

---

# Securing Your Windows Domain

Engagent White Paper Series  
March 19, 2003



Engagent, Inc.  
17455 68<sup>th</sup> Ave. NE Suite 103  
Kenmore, WA 98028

Phone: 877-820-7980

[www.engagent.com](http://www.engagent.com)

## Table Of Contents

Introduction.....	3
Event Log Management.....	4
Watching for Access Violations through Your Event Logs .....	5
Events That Security Administrators Should Monitor.....	6
Archiving Event Logs .....	8
Forensic Investigation of Event Logs .....	9
Engagent’s Event Log Management Suite.....	9
Monitoring Access to Sensitive Files .....	12
Controlling User Logons .....	14
Eliminating Concurrent Logons.....	14
Limiting Logon Range .....	14
Monitoring Logons .....	15
Managing and Documenting Access to Applications .....	17
Auditing Workstations and Servers .....	20
Conclusion .....	22

## Introduction

Securing computer domains has never been more important. Nor has it ever been more difficult. The growing interdependence among information systems has caused all systems to be interconnected in more ways than ever. Information and processing is distributed ever more widely, creating ever more exposure for sensitive data and applications. Today's rich networks offer exponentially more points of vulnerability than any IT configurations of the past.

Luckily security tools have evolved as rapidly as the networks. The latest generation of security software provides rich functionality to address each vulnerability.

Engagent specializes in offering *software to help administrators manage software*. Engagent's security solutions will not magically protect your domain against all possible harm, but implementing the *best practices* allowed by Engagent's security software will go a long way toward making your domain more secure, while also reducing the amount of administrative time required to be devoted to security issues and reducing the total cost of software ownership.

Engagent's security software allows you to implement the following best practices:

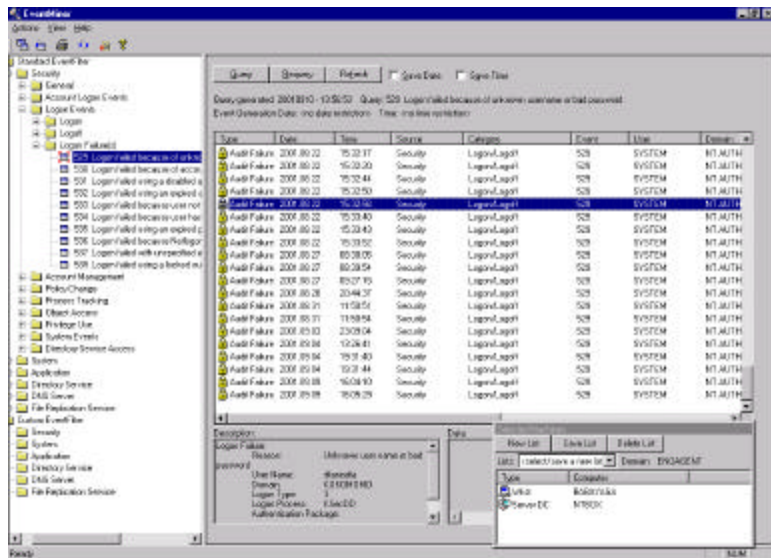
- Efficiently sort through the information in Windows Event Logs.
- Request alerts whenever specified Events occur.
- Control user logon and eliminate multiple use of single User-IDs.
- Report critical file access.
- Control access to critical applications.
- Maintain up-to-date security information by scheduling regular hardware, software, and security inventories of workstations and servers.

The following sections of this White Paper explain each of these best practices in detail.

## Event Log Management

Windows Event Logs are one of the most powerful sources of information for the IT security administrator. In their raw form, however, the information they present is difficult to schematize, and deriving patterns from the event logs is an extremely time-intensive process. Engagent's suite of Event Log Administration and Management software allows you to leverage the information in Windows Event Logs and greatly improve network security.

Automation is critical to managing event logs. There is simply too much information in the event logs to manually monitor all server and workstation event logs, and it is unrealistic to expect a full-time security administrator to be looking at the logs around the clock. You need *software that can notify you* of critical security and server integrity events whenever they happen. You also need to be able to *archive all events to maintain an audit trail* that proves you are monitoring critical events and to have information central to IT planning.



