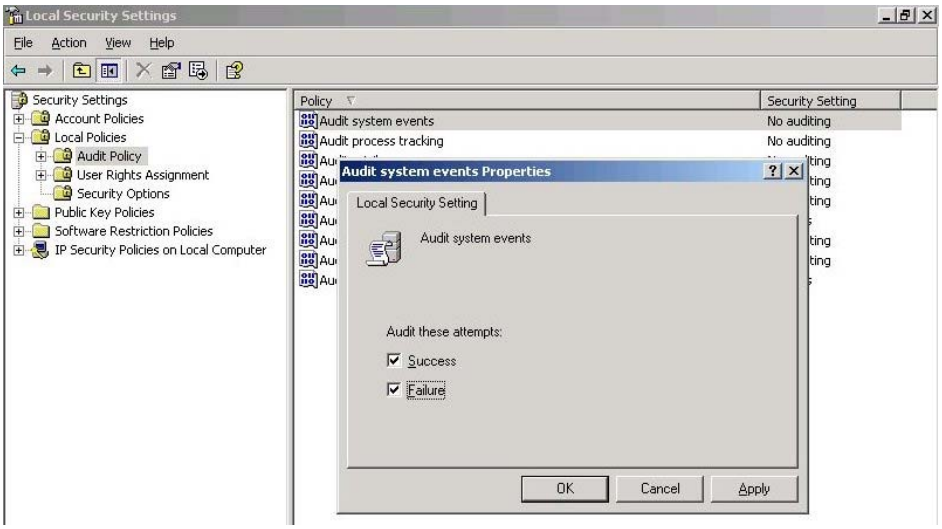

Figure 6 – Configuration for audit system events. (English language version - Windows 2000/XP/ 2003)

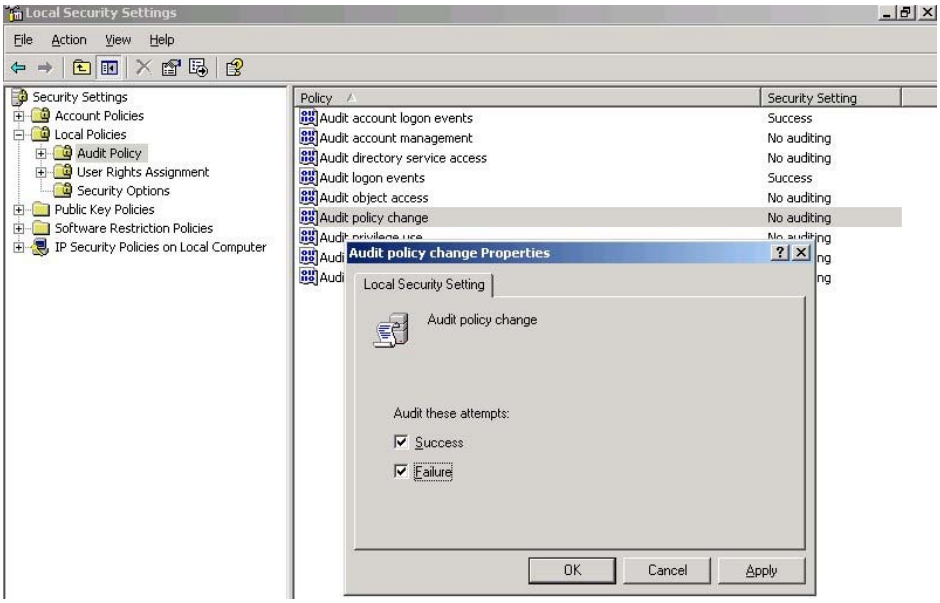

Figure 7 – Configuration for audit policy changes. (English language version - Windows 2000/XP/ 2003)

2.2 At Sensitive File Level

For each server containing sensitive files enable the relevant ACL entries (Access Control List) according to the criticalness of each file.

Step 1. For the most sensitive files, activate auditing for success and failure of the following events:

- Read extended attributes
- Write extended attributes
- Delete
- Change permissions
- Take ownership

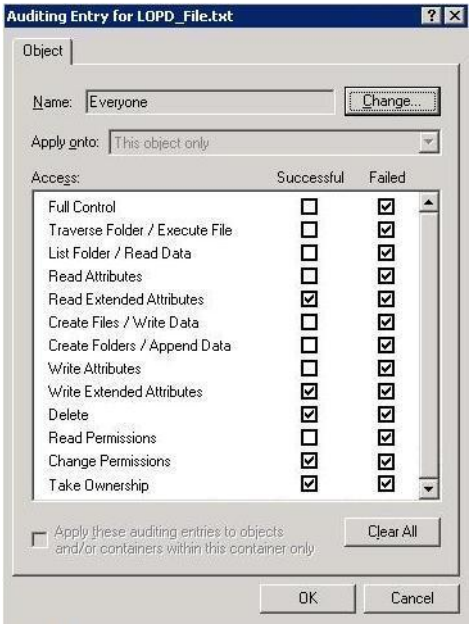

Figure 8 – Audit configuration for highly sensitive files (English language version - Windows 2000/ XP/2003)

