Microsoft Windows Vista and Windows Server 2008 EAL1 Security Target

Version 1.0
August 14, 2008

Prepared For:

Microsoft Corporation
Corporate Headquarters
One Microsoft Way
Redmond, WA 98052-6399

Prepared By:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Gateway Drive
Columbia, MD 21046-2554

Version 1.0, 8/14/2008

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. SECURITY TARGET INTRODUCTION 1

1.1 SECURITY TARGET, TOE, AND COMMON CRITERIA (CC) IDENTIFICATION 1
1.2 CC CONFORMANCE CLAIMS 2
1.3 CONVENTIONS, TERMINOLOGY, ACRONYMS 2
1.3.1 Conventions 2
1.3.2 Terminology 2
1.3.3 Acronyms 3
1.4 ST OVERVIEW AND ORGANIZATION 3

2. TOE DESCRIPTION 4

2.1 PRODUCT TYPES 4
2.2 PRODUCT DESCRIPTION 4
2.3 SECURITY ENVIRONMENT AND TOE BOUNDARY 5
2.3.1 Logical Boundaries 5
2.3.2 Physical Boundaries 7
2.4 TOE SECURITY SERVICES 7

3. SECURITY OBJECTIVES 9

3.1 SECURITY OBJECTIVES FOR THE ENVIRONMENT 9
3.2 ASSUMPTIONS 9

4. IT SECURITY REQUIREMENTS 10

4.1 EXTENDED COMPONENTS DEFINITIONS 10
4.2 TOE SECURITY FUNCTIONAL REQUIREMENTS (SFRS) 10
4.2.1 Security audit (FAU) 11
4.2.2 User data protection (FDP) 14
4.2.3 Identification and authentication (FIA) 15
4.2.4 Security management (FMT) 16
4.2.5 Protection of the TSF (FPT) 18
4.2.6 TOE access (FTA) 18
4.3 TOE SECURITY ASSURANCE REQUIREMENTS (SARS) 19
4.3.1 Development (ADV) 19
4.3.2 Guidance documents (AGD) 20
4.3.3 Life-cycle support (ALC) 20
4.3.4 Tests (ATE) 21
4.3.5 Vulnerability assessment (AVA) 21
4.4 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 21

5. TOE SUMMARY SPECIFICATION (TSS) 22

5.1 TOE SECURITY FUNCTIONS 22
5.1.1 Audit Function 22
5.1.2 User Data Protection Function 26
5.1.3 Identification and Authentication Function 32
5.1.4 Security Management Function 38
5.1.5 TOE Access Function 41

APPENDIX A—LIST OF ACRONYMS 43

APPENDIX A—LIST OF ACRONYMS 43

APPENDIX B – GUIDANCE ADDENDUM 47

1. Security Target Introduction

This section presents the following information:

- Identifies the Security Target (ST) and Target of Evaluation (TOE);
- Specifies the ST conventions and ST conformance claims; and,
- Describes the ST organization.

1.1 Security Target, TOE, and Common Criteria (CC) Identification

ST Title - Microsoft Windows Vista and Windows Server 2008 EAL1 Security Target

ST Version – Version 1.0, 8/14/2008

TOE Software Identification – The following Windows Operating Systems (OS'):

- Microsoft Windows Vista Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2008 Standard Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2008 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2008 DataCenter Edition (64-bit version)

The following security updates and patches must be applied to the above stated products:

KB	951376	950759	951698	953235	950762	950760	941693	948590
OS/app Bulletin	MS08-030	MS08-031	MS08-033	MS08-035	MS08-036	MS08-032	MS08-025	MS08-021
Vista SP1	X	X	X	N/A	X	X	X	X
Vista x64 SP1	X	X	X	N/A	X	X	X	X
Windows Server 2008	N/A	X	X	X	X	X	X	X
Windows Server 2008 x64	N/A	X	X	X	X	X	X	X
Windows Server 2008 Itanium	N/A	X	X	N/A	X	X	X	X
Internet Explorer 7 for Vista	N/A	X	N/A	N/A	N/A	N/A	N/A	N/A
IE7 for Vista x64	N/A	X	N/A	N/A	N/A	N/A	N/A	N/A
IE7 for WS08	N/A	X	N/A	N/A	N/A	N/A	N/A	N/A
IE7 for WS08 x64	N/A	X	N/A	N/A	N/A	N/A	N/A	N/A
IE7 for WS08 Itanium	N/A	X	N/A	N/A	N/A	N/A	N/A	N/A

Evaluation Assurance Level (EAL) – EAL1

CC Identification – CC for Information Technology (IT) Security Evaluation, Version 3.1, R**evision 2, September 2007** (CCv3.1).

International Standard – International Organization for Standardization (ISO)/International Electro-technical Commission (IEC) 15408:1999.

Keywords – OS, sensitive data protection device, directory service, network management, desktop management, single sign on, Discretionary Access Control (DAC), Data Execution Prevention (DEP), ST, access control, EAL1, Microsoft Windows, 32 bit, 64 bit, x64.

1.2 CC Conformance Claims

This TOE and ST are consistent with the following specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 2, September 2007, conformant.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1, Revision 2, September 2007, conformant, EAL1.

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the ST.

1.3.1 Conventions

The notation, formatting, and conventions used in this security target are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, section C.4 as:

- assignment: allows the specification of parameters;
- refinement: allows the addition of details;
- selection: allows the specification of one or more items from a list; and
- iteration: allows a component to be used more than once with varying operations.

Within Section 5 of this ST, the following conventions are used to signify how the requirements stated have been modified from the CC text. Outside of section 5, special formatting does not have this same meaning.

- Assignments or selections specified by this security target are **bold** and identified between brackets ("[ ]"). Selections are also italicized to distinguish them from assignments.
- Additions or changes (i.e., refinements) to the CC are specified in bold.

Iterations are identified with a letter following the component number (e.g., "1a"). These follow the short family name and allow components to be used more than once with varying operations.

1.3.2 Terminology

The following terminology is used in the ST:

- Authorized User – an entity that has been properly identified and authenticated. These users are considered to be legitimate users of the TOE.
- Authorized administrator/Administrator – A user in the administrator role is an authorized user who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given them. The term authorized administrator is taken from the CC and is used in the ST in those sections that are derived from the CC directly. Otherwise, the term administrator is used. These terms are used interchangeably.
- Security-Relevant TSF data – Data used by the TSF that which defines, controls or monitors the configuration of the security features of the system. This data includes system security configuration information, audit records, user security attributes, authentication data, and access control policy information.

1.3.3 Acronyms

The acronyms used in this ST are specified in Appendix A – Acronym List.

1.4 ST Overview and Organization

The Microsoft Windows Vista and Windows Server 2008 TOE is a general-purpose, distributed, network OS that provides controlled access between subjects and user data objects. Microsoft Windows Vista and Windows Server 2008 TOE has a broad set of security capabilities including single network logon (using password); access control; extensive security audit collection; and Light-weight Directory Access Protocol (LDAP) Directory-based resource management. The Windows Vista TOE provides the following security services: audit, user data protection (DAC), Identification and Authentication (I&A), security management, and TOE access. The Windows Vista and Windows Server 2008 security policies provide network-wide controlled access protection (access control for user data). These policies enforce access limitations between individual users and data objects. The TOE is capable of auditing security relevant events that occur within a Windows Vista network. All these security controls require users to identify themselves and be authenticated prior to using any node on the network.

The Microsoft Windows Vista and Windows Server 2008 ST contains the following additional sections:

- TOE Description (Section 2) – Provides an overview of the TSF and boundary.
- Security Objectives (Section 3) – Identifies the security objectives that are to be satisfied by the TOE environment.
- IT Security Requirements (Section 4) – Presents the security functional and assurance requirements met by the TOE.
- TOE Summary Specification (Section 5) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.

2. TOE Description

The TOE includes the Windows Vista™ operating system, Microsoft Windows Server® 2008 operating system, supporting hardware, and those applications necessary to manage and support the operating system.

2.1 Product Types

Windows Vista and Windows Server 2008 are preemptive multitasking, multiprocessor, and multi-user operating systems. In general, operating systems provide users with a convenient interface to manage underlying hardware. They control the allocation and manage computing resources such as processors, memory, and Input/Output (I/O) devices. Windows Vista and Windows Server 2008 expand on these basic OS capabilities to managing and controlling the allocation of higher level IT resources such as security principals (i.e. user or machine accounts), files, printing objects, services, windows stations, desktops, network ports/traffic, and directory objects. Multi-user OS', such as Windows Vista and Windows Server 2008, keep track of which user is using which resource, grant resource requests, account for resource usage, and mediate conflicting requests from different programs and users.

Windows Vista and Windows Server 2008 provides an interactive user interface (UI), as well as a network interface. The TOE includes a homogenous set of Windows Vista and Windows Server 2008 systems that can be connected via their network interfaces and may be organized into domains. A domain is a logical collection of Windows Vista and Windows Server 2008 systems that allows the administration and application of a common security policy and the use of a common accounts database. Windows Vista and Windows Server 2008 support single and multiple domain configurations. In a multi-domain configuration, the TOE supports implicit and explicit trust relationships between domains. Domains use established trust relationships to share account information and validate the rights and permissions of users. A user with one account in one domain can be granted access to resources on any server or workstation on the network. Domains can have one-way or two-way trust relationships. Each domain must include at least one designated server known as a Domain Controller (DC) to manage the domain. The TOE allows for multiple DCs that replicate TOE Data among themselves to provide higher availability.

Each Windows Vista and Windows Server 2008 system, whether it is a DC server, non-DC server, or workstation, is part of the TOE and provides a subset of the TSFs. The TSF for Windows Vista and Windows Server 2008 can consist of the security functions from a single system (in the case of a stand-alone system) or the collection of security functions from an entire network of systems (in the case of domain configurations).

Within this ST, when specifically referring to a type of TSF (e.g., DC), the TSF type will be explicitly stated. Otherwise, the term TSF refers to the total of all TSFs within the TOE.

Other than an operating system Windows Vista and Windows Server 2008 can also be categorized as the following type of **Information Assurance** (**IA**) or IA enabled IT product:

- Windows Vista and Windows Server 2008 is a **Desktop Management** product to support the Security Infrastructure. Group Policy Service, which is part of Windows Vista and Windows Server 2008 TOE, provides the desktop management of Windows Vista and Windows Server 2008 TOE desktops.

2.2 Product Description

Windows Vista and Windows Server 2008 are operating systems that support both workstation and server installations. The TOE includes five product variants of Windows Vista and Windows Server 2008: Windows Vista Enterprise, Windows Server 2008 Standard, Windows Server 2008 Enterprise, Windows Server 2008 Datacenter, and Windows Server 2008 for Itanium-based Systems. The server products additionally provide DC features including the AD and Kerberos Key Distribution Center (KDC). The server products in the TOE also provide Content Indexing and Searching, RPC over HTTP Proxy, Simple

Service Discovery Protocol (SSDP), Distributed Transaction Coordinator (DTC), File Replication, Directory Replication, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Distributed File System (DFS), Removable Storage Manager, and Virtual Disk Service. All server variants include the same security features. The primary difference between the variants is the number of users and types of services they are intended to support.

Windows Vista is a client operating system product, suited for business desktop and portable computers (note that portable computers are not included in the evaluated configuration). Windows Server 2008 Standard is designed for departmental and standard workloads, Windows Server 2008 delivers intelligent file and printer sharing; secure connectivity based on Internet technologies, and centralized desktop policy management. Windows Server 2008 Enterprise differs from Windows Server 2008 Standard primarily in its support for high-performance servers for greater load handling. These capabilities provide reliability that helps ensure systems remain available. Windows Server 2008 Datacenter provides the necessary scalable and reliable foundation to support mission-critical solutions for databases, enterprise resource planning software, high-volume/real-time transaction processing, and server consolidation.

