****

**Microsoft Windows**

**Common Criteria Evaluation**

**Microsoft Windows 7**

**Microsoft Windows Server 2008 R2**

|  |  |
| --- | --- |
| Document Information |  |
| Version Number | 0.5 Revision A |
| Updated On | Friday, ~~January 7, 2011~~ February 24, 2012 |
|  |  |

*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.*

*Complying with all applicable copyright laws is the responsibility of the user.* This work is licensed under the Creative Commons Attribution-NoDerivs-NonCommercial License (which allows redistribution of the work). To view a copy of this license, visit<http://creativecommons.org/licenses/by-nd-nc/1.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

*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.*

*© 2011 Microsoft Corporation. All rights reserved.*

*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 Overview 5](#_Toc269719065)

[1.1 Who Should Read This Guide 5](#_Toc269719066)

[1.1.1 Skills and Readiness 6](#_Toc269719067)

[1.2 Section Summaries 6](#_Toc269719068)

[1.2.1 Overview 7](#_Toc269719069)

[1.2.2 Section 1: Introduction 7](#_Toc269719070)

[1.2.3 Section 2: Specifications and References for a CC-evaluated System 7](#_Toc269719071)

[1.2.4 Section 3: Security Policy Assumptions and Conditions 7](#_Toc269719072)

[1.2.5 Section 4: Configuring Elevated Security Functionality 7](#_Toc269719073)

[1.3 Style Conventions 7](#_Toc269719074)

[1.4 More Information 8](#_Toc269719075)

[1.5 Support and Feedback 8](#_Toc269719076)

[2 Introduction 9](#_Toc269719077)

[2.1 What is Common Criteria? 9](#_Toc269719078)

[2.2 What is a CC compliant System? 10](#_Toc269719079)

[2.3 What This Guide Describes 10](#_Toc269719080)

[2.4 Configuration Roadmap 10](#_Toc269719081)

[3 Specification and References for a CC-evaluated System 11](#_Toc269719082)

[3.1 About the Evaluated Version of Windows 7 and Server 2008 R2 12](#_Toc269719083)

[3.1.1 Detailed Hardware Requirements 12](#_Toc269719084)

[3.1.1.1 Memory 12](#_Toc269719085)

[3.1.1.2 Processors 13](#_Toc269719086)

[3.1.2 Networking 13](#_Toc269719087)

[3.1.2.1 Storage 13](#_Toc269719088)

[3.1.2.2 Peripheral Hardware Components 14](#_Toc269719089)

[3.2 Evaluated Security Functionality 14](#_Toc269719090)

[3.2.1 Security Features 15](#_Toc269719091)

[4 Security Policy Assumptions and Conditions 25](#_Toc269719092)

[4.1 Security Policy Assumptions 25](#_Toc269719093)

[4.1.1 Assumptions on the System Environment 25](#_Toc269719094)

[4.2 Installation and Configuration Constraints 25](#_Toc269719095)

[4.2.1 Installing the TOE (Windows 7) 25](#_Toc269719096)

[4.2.2 Installing the TOE (Server 2008 R2) 25](#_Toc269719097)

[4.2.3 Verifying the TOE version 26](#_Toc269719098)

[4.3 Modes of Operation 26](#_Toc269719099)

[5 Configuring Elevated Security Functionality 27](#_Toc269719100)

[5.1 Hardening Windows 7 27](#_Toc269719101)

[5.2 Hardening Windows Server 2008 R2 28](#_Toc269719102)

[5.3 Additional Configuration 28](#_Toc269719103)

[5.4 Ongoing Maintenance 29](#_Toc269719104)

[6 Evaluated Windows Tools 29](#_Toc269719105)

[7 Administration Scenarios 40](#_Toc269719106)

[8 Evaluated Configuration and Windows Administration Settings 41](#_Toc269719107)

[9 Appendix: User Privileges and Assignments 44](#_Toc269719108)

# Overview

Welcome to the *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide*. This guide describes how to setup Windows 7 and Windows Server 2008 R2 to meet the same security conditions used by the Common Criteria (CC) evaluation.

Microsoft engineering teams, consultants, support engineers, partners, and customers have reviewed and approved this prescriptive guidance to make it:

* **Proven**. Based on field experience.
* **Authoritative**. Offers the best advice available.
* **Accurate**. Technically validated and tested.
* **Actionable**. Provides the steps to success.
* **Relevant**. Addresses real-world security concerns.

This guide is a supplement to the [Windows 7 Security Baseline](http://technet.microsoft.com/en-us/library/ee712767.aspx) and the [Windows Server 2008 R2 Security Baseline](http://technet.microsoft.com/en-us/library/gg236605.aspx) published by Microsoft. It provides the additional installation, configuration, and security information required to reproduce the security level of a Common Criteria-evaluated system.

**Important** If configuration recommendations in the general technical documentation or Windows 7, Windows Server 2008 are not consistent with the instructions in the *Windows 7, Server 2008 R2 Common Criteria Guide*, the information in the *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide* takes precedence and applies as this was the configuration used during the Common Criteria Evaluation.

## Who Should Read This Guide

The *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide* is primarily for IT professionals, security specialists, network architects, computer engineers, and other IT consultants who plan application or infrastructure development and deployments of Windows 7 clients and Windows Server 2008 R2 servers in an enterprise environment. The guide is not intended for home users. This guide is for individuals whose jobs may include one or more of the following roles:

* **Security specialist**. Users in this role focus on how to provide security across computing platforms within an organization. Security specialists require a reliable reference guide that addresses the security needs of all segments of their organizations and also offers proven methods to implement security countermeasures. Security specialists identify security features and settings, and then provide recommendations on how their customers can most effectively use them in high risk environments.
* **IT operations, help desk, and deployment staff**. Users in IT operations focus on integrating security and controlling change in the deployment process, and deployment staff focuses on administering security updates quickly. Staff in these roles also troubleshoot security issues related to applications that involve how to install, configure, and improve the usability and manageability of software. They monitor these types of issues to define measurable security improvements with minimal impact on critical business applications.
* **Network architect and planner**. Users in this role drive the network architecture efforts for computers in their organizations.
* **Consultant**. Users in this role are aware of security scenarios that span all the business levels of an organization. IT consultants from both Microsoft Services and partners take advantage of knowledge transfer tools for enterprise customers and partners.

### Skills and Readiness

The following knowledge and skills are required for consultants, operations, help desk and deployment staff, and security specialists who develop, deploy, and secure server systems running Windows in an enterprise organization:

* MCSE on Microsoft Windows Server 2003 or a later certification and two or more years of security-related experience, or equivalent knowledge.
* Experience in the administration of Windows machines using command line management utilities and scripts.
* Experience in the administration of local users, groups, and policies using command line management utilities.
* Experience configuring Windows Management Instrumentation (WMI) for remote administration.
* Experience using WMI management tools for remote administration including Microsoft Management Console (MMC), eventvwr, and virtmgmt.
* Experience using the Security Configuration Wizard (SCW).
* Experience deploying applications and server computers in enterprise environments.
* In-depth knowledge of the organization’s domain and Active Directory environments (optional).
* Experience with the Group Policy Management Console and the administration of Group Policy using it (optional).

## Section Summaries

This release of the *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide* consists of this Overview and four sections that discuss how to setup your environment to match the security conditions of the evaluated configuration.

### Overview

The overview states the purpose and scope of the guide, defines the guide’s audience, and indicates the organization of the guide to assist you in locating the information relevant to you. It also describes the user prerequisites for the guidance. Brief descriptions follow for each chapter.

### Section 1: Introduction

This chapter introduces the Common Criteria standard, specifies further what this guide describes, and provides an implementation roadmap.

### Section 2: Specifications and References for a CC-evaluated System

This chapter provides specifications and references for implementing a CC-evaluated configuration with 7 and Windows Server 2008 R2.

### Section 3: Security Policy Assumptions and Conditions

A CC-evaluated configuration makes specific assumptions about the required security policy and installation restrictions. Assumptions are items and issues that cannot be formally evaluated under CC but are required to ensure the security level of a CC-evaluated system. Therefore, to reproduce the CC-evaluated implementation, you must review and apply the items in this chapter.

### Section 4: Configuring Elevated Security Functionality

A CC-evaluated configuration of Windows 7 and Windows Server 2008 R2 makes specific assumptions about the security functionality included in the evaluation. To install and configure a CC-evaluated configuration, you must first use the standard technical documentation and guidance for the product. Then you must review and apply the items in this chapter.

## Style Conventions

This guidance uses the style conventions that are described in the following table.

|  |  |
| --- | --- |
| Element | Meaning |
| Bold font | Signifies characters typed exactly as shown, including commands, switches, and file names. User interface elements also appear in bold. |
| *Italic font* | Titles of books and other substantial publications appear in italic. |
| *<Italic>* | Placeholders set in italic and angle brackets <Italic> represent variables. |
| Monospace font | Defines code and script samples. |
| Note | Alerts the reader to supplementary information. |
| Important | Alerts the reader to essential supplementary information. |

## More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this guide on Microsoft.com:

* [Windows 7 Security Baseline](http://technet.microsoft.com/en-us/library/ee712767.aspx) - <http://technet.microsoft.com/en-us/library/ee712767.aspx>
* [Windows](http://technet.microsoft.com/en-us/library/gg236605.aspx) Server 2008 R2 [Security](http://technet.microsoft.com/en-us/library/gg236605.aspx) Baseline - http://technet.microsoft.com/en-us/library/gg236605.aspx
* [Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP](http://go.microsoft.com/fwlink/?LinkId=111329) - http://go.microsoft.com/fwlink/?LinkId=111329
* [Microsoft Security Compliance Manager](http://go.microsoft.com/fwlink/?LinkId=107264) tool and guidance - http://go.microsoft.com/fwlink/?LinkId=107264
* [Infrastructure Planning and Design guides](http://go.microsoft.com/fwlink/?LinkId=100915) - http://go.microsoft.com/fwlink/?LinkId=100915
* [Microsoft Assessment and Planning Toolkit](http://go.microsoft.com/fwlink/?LinkId=105520) - http://go.microsoft.com/fwlink/?LinkId=105520
* [Microsoft Deployment Toolkit](http://go.microsoft.com/fwlink/?LinkId=102093) page on Microsoft TechNet - http://go.microsoft.com/fwlink/?LinkId=102093
* [Microsoft Assessment and Planning (MAP) Toolkit](http://go.microsoft.com/fwlink/?LinkId=74708) - http://go.microsoft.com/fwlink/?LinkId=74708
* [Microsoft Windows Security Resource Kit](http://go.microsoft.com/fwlink/?LinkId=29168) - http://go.microsoft.com/fwlink/?LinkId=29168
* [Security Guidance](http://go.microsoft.com/fwlink/?LinkId=67571) on Microsoft TechNet - http://go.microsoft.com/fwlink/?LinkId=67571
* [Solution Accelerators](http://go.microsoft.com/fwlink/?LinkId=108308) page on Microsoft TechNet - <http://go.microsoft.com/fwlink/?LinkId=108308>

## Support and Feedback

The Solution Accelerators – Security and Compliance (SASC) team would appreciate your thoughts about this and other Solution Accelerators. Please contribute comments and feedback to [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=The%20Fundamental%20Computer%20Investigation%20Guide%20for%20Windows). We look forward to hearing from you.