The screenshot displays the 'Event Viewer' application window. The left pane shows a tree view of event logs, with 'Logon Failed' selected. The main pane shows a list of events with columns for Type, Date, Time, Source, Category, Event ID, User, and Details. The events listed are 'Logon Failed because of unknown user name or bad password' (Error 528) and 'Logon Failed because user is disabled' (Error 502). A detailed view of a selected event is shown at the bottom, including the description, reason, and user information.

Type	Date	Time	Source	Category	Event ID	User	Details
Error	2008-08-02	15:22:17	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:22:20	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:22:44	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:22:50	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:23:00	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:23:40	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:23:52	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:28:05	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:28:59	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	15:27:19	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-02	20:44:37	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-21	11:58:51	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-21	11:58:54	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-23	23:29:04	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-04	10:26:41	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-04	10:31:40	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-04	10:31:44	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-08	16:04:10	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM
Error	2008-08-08	16:04:29	Security	LogonFailed	528	SYSTEM	NT AUTHORITY\SYSTEM

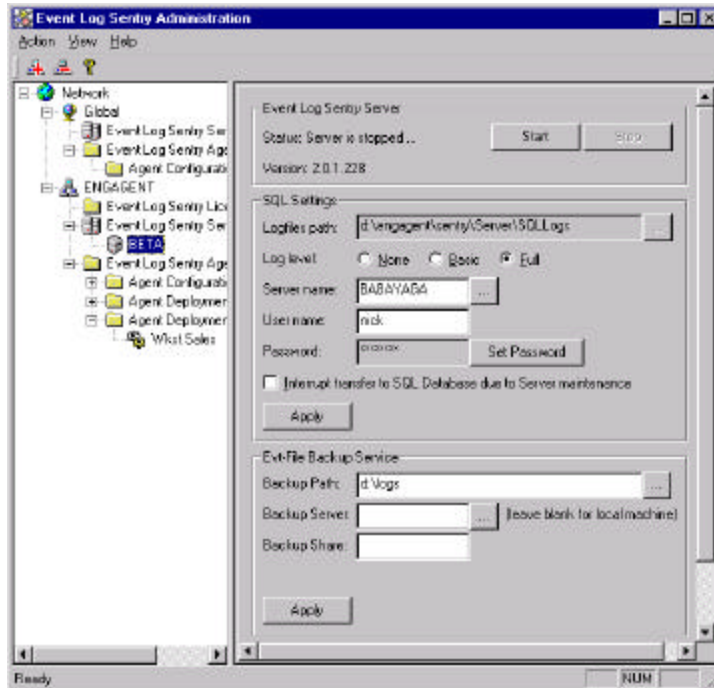
Event Log View Screen Shot

To secure your network, you need to be able to *analyze trends* across servers and workstations and the only way to accomplish this is by consolidating event logs from multiple servers and workstations into a single interface and then filter the information in order to identify critical event trends.

In addition, you need the ability to *store events in a database*. This allows you to use all the powerful tools you associate with relational databases, producing regular reports.

The sign that your Event Log Management is in shape is a *morning report* on the desk of the IT director showing any events in the previous day that merit action or further investigation.

Engagent provides the event log management functionality needed to satisfy these requirements in Windows. By implementing Engagent's Event Log Management, you can fully utilize the information in the event logs to increase security monitoring and decrease response time to critical events.



Event Log Sentry 'Security Administrator' Screen Shot

## Watching for Access Violations through Your Event Logs

Most organizations mistakenly assume access violations come from external sources. As *ComputerWorld* explains, the majority of security threats come from internal sources:

In fact, in the most recent survey on cybercrime by the FBI and the San Francisco-based Computer Security Institute, 81% of corporate respondents said the most likely source of attack was from inside the company. In addition, the U.S. Treasury Department reports that insiders committed 60% of the computer intrusions reported by banks and other financial institutions in the first four months of this year.

The problem, said Mike Hager, vice president of Network Security and Disaster Recovery at New York-based Openheimer Funds Inc., is that corporations have spent about 80% of their security dollars to protect against outside threats when, in fact, 80% of all attacks come from the inside.

—Dan Verton  
“Users are the Weakest Link”  
November 15, 2001

Since firewalls do not offer any protection from internal attacks, the best resource for protection are your event logs. By implementing automated, real-time, 24/7 monitoring on all event logs and receiving immediate notifications of possible intrusions or access violations, you can protect against internal attacks and catch hackers red-handed.