The security features addressed by this security target are those provided by Windows Vista and Windows Server 2008 as operating systems. Microsoft provides software applications, packaged with the operating systems, which are considered outside the scope of the defined TOE and thus not part of the evaluated configuration. Services outside this evaluation include: Internet Information Services, Windows Firewall, Certificate Services, Terminal Services, Microsoft Message Queuing, Rights Management Services, and Windows SharePoint Services. The features identified and described in this section are provided with the TOE, though not within the TSF. As these additional features are simply applications that run on the TOE, they may be installed. However, the administrator is required to ensure that they are run in a secure manner.

The following table summarizes the TOE configurations included in the evaluation. There are eleven stand-alone configurations and seventeen networked configurations.

	Windows Vista Enterprise (32 bit and 64 bit)	Windows Server 2008 Standard (32 bit and 64 bit)	Windows Server 2008 Enterprise (32 bit and 64 bit)	Windows Server 2008 Datacenter (64 bit)	Windows Server 2008 for Itanium-based Systems
Single Processor	X	X	X	N/A	X
Multiple Processor	X	X	X	X	N/A
Stand-alone	X	X	X	X	X
Domain Member	X	X	X	X	X
Domain Controller	N/A	N/A	X	X	X
Variations as a Domain Element	2	2	4	2	2
Total Variations	4	4	6	3	3

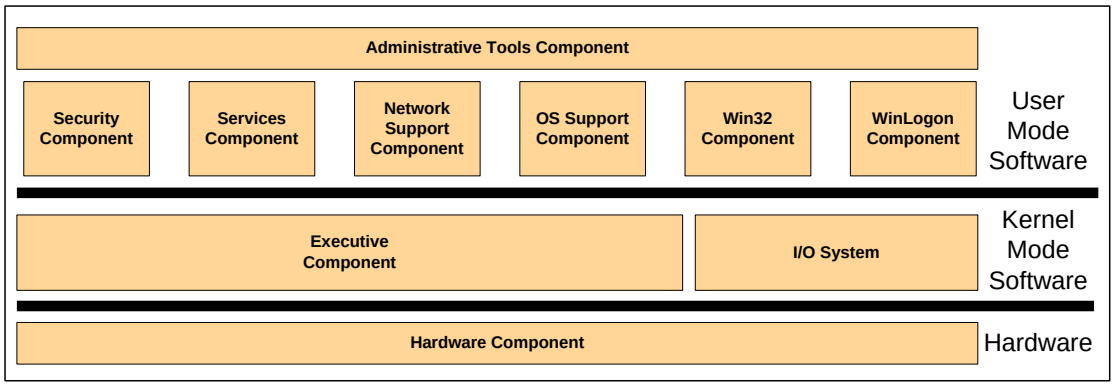
2.3 Security Environment and TOE Boundary

The TOE includes both physical and logical boundaries. Its operational environment is that of a homogenous, networked environment.

2.3.1 Logical Boundaries

The diagram below depicts components and subcomponents of Windows Vista and Windows Server 2008 that comprise the TOE. The components/subcomponents are large portions of the Windows Vista and

Windows Server 2008 operating systems, and generally fall along process boundaries and a few major subdivisions of the kernel mode software.



The system components are:

- Administrator Tools Module
  - Administrator Tools Component (aka GUI Component): This component represents the range of tools available to manage the security properties of the TSF.
- Hardware Module
  - Hardware Component: This component includes all hardware used by the TSF to include the processor(s), motherboard and associated chip sets, controllers, and I/O devices.
- Kernel Software Module
  - Executive Component: This is the kernel-mode software that provides core OS services to include memory management, process management, and inter-process communication. This component implements all the non-I/O TSF interfaces for the kernel-mode.
  - I/O System: This is the kernel-mode software that implements all I/O related services, as well as all driver-related services. The I/O System is further divided into:
    - I/O Core Component
    - I/O File Component
    - I/O Network Component
    - I/O Devices Component
- Miscellaneous OS Support Module
  - OS Support Component: This component is a set of processes that provide various other OS support functions and services
- Remote Procedure Call (RPC) and Network Support Module
  - Network Support Component: This component contains various support services for RPC, COM, and other network services.
- Security Module
  - Security Component: This component includes all security management services and functions.
- Services Module

  - Services Component: This is the component that provides many system services as well as the service controller.

- Win32 Module
  - Win32 Component: This component provides various support services for Win32 applications and the command console application.
- WinLogon Module
  - WinLogon Component: This component provides various interactive logon services to include interactive authentication, trusted path, session management and locking.

These components are further refined in Appendix B, TOE Component Decomposition.

2.3.2 Physical Boundaries

Physically, each TOE workstation or server consists of an x86, x64, or IA64 machine or equivalent processor (including AMD Opteron and Athlon 64; and Intel Xeon and Pentium families) with up to four (4) CPUs for a standard Server product, up to eight (8) CPUs for the Enterprise Server product, and up to 32 CPUs for the Data Center product. A set of devices may be attached and they are listed as follows:

- Display Monitor,
- Keyboard,
- Mouse,
- CD-ROM Drive
- Fixed Disk Drives,
- Audio Adaptor, and
- Network Adaptor.

The TOE does not include any physical network components between network adaptors. The ST assumes that any network connections, equipment, and cables are appropriately protected in the TOE security environment.

2.4 TOE Security Services

The security services included within the TSF are summarized below:

- **Security Audit** – Windows Vista and Windows Server 2008 have the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated, computer where the event occurred, and other event specific data. Authorized administrators can review audit logs and configure the TOE to only collect events for which the administrator is interested, based on a defined set of criteria.
- **User Data Protection** – Windows Vista and Windows Server 2008 protect user data by enforcing the access control policy (DAC) and object and subject residual information protection. Windows Vista and Windows Server 2008 use access control methods to allow or deny access to objects, such as files, directory entries, and printers. It authorizes access to these resource objects through the use of Security Descriptors (SDs) (which are sets of information identifying users and their specific access to resource objects). Windows Vista and Windows Server 2008 also protect user data by ensuring that resources exported to user-mode processes do not have any residual information.
- **Identification and Authentication** – Windows Vista and Windows Server 2008 require each user to be identified and authenticated (using a password) prior to performing any functions. An interactive user invokes a trusted path in order to protect their I&A information. Windows Vista and Windows Server 2008 maintain a database of accounts which includes user identities, authentication information, group associations, privileges and logon rights associations for each

security principal. Windows Vista and Windows Server 2008 provide a set of account policy functions that include the ability to define minimum password length, number of failed logon attempts, duration of lockout, and password age.

- **Security Management** – Windows Vista and Windows Server 2008 include a number of functions to manage policy implementation. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.
- **TOE Access** – Windows Vista and Windows Server 2008 enable a user to lock their session immediately or after a defined period of inactivity. The TOE constantly monitors input devices for activity and automatically locks the workstation after a defined period of inactivity, if so configured. Windows Vista and Windows Server 2008 allow an authorized administrator to configure the system to display a logon banner before the logon dialog is displayed.

3. Security Objectives

This section defines the security objectives for the supporting environment of Windows Vista.

3.1 Security Objectives for the Environment

Certain objectives with respect to the general operating environment must be met for the TOE to meets its security functional requirements. Those objectives are listed below.

Table 3-1 Security Objectives for the Environment

Security Objective	Description
O.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives.
O.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack which might compromise IT security objectives.
O.CREDEN	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users in a manner which maintains IT security objectives.
O.TIME	The IT environment must provide a reliable time source.

3.2 Assumptions

The following conditions are assumed to exist in the TOE operational environment.

Assumption	Description
A.ACCURATE_CLOCK	It is assumed that a reliable hardware clock is provided by the hardware.

4. IT Security Requirements

This section specifies the requirements for the TOE. This section includes a summary of the operations performed upon the requirements.

4.1 Extended Components Definitions

All requirements in this Security Target have been drawn from the CC so there are no extended components.

4.2 TOE Security Functional Requirements (SFRs)

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 4-1 lists all requirements found in this section.

Table 4-1 Security Functional Requirements by Class

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_SAR.3: Selectable audit review
	FAU_SEL.1: Selective audit
	FAU_STG.1: Protected audit trail storage
	FAU_STG.3: Action in case of possible audit data loss
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
	FDP_RIP.2: Full residual information protection
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Verification of secrets
	FIA_UAU.1: Timing of authentication
	FIA_UAU.6: Re-authenticating
	FIA_UAU.7: Protected authentication feedback
	FIA_UID.1: Timing of identification
	FIA_USB.1: User-subject binding
FMT: Security management	FMT_MOF.1a: Management of security functions behaviour
	FMT_MOF.1b: Management of security functions behaviour
	FMT_MSA.1a: Management of security attributes
	FMT_MSA.1b: Management of security attributes
	FMT_MSA.3: Static attribute initialisation
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_MTD.1c: Management of TSF data
	FMT_MTD.1d: Management of TSF data
	FMT_MTD.1e: Management of TSF data
	FMT_MTD.1f: Management of TSF data
	FMT_REV.1a: Revocation
	FMT_REV.1b: Revocation
	FMT_SAE.1: Time-limited authorisation

	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps
FTA: TOE access	FTA_SSL.1: TSF-initiated session locking
	FTA_SSL.2: User-initiated locking
	FTA_TAB.1: Default TOE access banners
	FTA_TAH.1: TOE access history
	FTA_TSE.1: TOE session establishment

4.2.1 Security audit (FAU)

4.2.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
- Start-up and shutdown of the audit functions;
- All auditable events for the [***minimum***] level of audit; and
- [**the events identified in the table below**].

Table 4-2 Auditable Events

Requirement	Audit events prompted by requirement
Audit Data Generation (FAU_GEN.1)	(none)
User Identity Association (FAU_GEN.2)	(none)
Audit Review (FAU_SAR.1)	• Opening the audit records.
Restricted Audit Review (FAU_SAR.2)	• Unsuccessful attempts to read information from the audit records.
Selectable Audit Review (FAU_SAR.3)	(none)
Selective Audit (FAU_SEL.1)	• All modifications to the audit configuration that occur while the audit collection functions are operating.
Protected Audit Trail Storage (FAU_STG.1)	(none)
Action in Case of Possible Audit Data Loss (FAU_STG.3)	Actions taken due to exceeding of a threshold
Complete Access Control (FDP_ACC.2)	(none)
Security Attribute Based Access Control (FDP_ACF.1)	• All requests to perform an operation on an object covered by the SFP. • The identity of the object
Full Residual Information Protection (FDP_RIP.2)	(none)

Authentication Failure Handling (FIA_AFL.1)	• The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
User Attribute Definition (FIA_ATD.1)	(none)
Verification of Secrets (FIA_SOS.1)	• Rejection or acceptance by the TSF of any tested secret.
Timing of Authentication (FIA_UAU.1)	• All use of the authentication mechanism.
Re-authenticating (FIA_UAU.6)	• All re-authentication attempts.
Protected Authentication Feedback (FIA_UAU.7)	(none)
Timing of Identification (FIA_UID.1)	• All use of the user identification mechanism, including the user identity provided, except during failures. • The origin of the attempt (e.g. terminal identification.)
User-Subject Binding (FIA_USB.1)	• Success and failure of binding of user security attributes to a subject (e.g. success and failure to create of a subject).
Management of Security Functions Behavior (for specification of auditable events) (FMT_MOF.1a	• All modifications in the behavior of the functions in the TSF.
Management of Security Functions Behavior (for authentication data) (FMT_MOF.1b	• All modifications in the behavior of the functions in the TSF.
Management of Security Attributes (FMT_MSA.1a)	• All modifications of the values of security attributes.
Management of Security Attributes (for Object Ownership) (FMT_MSA.1b)	• All modifications of the values of security attributes.
Static Attributes Initialization (FMT_MSA.3)	• Modifications of the default setting of permissive or restrictive rules. • All modifications of the initial values of security attributes.
Management of TSF Data (for general TSF data) (FMT_MTD.1a)	• All modifications of the values of TSF data.
Management of TSF Data (for audit data) (FMT_MTD.1b)	• All modifications of the values of audit data.
Management of TSF Data (for initialization of user security attributes) (FMT_MTD.1c)	• All initializations of the values of user security attributes.
Management of TSF Data (for modification of user security attributes, other than authentication data) (FMT_MTD.1d)	• All modifications of the values of user security attributes.
Management of TSF Data (for modification of authentication data) (FMT_MTD.1e)	• All actions associated with modifications of the values of authentication data.