Solution Accelerators provide prescriptive guidance and automation for cross-product integration. They present proven tools and content to help you plan, build, deploy, and operate information technology with confidence. To view the extensive range of Solution Accelerators and for additional information, visit the [Solution Accelerators](http://go.microsoft.com/fwlink/?LinkId=51571) page on Microsoft TechNet (<http://go.microsoft.com/fwlink/?LinkId=108308>).

# Introduction

This section focuses on how to setup a Windows 7 or Windows Server 2008 R2 system to match the security conditions used by the CC evaluation. This guidance is supplemental to the standard technical documentation and security guidance for the product and provides the additional installation, configuration, and security information required to reproduce the security assurance level of an evaluated system. As mentioned in Section 1, the guidance in this document has precedence over guidance in any other document in case of discrepancies. See also Section 2.4 for further clarification of the precedence rule.

This section covers the following topics:

* What is Common Criteria?
* What is a CC-compliant system?
* What this guide describes
* Implementation roadmap

## What is Common Criteria?

The Common Criteria for Information Technology (IT) Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO / IEC 15408) for IT security certification. CC provides a general model for evaluation based on constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. Common Criteria is used by governments and organizations around the world to assess the security assurance provided by IT products.

The Common Criteria provides a standardized methodology aimed at establishing the level of confidence that may be placed in the product's security features through expressing security requirements and defining rigorous criteria by which products are evaluated. A product that passes a Common Criteria evaluation receives officially recognized certification. Common Criteria certifications are recognized among IT professionals, organizations, government agencies, and customers as a seal-of-approval for mission-critical software. Note, however, that if a product is CC-certified, it does not necessarily mean it is completely secure. The process of obtaining a CC certification restricts the security analysis to certain security features taken in the context of specific assumptions about the operating environment and the strength of threats faced by the product in that environment. It is intended to provide a level of assurance about the security functions that have been examined by a neutral third party. The CC evaluation also provides help in deciding if the intended use of the system fits the described capabilities.

Common Criteria evaluations can take place in any certificate issuing member country participating in the Common Criteria Mutual Recognition Arrangement (CCMRA). The issued certificates are then accepted globally, up to a particular assurance level, by any national organization that participates in the CCMRA.

You can find more information about CC at the following Web site: [http://www.commoncriteriaportal.org](http://www.commoncriteriaportal.org/).

## What is a CC compliant System?

A system can be considered to be "CC compliant" if it matches an evaluated and certified configuration. This implies various requirements concerning hardware and software, as well as requirements concerning the operating environment, users, and the ongoing operating procedures.

The hardware and software must match the evaluated configuration. In the case of an operating system, this also requires that the installed kernel, system, and application software are exactly the same as the ones covered by the evaluation. The documentation (including this guide) will specify permitted variations, such as modifying certain configuration files and settings, and installing software that does not have the capability to affect the security of the system (typically those that do not require elevated privileges). Please refer to Section 4.2 of this guide for more information.

Stated requirements concerning the operating environment must also be met. Typical requirements include a secure location for the hardware (protected from physical access by unauthorized persons), level of training of the authorized personnel, as well as restrictions concerning permitted network connections.

The operation of the system must be in agreement with defined organizational security policies, to ensure that actions by administrators and users do not undermine the system’s security.

## What This Guide Describes

This guide makes a distinction between two types of usage scenarios:

* A utilization that serves a general-purpose environment
* A utilization that meets the conditions established for the Common Criteria evaluation of this product (cf. Section 2.2). The system configuration that meets these conditions is referred to as a CC-evaluated system in this guide.

A CC-evaluated configuration makes specific assumptions about installation, configuration, and security. This distinguishes it from most production usages of the product. A CC-evaluated version of the product includes certain restrictions on the way product components are employed and draws specific boundaries around functionality and performance. The purpose of this guide is to describe the assumptions, conditions, and boundaries required to reproduce the configuration and utilization of Windows 7 and Server 2008 R2 established in the Common Criteria evaluation.

## Configuration Roadmap

This Common Criteria evaluation is based on the English version of Windows 7 and Server 2008 R2 and its documentation. You use only the English-version and refer only to the English-version technical documentation when deploying the CC-evaluated version of Windows 7 and Server 2008 R2. To install and configure a CC-evaluated configuration, you must first use the standard technical documentation for Windows. Then apply all relevant hardening measures defined in the Security guidance documentation for Windows 7 and Server 2008 R2 listed in Section 1.4.

Next, refer to the *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide* (this document) for supplemental information specific to the Common Criteria requirements. If configuration recommendations in the technical documentation are not consistent with the instructions in the *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide*, the information in the *Windows 7, Server 2008 R2 Common Criteria Supplemental Administrator’s Guide* takes precedence and applies in order to replicated the evaluated configuration.

Use the following checklist as a roadmap to configuring a CC-evaluated system:

1. Understand the definition and purpose of the Common Criteria standard provided in Sections 2.1 and 2.2.
2. Review the CC-evaluated product specifications, documentation references, and summary of evaluated security functionality in Section 3.
3. Review and apply the policy conditions required for a CC-evaluated system provided in Section 4.
4. Install and configure Windows Server 2008 R2 according to the standard installation documentation [Installing Windows Server 2008](http://technet.microsoft.com/en-us/library/cc755116.aspx).
5. Install and configure Windows 7 according to the standard installation documentation at “[Getting Started](http://windows.microsoft.com/en-US/windows7/help)”.
6. Harden the Windows 7 installation according to [Windows 7 Security Baseline](http://technet.microsoft.com/en-us/library/ee712767.aspx) (http://technet.microsoft.com/en-us/library/ee712767.aspx)
7. Harden the Server 2008 R2 installation according to [Windows Server 2008 R2 Security Baseline](http://technet.microsoft.com/en-us/library/gg236605.aspx) http://technet.microsoft.com/en-us/library/gg236605.aspx)
8. Review and apply the security configuration required for a CC-evaluated system according to this guide.

# Specification and References for a CC-evaluated System

This section provides specifications and references for implementing a Common Criteria (CC)-evaluated Windows 7 and Windows Server 2008 R2 deployments. It covers the following topics

* About the Evaluated Version
* Technical Documentation Guidance and References
* Evaluated Security Functionality

## About the Evaluated Version of Windows 7 and Server 2008 R2

Windows 7 and Windows Server 2008 R2 contain security technology that meets the requirements of the Common Criteria Evaluation Assurance Level (EAL) 4+. The system configuration that meets these requirements is referred to as the CC-evaluated system in this guide.

The CC evaluation for Windows 7 and Server 2008 R2 was performed on the specific configuration defined in this guide. Note that this covers the use of additional hardware device drivers.

Any deviation from this configuration may result in a non-evaluated system, but does not necessarily mean that the security of the resulting system is reduced. It is the responsibility of the individual organization to determine the potential risks and benefits associated with installing newer product versions or additional software that was not subject to this evaluation, and correspondingly deviating from the evaluated configuration described in this document.

The Target of Evaluation (TOE) for this evaluation of Windows is defined as follows:

|  |  |
| --- | --- |
| Product: | *Microsoft Windows 7 Enterprise Edition (32-bit and 64-bit versions)* |
|  | *Microsoft Windows 7 Ultimate Edition (32-bit and 64-bit versions)* |
|  | *Microsoft Windows Server 2008 R2 Standard Edition* |
|  | *Microsoft Windows Server 2008 R2 Enterprise Edition* |
|  | *Microsoft Windows Server 2008 R2 Datacenter* |
|  | *Microsoft Windows Server 2008 R2 Itanium* |
| Language: | *English* |
| Version: | *6.1.7600* |

Security Updates installed:

* *All Critical updates as of September 14, 2010*
* [*MS10-073*](http://www.microsoft.com/technet/security/bulletin/MS10-073.mspx)
* [*MS10-085*](http://www.microsoft.com/technet/security/bulletin/MS10-085.mspx)
* *KB2492505*

If you choose to replicate the configuration used during the Common Criteria testing, the above products must be installed. However, it is a best practice to keep your software up to date with the current security updates.

### Detailed Hardware Requirements

#### Memory

The maximum amount of memory that can be used is determined by the type of operating system, as follows:

* For Windows 7 Enterprise, the computer can be configured with up to 4 GB of physical memory in 32-bit Windows and 192 GB of physical memory in 64-bit Windows.
* For Windows Server 2008 R2 Standard, the computer can be configured with up to 32 GB of physical memory.
* For Windows Server 2008 R2 Enterprise, 2008 R2 Datacenter, and Itanium editions, the computer can be configured with up to 2 TB of physical memory.

#### Processors

Depending on the edition of Windows, the largest number of logical processors a Windows operating system can support can be from four to as many as 64. A logical processor can be a core processor or a processor using hyper-threading technology.

The following are some examples of supported systems and the number of logical processors they provide:

* A single-processor/dual-core system provides 2 logical processors.
* A single-processor/quad-core system provides 4 logical processors.
* A dual-processor/dual-core system provides 4 logical processors.
* A dual-processor/quad-core system provides 8 logical processors.
* A quad-processor/dual-core system provides 8 logical processors.
* A quad-processor/dual-core, hyper-threaded system provides 16 logical processors.
* A quad-processor/quad-core system provides 16 logical processors.

### Networking

The following networking configurations are supported:

* Ethernet-based networking

#### Storage

The following list of supported physical storage options is supported:

* Direct-attached storage: Serial Advanced Technology Attachment (SATA), external Serial Advanced Technology Attachment (eSATA), Parallel Advanced Technology Attachment (PATA), Serial Attached SCSI (SAS), SCSI, USB, and Firewire.
* Storage area networks (SANs): Internet SCSI (iSCSI), Fibre Channel, and SAS technologies can be used.
* Network-attached storage

#### Peripheral Hardware Components

The following peripheral hardware components that can also be used with Windows:

* Internal or external DVD drive
* Universal Serial Bus (USB)
* Serial Port
* Parallel Port
* Small Computer System Interface (SCSI)
* Infineon-based smartcard reader

## Evaluated Security Functionality

Windows 7 is suited for business desktops and notebook computers; it is the workstation product and while it can be used by itself it is designed to serve as a client within Windows domains. Designed for departmental and standard workloads, Windows Server 2008 R2 Standard delivers intelligent file and printer sharing; secure connectivity based on Internet technologies, and centralized desktop policy management. Windows Server 2008 R2 Enterprise differs from Windows Server 2008 R2 Standard primarily in its support for high-performance server hardware for greater load handling. These capabilities provide reliability that helps ensure systems remain available. Windows Server 2008 R2 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. Windows Server 2008 R2 Itanium provides support for the alternate Intel Itanium CPU, but otherwise can serve where Standard or Enterprise edition products might be used.