Step 2. To open the window shown here, right-click the file in question and select Properties. Open the Security tab and click the Advanced button. Open the Auditing tab and click the Add button. Enter the name of the user/group and click the OK button. If you want this to apply to all users enter Everyone in the user/group field.

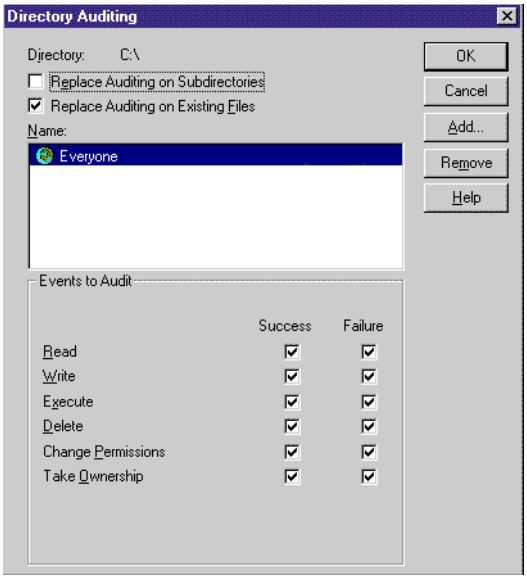

Figure 9 – Audit configuration of directory auditing for the most sensitive directories (English language version - Windows 2000/XP/2003)

Step 3. For medium to low level files activate auditing for success and failure for the following events:

- Delete
- Change permissions
- Take ownership

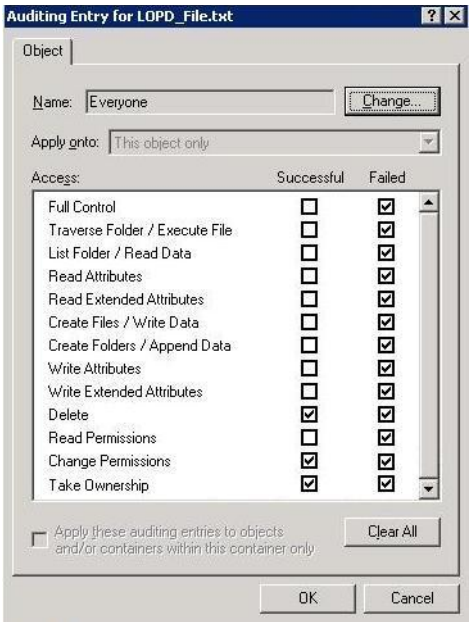

Figure 10 – Audit configuration for medium to low sensitive files (English language version - Windows 2000/XP/2003)

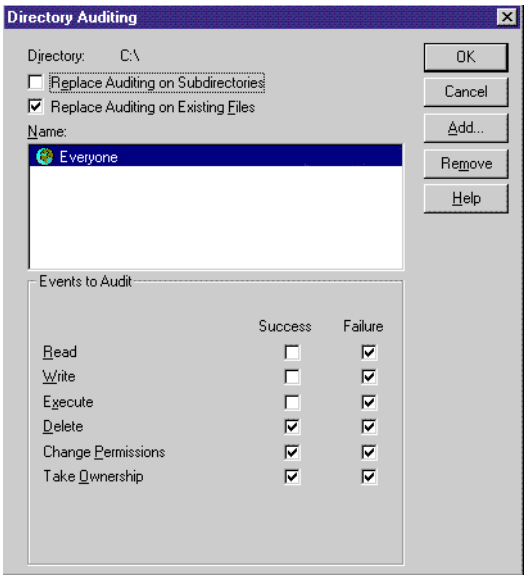

Figure 11 – Audit configuration of directory auditing for medium and low sensitive directories (English language version - Windows 2000/XP/2003)

In the event that your most sensitive files are located on a SQL Server use Data Monitor for SQL Server to audit these files (for which you want to store the vale inserted, the values deleted, and the values before the modification). Likewise auditing of your most sensitive files in Oracle databases should be done with Data Monitor for Oracle.

