# Contents

**Overview** ................................................................................................................................. 1  
Executive Summary .......................................................................................................................... 1  
Who Should Read This Guide ......................................................................................................... 3  
Skills and Readiness ....................................................................................................................... 3  
Guide Purpose and Scope .............................................................................................................. 3  
Microsoft Guidance and the FDCC ............................................................................................... 4  
Chapter Summaries ....................................................................................................................... 4  
Style Conventions .......................................................................................................................... 5  
More Information ........................................................................................................................... 5  
Support and Feedback .................................................................................................................... 5  
Acknowledgments ........................................................................................................................... 6  
Development Team ....................................................................................................................... 6  
Contributors and Reviewers ......................................................................................................... 6  

**Chapter 1: Implementing the Security Baseline** ....................................................................... 9  
Enterprise Client Environment ...................................................................................................... 10  
Specialized Security – Limited Functionality Environment ....................................................... 10  
Specialized Security ...................................................................................................................... 10  
Limited Functionality ................................................................................................................... 11  
Restricted Services and Data Access .......................................................................................... 11  
Restricted Network Access .......................................................................................................... 11  
Strong Network Protection ........................................................................................................... 12  
Security Design ............................................................................................................................. 12  
OU Design for Security Policies ..................................................................................................... 12  
  Domain Root................................................................................................................................. 13  
  Domain Controllers OU .............................................................................................................. 14  
  Member Servers OU ................................................................................................................... 14  
  Server Role OUs ......................................................................................................................... 14  
  Department OU .......................................................................................................................... 14  
  Windows 7 Users OU .................................................................................................................. 14  
  Windows 7 Computers OU ......................................................................................................... 14  
GPO Design for Security Policies ................................................................................................... 14  
  Recommended GPOs .................................................................................................................. 16  
  Using a GPO Created with the Security Compliance Manager Tool ........................................ 18  
Introducing the Local Policy Tool .................................................................................................. 19  
  Modifying Local Group Policy ................................................................................................... 19  
  Updating the Security Configuration Editor User Interface ................................................... 20  
Domain Policy Settings .................................................................................................................. 21  
  Password Policy Settings ............................................................................................................ 21  
    How to Make Users Change Passwords Only When Required ............................................... 22  
  Account Lockout Policy Settings ............................................................................................... 22  
Computer Policy Settings .............................................................................................................. 23  
  Audit Policy Settings .................................................................................................................. 23  
  User Rights Assignment Settings ............................................................................................... 25  
Security Options Settings .............................................................................................................. 25

Solution Accelerators  
microsoft.com/technet/SolutionAccelerators
Chapter 2: Defend Against Malware ................................................................. 33

Windows 7 Defense Technologies ................................................................. 34
Action Center ............................................................................................... 34
User Account Control .................................................................................. 36
  Risk Assessment ......................................................................................... 37
  Risk Mitigation .......................................................................................... 38
  Mitigation Considerations ......................................................................... 38
  Mitigation Process ..................................................................................... 39
Biometric Security ......................................................................................... 40
  Risk Assessment ......................................................................................... 40
  Risk Mitigation .......................................................................................... 41
  Mitigation Considerations ......................................................................... 41
  Mitigation Process ..................................................................................... 42
Windows Defender .......................................................................................... 43
  Microsoft SpyNet Community ................................................................... 44
  Risk Assessment ......................................................................................... 44
  Risk Mitigation .......................................................................................... 44
  Mitigation Considerations ......................................................................... 44
  Mitigation Process ..................................................................................... 45
Malicious Software Removal Tool ................................................................. 46
  Risk Assessment ......................................................................................... 47
  Risk Mitigation .......................................................................................... 47
  Mitigation Considerations ......................................................................... 47
  Mitigation Process ..................................................................................... 48
Windows Firewall .......................................................................................... 48
  Risk Assessment ......................................................................................... 49
  Risk Mitigation .......................................................................................... 49
  Mitigation Considerations ......................................................................... 49
  Mitigation Process ..................................................................................... 50
AppLocker ........................................................................................................ 50
  Risk Assessment ......................................................................................... 50
  Risk Mitigation .......................................................................................... 50
  Mitigation Considerations ......................................................................... 51
  Mitigation Process ..................................................................................... 51
Software Restriction Policies ........................................................................... 51
Microsoft Application Compatibility Toolkit .................................. 82
Windows XP Mode ........................................................................... 83
More Information.............................................................................. 83
Overview

Welcome to the *Windows 7 Security Guide*. This guide provides instructions and recommendations to help strengthen the security of desktop and laptop computers running Windows® 7 in a domain that uses Active Directory® Domain Services (AD DS). In addition to the solutions that the *Windows 7 Security Guide* prescribes, the guide includes tools, step-by-step procedures, recommendations, and processes that significantly streamline the deployment process. Not only does the guide provide you with effective security setting guidance, it also provides a reproducible method that you can use to apply the guidance to both test and production environments.