The security features addressed by this security target are those provided by Windows 7 and Windows Server 2008 R2 as operating systems. Microsoft provides several Window 7 and Windows Server 2008 R2 software applications that are considered outside the scope of the defined TOE and thus not part of the evaluated configuration. Services outside this evaluation include: e-mail service (SMTP), Remote Desktop, Right Management Service, Windows SharePoint Service, Microsoft Message Queuing, and ReadyBoost. These services are particularly complex or not recommended and in some cases essentially represent products in their own right. They have been excluded because they are not enabled or installed by default and are not necessary for the operation of the core security services.

The following table summarizes the Windows configurations included in the evaluation.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Windows 7 Enterprise | Windows 7 Ultimate | Windows Server 2008 R2 Standard | Windows Server 2008 R2 Enterprise | Windows Server 2008 R2 Datacenter | Windows Server 2008 R2 Itanium |
| 32-bit/64-bit | 32 & 64 | 32 & 64 | 64 | 64 | 64 | 64 |
| Single Core/Processor | X | X | X | X | N/A | X |
| Multiple Core/Processor | X | X | X | X | X | X |
| Domain Member | X | X | X | X | X | X |
| Domain Controller | N/A | N/A | X | X | X | X |

### Security Features

Windows 7 and Server 2008 R2 provide the following key security features. Refer to the product documentation and the CC security target for more information on the following features which were evaluated.

| Feature | Description |
| --- | --- |
| Access Control Lists (ACLs) | Windows 7 and Windows Server 2008 R2 permit only authenticated users to access system resources. The security model includes components to control who accesses objects (such as files, directories, and shared printers); what actions an individual can perform with respect to an object, and the events that are audited.  Every object has a unique Security Descriptor (SD) that includes an ACL. An ACL is a list of entries that grant or deny specific access rights to individuals or groups. The Windows 7 and Windows Server 2008 R2 object-based security model lets administrators grant access rights to a user or group-rights that govern who can access a specific object, a group of properties, or an individual property of an object. The definition of access rights on a per-property level provides the highest level of granularity of permissions. |
| Address Space Load Randomization | Buffer overflow vulnerabilities rely on being able to predict the memory location of system interfaces to accomplish their goal of reading user data or establishing a permanent presence by modifying user or system configuration settings. In the past system executable images and DLLs always loaded at the same location, allowing nefarious software to assume that interfaces reside at fixed addresses. The Address Space Load Randomization (ASLR) feature makes it difficult for nefarious software to predict where interfaces are located in memory because APIs are located by loading system DLLs and executables at a different location every time the system boots. |
| Auto-enrollment | Public Key Certificate auto-enrollment and auto-renewal in Windows Server 2008 R2 significantly reduce the resources needed to manage x.509 certificates. These features also make it easier to deploy smart cards faster, and to improve the security of the Windows PKI by automatically expiring and renewing certificates. |
| BitLocker To Go | New in this version of Windows, both Windows 7 and Windows Server 2008 R2 extend the previous BitLocker with the ability to also encrypt removable USB storage devices (e.g., USB flash drives). The removable USB storage device content can be encrypted using either a password or credentials on a smart card.  When a password is used, a version of the BitLocker To Go Reader application (that is capable of providing read access to the encrypted content when the appropriate credentials can be provided) is placed onto removable USB storage devices when configured to use this feature. While the content of a removable USB storage device can be read and written when using Windows 7 or Windows Server 2008 R2 (assuming appropriate credentials are available), the BitLocker Reader application provides a read-only dialog that allows content to be copied via the application, when provided the correct password, to the host operating system so that the decrypted file content can be accessed.  Note that while the ability to encrypt content placed on the USB device is within scope of the evaluation, the BitLocker Reader is not considered part of the TOE Security Functions since it cannot be reliably protected and as such could potentially be modified or replaced (by the user or anyone else that may come into possession of the USB device).  Additionally, the Group Policy can be used to configure USB storage devices to effectively require BitLocker To Go to be used in order to write content on removable USB storage devices. Otherwise, such devices can be only used for read-only access |
| Code Integrity Verification | Kernel-mode code signing (KMCS) prevents kernel-mode device drivers from loading unless they are published and digitally signed by developers who have been vetted by one of a handful of trusted certificate authorities (CAs). KMCS uses public-key cryptography technologies and requires that kernel-mode code include a digital signature generated by one of the trusted certificate authorities. When a driver tries to load, the TOE decrypts the hash included with the code using the public key stored in the certificate, then verifies that the hash matches the one computed with the code. The authenticity of the certificate is checked in the same way, but using the certificate authority's public key, which is trusted by Windows. |
| Constrained Delegation | Constrained Delegation is the act of allowing a service to impersonate a user account or computer account in order to access resources throughout the network. This feature in Windows Server 2008 R2 enables you to limit delegation to specific services, to control the particular network resources the service or computer can use. For example, a service that was previously trusted for delegation in order to access a backend on behalf of a user can now be constrained to use its delegation privilege only to that backend and not to other machines or services. |
| Credential Manager | This provides a secure store for usernames/passwords and also stores links to certificates and keys. This enables a consistent single sign-on experience for users, including roaming users. Single sign-on makes it possible for users to access resources over the network without having to repeatedly supply their credentials. |
| Cross–Certification Support | Also called qualified subordination[[1]](#footnote-1), Cross-Certification allows constraints to be placed on subordinate Certificate Authorities (CAs) and on the certificates they issue, and allows trust to be established between CAs in separate hierarchies. Cross-Certification support improves the efficiency of administering PKI. |
| Cryptographic API: Next Generation | Windows 7 and Windows Server 2008 R2 supplement the legacy CryptoAPI with the Cryptography API: Next Generation (CNG). CNG provides applications with access to cryptographic functions, public keys, credential management and certificate validation functions and provides support for the National Security Agency’s Suite B crypto algorithms. CNG also provides extensive auditing support, support for replaceable random number generators, and keys are managed within a key isolation service to limit the exposure of secret and private keys. |
| Data Protection | Windows 7 and Windows Server 2008 R2 have improved support for data protection at the file, directory, and machine level.  The Encrypting File System (EFS) provides user-based file and directory encryption and has been enhanced to allow storage of encryption keys on smart cards, providing better protection of encryption keys.  The new BitLocker Drive Encryption enterprise feature adds machine-level data protection. On a computer with appropriate hardware (e.g., Trusted Platform Module (TPM) support), BitLocker Drive Encryption provides full volume encryption of the system volume, including Windows system files and the hibernation file, which helps protect data from being compromised on a lost or stolen machine.  BitLocker also stores measurements of core operating system files. Every time the computer is started, Windows verifies that the operating system files have not been modified outside of Windows control. If the files have been modified, Windows alerts the user and then goes into a recovery mode, prompting the user to provide a recovery key (created previously when BitLocker was configured) to allow access to the encrypted disk volume. |
| Delegated Administration | Windows includes Active Directory (AD), a scalable, standard-compliant directory service. AD centrally manages Windows-based clients and servers, through a single consistent management interface, reducing redundancy and maintenance costs.  AD enables authorized administrators to delegate a selected set of administrative privileges to appropriate individuals within the organization to distribute the management and improve accuracy of administration. Delegated Administration helps companies reduce the number of domains they need to support a large organization with multiple geographical locations by allowing the delegation of only appropriate authorities, as opposed to creating new domains in order to define and limit the scope of administrative authorities.  AD can interoperate or synchronize data with other directory services using LDAP. |
| Delta Certificate Revocation Lists (CRLs) | The certificate server included in Windows Server 2008 R2 TOE supports Delta CRL, which makes publication of revoked X.509 certificates more efficient. A Delta CRL is a list containing only certificates whose status has changed since the last full (base) CRL was compiled. This is a much smaller object than a full CRL and can be published frequently with little or no impact on client machines or network infrastructure. |
| Digest Authentication | Digest authentication operates much like Basic authentication. However, unlike Basic authentication, Digest authentication transmits credentials across the network as a hash value, also known as a message digest. The user name and password cannot be deciphered from the hash value. Conversely, Basic authentication sends a Base 64 encoded password, essentially in clear text, across the network. Basic authentication is not supported in the TOE. Digest authentication does not have to use reversible password encryption. The AD extended schema properties ensures that every newly created user account automatically has the Digest authentication password hashed and stored as a field in the “AltSecId” property of the user object. Note that the hash is protected from replay using a challenge response protocol to introduce some unpredictable data. |
| DirectAccess | Windows 7 and Windows Server 2008 R2 introduce DirectAccess. DirectAccess allows clients to securely access file shares, web sites, and applications without connection to a virtual private network (VPN). DirectAccess involves the establishment of bi-directional communication paths between applicable Windows operating systems when suitable network connectivity (e.g., to the Internet) exists. |
| EFS Multi-user Support | Windows 7 and Windows Server 2008 R2 support file sharing between multiple users of an individual encrypted data file. Encrypted file sharing is a useful and easy way to enable collaboration without having to share private keys among users. |
| Encrypting File System (EFS) | Windows 7 and Windows Server 2008 R2 continue to provide security of data on the hard disk by encrypting it. This data remains encrypted even when backed up or archived. EFS runs as an integrated system service making it easy to manage, difficult to attack, and transparent to the user. The encryption and decryption processes are transparent to the user, once files are marked for encryption. Performance enhancements in Windows 7 and Windows Server 2008 R2 include support for encrypting the paging file, and storage of user EFS keys on smart cards.. |
| Forest Trust | Forest trust is a type of Windows trust for managing the security relationship between two forests. This feature enables the trusting forest to enforce constraints on which security principal names it trusts other forests to authenticate. This new trust type that 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. Cross-forest authentication enables secure access to resources when the user account is in one forest and the computer account is in another forest. This feature allows users to securely access resources in other forests, using either Kerberos or NTLM[[2]](#footnote-2), without sacrificing the single sign-on benefits of having only one user Identification (ID) and password maintained in the user’s home forest. |
| Group Policy | Windows 7 and Windows Server 2008 R2 Group policy allows central management of collections of users, computers, applications, and network resources instead of managing entities on a one-by-one basis. Integration with AD delivers granular and flexible control. It permits authorized administrators to define customized rules about virtually every facet of a user's computer environment such as security, user rights, desktop settings, applications, and resources, minimizing the likelihood of misconfiguration. Windows 7 and Windows Server 2008 R2 add numerous additional policy settings to those available in previous versions of the operating system.  Upon installation, Windows 7 and Windows Server 2008 R2 offer groups that are pre-configured with specific user rights and/or privileges. These groups are referred to as “built-in groups.” The Windows 7 and Windows Server 2008 R2 built-in groups fall into three (3) categories: built-in local groups (e.g., Administrator, Backup Operator); built-in domain local groups (e.g., Administrator, Account Operator); and built-in global groups (e.g. Enterprise Administrator, Domain Administrator). The authorized administrator can conveniently take advantage of these built-in groups by assigning these groups to specific user accounts allowing users to gain the rights and/or privileges associated with these groups. |
| Hardware Data Execution Prevention | 64-bit hardware support adds a set of Data Execution Prevention (DEP) security checks to the TOE. These checks, known as hardware-enforced DEP, are designed to block malicious code that takes advantage of exception-handling mechanisms by intercepting attempts to execute code in memory that is marked for data only. This hardware protection feature is present in all 64-bit hardware architectures in the evaluated configuration.  While not available for 32-bit hardware architectures, due to hardware limitations, the only limitation is that application programs are not afforded additional protection from potential programming errors that might be exploitable by malicious users. |
| Integrated IPSec Support | Windows 7 and Windows Server 2008 R2 include identical IPSec support for both IPv4 and IPv6. Full support for Internet Key Exchange (IKE) and data encryption is provided for both IP stacks. IPSec configuration is integrated with the Windows Firewall with Advanced Security MMC snap-in to improve manageability and reduce the likelihood of conflicting firewall and IPSec rules. |
| Kerberos Authentication Support | Full support for Kerberos Version 5 (v5) protocol Windows 7 and Windows Server 2008 R2 provides fast, single sign-on to Windows-based enterprise resources. It is used to support Transitive Domain Trust to reduce the number of trust relationships required to manage users and resources between Windows domains |
| Mandatory Integrity Control | In addition to Discretionary Access Control (DAC), Windows provides Mandatory Integrity Control (MIC). MIC uses integrity levels and a mandatory policy to evaluate access. Processes and securable objects (e.g., files) are assigned integrity levels that determine their levels of protection or access.  As an integrity policy, a process with a lower integrity level (e.g., low) cannot write to an object with a higher integrity level (e.g., medium), even if that object's DAC policy allows write access. On the other hand, processes can access objects that have an integrity level lower than or equal to their own integrity level. In addition, to controlling write access, the MIC policy addresses read and execute accesses and can be configured to restrict a process with a lower integrity level from reading and/or executing objects with a higher integrity level.  The integrity labels defined in Windows are:   * Untrusted – Used by processes started by the Anonymous group; * Low – Used by protected mode IE, blocks write access to most objects (such as files and registry keys) on the system; * Medium – Normal applications being launched while user account control (UAC) is enabled; * High – Applications launched through administrator elevation when UAC is enabled, or normal applications if UAC is disabled; and * System – Services and other system-level applications (such as WinLogon). |
| Network Access Protection (NAP) | While present in previous versions of Windows, the Network Access Protection (NAP) feature hasn’t previously been subject to evaluation. This feature allows access to network resources to be controlled based on a computer’s identity and compliance with configurable governance policies. The NAP mechanism is capable of automatically bringing a client workstation or server into compliance with defined governance policies so that access is subsequently allowed.  The NAP feature involves a NAP agent running on NAP clients and a NAP health policy server (NAP server) running on a Windows 2008 R2 server, with the Network Policy Server (NPS) role. The NAP agents collect relevant health information for their host NAP client and provide it to the NAP server when network access is required. The NAP server uses NPS policies and settings to evaluate the health of NAP clients in order to determine whether to grant network access (full or restricted). When a NAP client isn’t conformant with configured settings and policies only restricted network access would be allowed, but the NAP server and NAP agent can cooperate to remedy some identified problems in order to bring a NAP client into compliance so that its network access can be elevated.  Access to a network subsequent to NAP server approval can be enforced using the following mechanisms: IPsec, 802.1X, VPN, DHCP, and NAP-NAC (this last mechanism applies only when suitable Cisco devices are employed).  Note that if the organization defines a NAP health policy that may, for example, require automatic updating to be enabled or require critical security updates to be installed.. Those computers that do not comply to the NAP policy may either have restricted access to the network, or a NAP remediation server may install any critical Windows security updates. In the latter case, the result may be that the Windows configuration is different from the configuration examined during the Common Criteria evaluation.  Finally, the Common Criteria evaluation did not extend to including the integration of NAP policies for 802.1X and NAC-managed networks. |
| Public Key Certificate Issuing and Management Service | The Windows Server 2008 R2 Certificate Server issues and manages public key certificates for the following Windows 7 and Windows Server 2008 R2 TOE services: digital signatures, software code signing, TLS/SSL authentication for Web traffic, IPSec, Smart card logon, EFS user and recovery certificates. |
| Secure Network Communications | Windows 7 and Windows Server 2008 R2 support end-to-end encrypted communications across network using the IPSec standard. It protects sensitive internal communications from intentional or accidental viewing. AD provides central policy control for its use to make it deployable. |
| Smart Card Support for Authentication | Smart Card technology is fully integrated into the Windows 7 and Windows Server 2008 R2 TOE, and is an important component of the operating system's Public Key Infrastructure (PKI) security feature. The smart card serves as a secure store for public and private keys and as a cryptographic engine for performing a digital signature or key-exchange operation. Smart card technology allows Windows 7 and Windows Server 2008 R2 TOE to authenticate users by using the private and public key information stored on a card. The Smart Card subsystem on the Windows 7 and Windows Server 2008 R2 TOE supports industry standard Personal Computer/Smart Card (PC/SC)–compliant cards and readers, and provides drivers for commercially available Plug and Play smart card readers. Smart card readers attach to standard peripheral interfaces, such as Universal Serial Bus (USB). The Windows 7 and Windows Server 2008 R2 TOE detects Plug and Play-compliant smart card readers and installs them using the Add Hardware wizard. |
| Support for Security Standards | Windows 7 and Windows Server 2008 R2 build secure network sites using the latest standards, including 128-bit SSL/TLS, IPSec and Kerberos v5 authentication. |
| URL-Based authorization | This authorization mechanism enables businesses to control access to applications exposed through the Web by restricting user access to URLs. For example, one user may be restricted from access to certain applications, whereas another user can be allowed to execute other applications. |
| User Account Control | User Account Control (UAC) (alternately known as LUA – Least Privilege User Access) enables users to perform common tasks as non-administrators, called standard users, and as administrators without having to switch users, log off, or use Run As. A standard user account is synonymous with a user account in Windows 7 and Windows Server 2008 R2. User accounts that are members of the local Administrators group will run most applications as a standard user.  When an administrator logs on to a computer running Windows 7 or Windows Server 2008 R2, the user is assigned two separate access tokens. Access tokens, which contain a user's access control data, group membership and authorization data, are used by Windows to control what resources and tasks the user can access. In early versions of Windows, an administrator account received only one access token, which included data to grant the user access to all Windows resources. This access control model did not include any failsafe checks to ensure that users truly wanted to perform a task that required their administrative access token.  When an administrator logs on to a computer running Windows 7 or Windows Server 2008 R2, the user’s full administrator access token is split into two access tokens: a full administrator access token and a standard user access token. During the logon process, authorization and access control components that identify an administrator are removed, resulting in a standard user access token. The standard user access token is then used to start the Widows desktop process. Because all applications inherit their access control data from the initial launch of the desktop, they all run as a standard user as well.  After an administrator logs on, the full administrator access token is not invoked until the user attempts to perform an administrative task at which point the user will be interactively prompted to confirm this access escalation. |
| Web Site Permissions | Web Site permissions are not meant to be used in place of NTFS permissions. Instead, they are used with NTFS permissions to strengthen the security of specific Web site content maintained by the IIS web server of the Windows Server 2008 R2 TOE. An authorized user can configure web site's access permissions for specific sites, directories, and files. Unlike NTFS permissions, Web site permissions affect everyone who tries to access the configured Web sites. If Web permissions conflict with NTFS permissions for a directory or file, the more restrictive settings are applied.  Note that the server-side execution of web content is not allowed as part of the evaluated configuration. |
| Windows Firewall (previously known as Internet Connection Firewall (ICF)) | Windows Firewall is a stateful firewall that drops unsolicited incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). Windows Firewall provides a level of protection from malicious users and programs that rely on unsolicited incoming traffic to attack computers. Windows Firewall supports IPv4 and IPv6. The firewall drivers (for IPv4 and for IPv6 respectively) have a static rule called a boot-time policy to perform stateful filtering. This allows the Windows 7 and Windows Server 2008 R2 to perform basic networking tasks such as DNS and DHCP and communicate with a DC to obtain policy. Once the firewall service is running, it will load and apply the run-time ICF policy and remove the boot-time filters. |
| Windows Security Center Service (WSC) | WSC is a service that monitors, among other things, the status of Windows firewall running on the Windows 7 and Windows Server 2008 R2. It also provides the logged-on interactive user certain visual notifications when it detects that the status of Windows firewall has changed. |