Management of TSF Data (for reading of authentication data) (FMT_MTD.1f)	(none)
Revocation (to authorized administrators) (FMT_REV.1a)	• All attempts to revoke security attributes.
Revocation (to owners and authorized administrators) (FMT_REV.1b)	• All attempts to revoke security attributes.
Time-Limited Authorization (FMT_SAE.1)	• Specification of the expiration time for an attribute. • Action taken due to attribute expiration.
Security Roles (FMT_SMR.1)	• Modifications to the group of users that are part of a role.
Reliable Time Stamps (FPT_STM.1)	• Changes to the time.
TSF-Initiated Session Locking (FTA_SSL.1)	• Locking of an interactive session by the session locking mechanism. • Any attempts at unlocking of an interactive session.
User-Initiated Locking (FTA_SSL.2)	• Locking of an interactive session by the session locking mechanism. • Any attempts at unlocking of an interactive session.
Default TOE Access Banners (FTA_TAB.1)	(none)
TOE Access History (FTA_TAH.1)	(none)
TOE Session Establishment (FTA_TSE.1)	• All attempts at establishment of a user session.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no additional information**].

4.2.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

4.2.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**authorised administrators**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

4.2.1.4 Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

4.2.1.5 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches and sorting**] of audit data based on [**the following attributes:**

a) user identity,
b) object identity,
c) date of the event,
d) time of the event,
e) type of event,
f) success of auditable security events, and
g) failure of auditable security events]

4.2.1.6 Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

- [***object identity, user identity, host identity, event type,***]
- [**success of auditable security events, and failure of auditable security events**].

4.2.1.7 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

4.2.1.8 Action in case of possible audit data loss (FAU_STG.3)

FAU_STG.3.1 The TSF shall [**generate an alarm to the authorized administrator**] if the audit trail exceeds [**the authorized administrator specified log size**].

4.2.2 User data protection (FDP)

4.2.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the [**Discretionary Access Control policy**] on [**all subjects and all named objects**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

4.2.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Discretionary Access Control policy**] to objects based on the following: [

a) the authorized user identity and group membership(s) associated with a subject and
b) the authorized user (or group) identity/access operation pairs associated with a named object.].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) The Discretionary Access Control policy mechanism shall, either by explicit authorized user action or by default, provide that named objects are protected from unauthorized access according to the following ordered rules:

1. **If the ACL fails to allow or explicitly denies a requested access permission to the user and associated groups, the access attempt will fail and no access is granted to the user.**
2. **If the ACL allows all requested access permissions to the user and associated groups, the access attempt will succeed and the requested access is granted to the user.**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**none**].

4.2.2.3 Full residual information protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

4.2.3 Identification and authentication (FIA)

4.2.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [*32-bits*]***] unsuccessful authentication attempts occur related to [**any authorized user authentication process**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [

a) For the built-in administrator account, disable the account for an authorized administrator configurable time period[1];
b) For all other accounts, disable the user logon account until it is re-enabled by the authorized administrator; and,
c) For all disabled accounts, respond with an 'account disabled' message without attempting any type of authentication].

4.2.3.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

a) unique identifier;
b) group memberships;
c) authentication data;
d) security-relevant roles (see FMT_SMR.1);
e) privileges;
f) logon rights on specific physically separated parts of the TOE; and,
g) allowable time and day to logon].

4.2.3.3 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

a) For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 5 x 10^{15};
b) The authentication mechanism must provide the capability for an administrator to specify the conditions that need to be met before an individual user can reuse a secret;
c) For all non-administrator accounts, multiple attempts to use the authentication mechanism during a one minute period, the probability that a random attempt during that minute will succeed is less than one in 25,000,000,000,000;
d) For all administrator accounts, the authentication mechanism must provide a delay such that there can be no more than ten attempts per minute; and
e) Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics].

[1] Note that the Built-in administrator cannot be locked out, but users in the administrator group can be.

4.2.3.4 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**read access to public objects**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

4.2.3.5 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**changing authentication data and unlocking locked sessions**].

4.2.3.6 Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only [**obscured feedback**] to the user while the authentication is in progress.

4.2.3.7 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**read access to public objects**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

4.2.3.8 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [

a) the unique user identity that is associated with auditable events;
b) the user identity or identities that are used to enforce the Discretionary Access Control Policy;
c) the group identity or identities that are used to enforce the Discretionary Access Control Policy;
d) the user's authorized roles; and,
e) privileges].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**every subject will be assigned a subset of security attributes associated with the user on whose behalf the subject will act**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**subjects acting on behalf of users cannot add additional security attributes beyond those initially assigned**].

4.2.4 Security management (FMT)

4.2.4.1 Management of security functions behaviour (FMT_MOF.1a)

FMT_MOF.1a.1 The TSF shall restrict the ability to [***disable and enable***] the functions [**audit functions, including the specification of which events are to be audited**] to [**authorised administrator**].

4.2.4.2 Management of security functions behaviour (FMT_MOF.1b)

FMT_MOF.1b.1 The TSF shall restrict the ability to [***modify the behaviour of***] the functions [**user authentication**] to [**authorised administrators**].

4.2.4.3 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the [**Discretionary Access Control policy**] to restrict the ability to [***modify***] the security attributes [**object security attributes, except the object owner**] to [**authorised administrators and owners of the object**].

4.2.4.4 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The TSF shall enforce the [**Discretionary Access Control policy**] to restrict the ability to [***modify***] the security attributes [**object owner**] to [**authorised administrators**].

4.2.4.5 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Discretionary Access Control policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**authorised administrators**] to specify alternative initial values to override the default values when an object or information is created.

4.2.4.6 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [***[manage]***] the [**security-relevant TSF data except for audit records, user security attributes, and authentication data**] to [**authorised administrators**].

4.2.4.7 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to [***query, delete, and clear***] the [**audit data**] to [**authorised administrators**].

4.2.4.8 Management of TSF data (FMT_MTD.1c)

FMT_MTD.1c.1 The TSF shall restrict the ability to [***[initialise]***] the [**user security attributes**] to [**authorised administrators**].

4.2.4.9 Management of TSF data (FMT_MTD.1d)

FMT_MTD.1d.1 The TSF shall restrict the ability to [***modify***] the [**user security attributes, other than authentication data**] to [**authorised administrators**].

4.2.4.10 Management of TSF data (FMT_MTD.1e)

FMT_MTD.1e.1 The TSF shall restrict the ability to [***modify***] the [**authentication data**] to [**authorised administrators and users authorized to modify their own authentication data**].

4.2.4.11 Management of TSF data (FMT_MTD.1f)

FMT_MTD.1f.1 The TSF shall restrict the ability to [***query***] the [**authentication data**] to [**no role**].

4.2.4.12 Revocation (FMT_REV.1a)

FMT_REV.1a.1 The TSF shall restrict the ability to revoke security attributes associated with the [***users, subjects***] under the control of the TSF to [**authorised administrators**].

FMT_REV.1a.2 The TSF shall enforce the rules [**immediate revocation of security-relevant authorizations**].

4.2.4.13 Revocation (FMT_REV.1b)

FMT_REV.1b.1 The TSF shall restrict the ability to revoke security attributes associated with the [***objects***] under the control of the TSF to [**owners of the named object and authorised administrators**].

FMT_REV.1b.2 The TSF shall enforce the rules [**revocation of access rights associated with named objects when an access check is made**].

4.2.4.14 Time-limited authorisation (FMT_SAE.1)

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [**authorized user authentication data**] to [**authorised administrators**].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [**lock out the associated authorized user account**] after the expiration time for the indicated security attribute has passed.

4.2.4.15 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- Modify the time;
- Disable and enable the audit functions, including the specification of which events are to be audited;
- Modify the behavior of user authentication functions;
- Manage security-relevant TSF data;
- Query, delete and clear audit data;
- Modify security attributes associated with users, subjects and objects;
- Modify authentication data;
- Specify an expiration time for authorized user authentication data].

4.2.4.16 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [
a) authorized administrator;
b) users authorized by the Discretionary Access Control Policy to modify object security attributes; and,
c) users authorized to modify their own authentication data].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

4.2.5 Protection of the TSF (FPT)

4.2.5.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

4.2.6 TOE access (FTA)

4.2.6.1 TSF-initiated session locking (FTA_SSL.1)

FTA_SSL.1.1 The TSF shall lock an interactive session after [**an authorised administrator-specified time interval of user inactivity**] by:
- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [**re-authentication**].

4.2.6.2 User-initiated locking (FTA_SSL.2)

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:
- clearing or overwriting display devices, making the current contents unreadable;
- disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [**re-authentication**].

4.2.6.3 Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

4.2.6.4 TOE access history (FTA_TAH.1)

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [***date and time***] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [***date and time***] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

4.2.6.5 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**location, time, and day**].

4.3 TOE Security Assurance Requirements (SARs)

The SARs for the TOE are the EAL 1 components.

Table 4-3 EAL 1 Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM coverage
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

4.3.1 Development (ADV)

4.3.1.1 Basic functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

4.3.2 Guidance documents (AGD)

4.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

4.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

4.3.3 Life-cycle support (ALC)

4.3.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.1.1c The TOE shall be labelled with its unique reference.
ALC_CMC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

4.3.3.2 TOE CM coverage (ALC_CMS.1)

ALC_CMS.1.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.1.1c The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

4.3.4 Tests (ATE)

4.3.4.1 Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1d The developer shall provide the TOE for testing.
ATE_IND.1.1c The TOE shall be suitable for testing.
ATE_IND.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2e The evaluator shall test a subset of the TSF interfaces to confirm that the TSF operates as specified.

4.3.5 Vulnerability assessment (AVA)

4.3.5.1 Vulnerability survey (AVA_VAN.1)

AVA_VAN.1.1d The developer shall provide the TOE for testing.
AVA_VAN.1.1c The TOE shall be suitable for testing.
AVA_VAN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

4.4 Security Requirements for the IT Environment

The TOE has no security requirements allocated to its IT environment.

5. TOE Summary Specification (TSS)

This chapter describes the Windows Vista and Windows Server 2008 security functions and associated assurance measures. The SFs and SAMs performed by Windows Vista and Windows Server 2008 are described in the following sections, as well as a mapping to the security functional and assurance requirement satisfied by the TOE.

5.1 TOE Security Functions

This section presents the TSFs and a mapping of security functions to SFRs. The TOE performs the following security functions:

- Audit,
- User Data Protection,
- Identification and Authentication,
- Security Management, and
- TOE Access.

5.1.1 Audit Function

The TOE Audit security function performs:

- Audit Collection,
- Audit Log Review,
- Selective Audit,
- Audit Log Overflow Protection,
- Audit Log Restricted Access Protection, and
- Time Service.

5.1.1.1 Audit Collection

The Event logger service creates the security event log, which contains the security relevant audit records collected on a system. There is one security log (audit log) per machine. The Local Security Authority (LSA) server collects audit events from all other parts of the TSF and forwards them to the Event Logger for storage in the security log. For each audit event, the Event Logger stores the following data in each audit record:

Date:	The date the event occurred.
Time:	The time the event occurred.
User:	The security identifier (SID) of the user on whose behalf the event occurred that represents the user. SIDs are described in more detail in Section 5 under Identification and Authentication Function,
Event ID:	A unique number identifying the particular event class.
Source:	The system restricts what processes are capable of writing events to the security event log. Because the LSA process is the only process capable of writing audit events destined for the security event log, this value will always be “Security-Auditing.”

Types: Indicates whether the security audit event recorded is the result of a successful or failed attempt to perform the action.

Category: A classification of the event defined by the event source. For security log, the LSA service defines the following categories for security audit events: System, Logon, Object Access, Privilege Use, Detailed Process Tracking, Policy Change, Account Management, Directory Service Access, and Account Logon.