Chapter 3
Controls

3.1 Access over the Communication Network

All servers should restrict remote access to domain users and the domain or machine administrator.

Databases storing sensitive data should be protected with username and password.

Servers should not share folders containing sensitive data over the network; if for whatever reason you are forced to share sensitive data over the network (for example files used by IIS) the folders should have the appropriate authority settings.

3.2 Eliminating Temporary Ffiles

If in your Windows environment temporary files inherit the permissions of the object that creates them configure each Server or PC that processes sensitive data as follows:

- Clear virtual memory pagefile: Forces the operating system to delete data stored in virtual memory on the disk when restarting the system

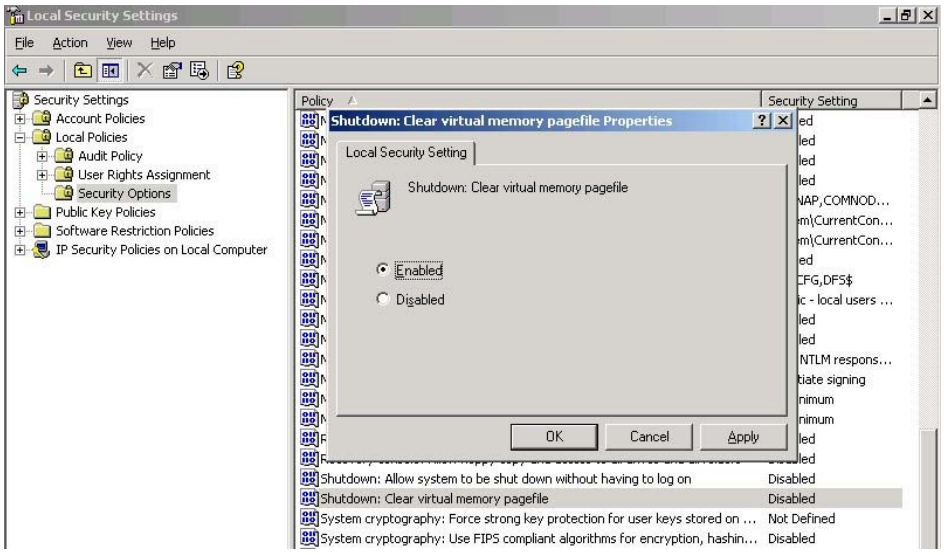

Figure 12 – Enable clear virtual memory upon shutdown (English language version – Windows XP/ 2003)

To access this window go to the Windows control panel and open Administrative Tools. Double-click Local Security Policy and open the folder Local Policies. In the folder Security Options double-click the security policy Shutdown: Clear virtual memory pagefile.

On Windows 2000 systems this option is called “Clear virtual memory pagefile when system shuts down” (English language version).

3.3 Communicate the policies

Each Server or PC that contains or processes sensitive data should show a legal notice each time a user logs on to an interactive session and ensure that authenticated users are aware of the security policy.

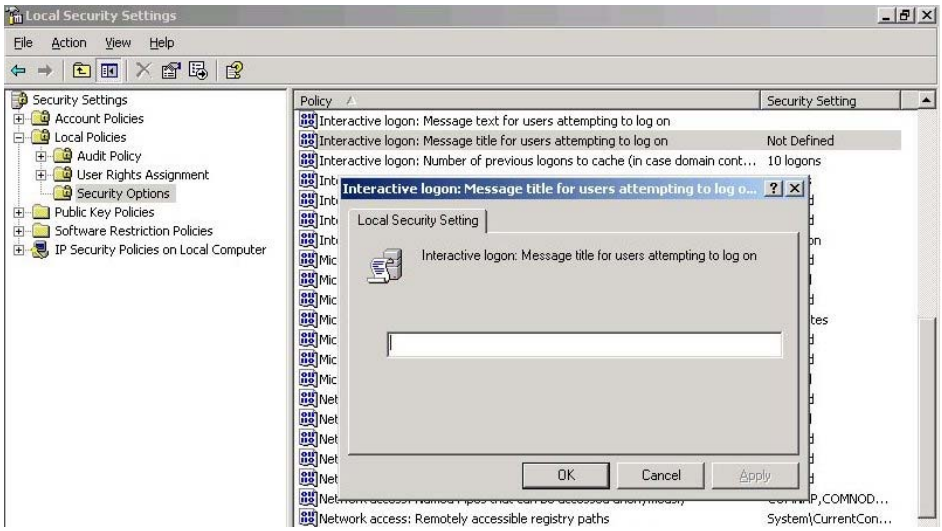

Figure 13 – Configuration of the title for the legal notice at logon (English language version – Windows XP/2003)