Intrusions can be categorized into two main classes:

1. *Misuse intrusions* are well-defined attacks on known weak points of a system. They can be detected by watching for certain actions being performed on certain objects.
2. *Anomaly intrusions* are based on observations of deviations from normal system usage patterns. They are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile.

Since misuse intrusions typically follow well-defined patterns, they can be detected by frequently running filters on multiple, consolidated event logs. This functionality is available in Event Log View. On the other hand, anomalous intrusions are detected by observing significant deviations from normal behavior. An anomaly may be a symptom of a possible intrusion and needs to be monitored real-time in order to protect your organization. Event Log Sentry gives you the technology to detect anomaly events.

## Events That Security Administrators Should Monitor

<b>Events That Should Be Monitored for Optimal Security</b>	
In addition to the recommended monitoring detailed below, all events should either be automatically archived and/or stored in a database on a regular basis or as the events occur.	
<b>Event Log Event IDs or Categories</b>	<b>Recommended Monitoring</b>
Account logon failures 529-537	<ul style="list-style-type: none"> <li>• Immediate Notification Alert for any administrator account logon failure</li> <li>• Immediate Notification Alert for any logon failure during non-business hours</li> <li>• Daily Filter Viewing</li> </ul>
Profile Changes 624-630	<ul style="list-style-type: none"> <li>• Immediate Notification Alert</li> <li>• Daily Filter Viewing</li> </ul>
Password Changes 627,628	<ul style="list-style-type: none"> <li>• Notification alert for any administrator password change</li> <li>• Notification alert for password change during non-business hours</li> <li>• Daily Filter Viewing</li> </ul>
All error events	<ul style="list-style-type: none"> <li>• Daily Filter Viewing</li> </ul>
User or Group Changes	<ul style="list-style-type: none"> <li>• Immediate Notification Alert</li> <li>• Daily Filter Viewing</li> </ul>

Policy Changes	<ul style="list-style-type: none"> <li>• Immediate Notification Alert</li> <li>• Daily Filter Viewing</li> </ul>
Handle Duplication/Handle Closed	<ul style="list-style-type: none"> <li>• Daily Filter Viewing of critical files</li> </ul>
System Events	<ul style="list-style-type: none"> <li>• Daily Filter Viewing</li> </ul>

Listed below are some of the more important security events. While security monitoring needs vary between different organizations, this list will provide a baseline level of monitoring for general security purposes.

Event ID	Type	Description
512	Success Audit	NT starts
513	Success Audit	NT is shut down
514	Success Audit	Authentication Package is loaded by the LSA (Local Security Authority)
515	Success Audit	A trusted logon process has registered with the LSA
516	Success Audit	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits
517	Success Audit	Security log is cleared
518	Success Audit	SAM has loaded a notification package
528	Success Audit	Successful logon
529	Failure Audit	Logon failure: unknown username or password
530	Failure Audit	Logon failure: account logon time restriction violation
531	Failure Audit	Logon failure: account currently disabled
532	Failure Audit	Logon failure: the specified user account has expired
533	Failure Audit	Logon failure: user not allowed to logon at this computer
534	Failure Audit	Logon failure: the user has not been granted the requested logon type at this machine
535	Failure Audit	Logon failure: the specified account's password has expired
536	Failure Audit	Logon failure: the Netlogon component is not active
537	Failure Audit	Logon failure: An unexpected error occurred during logon
538	Success Audit	User logoff
539	Failure Audit	Logon failure: Account locked out
540	Success Audit	Successful network logon
560	Success Audit	Object access success audit event
561	Success Audit	Handle allocated
562	Success Audit	Handle closed
563	Success Audit	Object opened for delete
564	Success Audit	Object deleted
576	Success Audit	Special privileges assigned to new logon
577	Success Audit	Privilege service called
578	Success Audit	Privilege object operation
592	Success Audit	A new process has been created
593	Success Audit	A process has been exited
594	Success Audit	A handle to an object has been obtained
595	Success Audit	Indirect access to an object has been obtained
608	Success Audit	User right assigned. The event message lists the assigned rights
609	Success Audit	User right removed. The event message lists the removed rights
610	Success Audit	New domain trust created
611	Success Audit	Trust relationship removed
612	Success Audit	The audit policy has been changed. The event message describes the new policy