Each audit event may also contain category-specific data that is contained in the body of the event such as described below:

- For the System Category, the audit records additionally include information relating to the system such as the time of clearing the audit trail, start or shutdown of the audit function, and startup and shutdown of the TOE.
- For the Object Access and the Directory Service Access Category, the audit records additionally include the object name and the desired access requested.
- For the Privilege Use Category, the audit records additionally identify the privilege.
- For the Detailed Process Tracking Category, the audit records additionally include the process identifier.
- For the Policy Change and Account Management Category, the audit records additionally include old and new values of the policy or account attributes.
- For the Logon and Account Logon Category, the audit records additionally include the reason for failure of attempted logons.
- For the Logon Category, the audit records additionally include the logon type that indicates the source of the logon attempt by indicating one of the following types in the audit record:
    - Interactive (local logon)
    - Network (logon from the network)
    - Service (logon as a service)
    - Batch (logon as a batch job)
    - Unlock (for Unlock screen saver)

For the Network logon category, the following additional network information is included: Workstation Name, Source network IP Address, Source IP Port Number. There are two places within the TSF where security audit events are collected. The Security Reference Monitor (SRM) is responsible for the generation of all audit records for the object access, privilege use, and detailed process tracking event categories. With one exception, audit events for the remainder of the event categories are generated by various services that co-exist in the security process with the LSA server or that call the Authz Report Audit APIs provided by the LSA Policy subcomponent. The exception is that the Event Logger itself records an event record when the security log is cleared and when the security log exceeds the warning level configured by the authorized administrator.

The LSA server maintains an audit policy in its database that determines which categories of events are actually collected. Defining and modifying the audit policy is restricted to the authorized administrator. The authorized administrator can select events to be audited by selecting the category or categories to be audited. An authorized administrator can individually select each category. Those services in the security process can determine the current audit policy via direct local function calls. The only other TSF component that uses the audit policy is the SRM in order to control object access, privilege use, and detailed tracking audit.: LSA and the SRM share a private local connection port, which is used to pass the audit policy to the SRM. When an authorized administrator changes the audit policy, the LSA updates its database and notifies the SRM. The SRM receives a control flag indicating if auditing is enabled and a data structure indicating that the events in particular categories will be audited.

In addition to the system-wide audit policy configuration, it is possible to define a per-user audit policy. This allows individual audit categories (of success or failure) to be enabled or disabled on a per user basis. The per-user audit policy refines the system-wide audit policy, allowing a more precise definition of the audit policy.

Within each category, auditing can be performed based on success, failure, or both. For object access events, auditing can be further controlled based on user/group identify and access rights using System Access Control Lists (SACLs). SACLs are associated with objects and indicate whether or not auditing for a specific object, or object attribute, is enabled.

The TSF is capable of generating the audit events associated with each audit category, as described in the Description column of Table 5-1 Audit Event Categories. The auditable events associated with each category capture the events listed in Table 4-2 Auditable Events. For each category, the associated audit events (listed in Table 4-2 Auditable Events) for each of the requirements in the FAU_GEN Required Events column of Table 5-1 are captured.

Table 5-1 Audit Event Categories

Category	Description	FAU_GEN Required Events
System	Audit attempts that affect security of the entire system such as clearing the audit trail and audit alarms	FAU_STG.3; FMT_MTD.1a
Object Access	Audit attempts to access user objects, such as files.	FDP_ACF.1; FMT_MSA.1a; FMT_MSA.3; FMT_REV.1b
Privilege Use	Audits attempts to use security relevant privileges. Security relevant privileges are those privileges that are related to the TSFs and can be assigned in the evaluated configuration.	FMT_SMR.1; FPT_STM.1; FMT_MOF.1a; FMT_MTD.1a; FAU_SAR.1; FAU_SAR.2
Detailed Process Tracking	Audit subject-tracking events, including program activation, handle duplication, indirect access to an object, and process exit.	FIA_USB.1; FDP_ACF.1
Policy Change	Audit attempts to change security policy settings such as the audit policy and privilege assignment.	FMT_MTD.1a; FMT_MTD.1b; FMT_REV.1a; FMT_SMR.1; FMT_MOF.1a; FAU_GEN.1; FAU_SEL.1
Account Management	Audit attempts to create, delete, or change user or group accounts and changes to their attributes.	FMT_MTD.1a; FMT_MTD.1c; FMT_MTD.1d; FMT_MTD.1e; FMT_MTD.1f; FMT_REV.1a; FMT_SMR.1; FIA_AFL.1; FMT_SAE.1;
Directory Service Access	Audit access to directory service objects and associated properties.	FDP_ACF.1
Logon	Audit attempts to logon or logoff the system, attempts to make a network connection.	FIA_SOS.1; FIA_UAU.1; FIA_UID.1; FIA_AFL.1; FIA_USB.1; FTA_SSL.1; FTA_SSL.2; FTA_TSE.1; FIA_UAU.6
Account Logon	Audit when a DC receives a logon request.	FIA_SOS.1; FIA_UAU.1; FIA_UID.1;

5.1.1.2 Audit Log Review

The event viewer administrator tool provides a user interface to view, sort, and search the security log. The security log can be sorted and searched by user identity, object identity, event type, date, time, source, category, event ID, and computer. The security log can also be searched by free form texts occurring in the audit records.

5.1.1.3 Selective Audit

The authorized administrator is provided the ability to select events to be audited based upon object identity, user identity, workstation (host identity), event type, and success or failure of the event.

5.1.1.4 Audit Log Overflow Protection

The TSF protects against the loss of events through a combination of controls associated with audit queuing and event logging. As configured in the TOE, audit data is appended to the audit log until it is full. The TOE protects against lost audit data by allowing the authorized administrator to configure the system to generate an audit event when the security log reaches a specified capacity percentage (e.g., 90%). Additionally, the authorized administrator can configure the system not to overwrite events and to shutdown when the security log is full. When so configured, after the system has shutdown due to audit overflow, only the authorized administrator can log on. When the security log is full, a message is written to the terminal display of the authorized administrator indicating the audit log has overflowed.

As described earlier, the TSF collects audit data in two ways, via the SRM and via the LSA server. Both components maintain audit event queues. The SRM puts audit records on an internal queue to be sent to the LSA server. The LSA maintains a second queue where it holds the audit data from SRM and the other services in the security process. Both audit queues detect when an audit event loss has occurred. The SRM service maintains a high water mark and a low water mark on its audit queue to determine when full. The LSA also maintains marks in its queue to indicate when full.

Audit events may be lost if the SRM or the LSA queues reach their high-water mark, or if the security log file is full. The TOE can be configured to crash when the audit trail is full. The security log file is limited in size by the resources available on the system.

5.1.1.5 Audit Log Restricted Access Protection

The Event Logger controls and protects the security event log. To view the contents of the security log, the user must be an authorized administrator. The security event log is a system resource, created during system startup. No interfaces exist to create, destroy, or modify a security event within the security event log. The LSA subsystem is the only service registered to enter events into the security log. The TOE only offers user interfaces to read and clear the security event log and these interfaces require the user to be an authorized administrator.

5.1.1.6 Time Service

Each hardware platform supported by the TOE includes a real-time clock. The real-time clock is a device that can only be accessed using functions provided by the TSF. Specifically, the TSF provides functions that allow users, including the TSF itself, to query and set the clock, as well as functions to synchronize clocks within a domain. The ability to query the clock is unrestricted, while the ability to set the clock requires a privilege dedicated to that purpose. This privilege is only granted to authorized administrators to protect the integrity of the time service.

Each clock may be subject to some amount of error (e.g., “drift”), and management of that error is a topic in the administrator guidance. Additionally, since it may be important to have temporal correspondence across systems within a single domain, the TSF includes a domain clock synchronization function. One of the DCs is designated to provide the reference time. All clients (including other DCs) within the domain periodically contact the reference DC to adjust their local clock. The time between synchronization actions

depends on the deviation between the local and reference clock (i.e., the more deviation, the sooner the next synchronization will be scheduled).

SFR Mapping:

The Audit function satisfies the following SFRs:

- FAU_GEN.1 – The TOE audit collection is capable of generating audit events for items identified in Table 6-1, TOE audit events. For each audit event the TSF records the date, time, user Security Identifier (SID) or name, logon type (for logon audit records), event ID, source, type, and category.
- FAU_GEN.2 – All audit records include the user SID, which uniquely represents each user.
- FAU_SAR.1 – The event viewer provides authorized administrators with the ability to review audit data in a readable format.
- FAU_SAR.2 and FMT_MTD.1(a) – Only authorized administrators have any access to the audit log.
- FAU_SAR.3 – The audit function provides capabilities for selective auditing and review using the event viewer. The TOE provides the capability to select events to be audited based on the success and/or failure at the category level. Additionally, for the object access category of events, events can be selected based on user identity. The TSF determines which audit events to record based on the current audit policy and the specific settings in the SACLs. The event viewer provides the capability to perform searches and sorting of audit data by date, time, user SID or name, computer, event ID, source, type, and category. Additionally, the event viewer provides the capability to perform searching based upon specified free form text substrings within the audit records.
- FAU_SEL.1 – The TSF provides the ability for the authorized administrator to select the events to be audited based upon object identity, user identity, workstation (host identity), event type, and success or failure of the event.
- FAU_STG.1 – The interface to the security log is limited by the event logger. The interface to the security log only allows for viewing the audit data and for clearing all the audit data. The interface to the security log is restricted to authorized administrators and does not allow for the modification of audit data within the security log.
- FAU_STG.3 – The authorized administrator can configure the system such that an audit event (alarm) is generated if the audit data exceeds a specified percentage of the security log.
- FMT_MTD.1a – The TSF restricts the ability to specify the size of the security log to an authorized administrator.
- FPT_STM.1, FMT_MTD.1a – The real-time clock in each Windows platform, in conjunction with periodic domain synchronization and restricting the ability to change the clock to authorized administrators, provides a reliable source of time stamps for the TSF.

5.1.2 User Data Protection Function

The user data protection security services provided by the TOE are:

- Discretionary Access Control, and
- Residual Data Protection.

5.1.2.1 Discretionary Access Control

The TSF mediates access between subjects and user data objects, also known as named objects. Subjects consist of processes with one or more threads running on behalf of users. Table 5-2 Named Objects lists the specific user data objects under the control of the DAC policy for the TOE.

Table 5-2 Named Objects

Name	Description
Desktop	The primary object used for graphical displays. The interactive window station has three default desktops created by WinLogon.
Event	An object created for the interprocess communication mechanism.
Keyed Event	An object created for the interprocess communication mechanism.
Event Pair	An object created for the interprocess communication mechanism.
I/O Completion Port	An object that provides a means to synchronize I/O.
Job	An object that allows for the management of multiple processes as a unit.
Registry Key	Registry Keys are the objects that form the Registry.
Mutant	An object created for the interprocess communication mechanism (known as Mutex at the win32 interface).
Object Directory	A directory in the object namespace.
LPC Port	A connection-oriented local process communication mechanism object that supports client and server side communication end points, message queues, etc.
Mailslot	An I/O object that provides support for message passing IPC via the network.
Named Pipe	An I/O object used for IPC over the network.
NTFS Directory	NT file system file object.
NTFS File	A user data file object managed by NTFS.
Printer	Represents a particular print queue and its association with a print device.
Active Directory	Represents shared resources defined and maintained by Active Directory services.
Process	An execution context for threads that has associated address space and memory, token, handle table, etc.
Section	A memory region.
Semaphore	An object created for interprocess communication mechanism.
Symbolic Link	A means for providing name aliasing in the object name space.
Scheduled Task	A program that is executed at a predefined time or when a predefined event occurs
Thread	An execution context (registers, stacks, etc.) All user-mode threads are associated with a process.
Timer	A means for a thread to wait for a specified amount of time to pass.

Name	Description
Tokens	These objects represent the security context of a process or thread.
Volume	A partition or collection of partitions that have been formatted for use by a file system.
Window Station	A container for desktop objects and related attributes.
Debug	A set of resources used for debugging a process.
Filter Connection Port	Represents a mini-filter driver.
Filter Communication Port	Represents a port to communicate with a mini-filter driver.