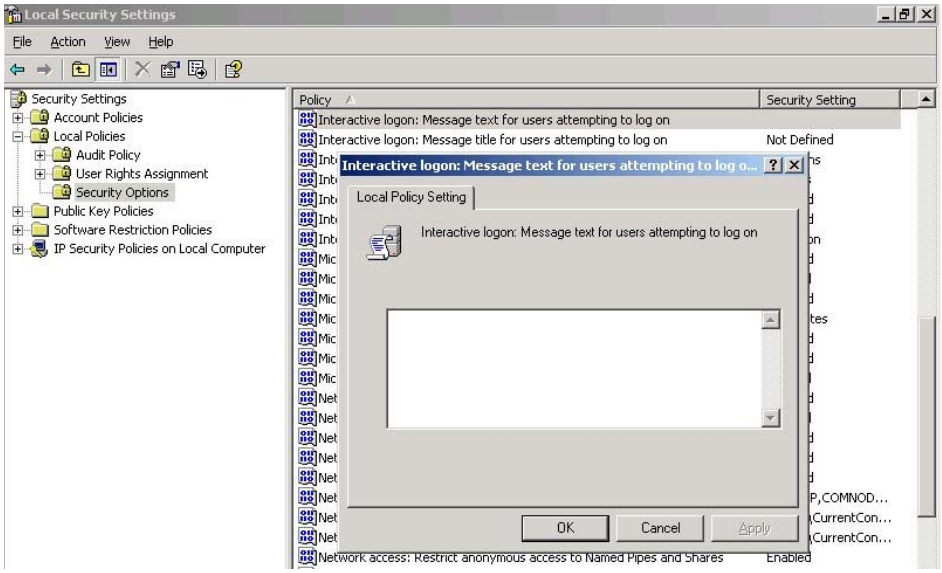

Figure 14 – Configuration of the message body of the legal notice at logon (English language version - Windows XP/2003)

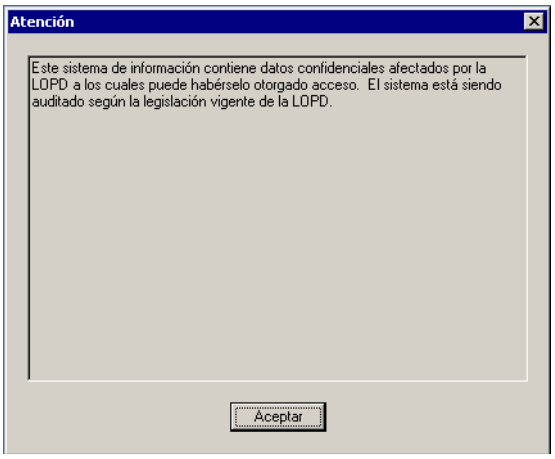

Figure 15 – Example of the legal notice that appears upon logon to an interactive session

3.4 Record of Incidences

Tango/04 products allow you to automatically create a record of an incidence in a database based on the auditing messages mentioned above. It is possible to configure the SmartConsole to insert a record in an incidences database for only those messages that need to be recorded.

3.5 Audited Events

By activating the operating systems auditing instructions the following events are monitored and recorded in the incidences database:

3.5.1 Account logon events (start of interactive session)

ID	Event
528	Interactive logon successful.
529	Logon failure. Unknown user name or bad password.
530	Logon failure. Account logon time restriction violation.
531	Logon failure. Account currently disabled.
532	Logon failure. The specified user account has expired.
533	Logon failure. User not allowed to logon at this computer.
534	Logon failure. The user has not been granted the requested logon type at this machine.
535	Logon failure. The specified account's password has expired.
536	Logon failure. The NetLogon component is not active.
537	Logon failure. An unexpected error occurred during logon.
538	User logoff.
539	Logon failure. Account locked out.
540	Successful Network Logon.

ID	Event
682	Session reconnected to Terminal Service.
683	Session disconnected from Terminal Service.

3.5.2 Logon events (start of domain session)

ID	Event
672	Authentication Ticket Granted (AS).
673	Service Ticket Granted (TGS).
674	Ticket Granted Renewed (AS or TGS)
675	Pre-authentication failed.
676	Authentication Ticket Request Failed.
677	Service Ticket Request Failed (TGS)
678	Successful assignation of an account to a domain account.
680	Successful logon and authentication package used.
681	Logon failure using a domain account.
682	User reconnects to a Terminal Service session previously disconnected.
683	Terminal Service session disconnected.