# Security Policy Assumptions and Conditions

A CC-evaluated configuration of Windows 7 and Server 2008 R2 makes specific assumptions about the required security policy and installation restrictions. Assumptions are items and issues that cannot be formally evaluated under CC but are required to ensure the security level of a CC-evaluated system. Therefore, to reproduce the CC-evaluated configuration, you must review and apply the items in this chapter.

This chapter covers the following topics:

• Security Policy Assumptions

• Installation and Configuration Constrains

## Security Policy Assumptions

The *Microsoft Windows 7 and Server 2008 R2 Security Target* (<http://www.commoncriteriaportal.org/products_ALL.html>) specifies security policy assumptions for the target of evaluation (TOE) on which the evaluation of Windows (the TOE) is based. Therefore, to comply with the CC-evaluated system, enforcing and maintaining the conditions defined in the assumptions listed below is mandatory.

### Assumptions on the System Environment

It is assumed that the non-IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.

## Installation and Configuration Constraints

### Installing the TOE (Windows 7)

Administrators installing the system must follow the step-by-step procedure outlined “[Windows 7 Help & How-to](http://windows.microsoft.com/en-US/windows7/help) (http://windows.microsoft.com/en-US/windows7/help) for Windows 7.

Administrators are advised to familiarize themselves with and follow the guidance in the *Windows 7 Security Baseline*.

### Installing the TOE (Server 2008 R2)

Administrators installing the system must follow the step-by-step procedure outlined in the [Installing Windows Server 2008](http://technet.microsoft.com/en-us/library/cc755116(WS.10).aspx) (<http://technet.microsoft.com/en-us/library/cc755116(WS.10).aspx)> for Windows Server 2008 and Windows Server 2008 R2.

Administrators are advised to familiarize themselves with and follow the guidance in the *Windows Server 2008 R2 Security Baseline*.

### Verifying the TOE version

In order to verify that the installed version of Windows in fact matches the evaluated version of Windows as identified in Section 3.1, the following command can be executed at the command prompt:

systeminfo

The OS Name, OS Version, and list of installed Hotfixes should match the information provided above.

## Modes of Operation

One aspect of a Common Criteria evaluation is an analysis of how the product may be used or misused by a malicious end-user, and which modes of operation are available for users.