5.1.2.1.1 Subject DAC Attributes

Tokens contain the security attributes for a subject. Tokens are associated with processes and threads running on behalf of the user. The DAC related information in the token includes: the SID for the user, SIDs representing groups for which the user is a member, privileges assigned to the user, an owner SID identifying SID to assign as owner for newly created objects, a default DACL (for newly created objects), token type (primary or impersonation), impersonation level (for impersonation tokens), an optional list of restricting SIDs, and a logon ID for the session.

As described in the I&A function, a thread can be assigned an impersonation token that would be used instead of the process' token when making access checks and generating audit data. Hence, that thread is impersonating the client that provided the impersonation token. Impersonation stops when the impersonation token is removed from the thread or when the thread terminates.

A token may also include a list of restricting SIDs which are used to limit access to objects. Restricting SIDs are contained in restricted tokens, (which is a special form of a thread impersonation token).

Access decisions are made using the impersonation token of a thread if it exists, and otherwise the thread's process primary token (which always exits).

5.1.2.1.2 Object DAC Attributes

Security Descriptors (SDs) contain all of the security attributes associated with an object. All objects in Table 6-2 have an associated SD. The security attributes from a SD used for access control are the object owner SID, the DACL present flag, and the DACL itself, if present.

DACLs contain a list of Access Control Entries (ACEs). Each ACE specifies an ACE type, a SID representing a user or group, and an access mask containing a set of access rights. Each ACE has inheritance attributes associated with it that specify if the ACE applies to the associated object only, to its children objects only, or to both its children objects and the associated object.

There are two types of ACEs that apply to access control:

1. ALLOW ACES
    a. ACCESS_ALLOWED_ACE – used to grant access to a user or group of users
    b. ACCESS_ALLOWED_OBJECT_ACE – (for DS objects) used to grant access for a user or group to a property or property set on the directory service (DS) object, or to limit the ACE_inheritance to a specified type of child object. This ACE type is only supported for directory service objects.
2. DENY ACES
    a. ACCESS_DENIED_ACE – used to deny access to a user or group of users
    b. ACCESS_DENIED_OBJECT_ACE – (for DS objects) used to deny access for a user or group to a property or property set on the directory service object or to limit the

ACE_inheritance to a specified type of child object. This ACE type is only supported for directory service objects.

An access mask contains object access rights granted (or denied) to the SID, representing a user or group, in the ACE. An access mask is also used to specify the desired access to an object when accessing the object and to identify granted access associated with an opened object. Each bit in an access mask represents a particular access right. There are four categories of access rights: standard, specific, special, and generic. Standard access rights apply to all object types. Specific access rights have different semantic meanings depending on the type of object. Special access rights are used in desired access masks to request special access or to ask for all allowable rights. Generic access rights are convenient groupings of specific and standard access rights. Each object type provides its own mapping between generic access rights and the standard and specific access rights.

For most objects, a subject requests access to the object (e.g., opens it) and receives a pointer to a handle in return. The TSF associates a granted access mask with each opened handle. For kernel-mode objects, handles are maintained in a kernel-mode handle table. There is one handle table per process; each entry in the handle table identifies an opened object and the access rights granted to that object. For user-mode TSF servers, the handle is a server-controlled context pointer associated with the connection between the subject and the server. The server uses this context handle in the same manner as with the kernel mode (i.e., to locate an opened object and its associated granted access mask). In both cases (user and kernel-mode objects), the SRM makes all access control decisions.

For some objects (in particular, DS objects), the TSF does not maintain an opened context (e.g., a handle) to the object. In these cases, access checks are performed on every reference to the object (in place of checking a handle's granted access mask). DS objects also differ from other objects in that they have additional attributes, known as properties and property sets (groups of properties). Properties reference specific portions of a DS object. Property sets reference a collection of properties. Every DS object, property set and property has an associated object type GUID (Globally Unique Identifier). The TOE allows access control for DS objects to the level of GUIDs (i.e., the entire DS object, a given property set, and or a specific property). Like all objects, DS objects still have a single security descriptor for the entire object; however the DACL for a DS object can contain ACEs the grants/denies access to any of the associated GUIDs.

5.1.2.1.3 DAC Enforcement Algorithm

The TSF enforces the DAC policy to objects based on SIDs and privileges in the requestor's token, the desired access mask requested, and the object's security descriptor.

Below is a summary of the algorithm used to determine whether a request to access a user data object is allowed. In order for access to be granted, all access rights specified in the desired access mask must be granted by one of the following steps. At the end of any step, if all of the requested access rights have been granted then access is allowed. At the end of the algorithm, if any requested access right has not been granted, then access is denied.

1. Privilege Check –
    a. Check for SeSecurity privilege – This is required if ACCESS_SYSTEM_SECURITY is in the desired access mask. If ACCESS_SYSTEM_SECURITY is requested and the requestor does not have this privilege, access is denied. Otherwise ACCESS_SYSTEM_SECURITY is granted.
    b. Check for SeTakeOwner privilege and SeRelabel privilege – If the desired mask has WRITE_OWNER access right, and either privilege is found in the requestor's token, then WRITE_OWNER access is granted.
2. Owner Rights Check –
    a. If the DACL contains one or more ACEs with the OwnerRights SID, those entries, along with all other applicable ACEs for the user, are used to determine the owner's rights.

b. Otherwise, checks all SIDs in token to determine if there is a match with the object owner. If so, the READ_CONTROL and WRITE_DAC rights are granted if requested.

3. DACL not present –
   a. All further access rights requested are granted.
4. DACL present but empty –
   a. If any additional access rights are requested, access is denied.
5. Iteratively process each ACE in the order that they appear in the DACL as described below:
   a. If the inheritance attributes of the ACE indicate the ACE is applicable only to children objects of the associated object, the ACE is skipped.
   b. If the SID in the ACE does not match any SID in the requestor's access token, the ACE is skipped.
   c. If a SID match is found, and the access mask in the ACE matches an access in the desired access mask:
      i. Access Allowed ACE Types — If the ACE is of type ACCESS_ALLOWED_OBJECT_ACE and the ACE includes a GUID representing a property set or property associate with the object, then the access is granted to the property set or specific property represented by the GUID (rather than to the entire object). Otherwise the ACE grants access to the entire object.
      ii. Access Denied ACE Types –- If the ACE is of type ACCESS_DENIED_OBJECT_ACE and the ACE includes a GUID representing a property set or property associate with the object, then the access is denied to the property set or specific property represented by the GUID. Otherwise the ACE denies access to the entire object. If an ACE specifically denies a requested access, then the entire access request fails.
6. If all accesses are granted but the requestor's token has at least one restricting SID, the complete access check is performed against the restricting SIDs. If this second access check does not grant the desired access, then the entire access request fails.

5.1.2.1.4 Default DAC Protection

The TSF provides a process ensuring a DACL is applied to all new objects. When new objects are created, the appropriate DACL is determined. The default DAC protection for DS and that for non-DS objects are slightly different.

The TOE uses the following rules to set the DACL in the SDs for new non-DS securable objects:

- The object's DACL is the DACL from the SD specified by the creating process. The TOE merges any inheritable ACEs into the DACL unless SE_DACL_PROTECTED is set in the SD control flags. The TOE then sets the SE_DACL_PRESENT SD control flag.
- If the creating process does not specify a SD, the TOE builds the object's DACL from inheritable ACEs in the parent object's DACL. The TOE then sets the SE_DACL_PRESENT SD control flag.
- If the parent object has no inheritable ACEs, the TOE uses its object manager subcomponent to provide a default DACL. The TOE then sets the SE_DACL_PRESENT and SE_DACL_DEFAULTED SD control flags.
- If the object manager does not provide a default DACL, the TOE checks the subject's access token for a default DACL. The TOE then sets the SE_DACL_PRESENT and SE_DACL_DEFAULTED SD control flags.

- The subject's access token always has a default DACL, which is set by the LSA subcomponent when the token is created.

The method used to build a DACL for a new DS object is slightly different. There are two key differences, which are as follows:

- The rules for creating a DACL distinguish between generic inheritable ACEs and object-specific inheritable ACEs in the parent object's SD. Generic inheritable ACEs can be inherited by all types of child objects. Object-specific inheritable ACEs can be inherited only by the type of child object to which they apply.
- The AD schema can provide a SD. Each object class defined in the schema has a defaultSecurityDescriptor attribute. If neither the creating process nor inheritance from the parent object provides a DACL for a new AD object, the TOE uses the DACL in the default SD specified by the schema.

The TOE uses the following rules to set the DACL in the security descriptor for new DS objects:

- The object's DACL is the DACL from the SD specified by the creating process. The TOE merges any inheritable ACEs into the DACL unless SE_DACL_PROTECTED is set in the SD control flags. The TOE then sets the SE_DACL_PRESENT SD control flag.
- If the creating process does not specify a SD, the TOE checks the parent object's DACL for inheritable object-specific ACEs that apply to the type of object being created. If the parent object has inheritable object-specific ACEs for the object type, the TOE builds the object's DACL from inheritable ACEs, including both generic and object-specific ACEs. It then sets the SE_DACL_PRESENT SD control flag.
- If the parent object has no inheritable object-specific ACEs for the type of object being created, the TOE uses the default DACL from the AD schema for that object type. It then sets the SE_DACL_PRESENT and SE_DACL_DEFAULTED SD control flags.
- If the AD schema does not specify a default DACL for the object type, the TOE checks the subject's access token for a default DACL. It then sets the SE_DACL_PRESENT and SE_DACL_DEFAULTED SD control flags.
- The subject's access token always has a default DACL, which is set by the LSA subcomponent when the token is created.

All tokens are created with an appropriate default DACL, which can be applied to the new objects as appropriate. The default DACL is restrictive in that it only allows the SYSTEM SID and the user SID that created the object to have access. The SYSTEM SID is a special SID representing TSF trusted processes.

5.1.2.2 Residual Data Protection Function

The TOE ensures that any previous information content is unavailable upon allocation to subjects and objects. The TSF ensures that resources exported to user-mode processes do not have residual information in the following ways:

- All objects are based on memory and disk storage. Memory allocated for objects is either overwritten with all zeros or overwritten with the provided data before being assigned to an object.2 Objects stored on disk are restricted to only disk space used for that object. Read/write pointers prevent reading beyond the space used by the object. Only the exact value of what is most recently written can be read and no more. For varying length objects, subsequent reads only return the exact value that was set, even though the actual allocated size of the object may be greater than this.
- Subjects have associated memory and an execution context. The TSF ensures that the memory associated with subjects is either overwritten with all zeros or overwritten with user data before

[2] For APIs that create objects, the caller may provide data to initialize the object.

allocation as described in the previous bullet for memory allocated to objects. In addition, the execution context (registers) is initialized when new threads within a process are created and restored when a thread context switch occurs.

SFR Mapping:

The User Data Protection function satisfies the following SFRs:

- FDP_ACC.2 – The SRM mediates all access to objects, including kernel-based objects and user-mode TSF server-based objects. All access to objects is predicated on the SRM validating the access request. In the case of most objects, this DAC validation is performed on initial access (e.g., "open") and subsequent use of the object is via a handle that includes a granted access mask. For some objects (in particular DS objects), every reference to the object requires a complete DAC validation to be performed.
- FDP_ACF.1 – The TSF enforces access to user objects based on SIDs and privileges associated with subjects contained in tokens (impersonation token, if one exist), and the security descriptors for objects. The rules governing the access are defined as part of the DAC algorithm described above.
- FMT.MSA.1a, FMT_MSA.1b – The ability to change the DAC policy is controlled by the ability to change an object's DACL. The following are the four methods that DACL changes are controlled:
    - Object owner - Has implicit WRITE_DAC access.
    - Explicit DACL change access – A user granted explicit WRITE_DAC access on the DACL can change the DACL.
    - Take owner access – A user granted explicit WRITE_OWNER access on the DACL can take ownership of the object and then use the owner's implicit WRITE_DAC access. The only way to have explicit WRITE_OWNER access on the DACL is to either be the creator of the object or be a member of the Administrators group.
    - Take owner privilege – A user with SeTakeOwnershipPrivilege can take ownership of the object and then use the owner's implicit WRITE_DAC access.
- FMT.MSA.3a - The TSF provides restrictive default values for security attributes used to provide access control via the process's default DACLs which only allows access to the SYSTEM and the user creating the object. The composition of a process's default DACL can only be set by the authorized administrator. Users who create objects can specify a SD with a DACL to override the default.
- FMT_REV.1b – The ability to revoke access to an object is controlled by the ability to change the DACL and is governed by the same conditions for FMT_MSA.1 above. The changed DACL is effective upon subsequent access checks against the object.
- FDP_RIP.2 - The TSF ensures that previous information contents of resources used for new objects are not discernable in the new object via zeroing or overwriting of memory and tracking read/write pointers for disk storage. Every process is allocated new memory and an execution context. Memory is zeroed or overwritten before allocation. The execution is initialized or restored when threads are created or when a context switch occurs.