624	Success Audit	New user account created. The event message lists the new account name and SID
625	Success Audit	User account changed. The event message lists the affected user account
626	Success Audit	User account enabled (from disabled state). The event message lists the affected user account
627	Success Audit	Attempt to change password. The event message lists the affected user
628	Success Audit	User account password set. The event message lists the affected user
629	Success Audit	Account disabled. The event message lists the affected user
630	Success Audit	Account deleted. The event message lists the affected user
631	Success Audit	Global group created. The event message lists the group
632	Success Audit	New member added to global group. The event message lists the affected group, as well as the name of the added account
633	Success Audit	Member removed from global group. The event message lists the affected group, as well as the name of the removed account
634	Success Audit	Global group deleted. The event message lists the affected group
635	Success Audit	Local group created. The event message lists the affected group
636	Success Audit	New member added to local group. The event message lists the affected group, as well as the name of the added account
637	Success Audit	Member removed from local group. The event message lists the affected group, as well as the name of the removed account
638	Success Audit	Local group deleted. The event message lists the affected group
639	Success Audit	Local group changed. The event lists the affected group
640	Success Audit	General account database change. The event lists the change that was made
641	Success Audit	Global group changed. The event message lists the affected group
642	Success Audit	User account changed. The event lists the affected account
643	Success Audit	Domain policy changed. The event lists the affected domain
644	Success Audit	User account locked out. This event is logged when an account is locked out due to repeated logon failures. On Windows NT computers, this event is only logged if Service Pack 4 or higher is installed

## Archiving Event Logs

Event Logs fill up quickly, and at many sites valuable (and irreplaceable) Event Log information is casually overwritten. Attempting not to lose events in Event Logs has previously meant a very time-intensive process of managing event logs individually: determining thresholds for actual file size of the logs and dealing with them when they reach that size. Event Log Sentry gives you a consolidated central interface from which you can configure maximum size by event age or by file size, but more importantly, it will **back up event logs to an external server**. This best practice ensures that even if a malicious user intentionally tries to eliminate evidence by clearing event logs, the information will be preserved. (This external storage can be managed with hierarchical storage practices which reduce cost by progressively shifting the data over time to less expensive storage such as tape or other backup devices.)

Event Log Sentry stores the raw .EVT files, ensuring that you have a **complete and documented audit trail of all original evidence**. Additionally, you may configure triggers causing Event Log Sentry to migrate specific events to an SQL server (using MS SQL's native API). Having the events in a database allows you to perform more powerful queries on them, analyze trends, spot anomalies, and create triggers on specific events. Having events in the database greatly facilitates analysis, but it is no substitute

for also preserving the original raw .EVT files. The best security practice is to archive all event logs externally.

## Forensic Investigation of Event Logs

Most security efforts are (appropriately) spent on attempting to keep bad events – particularly unauthorized access to data, or, worse, modification of data – from happening. Sometimes, however, despite all best efforts, bad things do happen.

In addition to repairing any damage and eliminating vulnerabilities to prevent a recurrence, security efforts after the fact concentrate on

- Determining exactly what has happened

- Finding out who did it

- Preserving and organizing evidence in case of legal action.

The ideal solution for forensic investigation of Event Logs is Engagent’s Event Log View EVT. View EVT extends the comprehensive power of Event Log View to archived EVT files, providing a powerful search and query tool that allows investigators to search through a collection of archived .EVT files and quickly find exactly the events they are seeking. The custom reports generated from View EVT provide proof positive of exactly what happened on your network

## Engagent’s Event Log Management Suite

Engagent’s comprehensive Event Log Management suite offers software to handle every aspect of Event Log administration. The following table is designed to help clarify which products you need in order to accomplish what you are trying to do:

	Event Log View EVT	Event Log View	Event Log View Server	Event Log Sentry
Collects events from multiple Server / Workstation		✓	✓	✓
Agentless	✓	✓	✓	
Generate Reports	✓	✓	✓	✓
Store events to SQL Database			✓	✓
Multiple Response Actions			✓	✓
Database Maintenance			✓	✓
Build Multiple Templates for Servers / Workstations				✓

Set and enforce security auditing



Set and enforce event log size and overwrite



Archiving of event logs



Real Time Event Notification



Set Audit Policies



View Archived Logs



## Real-Life Scenarios Using Event Log Sentry

### **Scenario**

An intruder attempts to log on to an Administrative account by guessing the password.