For the purposes of this misuse evaluation, the two modes of operation defined for Windows Server 2008 R2 and Windows 7 are:

* **Operational Mode** – This is the normal mode of operation:
  + Standard users can shut down only workstations, not servers.
  + Standard users cannot modify system-wide registry settings, operating system files, and/or programs.
* **Failure Mode Crash and Audit Fail Mode** – This is operation following a failure or operational error:
  + When the system shuts down due to the audit log becoming full. Only an administrator can log on to Windows in this mode. The user notices that the system is shut down when the audit log becomes full; however, there is no further impact to the user because the system is disabled for the user.
  + If the domain policy includes a threshold for account lockout, the user account is locked immediately after exceeding the specified number of invalid login attempts. The user does not receive any error messages indicating what went wrong; rather the message displayed notifies the user that the system cannot log on the user. If the user persists attempting to log on unsuccessfully, a final message notifies the user that his/her account is disabled, and an administrator must rectify the problem.
  + “When the administrator selects the **Deny disk space to users exceeding quota limit** option, users who exceed their quota limit receive an "insufficient disk space" error from Windows and cannot write additional data to the volume without first deleting or moving some existing files from it.”
  + “When the administrator selects the **Log event when a user exceeds their quota limit** option, an event is written to the Windows system log on the computer running disk quotas whenever users exceed their quota limit. Administrators can view these events with Event Viewer, filtering for disk event types.”
  + “When the administrator selects the **Log event when a user exceeds their warning level** option, an event is written to the Windows system log on the computer running disk quotas whenever users exceed their quota warning level. Administrators can view these events with Event Viewer, filtering for disk event types. Unless you set a trigger to do so, users are not warned of this event.”

Note:    Only an authorized administrator can install or modify a program or change the Crash and Audit Fail Mode of operation to Operational Mode.

# Configuring Elevated Security Functionality

A CC-evaluated implementation of Windows 7 and Windows Server 2008 R2 makes specific assumptions about the security functionality included in the evaluation. To install and configure a CC-evaluated configuration, you must first use the standard technical documentation and guidance for the product introduced in Section 4.2. Then you must review and apply the items in this chapter.

This chapter covers the following topics

* Hardening Windows 7
* Hardening Server 2008 R2

Because Windows 7 and Server 2008 R2 were designed from the beginning with security in mind, the default configuration is already secure. The instructions in this chapter are to provide a further level of lockdown that was used during the Common Criteria testing. Therefore, there is no need to change a setting from the default configuration setting unless explicitly told to do so.

## Hardening Windows 7

* Install the additional security settings as described in [*Windows 7 Security Baseline*](http://technet.microsoft.com/en-us/library/ee712767.aspx).
  1. Common Criteria evaluation uses the “***Specialized Security – Limited Functionality***” (SSLF) environment as described in the *Windows 7 Security Baseline*.
  2. The version of the *Windows 7 Security Baseline* used during the evaluation was last updated on April 6, 2010.

## Hardening Windows Server 2008 R2

* Install the additional security settings as described in the [*Windows Server 2008 R2 Security Baseline*](http://technet.microsoft.com/en-us/library/gg236605.aspx).

1. Common Criteria evaluation uses the “***Specialized Security – Limited Functionality***” (SSLF) environment as described in the *Windows Server 2008 R2 Security Baseline*.
2. The version of the *Windows Server 2008 R2 Security Baseline* used during the evaluation was last updated on April 6, 2010.

## Additional Configuration

This section describes the additional configuration steps that you must perform in order to replicate the conditions of the Windows 7 and Server 2008 R2 evaluation:

1. Disable LUA File/Registry Virtualization.
   1. Edit the Group Policy for the Domain by first selecting Administrative tools from the Start menu.
   2. Next, select Group Policy Management
   3. Expand the Domain by clicking on the “+” sign if it is not expanded
   4. Locate the VSG SSLF Domain Policy
   5. Right click on it and select Edit from the menu
   6. Under the Computer Configuration section, click on the Policies folder to open it.
   7. Then open the Windows Settings folder, the Security Settings folder, and the Local Policies folder
   8. Open the Security Options folder and scroll down the right side of the window to the bottom.
   9. Double click on the policy: User Account Control: Virtualize file and registry write failures to per-user locations
   10. Select the “Define this policy setting” checkbox
   11. Select Disabled
   12. Click Apply
   13. Click OK
2. If desired, change the default timeout for locking the monitor display after user inactivity.
   1. After the security templates are applied, Windows enables the “Password protect the screen saver” user security policy, and the default value before the screen is locked is after 15 minutes (900 seconds) user inactivity. The administrator can change this value by modifying the “Screen Saver timeout” user security policy.
3. To further restrict standard users from installing additional drivers, modify the following security policies:
   1. Ensure that the “Allow non-administrators to install drivers for these device setup classes” policy is not enabled. This policy is located under Computer Configuration \ Administrative Templates \ System \ Driver Installation.
   2. Ensure that the “Turn off Windows Update device driver searching” policy is enabled. This policy is located under Computer Configuration \ Administrative Templates \ System \ Internet Communication Management \ Internet Communication Settings.
   3. Ensure that the “Turn off Windows Update device driver search prompt” policy is disabled to ensure that the administrator is prompted for consent before installing a new device driver. This policy is located under Computer Configuration \ Administrative Templates \ System \ Driver Installation.
4. Disable the Fast User Switching policy. This policy is located under Computer Configuration \ Administrative Templates \ System \ Logon \ Hide Entry Points for Fast User Switching, and should be set to “Enabled”.
5. When configuring the Certificate Services and role-based administration, follow the instructions at <http://technet.microsoft.com/en-us/library/cc738189(WS.10).aspx>.

## Ongoing Maintenance

Please refer to the online documentation at [www.microsoft.com](http://www.microsoft.com) for general administration and ongoing monitoring and maintenance tasks for Windows 7 and Server 2008 R2.

This section briefly mentions additional management concerns to be aware of:

* Ensure that there is sufficient disk space to store the databases used by the Active Directory and the Certificate Services databases. By monitoring the amount of remaining disk space, the administrator can ensure that directory and certificate service request processing will not be interrupted due to lack of storage resources.
* User passwords should be limited to 127 characters or less. Note that the security target specifies that user passwords must be at least 16 characters in length and any combination of upper and lower case letters, numbers, and symbols.
* When using the Computer Management MMC Snap-In to reset a user’s password, the Set Password dialog will display a maximum of 32 \* characters obscured feedback in the input edit control, however the control accepts a maximum 128 characters.

# Evaluated Windows Tools

As part of the Windows 7 and Server 2008 R2 Common Criteria evaluation, the evaluation staff reviewed the following tools and determined that they meet the level of assurance expected for the intended usage environment as described in the Windows 7 / Windows Server 2008 R2 Security Target.