3.5.3 Account management events

ID	Event
624	User Account Created.
625	User Account Type Change.
626	User Account Enabled.
627	Change Password Attempt.
628	User Account password set.
629	User Account Disabled.
630	User Account Deleted.
631	Global Group Created.
632	Global Group Member Added.
633	Global Group Member Removed.
634	Global Group Deleted.

ID	Event
635	Local Group Created.
636	Local Group Member Added.
637	Local Group Member Removed.
638	Local Group Deleted.
639	Local Group Changed.
641	Global Group Changed.
642	User Account Changed.
643	Domain Policy Changed.
644	User Account Locked Out.

3.5.4 Object access events

ID	Event
560	Object access granted
563	Object Open for Delete.
564	Object Deleted.
565	Object type access granted

3.5.5 System events

ID	Event
512	System is starting up.
513	System is shutting down
514	An authentication package has been loaded by the LSA.
515	A trusted logon process has registered with the LSA.
516	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
517	The audit log was cleared.
518	A notification package has been loaded by the SAM.
520	The system time was changed.

3.5.6 Audit privilege use and policy changes events

ID	Event
608	User Right Assigned.
609	User Right Removed.
610	New Trusted Domain.
611	Removing Trusted Domain.
612	Audit Policy Change.
768	Namespace collision between two forests.

3.6 Backup Copies

We highly recommend you backup your sensitive files. We further recommend that the software you use to backup your files allows access to its messages so that you can monitor the backup process to check that it completes successfully.

If your software stores messages from the backup process in the Windows event log, you can use VISUAL Message Center ThinkServer's Event Log ThinAgent to monitor the process. If the applications writes the messages to a proprietary log file you can use the VISUAL Message Center Monitoring Engine Applications Agent to retrieve the information.

3.7 Testing with Real Data

If you use real data when testing in your development environment, apply the same security measures in the development environment. The Tango/04 Computing Group tools to use are the same as in the production environment.

3.8 Recording Access

For monitoring access to sensitive data at object level, use the ThinkServer Windows Event Log ThinAgent, which retrieves access recorded by the operating system in the Windows event log. Both successful and failed access is recorded according to the configuration of the sensitive files.

It is not possible to retrieve record-level read access for databases on SQL Server. However, update and delete access to SQL Server databases can be monitored using Data Monitor for SQL Server.

About Tango/04 Computing Group

Tango/04 Computing Group is one of the leading developers of systems management and automation software. Tango/04 software helps companies maintain the operating health of all their business processes, improve service levels, increase productivity, and reduce costs through intelligent management of their IT infrastructure.

Founded in 1991 in Barcelona, Spain, Tango/04 is an IBM Business Partner and a key member of IBM's Autonomic Computing initiative. Tango/04 has more than a thousand customers who are served by over 35 authorized Business Partners around the world.

Alliances

Partnerships

IBM Business Partner

IBM Autonomic Computing Business Partner

IBM PartnerWorld for Developers Advanced Membership

IBM ISV Advantage Agreement

IBM Early code release

IBM Direct Technical Liaison

Microsoft Developer Network

Microsoft Early Code Release

Awards

Legal Notice

The information in this document was created using certain specific equipment and environments, and it is limited in application to those specific hardware and software products and version and releases levels.

Any references in this document regarding Tango/04 Computing Group products, software or services do not mean that Tango/04 Computing Group intends to make these available in all countries in which Tango/04 Computing Group operates. Any reference to a Tango/04 Computing Group product, software, or service may be used. Any functionally equivalent product that does not infringe any of Tango/04 Computing Group's intellectual property rights may be used instead of the Tango/04 Computing Group product, software or service

Tango/04 Computing Group may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

The information contained in this document has not been submitted to any formal Tango/04 Computing Group test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility, and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. Despite the fact that Tango/04 Computing Group could have reviewed each item for accurateness in a specific situation, there is no guarantee that the same or similar results will be obtained somewhere else. Customers attempting to adapt these techniques to their own environments do so at their own risk. Tango/04 Computing Group shall not be liable for any damages arising out of your use of the techniques depicted on this document, even if they have been advised of the possibility of such damages. This document could contain technical inaccuracies or typographical errors.

Any pointers in this publication to external web sites are provided for your convenience only and do not, in any manner, serve as an endorsement of these web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries: iSeries, iSeriese, iSeries, i5, DB2, e (logo)®Server IBM ®, Operating System/400, OS/400, i5/OS.

Microsoft, SQL Server, Windows, Windows NT, Windows XP and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries. UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group. Oracle is a registered trade mark of Oracle Corporation.

Other company, product, and service names may be trademarks or service marks of other companies.