### **Result**

Because you have configured Event Log Sentry to notify you on failed Administrative logons, you will be alerted immediately. You can observe where the intruder is coming from, and you can block the session to prevent further attempts.

### **Scenario**

An intruder succeeds in gaining access to your network and attempts to change user permissions.

### **Result**

Because you have configured Event Log Sentry to notify you on User Permission changes, you will be alerted immediately. You can terminate the intruder's session before damage can be done.

### **Scenario**

An authorized user attempts to access an unauthorized resource.

### **Result**

Your daily report will show you exactly what happened

### **Scenario**

An authorized user wants to do something they should not be doing, so they change audit policy or clear event logs in order to cover their tracks.

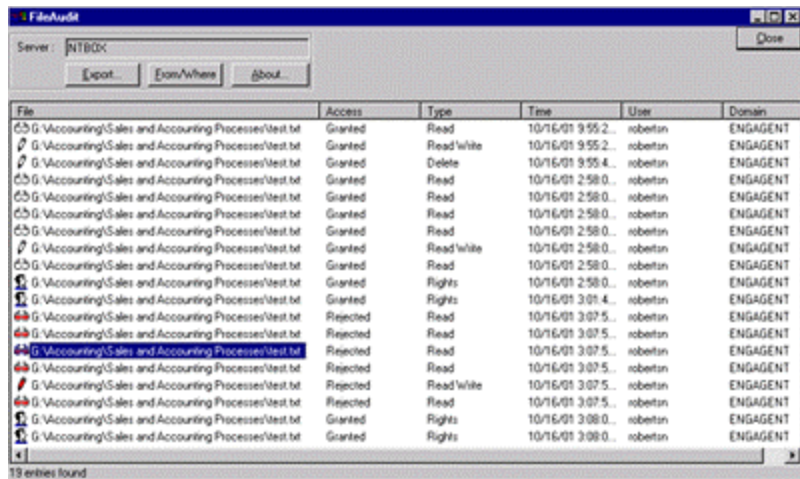
### **Result**

Your daily report will show you what the user has done.

## Monitoring Access to Sensitive Files

Monitoring and protecting access to sensitive files is crucial. Files need to be monitored constantly to assure file access is secure and only appropriate users are accessing the files.

The security event logs store information about file access (when the proper auditing is set for that object), but putting file access information into a useful format is difficult—even if you are using a powerful event log management solution like Event Log Sentry. To make monitoring file access easy, Engagent offers FileAudit. FileAudit's specializes in giving you the critical information pertaining to specific files and what users attempt access (successes and failures) and date and time information.



The screenshot shows the FileAudit application window. At the top, there is a 'Server' field set to 'NTBDC' and buttons for 'Export...', 'Exit/Where', and 'About...'. Below this is a table with columns: File, Access, Type, Time, User, and Domain. The table contains 18 rows of data, all for the file 'G:\Accounting\Sales and Accounting Processes\test.txt'. The access types include Read, Read/write, Delete, and Rights, with some entries marked as 'Granted' and others as 'Rejected'. The users listed are 'robertsn' and the domain is 'ENGAGENT'. At the bottom of the window, it says '18 entries found'.

File	Access	Type	Time	User	Domain
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read	10/16/01 9:55:2...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read/write	10/16/01 9:55:2...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Delete	10/16/01 9:55:4...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read	10/16/01 2:58:0...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read	10/16/01 2:58:0...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read	10/16/01 2:58:0...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read/write	10/16/01 2:58:0...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Read	10/16/01 2:58:0...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Rights	10/16/01 3:01:4...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Rights	10/16/01 3:01:4...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Rejected	Read	10/16/01 3:07:5...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Rejected	Read	10/16/01 3:07:5...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Rejected	Read	10/16/01 3:07:5...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Rejected	Read/write	10/16/01 3:07:5...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Rejected	Read	10/16/01 3:07:5...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Rights	10/16/01 3:08:0...	robertsn	ENGAGENT
G:\Accounting\Sales and Accounting Processes\test.txt	Granted	Rights	10/16/01 3:08:0...	robertsn	ENGAGENT

**FileAudit Example Report**

FileAudit displays a sorted list of all access or access attempts for one file, several files or several directories. FileAudit's user-friendly interface allows you to immediately identify:

- the type of access (reading, modification, deletion, etc.)
- the user attempting access,
- the date and time
- the workstation.