| Tool | Description |
| --- | --- |
| Active Directory Certificate Services Tools | The Certification Authority graphical user interface (GUI) includes snap-ins for the Certification Authority, Certificates, and Certificate Templates. The Certification Authority snap-in enables you to access customizable services for issuing and managing certificates that are used in software security systems that employ public key technology. A certification authority (CA) receives certificate requests, verifies the information in the request and the identity of the requester, issues certificates, revokes certificates, and publishes a certificate revocation list (CRL). |
| Active Directory Delegation of Control Wizard | The OU Delegation graphical user interface (GUI) is an automated wizard that allows authorized administrators to delegate control of Active Directory objects. You can grant users permissions to manage users, groups, computers, organizational units, and other objects stored in Active Directory. |
| Active Directory Domains and Trusts Snap-in | The Active Directory Domains and Trusts graphical user interface (GUI) allows users to:   * Administer user principal name suffixes (adding and removing alternate UPN suffixes used to create user logon names), * Raise domain and forest functional levels, * Administer trusts (create shortcut, external, and forest trusts providing interoperability with other domains and forests by managing the trusts; verify trusts; and remove trusts), * Transfer the domain naming operations master role from one domain controller to another, * Select the scope of authentication for users for external and forest trusts, * Change the routing status of a name suffix for forest trusts, * Enable or disable an existing name suffix for a forest from routing, and * Exclude name suffixes from routing to a local forest. |
| Active Directory Sites and Services Snap-in | The Active Directory Sites and Services graphical user interface (GUI) enables users to configure server and site settings, and administer and optimize directory information availability and replication. Active Directory Sites and Services can only be used from a computer that has access to a Windows 2000 or greater domain. |
| Audit Policy Command Line Interface | Displays information about and performs functions to manipulate audit policies. For more information see <http://technet.microsoft.com/en-us/library/cc731451.aspx>. |
| Authorization Manager | Authorization Manager provides a flexible framework for integrating role-based access control into applications. It enables administrators who use those applications to provide access through assigned user roles that relate to job functions. Authorization Manager applications store authorization policy in the form of authorization stores that are stored in Active Directory or XML files and apply authorization policy at runtime. |
| BitLocker Drive Encryption Control Panel [new] | BitLocker Drive Encryption (BDE) is a data protection feature for client computers and server operating systems. Through the BitLocker Control Panel, administrators have access to BitLocker functionality designed to enhance protection against data theft or exposure on computers that are lost or stolen, and more secure data deletion when BitLocker-protected computers are decommissioned. BitLocker helps protect the operating system volume of the hard disk from unauthorized access while the computer is offline. To achieve this, BitLocker uses full-volume encryption and the security enhancements offered by the TPM. On computers that have a TPM, BitLocker also supports multifactor authentication. |
| Certificates Snap-in [new] | The Certificates Snap-in (certmgr.msc) is the primary tool for users and administrators to view and manage certificates for a user, computer, or service.  The Certificates snap-in allows the user to request, renew, find, view, move, copy, and delete certificates. |
| Component Services Snap-in | The Component Object Model (COM) enables functionality to be encapsulated in a COM application that can be reused by many different applications. DCOM technology enables a COM application to be accessed from different computers over a network.  This application manages both computer-wide and application-wide DCOM security.  COM+ Applications enables authorized administrators to manage COM+ applications and their components. Administrators can create and delete COM+ applications, or create, enable, disable, or delete COM+ application components and legacy components. It is also possible to create or delete roles for COM+ applications and to add or remove users from these roles. |
| Computer Management Snap-in | The Computer Management Graphical User Interface (GUI) allows authorized users to perform remote and local administrative tasks. You can manage any remote computer within the Active Directory forest for which you are a member of the Administrators group. |
| Control Panel | The Control Panel is a part of the Microsoft Windows graphical user interface which allows users to view and manipulate basic system settings and controls via applets, such as adding hardware, adding and removing software, controlling user accounts, and changing accessibility options.  Control Panel applets that manage security functionality and were evaluated as part of the Windows Common Criteria evaluation are listed as part of this table. |
| Create A Shared Folder Wizard | The Create A Shared Folder Wizard is accessed from the Computer Management Snap-in and simplifies the process of sharing a folder, enabling offline access and assigning permissions. |
| Date and Time Control Panel | The computer's real-time clock is used to record the time whenever a user creates or modifies files on the computer. Authorized administrators can change the computer’s time and time zone, thus adjusting the clock.  The date and time are set using the Date and Time user interface (UI) by authorized users having administrative privileges. Computer time, including some time intervals based on computer time differences, is used in several security policies and settings. |
| Default Group Policy Object Restore Command Line Utility | The Default Group Policy Object Restore Utility is a command-line application that restores the Group Policy objects (GPOs) on a domain controller and/or domain to their default states. Unless otherwise specified by the user, use of this command updates the Group Policy objects on both the domain controller and the domain. Only domain Administrators and enterprise Administrators have access to this utility. |
| Device Manager Snap-in | The Device Manager graphical user interface (GUI) enables users to install and update the drivers for hardware devices, modify hardware settings for those devices, and troubleshoot problems. Not all of this functionality is included in the TOE. Within the TOE, the Device Manager GUI enables users to check the status of their hardware devices, and disable or uninstall devices on a local computer. (Device Manager will work only in read-only mode on a remote computer.)  You must be logged on as an administrator or member of the Administrators group in order to complete procedures using Device Manager. If your computer is connected to a network, network policy settings may also prevent you from completing the procedures. |
| Devices and Printers Control Panel | The Devices and Printer Control Panel allows you to configure printing properties for a specific document, and printer properties for a specific printer. |
| DHCP Snap-in | Dynamic Host Configuration Protocol (DHCP) is an IP standard designed to reduce the complexity of administering address configurations by using a server computer to centrally manage IP addresses and other related configuration details used on the network. The Microsoft® Windows Server 2008 family provides the DHCP service which enables the server computer to perform as a DHCP server and configure DHCP-enabled client computers on the network as described in the current DHCP draft standard, RFC 2131.  The DHCP console is used to manage the DHCP service. It is added to the Administrative Tools folder in Control Panel when installing a DHCP server running Windows Server. To further integrate DHCP administration into the overall network management, the DHCP console appears as a Microsoft Management Console (MMC) snap-in. |
| Disk Management Snap-in | The Disk Management Graphical User Interface (GUI) allows authorized users to perform remote and local disk (and volume) management. You can manage any remote Windows Server 2008 R2 or Windows 7 computer on which you are a member of the Administrators or Backup Operators group. Most configuration changes take effect almost immediately; it is not necessary to save or commit changes before they take effect. |
| DNS Snap-in | Domain Name System (DNS) servers host records of a distributed DNS database and use the records they host to resolve DNS name queries sent by DNS client computers, such as queries for the names of Web sites or computers in your network or on the Internet. If you plan to use this computer to answer DNS queries for computers in your network, then add the DNS server role.  The DNS console is used to manage the DNS service. It is added to the Administrative Tools folder in Control Panel when installing a DNS server running Windows Server. To further integrate DNS administration into the overall network management, the DNS console appears as a Microsoft Management Console (MMC) snap-in. |
| Driver Verifier Manager | The Driver Verifier Manager (Verifier.exe) subcomponent allows authorized users to monitor device drivers to determine whether or not they are functioning correctly. The application also allows specific monitoring options to be configured, such as memory pool tracking and deadlock detection. Both a graphical user interface and a command line interface are available for Driver Verifier Manager. |
| Encrypting File System Dialog Boxes | The Encrypting File System Active Directory User (efsadu) Dynamic Link Library is part of EFS file sharing. Specifically, the dll is a secondary window which provides information on revocation checking. The Efsadu dynamic link library (DLL) provides the EFS user interface. Efsadu is called when a user accesses the Advanced Properties page for a file or folder to modify file or folder encryption options. The options processed through Efsadu include whether to apply the encryption to file or folder only, or to a folder and all subfolders and files that it contains. Efsadu also contains the user interface for adding users to an encrypted file. |
| Event Viewer Snap-in | The Event Viewer Graphical User Interface (GUI) allows users to gather information about hardware, software, and system problems and monitor Windows 7 and Windows Server 2008 R2 security events. |
| Explorer | The functionality of the Windows Explorer Graphical User Interface (GUI) covered in this evaluation is the portion that allows users to set, change, or remove permissions, auditing, and ownership by viewing the security properties of files, folders, and shared folders. You can set file and folder permissions and auditing only on drives formatted to use the NTFS filesystem. |
| Explorer Quota Property Tab | Disk Quota tracks and controls the disk space an individual user can take on a specific volume. Volumes are a portion of a physical disk that functions as though it were a physically separate disk. In My Computer and Windows Explorer, volumes appear as local disks such as C: or D: |
| File Encryption Command Line Utility | Cipher.exe is a command line utility that displays the status or alters the encryption of directories and files on NTFS volumes. For more information see <http://technet.microsoft.com/en-us/library/cc771346(WS.10).aspx>. |
| Group Policy Editor Snap-in | The Group Policy graphical user interface (GUI) enables users to manage and administer group policy objects. A Group Policy object is a collection of settings that affects computer or user accounts, and can be applied to sites, domains, or organizational units. It can be used to configure security options, manage applications, manage desktop appearance, assign scripts, and redirect folders from local computers to network locations. A user or computer contained in a site, domain, or organizational unit is subject to a Group Policy object, either directly through a link, or indirectly through inheritance. |
| Group Policy Update Command Line Utility | The Group Policy Refresh Utility (gpupdate.exe) is a command-line tool used to apply Group Policy settings. Group policy settings are automatically applied by Windows in two situations: foreground policy application and background policy application. In the case of foreground policy application, group policy settings are applied to users when they log on, and to computers when the computer boots. |
| Internet Information Service (IIS) Manager Snap-in | The Internet Information Services (IIS) Manager Graphical User Interface (GUI) is used by authorized users to administer IIS servers. |
| IP Security Monitor Snap-in | The provides a user interface to configure and maintain the IPv6 environment. This configuration environment is managed through the command line based management program NetShell (netsh.exe). There is no graphical user interface for configuring IPv6 since as most of this protocol is auto-configuring. Mand managing IPv6 is an administrator-only task and that is not designed for the ordinary user population. |
| IP Security Policies Snap-in | The Internet Protocol Security (IPSec) Settings graphical user interface (GUI) allows users to activate local IP security to protect data by securing and optionally encrypting IP packets prior to transmission on the network. |
| NAP Client Configuration Snap-in [new] | Network Access Protection (NAP), a feature first introduced in Windows Vista and Windows Server 2008, allows you to control the access of client computers to network resources based on computer identity and compliance with corporate governance policy. To implement NAP, you must configure NAP settings on both servers and client computers. |
| Network and Sharing Center Control Panel | Network and Sharing Center provides real-time status information about your network. You can see if your computer is connected to your network or the Internet, the type of connection, and what level of access you have to other computers and devices on the network. This information can be useful when you set up your network or if you have connection problems. You can find more detailed information about your network in the network map, which is accessible from Network and Sharing Center. |
| Registry Editor | The Registry Editor graphical user interface (GUI) is an advanced tool that allows users to change settings in a local computer’s system registry. The system registry is a database repository for information about a computer’s configuration. The registry contains information that Windows continually references during operation, such as: user profiles, programs installed on the computer and the types of documents each can create, property settings for folders and program icons, the system’s hardware, and which ports are being used. |
| Resultant Set of Policy Snap-in | The Resultant Set of Policy (RSoP) MMC Snap-in is an administrative tool that utilizes the RSoP Service Application. Administrators use the RSoP MMC Snap-in to see how multiple Group Policy objects affect various combinations of users and computers, or to predict the effect of Group Policy settings on the network. |
| SAM Lock Tool | The Security Accounts Management Database (SAM) stores hashed copies of user passwords. This database is encrypted with a locally stored system key. To keep the SAM database secure, Windows requires that the password hashes are encrypted. Windows prevents the use of stored, unencrypted password hashes.  You can use the SysKey utility to additionally secure the SAM database by moving the SAM database encryption key off the Windows-based computer. The SysKey utility can also be used to configure a start-up password that must be entered to decrypt the system key so that Windows can access the SAM database. |
| Schedule Service Command Line Interface | Enables an administrator to create, delete, query, change, run, and  end scheduled tasks on a local or remote system (schtasks.exe). For more information, see <http://technet.microsoft.com/en-us/library/cc725744(WS.10).aspx> |
|  |  |
| Security Configuration Wizard | The Security Configuration Wizard (SCW) graphical user interface (GUI) is an automated wizard that provides guided attack surface reduction for your server. SCW is installed by default in Windows Server. SCW is highly recommended for configuring Windows Firewall and creating security lockdown templates for servers based on their roles. |
| Security Configuration Wizard Command Line Utility | The Security Configuration Wizard Command Line Utility (scwcmd.exe) is a supplement to the Security Configuration Wizard (SCW). SCWcmd.exe uses with the security policies that are generated with the SCW. The Security Configuration Wizard Command Line Utility can perform the following tasks:   * Configure one or many servers with an SCW-generated policy. * Analyze one or many servers with an SCW-generated policy. * View XML policy files or analysis results in HTML. * Roll back SCW policies. * Transform an SCW-generated policy into native files that are supported by Group Policy. * Register a knowledge base extension with SCW.   See the Security Configuration Wizard design specification for more information on SCW and security policies. |
| Security Policy Snap-in | Security Policies are managed by users with appropriate administrator permissions through unique instances of the Microsoft Management Console (MMC) graphical user interface (GUI). Security Policies apply primarily to a workstation, domain, or domain controller (rather than to users).  The GUIs used to manage each Security Policy level are named as follows: Local Security Policy and Group Policy Management Editor. Each GUI is accessed from within the Administrative Tools folder of the Control Panel. The Domain and DC Security Policy GUIs (Group Policy Management Editor) are only available from DC machines. |
| Security Templates and Security Configuration and Analysis Snap-in | The Security Templates and Security Configuration and Analysis snap-ins’ graphical user interfaces (GUIs) allows administrators to create a text-based template file that contains security settings for all of the security areas supported by the Security Configuration Tool Set. Administrators can then apply and use these template files to configure or analyze system security using other tools. |
| Server Manager | Windows Server® eases the task of managing and securing multiple server roles in an enterprise with the Server Manager graphical user interface application. Server Manager provides a single source for managing a server's identity and system information, displaying server status, identifying problems with server role configuration, and managing all roles installed on the server. |
| Services Snap-in | The Services User Interface (UI) allows authorized administrators to manage services on local and remote computers. Using the Services UI, you can start, stop, pause, resume, or restart services, and set up recovery actions to take place if a service fails (such as restarting the service automatically or restarting the computer). You can also enable or disable services for a particular hardware profile. |
| Signature Verification Command Line Utility | The **Signature Verification** graphical user interface allows authorized users the ability to scan the file system looking for system files that are not digitally signed.  To help maintain the integrity of the system, critical files have been digitally signed in order to quickly detect any changes to these files. |
| System Control Panel, Computer Name Tab | The Computer Name tab in the System control panel allows an authorized administrator to change the computer domain and join or leave an Active Directory forest. |
| System Integrity Check and Repair Command Line Utility | The System Integrity Check and Repair utility (sfc.exe) Scans the integrity of all protected system files and replaces incorrect versions with correct Microsoft versions. |
| Task Scheduler Snap-in | The Task Scheduler User Interface (UI) is a In Microsoft Management Console (MMC) 3.0 snap-in tool that allows authorized administrators to use the Scheduled TasksTask Scheduler to interface to display, create, delete, or modify scheduled tasks. Task Scheduler provides controlled, unattended management of task execution, launched either on schedule in response to events or system state changes. Administrators can configure machines to automatically react to potential system problems, including, intermittent, hard-to-reproduce failures; can set up complex and demanding tasks to run in sequence or in response to multiple triggers and condition changes; and, a task can notify an administrator of a problem on a desktop by e-mail, and can launch a diagnostic program or an automated resolution. The administrator Using Scheduled Tasks, you can schedule any script, program, or document to run at a time that is most convenient for you. You can also:   * Schedule a task to run daily, weekly, monthly, or at certain times (such as system startup) * Modify or delete a scheduled task * Stop a scheduled task that is running * Disable all scheduled tasks |
| TPM Management Snap-in [new] | TPM Management is a Microsoft Management Console (MMC) snap-in that allows administrators to interact with Trusted Platform Module (TPM) Services. TPM Services is used to administer the TPM security hardware in your computer. The TPM Services architecture provides the infrastructure for hardware-based security by providing access to and assuring application-level sharing of the TPM. |
| User Account Control Settings | User Account Control (UAC) enables users to run with standard user rights, as opposed to administrative rights. Administrative rights give users the ability to read and modify any part of the operating system, including the code and data of other users—and even the operating system itself. Without administrative rights users cannot accidentally (or deliberately) modify system settings, malware can’t alter system security settings or disable antivirus software, and users can’t compromise the sensitive information of other users on shared computers. Running with standard user rights can therefore prevent accidental modification of code, mitigate the impact of malware, keep computers running more smoothly, while protecting sensitive data on shared computers. |
| Users and Groups Snap-in | The Users and Groups Graphical User Interface (GUI) allows you to manage user and group accounts. Users and Groups are important in Windows Server 2008 R2 and Windows 7 security because you can limit the ability of users and groups to perform certain actions by assigning rights and permissions. The Users and Groups Snap-in is available on computers running Windows 7 Professional and member servers running Windows Server. For domain controllers, user and group management is available in the Active Directory Users and Computers interface. (It is not available on domain controllers.) |
| Volume Shadow Copy Service Command Line Utility | The Volume Shadow Copy Service (vssadmin.exe) utility allows authorized administrators to create, delete, and manage shadow copies. Shadow copies are a form of backup that can be performed even when the files being backed up are currently in use. |
| Windows Authentication User Interface | When users log on to a Windows 7 or Windows Server machine, they initiate a session of activity (opening and using applications and/or Windows features). Session locking provides users with the ability to manually lock a session that they have opened or set a time period that, when expired, will automatically lock the session. Locking a session forces a user to enter a correct user name and password prior to regaining access to the session. |
| Windows Firewall with Advanced Local Security Snap-in | Windows Firewall is a stateful host-based firewall that provides protection from malicious users and programs that rely on unsolicited incoming traffic to attack computers on a network. For computers connected to a network, the firewall rejects unsolicited incoming traffic that does not correspond either to traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic).  Windows Firewall in Windows 7 and Server 2008 R2 enables the configuration of firewall settings that apply to all the connections of the computer (global configuration). When a global Windows Firewall setting is changed, the change is applied to all the connections on which Windows Firewall is enabled. Global configuration options are available on all tabs in of the Windows Firewall management interface. |
| Windows Management Infrastructure (WMI) Control Snap-In | The WMI Control Snap-In enables administrators to view and configure WMI settings on a remote computer or local computer. The actual capabilities made visible through the WMI Control Snap-In are implemented by underlying WMI providers. It is the provider that enforces its security checks and effects, not the WMI Control Snap-In. The WMI Control Snap-In is merely responsible for properly collecting and passing information to the provider. |
|  |  |