5.1.3 Identification and Authentication Function

The TOE requires each user to be identified and authenticated prior to performing TSF-mediated functions on behalf of that user regardless of whether the user is logging on interactively or is accessing the system via a network connection.

5.1.3.1 Logon Type

The TOE supports six types of user logon: interactive ("Logon locally"), network ("Access this computer from Network"), batch ("Logon as a batch job"), service ("Logon as a service"), unlock ("Unlock screen saver"), and Network_ClearText ("Anonymous authentication to IIS"). The interactive logon type is for users who will be interactively using the system, such as a user being logged on at a workstation console. The network logon type is used when a user logs onto a remote network server to access resources. The batch logon type is intended for batch servers, where processes may be executing on behalf of a user without their direct intervention (e.g., COM - servers). The service logon type is used when a service process is started to provide a user context in which that service will operate. The unlock logon type is used when a user is forced to re-authenticate interactively after a specified time of inactivity. The network_clearText logon type is used when IIS is configured to not require a client requesting IIS services to re-authenticate and assigns a specified account for users to be associated with the anonymous connection. In the evaluated configuration IIS will only accept request from authenticated clients.

Each of the logon types has a corresponding user logon right that can be assigned to user and group accounts to control the logon methods available to users associated with those accounts.

5.1.3.2 Re-authentication

A user can change their password either during the initial interactive log or while logged on. To change a user's password, the user must invoke a trusted path by using the Ctrl+Alt+Del key sequence. The logon dialog displayed allows the user to select an option to change their password. If selected, a change password dialog is displayed which requires the user to enter their current password and a new password. The TSF will change the password only if the TSF can successfully authenticate the user using the current password that is entered (see section Logon Process for a description of the authentication process).

Other actions that require the user to invoke the trusted path by using the Ctrl+Alt+Del key sequence and re-authenticate themselves are: changing passwords and session unlocking (see section TOE Access Function).

5.1.3.2.1 Logon Banner

An authorized administrator can configure the interactive logon screen to display a logon banner with a title and warning. This logon banner will be displayed immediately before the interactive logon dialog (see above) and the user must select "OK" to exit the banner and access the logon dialog.

5.1.3.3 User Attribute Database

5.1.3.3.1 User and Group Accounts Definitions

Each TSF maintains databases (collectively referred to as user attribute database) that fully define user and group accounts. These definitions include:

- Account name – used to represent the account in human-readable form;
- SID – a User Identifier (UID) or group identifier used to represent the user or group account within the TOE;
- Password (only for user accounts) – used to authenticate a user account when it logs on (stored in hashed form and is encrypted when not in use using a Rivest's Cipher (RC)4 algorithm and a RC4 system generated key);
- Groups – used to associate group memberships with the account
- Privileges – used to associated TSF privileges with the account;
- Logon rights – used to control the logon methods available to the account (e.g. the "logon locally" right allows a user to interactively logon to a given system);

- Miscellaneous control information – used to keep track of additional security relevant account attributes such as allowable periods of usage, whether the account has been locked, whether the password has expired, password history, maximum number of concurrent interactive sessions and time since the password was last changed; and,
- Other non-security relevant information – used to complete the definition with other useful information such a user's real name and the purpose of the account.

The actual composition of the user attribute database depends upon the type of TSF (e.g., stand-alone, domain member, DC). Specifically, the TOE allows the establishment of domains. Domains are used to allow a collection of TSFs to share a common set of policies and accounts. This is accomplished by establishing DCs that instantiate AD services (every TSF with the AD service is a DC) that define policies and accounts to be shared by TSFs in the domain. Note that group policies (see Security Management) can also be defined in the AD that apply to selected TSFs (e.g., systems) and accounts within the domain. If a TSF type is not a domain member, it will have only its own user attribute database. If a TSF type is a domain member, but not a DC, it will also have its own user attribute database. However, the policies and accounts of its DC will logically be included in that TSF's user attribute database. If a TSF type is a DC, its user attribute database is defined within its AD and is generally shared with other TSFs in the domain.

In a domain, a user attribute database can be logically extended even further through trust relationships. Each DC can be configured to trust other domains. The result is that accounts from trusted domains can be used to access the trusting domain.

A forest is a set of one or more trees that do not form a contiguous namespace. The TSF allows a forest to enforce constraints on which users it trusts the other forest to authenticate. This allows all domains in one forest to (transitively) trust all domains in another forest via a single trust link between the two forest root domains. This cross-forest authentication enables secure access to resources when the user account is in one forest and the computer account is in another forest. A computer account is a user account where the user identity of the account is a computer identity belonging to a Windows domain.

5.1.3.3.2 Account Policies

Complimentary to the user account database is the account policy that is defined on each TSF and in each domain. The account policy is controlled by an authorized administrator and allows the definition of a password account lockout policy with respect to interactive logons.

The password policy includes:

- The number of historical password to maintain to restrict changing passwords back to a previous value;
- The maximum password age before the user is forced to change their password;
- The minimum password age before the user is allowed to changed their password; and,
- The minimum password length when changing to a new password (0-14).

The account lockout policy includes:

- Duration of the account lockout once it occurs;
- Number of failed logon attempts before the account will be locked out; and,
- The amount of time after which the failed logon count will be reset.

These policies allow the TSF to make appropriate decisions and change user attributes in the absence of an authorized administrator. For example, the TSF will "expire" a password automatically when the maximum password age has been reached. Similarly, it will lock an account once a predefined number of failed logon attempts have occurred and will subsequently only unlock the account as the policy dictates. These policies also serve to restrict features available to authorized users (e.g., frequency of password change, size of password, reuse of passwords).

5.1.3.4 Logon Process

All logons are treated essentially in the same manner regardless of their source (e.g., interactive logon dialog, network interface, internally initiated service logon). They begin with an account name, domain name (which may be NULL; indicating the local system), and password that must be provided to the TSF.

The domain name indicates where the account is defined. If the local TSF (or NULL) is selected for the domain name, the local user account database is used. Otherwise the user account database on the target TSF's DC will be used. If the domain name provided does not match that of the DC, the DC will attempt to determine whether the target domain is a trusted domain. If it is, the trusted domain's user account database will be used. Otherwise, the logon attempt will fail.

At this point, two types of logon may occur: NTLM or Kerberos. Kerberos is the default logon method and will be used if a Kerberos KDC is available. Generally, each DC includes a KDC in addition to its AD. If no KDC is available, NTLM will be used. In the evaluated configuration a KDC is available to each DC.

There are two primary differences between NTLM and Kerberos logons. The first is that NTLM requires that the username and a hashed version of the password be sent to the appropriate DC (or local TSF for a local account). The receiving TSF will compare the provided hashed password with the version stored in its database for the user identified by the username. If the hashed passwords match, authentication is successful. Kerberos, on the other hand, requires that a time-stamped logon request be partially encrypted with the hashed password. The encrypted request is sent to the appropriate DC, which in turn looks up the user's hashed password in its database. The hashed password is used to decrypt the logon request. If the decrypt operation succeeds and the logon request has an appropriate time stamp (i.e., within a time period set by an authorized administrator), authentication is successful. In either case, a successful authentication yields the user's SID and the SIDs of the user's groups as defined on the authenticating DC (or local TSF for a local account). Note that a failed authentication attempt yields an increment in failed logon attempts for the user account and may result in the account being locked out (i.e., unable to logon).

The second primary difference between NTLM and Kerberos logon is in how subsequent requests for service (i.e., network logons) will occur. In the case of NTLM, the user must logon to every TSF in order to obtain a service (e.g., access to a file). These will be network logons and will essentially follow the same process as the initial interactive logon. A Kerberos logon yields a Ticket Granting Ticket that is used to subsequently request Service Tickets from the KDC each time the user process wants to access a network service. The Service Ticket, containing some of the user's security attributes, will serve to authenticate the user rather than effectively requiring re-authentication using a hashed password.

Once a successful authentication occurs, the TSF will query its AD (via its DC), if applicable, for group policies relevant to the user that is attempting to logon. The TSF will use its user attributes database (including domain properties, such as from a group policy) to derive additional security attributes for the user (e.g., privileges and user rights). The TSF will then ensure that any logon constraints defined in its user attributes database (including domain properties applicable to the user) to the user are enforced prior to completing a successful logon. If there are no constraints that would prevent a successful logon, a process (or thread, when the logon server is going to impersonate the user) is created and assigned a token that defines a security context based on the attributes collected during the logon process (user and group SIDs, privileges, logon rights, as well as a default DACL created by the logon process).

The next time that service is used, the Credential Manager automatically supplies the stored credential. If it is not accepted, the user is prompted for the correct access information. If access is granted, the Credential Manager overwrites the previous credential with the new one.

5.1.3.4.1 Network Logon Support

PK-certificate network logon is supported by the TLS/SSL Security Provider that implements the Microsoft Unified Security Protocol Provider security package. This package provides support for four network security protocols, namely SSL versions 2.0 and 3.0, TLS version 1.0. In the TOE, security package APIs are not directly accessible, rather they are accessed via LSA Authentication APIs. The TLS/SSL Security Provider authenticates connections, and/or encrypts messages between clients and servers. When an

application needs to use a network resource on an authenticated channel, the LSA accesses the TLS/SSL Security Service Provider (SSP) via the SSP interfaces.

Digest network logon is supported by the Microsoft Digest Access Authentication Package. Digest performs user authentication for LSA Authentication in support of network logon attempts. Interactive logons cannot be performed using Digest Access. Digest implements a network security protocol, in this case digest challenge/response authentication, that supports remote network logon user authentication and other network security services according to RFC 2617 "HTTP Authentication: Basic and Digest Access Authentication."

5.1.3.5 Impersonation

In some cases, specifically for server processes, it is necessary to impersonate another user in order to ensure that access control and accountability are performed in an appropriate context. To support this, the TSF includes the ability for a server to impersonate a client. As described above, each process has a token that primarily includes account SIDs, privileges, logon rights, and a default DACL. Normally, each thread within a process uses the process' token for its security context. However, a thread can be assigned an impersonation token that would be used instead of the processes token when making access checks and generating audit data. Hence, that thread is impersonating the client that provided the impersonation token. Impersonation stops when the impersonation token is removed from the thread or when the thread terminates.

When communicating with a server, the client can select an impersonation level that constrains whether and how a server may impersonate the client. The client can select one of four available impersonation levels: anonymous, identify, impersonate, and delegate. Anonymous allows the server to impersonate the client, but the impersonation token doesn't contain any client information. Identify allows the server to impersonate the client to perform access checks. Impersonate allows the server to impersonate the clients entire security context to access resources local to the server's TSF. Delegate allows the server to impersonate the client on local and remote TSFs.

5.1.3.6 Restricted Tokens

Whenever a process is created, or a thread is assigned an impersonation token, the TSF allows the caller to restrict the token that will be used in the new process or impersonation thread. Specifically, the caller can remove privileges from the token, assign a deny-only attribute to SIDs, and specify a list of restricting SIDs. The following pertains:

- Removed privileges are simply not present in the resulting token.
- SIDs with the deny-only attribute are used only to identify access denied settings when checking for access, but ignore any access allowed settings.
- When a list of restricting SIDs is assigned to a token, access is checked twice once using the tokens enabled SIDs and again using the restricting SIDs. Access is granted only if both checks allow the desired access.