## Real-Life Scenarios Using FileAudit

**Scenario**

A curious user tries to access confidential proprietary specifications of a forthcoming product.

**Result**

When you come in and review your daily FileAudit report, you will see a list of everything the user tried to look at.

**Scenario**

An important file has been corrupted.

**Result**

FileAudit quickly gives you a list of everyone who has recently updated the file.

## Controlling User Logons

### Eliminating Concurrent Logons

Proper event log management can *identify* intrusions. However, the best practices approach takes extra precautions to *prevent* intrusions. Because Windows security relies on unique logons, the first level of defense is to ensure that only the appropriate user utilizes their account. Some users may leave open sessions unattended for periods of time, sometimes even overnight. Others may share their passwords with coworkers. ***Leaving sessions open and sharing passwords are security threats.*** Without a solution to ensure that users do not share passwords or have multiple sessions open, your network will never be secure.

Here is a real-life example:

A user logs onto a computer and then leaves that session open; all of the information that the user has access to is now available to any person who walks by that workstation. Screen savers are designed to protect against this potential problem but screen savers take time to kick in, and many users disable the screen saver, remove the password requirement, or alter the screen saver settings. Some employees will even leave their account logged on for a series of shifts from one day to the next.

If you cannot ensure that only the appropriate user is utilizing an account, the foundation for Windows security is gone and you are unable to hold users accountable and impose security. The best practice to protect against intrusions and access violation is to limit concurrent logons and to limit either workstations or IP ranges that users and groups can log onto.

Engagent UserLock gives you the technology to do just this. UserLock adds protection to built-in Windows NT logon security by allowing you to enforce a policy that each user account may be logged into your network only once. By implementing UserLock, you protect against stolen passwords and prevent users from leaving open sessions.

### Limiting Logon Range

In addition to allowing each user account to log on only once, UserLock also allows you to restrict certain users to certain workstations. Restrict the range and power of user logon accounts is a key step in securing a Windows network. Every organization has different needs, but most organizations would benefit from some combination of the following restrictions:

***Restrict most user accounts to individual workstations or groups of workstation.***

If Joe works in the shipping department, he probably never needs to log on to any workstation other than those in the shipping department. If Joe (or, more probably,

someone using Joe's password) tries to log on to any other system on your network, such as the file server in the server room, the logon should be disallowed, and an administrator should be alerted.

***Disable most user accounts from logging in from outside your network's IP range.***

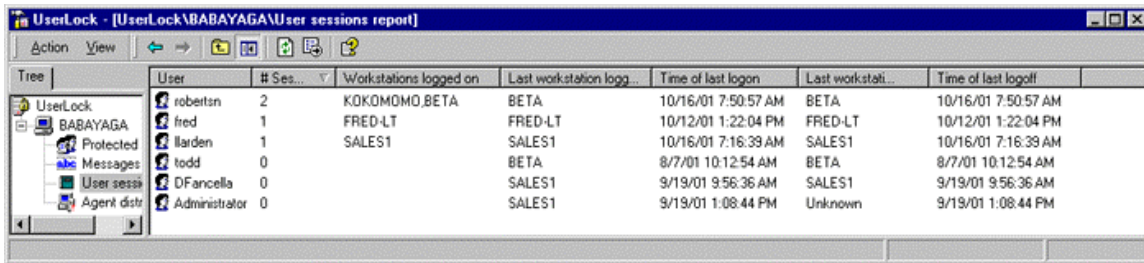
Some of your users may need to log onto your domain remotely, but probably most don't. Setting a policy that user accounts cannot log onto the domain unless they are physically in the domain will eliminate most intruders. Then exceptions to this policy can be made for those who require remote access.

UserLock makes setting these policies simple and straightforward.

## Monitoring Logons

UserLock contains detailed built-in reports for user logon history, as well as their current status. UserLock reports detail:

1. The number of open sessions for a specific user;
2. The name(s) of the workstation(s) the user is currently logged onto;
3. The last workstation logged onto;
4. The time of last logon;
5. The last workstation logged off; and
6. The time of last logoff.