# Administration Scenarios

As part of the Windows 7 and Server 2008 R2 Common Criteria evaluation, the evaluation staff examining the following end-user and administrator scenarios. The table indicates which evaluated administration tool was used to accomplish each scenario.

|  |  |  |
| --- | --- | --- |
| Scenario | Used By | Tool(s) Used |
| Locking out user accounts | Administrators | [Local or Domain] Users and Groups MMC Snap-in |
| Managing access to files and directories | End-users,  Administrators | Windows Explorer |
| Managing audit policy | Administrators | Auditpol.exe; Event Viewer MMC Snap-In |
| Managing BitLocker | End-Users | BitLocker Drive Encryption Control Panel |
| Managing BitLocker To Go | End-Users | BitLocker Drive Encryption Control Panel |
| Managing certificates | Administrators | Certificates MMC Snap-In |
| Managing failed logon handling | Administrators | Group Policy Object Editor MMC Snap-In |
| Managing Internet Information Services | Administrators | Internet Information Services MMC Snap-In |
| Managing NTFS Quotas | Administrators | Windows Explorer |
| Managing password complexity policies | Administrators | Group Policy Object Editor MMC Snap-In |
| Managing the Encrypting File System | End-Users, Administrators | Windows Explorer; cipher.exe |
| Managing the Windows Firewall | Administrators | Windows Firewall with Advanced Security MMC Snap-In |
| Managing users and groups | Administrators | [Local or Domain] Users and Groups MMC Snap-in |
| Managing workstation locking policies | Administrators | Group Policy Object Editor MMC Snap-In |
| Protecting management data on a network | Administrators | IP Security Policies MMC Snap-In |
| Setting a logon advisory warning | Administrators | Group Policy Object Editor MMC Snap-In |
| Setting the time for the machine | Administrators | Group Policy Object Editor MMC Snap-In |
| Obtaining the latest set of Windows updates | End-users | Windows Update Control Panel applet |
| Managing the Windows Firewall | End-users | Windows Firewall Control Panel applet |
| Changing the machine name or domain | End-users | System Control Panel applet |
| Viewing the status of the Windows Firewall and automatic updating | End-users | Security Center Control Panel applet |
| Installing a local or network printer | End-users | Printer Control Panel applet |
| Caching files for offline access | End-users | Offline Files Control Panel applet |
| Configuring network access | End-users | Networking and Sharing Center Control Panel applet |
| Configuring your mouse | End-users | Mouse Control Panel applet |
| Configuring your keyboard | End-users | Keyboard Control Panel applet |
| Manually adding hardware devices | End-users | Device Manager Control Panel applet |
| Setting the time for the machine | End-users | Date and Time Control Panel applet |
| Managing full disk encryption | End-users | BitLocker Drive Encryption Control Panel applet |
| Backing up and restoring files | End-users | Backup and Restore Center Control Panel applet |

# Evaluated Configuration and Windows Administration Settings

The Common Criteria evaluation includes a precisely defined and tested configuration of Windows, the “evaluated configuration”.

If you choose to run your Windows deployments using the evaluated configuration, you must follow the deployment steps described in this document, and then ensure that the following policy settings are not changed. Note that running in the evaluated configuration will result in reduced Windows functionality and may introduce compatibility problems.

| Security Policy Setting | SSLF Setting | Comments / Change needed to replicate the evaluated configuration |
| --- | --- | --- |
| Interactive logon: Do not require CTRL+ALT+DEL | Disabled | Must be set to disabled ~~enabled~~. |
| Interactive logon: Number of previous logons to cache (in case domain controller is not available) | 0 logons | Must not be changed post-deployment. |
| Microsoft network client: Digitally sign communications (if server agrees) | Enabled | Must not be changed post-deployment. |
| Microsoft network server: Digitally sign communications (if client agrees) | Enabled | Must not be changed post-deployment. |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | Enabled | Set the value to MACHINE\System\  CurrentControlSet\Control\Lsa\MSV1\_0\  NTLMMinClientSec=4, 537395248 |
| Shutdown: Clear virtual memory pagefile | Disabled | Must be set to enabled to ensure that user data in the page file is deleted when the operating system shuts down. |
| System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing | Disabled | In order to replicate the evaluated configuration, this setting must be set to enabled. |
| System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Enabled | Must not be changed post-deployment. |
| System settings: Optional Subsystems | Enabled, not assigned (Server 2008 R2 member server & Server 2008 R2 SSLF domain controller only) | Must not be changed post-deployment. |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled | Must not be changed post-deployment. |
| Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings | Enabled | Can be changed post-deployment. |
| MSS[[3]](#footnote-3): (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic. | Multicast, broadcast, & ISAKMP exempt (best for Windows 7) (Windows 7 and Server 2008 R2 SSLF)  Only ISAKMP is exempt (recommended for Windows Server 2008 R2) (Server 2008 R2 SSLF domain controller) | Enabled, but default exemptions removed. |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled | In order to replicate the evaluated configuration, this setting must be set to enabled. |
| Configure Automatic Updates[[4]](#footnote-4) | Enabled | Must be set to disabled – by definition of the CC standard, the software in the evaluated configuration must be updated. |
| Registry Modifications |  |  |
| MACHINE\System\CurrentControlSet\  Control\Lsa\FIPSAlgorithmPolicy | 0 | 1 |
| Security Guide Domain Policies |  |  |
| Minimum password length[[5]](#footnote-5) | 12 characters | ~~12~~ 16 characters |
| Security Guide User Policies |  |  |
| Remove Security Tab[[6]](#footnote-6) | Enabled | Must be set to disabled – users should be able to modify access permissions to data they own. |

# Appendix: User Privileges and Assignments

The following table enumerates the well-known privileges in Windows 7 and Server 2008 R2. The default assignment describes which built-in groups are assigned each privilege, and any changes to assigned privileges after applying the SSLF group policy template from the Windows Security Compliance Manager documentation.