5.1.3.7 Strength of Authentication

As indicated above, the TSF provides a set of functions that allow the account policy to be managed. These functions include the ability to define account policy parameters, including minimum password length. The minimum password length can be configured to require as large as 14 characters. However, the administrator guide recommends that the minimum password length be configured to no less than eight (8) characters (with 5490 available characters, the password space is 6,634,204,312,890,620 available combinations). Therefore, in the evaluated configuration, the probability that a random attempt will succeed is less than one (1) in $5x10^{15}$ and the probability that, for multiple attempts within one minute, the probability that a random attempt will succeed is less than one (1) in $25x10^{12}$.

During authentication, the TSF will not provide feedback that will reduce the probability before the metrics identified above. Furthermore, the TSF forces a delay between attempts, such that there can be no more than ten (10) attempts per minute.

For each subsequent failed logon following five (5) consecutive failed logon occurrences in the last 60 seconds, the Winlogon/Graphical Identification and Authentication (GINA) subcomponent sleeps for 30 seconds before showing a new logon dialog. It therefore supports the I&A function that no more than ten (10) interactive logon attempts are possible in any 60 second (one minute) period.

When Kerberos is used, the password requirements are the same as those described above. However, there are both Ticket Granting Tickets and Service Tickets that are used to store, protect, and represent user credentials and are effectively used in identifying and authenticating the user. Session keys are initially exchanged using a hash of the user's password for a key.

SFR Mapping:

The **Identification and Authentication function** satisfies the following SFRs:

- FIA_AFL.1 – The TSF locks the account after the administrator-defined threshold of unsuccessful logon attempts has occurred. The account will remain locked either until an authorized administrator unlocks it or until the duration defined by an authorized administrator has elapsed.
- FIA_ATD.1 – Each TSF has a user attribute database. Each user attribute database describes accounts, including identity, group memberships, password (e.g., authentication data), privileges, logon rights, allowable time periods of usage, as well as other security-relevant control information. Security-relevant roles are associated with users via group memberships and privileges.
- FIA_SOS.1 – The password and key spaces used by the TSF reduce the chance of guessing a password to less than one (1) in 2 x 1015 for a single random attempt and one (1) in 25x1012 for multiple attempts during a one minute period. The TSF can block a user from continuing to attempt to logon for a specified amount of time after a specified number of failed attempts such that there can be no more than ten attempts per minute and the TSF does not provide feedback during authentication that will reduce the probability of successfully guessing passwords.
- FIA_UAU.1 – An authorized administrator can configure the TSF to allow no TSF-mediated functions prior to authentication.
- FIA_UAU.6 – The TSF will only allow a password to be changed if the TSF can successfully authenticate the user using the current password which must be entered with the new password.
- FIA_UAU.7 – During an interactive logon, the TSF echoes the users password with "*" characters to prevent disclosure of the user's password.
- FIA_UID.1 – An authorized administrator can configure the TSF to allow no TSF-mediated functions prior to identification.
- FIA_USB.1 – Each process and thread has an associated token that identifies the responsible user (used for audit and access), associated groups (used for access), privileges, and logon rights held by that process or thread on behalf of the user.
- FTA_TAB.1, FMT_MTD.1a – An authorized administrator can define and modify a banner that will be displayed prior to allowing a user to logon.
- FTA_TSE.1 – Domain accounts can be restricted to a workstation during a specific time and day. If the account has these restrictions, the members of the domain will then restrict the ability to logon to a system based upon the Logon Locally right (allows the user to interactively logon to given system), the time, and the day. If on a given system, the user can logon at a given time and day, then the user will be allowed to logon.
- FMT_SAE.1 – The TSF will not allow a user to logon if the user's password has expired. The TSF will restrict the location a user can logon from based upon the logon rights associated with a user's

account (logon locally, logon as a batch job, access this computer from the network, and logon as a service). Additionally, the TSF restricts a user from logon based upon time or day in that a user will not be able to logon if attempts are made after an account has been locked out but within the account lockout duration defined by the authorized administrator.

- FMT_SMR.1 – In order to assume the authorized administrator role (see the Security management Function), a user with one of the security-relevant administrative groups or security-relevant privileges must successfully logon. Furthermore, to switch between roles, a user must logoff and re-logon to an account defined for the desired role.

5.1.4 Security Management Function

The TOE supports the definition of roles as well as providing a number of functions to manage the various security policies and features provided by the TOE.

5.1.4.1 Roles

The notion of role within the TOE is generally realized by assigning group accounts and privileges to a given user account. Whenever that user account is used to logon, the user will be assuming the role that corresponds with the combination of groups and privileges that it holds. While additional roles could be defined, this ST defines three logical roles: the *authorized administrator role*, the *users authorized by DAC policy to modify object security attributes* role, and the *users authorized to modify their own authentication data* role.

The Authorized Administrator role is defined as any user account that is assigned one of the security-relevant privileges (e.g., Take Owner privilege) or is made a member of one of the several pre-defined administrative groups (e.g., Administrators and Backup Operators local group). The Administrator Guide fully identifies all security-related privileges and administrative groups, and provides advice on how and when to assign them to user accounts. A user assumes the authorized administrator role by logging on using a user account assigned one of these privileges or group membership.

Any user that can successfully logon and is not in the authorized administrator role (as defined above) is considered to be an authorized user. All authorized users are members of the *users authorized to modify their own authentication data* role.

Membership in the *users authorized by DAC policy to modify object security attributes* is defined by the superset of authorized administrators and authorized users who have created the object for which they are attempting to modify the security attributes..

5.1.4.2 Security Management Functions

The TOE supports a number of policies and features that require appropriate management. With few exceptions, the security management functions are restricted to an authorized administrator. This constraint is generally accomplished by privilege or access control (e.g., SD), and occasionally by a specific SID requirement (e.g., “Administrators”). The TOE supports security management functions for the following security policies and features:

- **Audit Policy** – The audit policy management functions allow an authorized administrator the ability to enable and disable auditing, to configure which categories of events will be audited for success and/or failure, and to manage (e.g., clear) and access the security event log. An authorized administrator can also define specifically which user and access mode combinations will be audited for specific objects in the TOE.
- **Account Policy** – The account policy management functions allow only an authorized administrator to define constraints for passwords (password complexity requirements), account lockout (due to failed logon attempts) parameters, and Kerberos key usage parameters. The constraints for passwords restrict changes by including minimum password length, password history, and the minimum and maximum allowable password age. If the maximum password age is exceeded, the corresponding user cannot logon until the password is changed. The account

lockout parameters include the number of failed logon attempts (in a selected interval) before locking the account and duration of the lockout. The Kerberos key usage parameters primarily specify how long various keys remain valid. While an authorized administrator can change passwords and a user can change their own passwords, the TSF does not allow any user (including the authorized administrator) to read passwords. Additionally, the authorized administrator can defined the advisory warning message displayed before access to the TOE is granted.

- **Account Database Policy** – The account database management functions allow an authorized administrator to define and assign and remove security attributes to and from both user and group accounts, both locally and for a domain, if applicable. The set of attributes includes account names, SIDs, passwords, group memberships, and other security-relevant and non-security relevant information. Of the set of user information, only the password can be modified by a user that is not an authorized administrator. Specifically, an authorized administrator assigns an initial password when an account is created and may also change the password like any other account attribute. However, a user may change their password. This is enforced by requiring the user to enter their old password in order to change the password to a new value.
- **User Rights Policy** – The user rights management functions allow an authorized administrator to assign or remove user and group accounts to and from specific logon rights and privileges.
- **Domain Policy** – The domain management functions allow an authorized administrator to add and remove machines to and from a domain as well as to establish trust relationships among domains. Changes to domains and domain relationships effectively change the definition and scope of other security databases and policies (e.g., the account database). For example, accounts in a domain are generally recognized by all members of the domain. Similarly, accounts in a trusted domain are recognized in the trusting domain.
- **Group Policy** – The group policy management functions allow an authorized administrator to define accounts, user right assignments, and TOE machine/computer security settings, etc. for a group of TSFs or accounts within a domain. The group policies effectively modify the policies (e.g., machine security settings, and user rights policy) defined for the corresponding TSFs or users. Administrators also have the ability to calculate the result of apply two policies and determining its effects before applying a policy.
- **DAC Policy** – The DAC functions allow authorized users to modify access control attributes associated with a named object.
- **Other** – The TSF also allows the authorized administrator the ability to modify the time.

5.1.4.3 Valid Password Attributes

The TSF ensures that only valid values are accepted as security attributes for the password. Valid values are values that are meet the password complexity restrictions as defined by the administrator. For example, the minimum password length should be set to greater than or equal to 8 by the administrator. Subsequently, attempts to create passwords shorter than 8 will not be accepted by the TSF.

SFR Mapping;

The **Security Management function** satisfies the following SFRs:

- FMT_MOF.1a – Only an authorized administrator can enable and disable the audit mechanism, select which audit event categories will be audited, and also select whether they will be audited for success and/or failure.
- FMT_MOF.1b – The TSF allows only the authorized administrator to change the password complexity requirements. Only an authorized administrator can change the minimum password length.
- FMT_MTD.1a – The TSF allows only the authorized administrator to calculate the effect of multiple group policies on the TOE. Only an authorized administrator can change the duration of

lockouts. Only an authorized administrator can specify and modify the maximum amount of failed logon attempts that may occur before the account is locked out.

- FMT_MTD.1b – Only an authorized administrator can clear the security event log. There are no interfaces to create or delete the security event log entries (see Audit Log Restricted Access Protection). Only an authorized administrator can view the security event log. There are no interfaces to modify a security event (audit record) in the security event log (see Audit Log Restricted Access Protection).
- FMT_MTD.1c – Only an authorized administrator can define user accounts and group accounts, define user/group associations (e.g., group memberships), assign privileges and user rights to accounts, as well as define other security-relevant and non-security relevant user attributes. An authorized administrator can initially assign a password to a user account.
- FMT_MTD.1d – Only an authorized administrator can modify user accounts and group accounts, change user/group associations (e.g., group memberships), change privileges and user rights to accounts, as well as modify other security-relevant and non-security relevant user attributes.
- FMT_MTD.1e – Both an authorized administrator and the user corresponding to the password can change the password assigned to an account.
- FMT_MTD.1f – The TSF does not store passwords in clear text and does not provide any interfaces to read passwords.
- FMT_REV.1a – Only an authorized administrator can remove security attributes from users and group accounts. A procedure is described in the Administrator Guide that will instruct an authorized administrator on how to immediately remove security attributes from accounts.
- FMT_REV.1b – An authorized administrator or object owner can revoke security attributes from named objects.
- FMT_SAE.1 – Only an authorized administrator can set account policy parameters, including the maximum allowable password age before the account will be unable to logon.
- FMT_SMF.1 – The TSF provides the capability to modify the time, and define the following policies: Audit Policy, Account Policy, Account Database Policy, User Rights Policy, Domain Policy, Group Policy, and DAC Policy. Specifically, the TSF provides the capability to perform the following:
    - DAC Policy
        - modify access control attributes associated with a named object
    - Audit Policy
        - enable, disable, modify the behavior of the audit function and clear the audit trail
        - modify the set of events to be audited
        - read the audited events
        - modify the audit log size
    - Account Policy
        - modify the behavior of the locked user session function
        - modify the duration the user account is disabled after the unsuccessful authentication attempts threshold is exceeded
        - modify the minimum allowable password length
        - modify the advisory warning message displayed before establishment of a user session

        - modify the password complexity restriction
        - modify the unsuccessful authentication attempts threshold
    - Account Database Policy
        - initialize and modify user security attributes

- FMT_SMR.1 – The TOE supports the definition of an authorized administrator through the association of specific privileges and group memberships with user accounts. As described in the User Data Protection section, users are generally allowed to control the security attributes of objects depending upon the access that they have to those objects. Users can also modify their own authentication data (e.g., passwords) by providing their old password for authorization. Additionally, upon the creation of an object, the user creating the object (object creator) can define initial values for its security attributes that override the default values (e.g. DACL).