The screenshot shows a window titled "UserLock - [UserLock\BABAYAGA\User sessions report]". The window contains a table with the following columns: User, # Ses..., \Workstations logged on, Last workstation logg..., Time of last logon, Last workstati..., and Time of last logoff. The table lists several users and their session details.

User	# Ses...	\Workstations logged on	Last workstation logg...	Time of last logon	Last workstati...	Time of last logoff
robertsn	2	KOKOMOMO.BETA	BETA	10/16/01 7:50:57 AM	BETA	10/16/01 7:50:57 AM
fred	1	FRED-LT	FRED-LT	10/12/01 1:22:04 PM	FRED-LT	10/12/01 1:22:04 PM
larden	1	SALES1	SALES1	10/16/01 7:16:39 AM	SALES1	10/16/01 7:16:39 AM
todd	0		BETA	8/7/01 10:12:54 AM	BETA	8/7/01 10:12:54 AM
DFancelli	0		SALES1	9/19/01 9:56:36 AM	SALES1	9/19/01 9:56:36 AM
Administrator	0		SALES1	9/19/01 1:08:44 PM	Unknown	9/19/01 1:08:44 PM

**UserLock User Session Report**

## Real-Life Scenarios Using UserLock

### Scenario

A user leaves workstation A without logging off, then tries to log on to workstation B.

### Result

The user is not allowed to log on to workstation B. He or she returns to workstation A and logs off. Private information on workstation A is now protected. After only a few repetitions, the user acquires the habit of always logging off a workstation before leaving it.

### Scenario

A hacker or disgruntled employee uses a stolen password to log on to a workstation not allowed for the account they are using.

### Result

The intruder is not able to log on to the domain. The Administrator is alerted immediately.

### Scenario

A hacker or disgruntled employee uses a stolen password to log on to a workstation. However, the authorized user is already logged on and this account is limited to a single network logon.

### Result

The intruder is not able to log on to the domain. The Administrator is alerted immediately.

### Scenario

A user trying to log on receives a UserLock message explaining that they are already logged on.

### Result

The user contacts the administrator about the message. The administrator determines what workstation this user's account is logged on. (UserLock's 'User Session Analysis Report' makes this easy to do.) The administrator can either go directly to the workstation or contact a local manager to either log off the account or to catch the unauthorized user who is using the account.

## Managing and Documenting Access to Applications

Your network is not secure until you can *document* that it is secure. Engagent Software Metering gives you an audit trail that documents *all* usage of your critical software. Engagent Software Metering will show you:

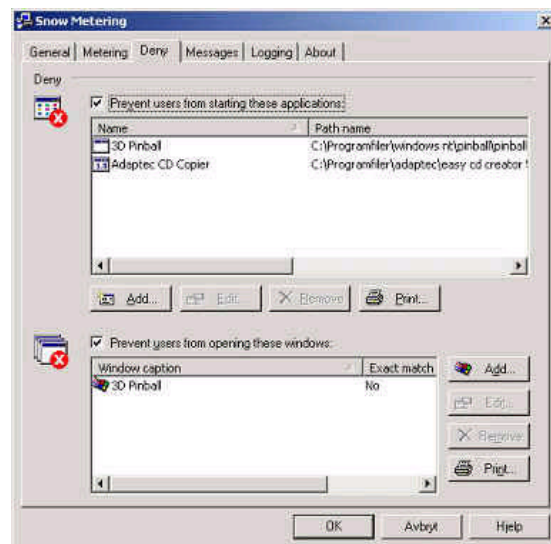
- *who* accessed the application
- *when* they used it
- *how long*
- *how often*
- *where* (from what workstation)

You can specify which applications will be metered, or you can meter all applications.

Engagent Software Metering is sparing in its use of system resources, and will not get in the way of normal workstation use.

Engagent Software Metering gives you complete control over software license usage. In addition to *monitoring software usage*, Engagent Software Metering will allow you to *control software usage*.

You can declare specific applications “illegal” on your domain. Engagent Software Metering will check each application every user launches to make sure it is not on your list of prohibited applications. When a user tries to launch the illegal application – whether the application is locally installed or a network share, downloaded from the Internet, even renamed – Engagent Software Metering will prevent the application from launching. If you choose, it will also present a custom message you have written explaining why the application has been prohibited, and it will log the event so you know the user tried to launch the application.