Note that any changes to the assignment of user privileges will cause the Windows machine to diverge from the configuration used during the Common Criteria evaluation.

| Privilege | Description | Default Assignment | Change After Applying Security Templates |
| --- | --- | --- | --- |
| Replace a process-level token | Required to assign the [primary token](http://msdn.microsoft.com/en-us/library/ms721603(VS.85).aspx) of a process. | Local Service  Network Service | Local Service  Network Service |
| SeAssignPrimaryTokenPrivilege |
| SE\_ASSIGNPRIMARYTOKEN\_NAME |
| Generate security audits | Required to generate audit-log entries. Give this privilege to secure servers. | Local Service  Network Service | Local Service  Network Service |
| SeAuditPrivilege |
| SE\_AUDIT\_NAME |
| Back up files and directories | Required to perform backup operations. This privilege causes the system to grant all read access control to any file, regardless of the [access control list](http://msdn.microsoft.com/en-us/library/ms721532(VS.85).aspx) (ACL) specified for the file. Any access request other than read is still evaluated with the ACL. This privilege is required by the [RegSaveKey](http://msdn.microsoft.com/en-us/library/ms724917(VS.85).aspx) and [RegSaveKeyEx](http://msdn.microsoft.com/en-us/library/ms724919(VS.85).aspx)functions. The following access rights are granted if this privilege is held:   * READ\_CONTROL * ACCESS\_SYSTEM\_SECURITY * FILE\_GENERIC\_READ * FILE\_TRAVERSE | Administrators  Backup Operators | Administrators |
| SeBackupPrivilege |
| SE\_BACKUP\_NAME |
| Bypass traverse checking | Required to receive notifications of changes to files or directories. This privilege also causes the system to skip all traversal access checks. It is enabled by default for all users. | Administrators  Backup Operators  Everyone  Local Service  Network Service  Users | Administrators  Local Service  Network Service  Users |
| SeChangeNotifyPrivilege |
| SE\_CHANGE\_NOTIFY\_NAME |
| Create global objects | Required to create named file mapping objects in the global namespace during Terminal Services sessions. This privilege is enabled by default for administrators, services, and the local system account. | Administrators  Local Service  Network Service  SERVICE | Administrators  Local Service  Network Service  SERVICE |
| SeCreateGlobalPrivilege |
| SE\_CREATE\_GLOBAL\_NAME |
| Create a pagefile | Required to create a paging file. | Administrators | Administrators |
| SeCreatePagefilePrivilege |
| SE\_CREATE\_PAGEFILE\_NAME |
| Create permanent shared objects | Required to create a permanent object. | No One | No One |
| SeCreatePermanentPrivilege |
| SE\_CREATE\_PERMANENT\_NAME |
| Create symbolic links | Required to create a symbolic link. | Administrators | Administrators |
| SeCreateSymbolicLinkPrivilege |
| SE\_CREATE\_SYMBOLIC\_LINK\_NAME |
| Create a token object | Required to create a primary token. | No One | No One |
| SeCreateTokenPrivilege |
| SE\_CREATE\_TOKEN\_NAME |
| Debug programs | Required to debug and adjust the memory of a process owned by another account. | Administrators |  |
| SeDebugPrivilege |
| SE\_DEBUG\_NAME |
| Enable computer and user accounts to be trusted for delegation | Required to mark user and computer accounts as trusted for delegation. | No One | No One |
| SeEnableDelegationPrivilege |
| SE\_ENABLE\_DELEGATION\_NAME |
| Impersonate a client after authentication | Required to impersonate. | Administrators  Local Service  Network Service  SERVICE | Administrators  Local Service  Network Service  SERVICE |
| SeImpersonatePrivilege |
| SE\_IMPERSONATE\_NAME |
| Increase scheduling priority | Required to increase the base priority of a process. | Administrators | Administrators |
| SeIncreaseBasePriorityPrivilege |
| SE\_INC\_BASE\_PRIORITY\_NAME |
| Adjust memory quotas for a process | Required to increase the quota assigned to a process. | Administrators  Local Service  Network Service | Administrators  Local Service  Network Service |
| SeIncreaseQuotaPrivilege |
| SE\_INCREASE\_QUOTA\_NAME |
| Increase a process working set | Required to allocate more memory for applications that run in the context of users. | Users | Administrators  Local Service |
| SeIncreaseWorkingSetPrivilege |
| SE\_INC\_WORKING\_SET\_NAME |
| Load and unload device drivers | Required to load or unload a device driver. | Administrators | Administrators |
| SeLoadDriverPrivilege |
| SE\_LOAD\_DRIVER\_NAME |
| Lock pages in memory | Required to lock physical pages in memory. | No One | No One |
| SeLockMemoryPrivilege |
| SE\_LOCK\_MEMORY\_NAME |
| Add workstations to domain | Required to create a computer account. | Not Assigned | Not Assigned |
| SeMachineAccountPrivilege |
| SE\_MACHINE\_ACCOUNT\_NAME |
| Manage the files on a volume | Required to enable volume management privileges. | Administrators | Administrators |
| SeManageVolumePrivilege |
| SE\_MANAGE\_VOLUME\_NAME |
| Profile single process | Required to gather profiling information for a single process. | Administrators | Administrators |
| SeProfileSingleProcessPrivilege |
| SE\_PROF\_SINGLE\_PROCESS\_NAME |
| Modify an object label | Required to modify the mandatory integrity level of an object. | Not Assigned | Not Assigned |
| SeRelabelPrivilege |
| SE\_RELABEL\_NAME |
| Force shutdown from a remote system | Required to shut down a system using a network request. | Administrators | Administrators |
| SeRemoteShutdownPrivilege |
| SE\_REMOTE\_SHUTDOWN\_NAME |
| Restore files and directories | Required to perform restore operations. This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file. Any access request other than write is still evaluated with the ACL. Additionally, this privilege enables you to set any valid user or group SID as the owner of a file. This privilege is required by the RegLoadKey function. The following access rights are granted if this privilege is held:  WRITE\_DAC  WRITE\_OWNER  ACCESS\_SYSTEM\_SECURITY  FILE\_GENERIC\_WRITE  FILE\_ADD\_FILE  FILE\_ADD\_SUBDIRECTORY  DELETE | Administrators  Backup Operators | Administrators |
| SeRestorePrivilege |
| SE\_RESTORE\_NAME |
| Manage auditing and security log | Required to perform a number of security-related functions, such as controlling and viewing audit messages. This privilege identifies its holder as a security operator. | Administrators | Administrators |
| SeSecurityPrivilege |
| SE\_SECURITY\_NAME |
| Shut down the system | Required to shut down a local system. | Administrators  Backup Operators  Users | Administrators  Users |
| SeShutdownPrivilege |
| SE\_SHUTDOWN\_NAME |
| Synchronize directory service data | Required for a domain controller to use the [LDAP](http://msdn.microsoft.com/en-us/library/ms721592(VS.85).aspx) directory synchronization services. This privilege enables the holder to read all objects and properties in the directory, regardless of the protection on the objects and properties. By default, it is assigned to the Administrator and LocalSystem accounts on domain controllers. | Not Assigned | Not Assigned |
| SeSyncAgentPrivilege |
| SE\_SYNC\_AGENT\_NAME |
| Modify firmware environment values | Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information. | Administrators | Administrators |
| SeSystemEnvironmentPrivilege |
| SE\_SYSTEM\_ENVIRONMENT\_NAME |
| Profile system performance | Required to gather profiling information for the entire system. | Administrators | Administrators |
| SeSystemProfilePrivilege |
| SE\_SYSTEM\_PROFILE\_NAME |
| Change the system time | Required to modify the system time. | Administrators  Local Service | Administrators  Local Service |
| SeSystemtimePrivilege |
| SE\_SYSTEMTIME\_NAME |
| Take ownership of files or other objects | Required to take ownership of an object without being granted discretionary access. This privilege allows the owner value to be set only to those values that the holder may legitimately assign as the owner of an object. | Administrators | Administrators |
| SeTakeOwnershipPrivilege |
| SE\_TAKE\_OWNERSHIP\_NAME |
| Act as part of the operating system | This privilege identifies its holder as part of the trusted computer base. Some trusted protected subsystems are granted this privilege. | No One | No One |
| SeTcbPrivilege |
| SE\_TCB\_NAME |
| Change the time zone | Required to adjust the time zone associated with the computer's internal clock. | Administrators  Local Service  Users | Administrators  Local Service  Users |
| SeTimeZonePrivilege |
| SE\_TIME\_ZONE\_NAME |
| Access Credential Manager as a trusted caller | Required to access Credential Manager as a trusted caller. | Not Assigned | Not Assigned |
| SeTrustedCredManAccessPrivilege |
| SE\_TRUSTED\_CREDMAN\_ACCESS\_NAME |
| Remove computer from docking station | Required to undock a laptop. | Administrators  Users | Administrators  Users |
| SeUndockPrivilege |
| SE\_UNDOCK\_NAME |
| User Right: No Display Name | Required to read unsolicited input from a [terminal](http://msdn.microsoft.com/en-us/library/ms721627(VS.85).aspx) device. | Not Assigned | Not Assigned |
| SeUnsolicitedInputPrivilege |
| SE\_UNSOLICITED\_INPUT\_NAME |
| Allow log on locally | Determine which users can log on at the computer. | Guest, Administrators, Users, Backup Operators | Administrators  Users |
| SeInteractiveLogonRight |
| SE\_INTERACTIVE\_LOGON\_NAME |
| Access this computer from the network | Determines which users can log on from the network for a non-interactive session. | Everyone, Administrators, Users, Backup Operators | Administrators  Users |
| SeNetworkLogonRight |
| SE\_NETWORK\_LOGON\_NAME |
| Log on as a batch job | Allows a user to be logged on by means of a batch-queue facility. | Administrators  Backup Operators | Administrators |
| SeBatchLogonRight |
| SE\_BATCH\_LOGON\_NAME |
| Log on as a service | Determines which service accounts can register a process as a service. | Not One | Not One |
| SeServiceLogonRight |
| SE\_SERVICE\_LOGON\_NAME |
| Deny log on locally | Determines which users are prevented from logging on at the computer. This policy setting supersedes the “Allow logon locally” policy setting if an account is subject to both policies. | Guests | Guests |
| SeDenyInteractiveLogonRight |
| SE\_DENY\_INTERACTIVE\_LOGON\_NAME |
| Deny access to this computer from the network | Determines which users are prevented from a network-based log on at the computer. This policy setting supersedes the “Access this computer from the network” policy setting if an account is subject to both policies. | Guests | Guests |
| SeDenyNetworkLogonRight |
| SE\_DENY\_NETWORK\_LOGON\_NAME |
| Deny log on as a batch job | Determines which accounts are prevented from being able to log on as a batch job. This policy setting supersedes the “Log on as a batch job” policy setting if a user account is subject to both policies. | No One | Guests |
| SeDenyBatchLogonRight |
| SE\_DENY\_BATCH\_LOGON\_NAME |

1. Qualified subordination is different from “qualified certificates” defined in RFC 3739. [↑](#footnote-ref-1)
2. NTLM is Windows Challenge / Response described below. [↑](#footnote-ref-2)
3. Maximum Segment Size [↑](#footnote-ref-3)
4. In addition to using Group Policy to control update policy for the machine; enabling automatic update can also be configured using the Windows Update Control Panel Applet. [↑](#footnote-ref-4)
5. In the absence of a domain policy for minimum password length, the local administrator can define a minimum password length for a machine’s local accounts. [↑](#footnote-ref-5)
6. On machines that are not configured for Group Policy, the Security Tab in Explorer can be removed by setting the HKLM\SW\MS\Windows\CurrentVersion\Policies\Explorer\NoSecurityTab registry key. [↑](#footnote-ref-6)