5.1.5 TOE Access Function

5.1.5.1 Session Locking

The TSF provides the ability for a user to lock their interactive logon session immediately or after a user-defined time interval. Additionally, the TSF provides the ability for the administrator to specify a defined interval of inactivity after which the session will be locked. Once a user is logged on, they can invoke the session locking function by using the same key sequence used to invoke a trusted path (**Ctrl+Alt+Del**). This key sequence is captured by the TSF and cannot be intercepted or altered by any user process. The result of that key sequence is a menu of functions, one of which is to lock the workstation. The user-defined interval of inactivity will only be applicable if it is more restrictive (e.g. less time) than the administrator defined interval of inactivity.

Alternately, a user can invoke a function to set screen saver properties for their interactive logon session. The user can select a program to use as a screen saver, the amount of inactivity before the screen saver will start, and whether a password will be required to resume the user's session (effectively making the screen saver a session lock). The TSF constantly monitors the mouse and keyboard for activity and if they are inactive for the user-specified time period, the TSF will lock the workstation (assuming the user configured it to lock the session) and execute the screen saver program (assuming the user selected a screen saver program). This scenario also assumes that the user specified period of inactivity is more restrictive than the administrator defined inactivity time interval. Note that if the workstation was not locked manually, the TSF will start the screen saver program if and when the inactivity period is exceeded.

When the workstation is locked manually, or when there is mouse or keyboard activity after the screen saver program has started (assuming a password is required, otherwise the session immediately resumes), the TSF will display the user's default background and a dialog indicating that the user must use the **Ctrl+Alt+Del** sequence to re-authenticate.

Regardless of how the workstation was locked, the user must use the **Ctrl+Alt+Del** function that will result in an authentication dialog. The user must then re-enter their password, which has been cached by the local system from the initial logon, after which the user's display will be restored and the session will resume. Alternately, an authorized administrator can enter their administrator identity and password in the authentication dialog. If the TSF can successfully authenticate the administrator, the user will be logged off, rather than returning to the user's session, leaving the workstation ready to authenticate a new user.

After a successful interactive logon through a domain controller, the user is shown via a dialog message on the Winlogon secure desktop the following information:

- the edata and time of the last successful interactive logon;
- the date and time of the last unsuccessful interactive logon; and
- the number of unsuccessful interactive logon attempts since the last successful logon

SFR Mapping:

The **TOE Access function** satisfies the following SFRs:

- FTA_SSL.1 –The TOE- allows users and the authorized administrator to define an inactivity interval, after which their session will be locked. The locked display has only the user's default background, instructions to unlock, and optionally the output from a user-selected screen saver program. The user must re-enter their password to unlock the workstation.
- FTA_SSL.2 - The TOE also allows a user to directly invoke the session lock as described above.
- FTA_TAH.1 – The TOE provides information to the user about successful and unsuccessful logon attempts immediately following a successful interactive logon. The user must acknowledge the information by pressing the "Ok" button of the dialog box that is displayed by the TOE..

APPENDIX A—List of Acronyms

3DES	Triple DES
ACE	Access Control Entry
ACL	Access Control List
ACM	Access Control Management
ACP	Access Control Policy
AD	Active Directory
AES	Advanced Encryption Standard
AGD	Administrator Guidance Document
AH	Authentication Header
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certificate Authority
CALG	Confidentiality Algorithm
CBC	Cipher Block Chaining
CC	Common Criteria
CCSE	Canadian Communication Security Establishment
CD-ROM	Compact Disk Read Only Memory
CI	Configuration Item
CIFS	Common Internet File System
CM	Configuration Management; Control Management
COM	Component Object Model
CP	Content Provider
CPU	Central Processing Unit
CRL	Certificate Revocation List
CryptoAPI	Cryptographic API
CSP	Cryptographic Service Provider
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DPAPI	Data Protection API
DC	Domain Controller
DEP	Data Execution Prevention
DES	Data Encryption Standard
DFS	Distributed File System
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DFS	Distributed File System
DNS	Domain Name System
DoS	Denial of Service
DO	Delivery Operation
DS	Directory Service
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EFS	Encrypting File System
ESP	Encapsulating Security Protocol
EWF	Enhanced Write Filter

FEK	File Encryption Key
FIPS	Federal Information Processing Standard
FRS	File Replication Service
FSMO	Flexible Single Master Operation
GB	Gigabyte
GC	Global Catalog
GHz	Gibahertz
GINA	Graphical Identification and Authentication
GPC	Group Policy Container
GPO	Group Policy Object
GPT	GUID Partition Table; Group Policy Template
GUI	Graphical User Interface
GUID	Globally Unique Identifiers
HMAC	Hash-Based Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	Secure HTTP
I/O	Input/Output
I&A	Identification and Authentication
IA	Information Assurance
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
ICS	Internet Connection Sharing
ID	Identification
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IFS	Installable File System
IIS	Internet Information Services
IIS6	IIS Version 6.0
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IPC	Inter-process Communication
IPSec	IP Security
ISAKMP	Internet Standard Association Key Management Protocol
ISAPI	Internet Server API
ISATAP	Intra-site Automatic Tunnel Addressing Protocol
ISO	International Organization for Standardization
IT	Information Technology
KDC	Key Distributed Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPC	Local Procedure Call
LSA	Local Security Authority
LSASS	LSA Subsystem Service
MAC	Message Authentication Code
MB	Megabyte
MBR	Master Boot Record

MMC	Microsoft Management Console
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
NSA	National Security Agency
NTLM	New Technology LAN Manager
OLE	Object Linking and Embedding
OS	Operating System
PAE	Physical Address Extension
PDC	Primary DC
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RC4	Rivest's Cipher 4
RID	Relative Identifier
RNG	Random Number Generator
RPC	Remote Procedure Call
RSA	Rivest, Shamir and Adleman
RSASSA	RSA Signature Scheme with Appendix
SA	Security Association
SACL	System Access Control List
SAM	Security Assurance Measure
SAR	Security Assurance Requirement
SAS	Secure Attention Sequence
SD	Security Descriptor
SHA	Secure Hash Algorithm
SID	Security Identifier
SF	Security Functions
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SOF	Strength of Function
SP	Service Pack
SPI	Security Parameters Index
SRM	Security Reference Monitor
SSL	Secure Sockets Layer
ST	Security Target
SYSVOL	System Volume
TCP	Transmission Control Protocol
TDI	Transport Driver Interface
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSS	TOE Summary Specification
UI	User Interface
UID	User Identifier
UNC	Universal Naming Convention
U.S.	United States

URL	Uniform Resource Locator
USB	Universal Serial Bus
USN	Update Sequence Number
v5	Version 5
VDS	Virtual Disk Service
VPN	Virtual Private Network
VSS	Volume Shadow Copy Service
WAN	Wide Area Network
WMD	Windows Driver Model
WMI	Windows Management Instrumentation
WSC	Windows Security Center
WWW	World-Wide Web
X86	Intel Microprocessors

Appendix B – Guidance Addendum

Windows Vista/Windows Server 2008
EAL 1 Evaluation
Guidance Addendum

6/27/2008

Administrator Account:
The default configuration for the built in administrator accounts in Windows Server 2008 and Windows Vista is different. The Windows Server 2008 administrator account is enabled and fully configured by default. The user must provide a valid password in order to successfully authenticate as the Server 2008 administrator. Administration of the Windows Server 2008 operating system is performed by the administrator (or member of the administrators group) and is a required account in order to setup/configure the Windows 2008 server.

The Window Vista administrator account is setup differently. By default, the Vista administrator account is disabled and comes shipped with a blank password. Windows Vista is a client operating system that has less critical administration requirements (changes to the operating system affects only the local user(s)). The local administrator account may be configured via Local Users and Groups within Computer Management (found with Control Panel – Administrative Tools).

Windows Vista introduces the concept of User Account Control (UAC) where all normal users are logged into Vista as non-administrators. One of the chief problems concerning Windows security was the fact that users logged into prior versions of Windows almost exclusively as administrators (either the default administrator or as a member of the administrator group). Once logged in as an administrator the user had unlimited access to all aspects of the operating system. If the user's account was compromised or some malware gained control within the user's session there was nothing preventing the unwanted software from gaining access to all aspects of the operating system. The limitation imposed by Vista's UAC helps protect the operating system from unwanted access in the event the user's account/session is compromised.

Windows Vista Default Local Groups:
The following default local groups are available in Windows Vista within Local Users and Groups in Computer Management:

Group Name	Description
Administrators	Administrators have complete and unrestricted access to the computer.
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files. They cannot change security settings.
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on the local machine.
Event Log Readers	Members of this group can read event logs from the local machine.

Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted. Members of this group are given a temporary profile, which is created at log on and destroyed at log off. The Guest account is disabled by default.
IIS_IUSRS	Built-in group used by Internet Information Services (IIS).
Network Configuration Operators	Member in this group can have some administrative privileges to manage configuration of networking features.
Performance Log Users	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to the local computer.
Performance Monitor Users	Members of this group can access performance counter data locally and remotely.
Power Users	Power Users are included for backwards compatibility and by default, have no more rights than standard users.
Remote Desktop Users	Members in this group are granted the right to logon remotely.
Replicator	Supports file replication in a domain.
Users	Users are prevented from making accidental or intentional system-wide changes and can run most applications.

Windows Vista introduces increased levels of access granularity in order to grant the specific rights to a user without having to grant administrator rights. This allows the correct amount of functionality without allowing unnecessary system-wide (administrator) access and the increased liability involved with the administrator level of access.

Online Resources
The online references within the help files have not been evaluated, and therefore should not be relied on for the evaluated configuration.

Scope of Evaluation
Microsoft provides software applications, packaged with the operating systems, which are considered outside the scope of the evaluated configuration. Services outside this evaluation include: Internet Information Services, Windows Firewall, Certificate Services, Terminal Services, Microsoft Message Queuing, Rights Management Services, and Windows SharePoint Services. These features are simply applications that run on the operating system and they may be installed. However, the administrator is required to ensure that they are run in a secure manner.

Password Recommendations
In order to meet the password complexity restrictions specified in the CC evaluation, the following parameters must be set using the Account Policies and Local Policies menus:

- The minimum password length must be set to 8 characters
- The failed logon attempts lockout value must be set to 5. Note the built-in Administrator will have a delay but will not actually be locked out.
- User accounts remain locked out until an administrator unlocks them.

Implementing an Authorized Usage Warning
For the Windows Vista/Server 2008 Evaluated Configuration, it is required that the system display a warning message to users before allowing them to log on. It may be necessary to get help with the wording of the message from the company's legal department. The message should inform users that the system is for authorized use only, and that they could be prosecuted if they misuse the system. To set the message, use the Local Security Policy or Domain Security Policy (on Server) menu.

Logon History
Windows Vista/Server 2008 provides information to the user about successful and unsuccessful logon attempts immediately following a successful interactive logon. The user must acknowledge the information by pressing the "Ok" button of the dialog box that is displayed.

Best Practices for Auditing
To minimize the risk of several specific security threats, administrators can take various auditing steps. Authorized administrators should select the events to be audited considering the set of threats specific to the environment. The following table provides an example of various events that could be audited, as well as the specific security threat that the audit event monitors.

Audit Event	Potential Threat
Failure audit for logon/logoff	Random password hack
Success audit for logon/logoff	Stolen password break-in
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	Misuse of privileges
Success and failure audit for file-access and object-access events. File Manager success and failure audit of Read/Write access by suspect users or groups for the sensitive files.	Improper access to sensitive files
Success and failure audit for file-access printers and object-access events. Print Manager success and failure audit of print access by suspect users or groups for the printers.	Improper access to printers
Success and failure write access auditing for program files (Execute (EXE) and Dynamic Link Library (DLL) extensions). Success and failure auditing for process tracking. Run suspect programs; examine security log for unexpected attempts to modify program files or create unexpected processes. Run only when actively monitoring the system log.	Virus outbreak

Evaluation Environment Assumptions
The following conditions were assumed to be present during the EAL1 evaluation:

- Administrators follow all provided guidance for installation and management.
- The product is protected from physical attack.
- All users of the product protect all access credentials, such as passwords or other authentication information.
- The hardware provides a reliable hardware clock.