**Engagent Software Metering’s  
Powerful “Deny” Capability**

## Real-Life Scenarios Using Engagent Software Metering

### **Scenario**

Your user James attempts to launch the password cracker “John the Ripper.”

### **Result**

James sees a dialog box explaining why that application is disallowed. The application does not launch. James’s attempt to launch it is recorded in a database. You receive an alert.

### **Scenario**

James renames the executable of “John the Ripper” to “Excel.”

### **Result**

Metering still recognizes the application as “John the Ripper.” It still will not launch. The action is recorded in a database. You receive an alert

### **Scenario**

Your user Vera attempts to launch the payroll application after hours.

### **Result**

Vera sees a dialog box explaining why access to the payroll application is disallowed after hours. The payroll application does not launch. Vera’s action is recorded in a database. You receive an alert.

### **Scenario**

You have reason to suspect that Dave, a recent hire in the IT department, is engaged in industrial espionage.

### **Result**

In seconds you access a complete report of every application Dave has launched since he was hired, when he launched each one, how long he kept the application running, and how much activity he engaged in.

### **Scenario**

You wonder whether Kazaa is in use on your network.

### **Result**

In seconds you access a complete report of every user on your network who has ever launched Kazaa.



## Auditing Workstations and Servers

Central to providing a complete audit trail is doing frequent domain inventories to obtain complete, up-to-date network views. This view comes from doing complete scans of workstations and servers to provide you with information about groups, users, shares, software, hot fixes, service packs, hardware and other valuable network information.

Security requires not only an up-to-date network view (i.e. network diagram) but also an the audit trail showing, for example, which users had membership to what groups during a specific date range and what software was installed on what workstations, you need to implement a solution that will frequently collect domain(s) information and store that information in a central database that can be relied on for date-specific and information-specific reports.

Engagent offers two automated inventory solutions: WinReporter and Engagent Domain Inventory (EDI). Both are easy to install, configure, and use. Both gather information quickly while requiring as little as possible in the way of network or desktop resources. WinReporter is a standalone “point” solution that delivers a snapshot of the network as it is seen at one instant in time. EDI offers more comprehensive detail, access to external relational databases, better capture of transient network nodes such as laptops, and integration with Engagent Software Metering and Engagent License Manager.

The following table lists some representative information that will be returned by both products:

Information returned by Engagent's Inventory Solutions	
Domain users	NT services and status
Domain groups	Files and ACLs
Machine users	Shares
Machine groups	Installed software
CPU type	Service packs
BIOS info	Hot fixes

Real-Life Scenarios Using Engagent's Inventory Solutions
<p><b>Scenario</b> A virus is loose on your network. You need to find out immediately what workstations are affected.</p>

**Result**

An inventory report will instantly show you exactly which systems have been compromised.

**Scenario**

Your operating vendor notifies you of a critical vulnerability in Version 4.05 of their software and issues a hot fix which should be installed on all copies of Version 4.05 immediately.

**Result**

It takes only seconds to create a custom report showing all copies of Version 4.05 on your network and to export the list to the hotfix distribution tool.

**Scenario**

Your security policy directs that the Messenger service be disabled on all servers..

**Result**

A single report quickly shows you any servers with the Messenger service running.

**Scenario**

After a merger, you are responsible for incorporating a new domain into existing trust relationships. Before you trust the domain, you want a complete report on all user permissions and policies on the domain.

**Result**

The report is quickly generated, and you require several permissions and policies to be changed before allowing the trust relationship.

## Conclusion

Even though the task of improving network security may initially appear daunting, your IT department can receive a range of benefits from the implementing *best practices* processes and strategies. Far from requiring more administrative time, once best practices are in place, you will benefit from *reduced* administrative overhead. By improving security, your IT Department can create consistent IT practices, automate processes, and—as a result—*reduce the total cost* of operation.

The individual components of the Engagent Security Compliance Suite offer a rich array of functionality in addition to their role in security. All Engagent products are available for evaluation in full-featured versions, downloadable at [www.engagent.com](http://www.engagent.com). Engagent software professionals are available to walk you through installation and configuration of these products, to obtain optimal results for your particular network configuration, to answer questions, to provide other information, and to make sure that the product meets all your requirements. Call 1-877-820-7980 today to arrange for your installation.