The key tool to use in combination with the *Windows 7 Security Guide* is the Security Compliance Manager (SCM). This tool enables you to run a script that automatically creates all the Group Policy objects (GPOs) you need to apply this security guidance.

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.

Consultants and system engineers develop best practices for the implementation of Windows 7, Windows Vista® Service Pack (SP1), Windows Server® 2003 SP2, and Windows Server® 2008 SP2 in a variety of environments. If you are evaluating Windows 7 for your environment, the [Microsoft Assessment and Planning Toolkit](https://www.microsoft.com/technet/SolutionAccelerators) can help mid-market sized organizations determine the readiness of their computers to run Windows 7. You can use the toolkit to quickly conduct computer inventories, identify supported Windows 7 scenarios, and obtain specific hardware upgrade recommendations.

Microsoft has published guides for Windows Vista SP1 and Windows® XP SP3. This guide references significant security enhancements in Windows 7. The *Windows 7 Security Guide* was developed and tested with computers running Windows 7 joined to a domain that uses Active Directory, as well as with stand-alone computers.

**Note**  All references to Windows XP in this guide refer to Windows XP Professional SP3 unless otherwise stated and all references to Windows Vista refer to Windows Vista SP1 unless otherwise stated.

Executive Summary

Whatever your environment, you are strongly advised to take security matters seriously. Many organizations underestimate the value of information technology (IT). If an attack on the servers in your environment is severe enough, it could significantly damage the entire organization. For example, if malware infects the client computers on your network, your organization could lose proprietary data, and experience significant overhead costs to return them to a secure state. An attack that makes your Web site unavailable also could result in a major loss of revenue or customer confidence.

Conducting a security vulnerability, risk, and exposure analysis informs you of the tradeoffs between security and functionality that all computer systems are subject to.
networked environment. This guide documents the major security-related countermeasures that are available in Windows 7, the vulnerabilities these countermeasures help address, and the potential negative consequences (if there are any) related to implementing each countermeasure.

This guide builds on the *Windows XP Security Guide* and the *Windows Vista Security Guide*, which provide specific recommendations about how to harden computers running Windows XP Professional SP3 and Windows Vista SP1. The *Windows 7 Security Guide* provides recommendations to harden computers that use specific security baselines for the following two environments:

- **Enterprise Client (EC).** Client computers in this environment are located in a domain that uses Active Directory and only need to communicate with systems running Windows Server 2008. The client computers in this environment include a mixture of computers running Windows 7 and Windows Vista SP1. For instructions about how to test and deploy the EC environment, see the "Enterprise Client Environment" section in Chapter 1, "Implementing the Security Baseline." You also can access the Microsoft Excel® workbook Windows 7 Security Baseline Settings for more information about the baseline security settings that this environment uses.

- **Specialized Security – Limited Functionality (SSLF).** Concern for security in this environment is so great that a significant loss of functionality and manageability is acceptable. For example, military and intelligence agency computers operate in this type of environment. The client computers in this environment run only Windows Vista SP1. For instructions about how to test and deploy the SSLF environment, see the "Specialized Security – Limited Functionality Environment" section in Chapter 1, "Implementing the Security Baseline." The Excel workbook Windows 7 Security Baseline Settings also includes more information about the baseline security settings for this environment.

**Warning** The SSLF security settings are not intended for the majority of enterprise organizations. The configuration for these settings has been developed for organizations where security is more important than functionality.

The organization of the guide enables you to easily access the information that you require. The guide and its associated tools help you to:

- Deploy and enable either of the security baselines in your network environment.
- Identify and use Windows Vista SP1 security features for common security scenarios.
- Identify the purpose of each individual setting in either security baseline and understand their significance.

In order to create, test, and deploy the security settings for either the EC environment or the SSLF environment, you must first run the Windows® Installer (.msi) file for the SCM tool that accompanies the download for this toolkit. You can then use this tool to automatically create all the GPOs for the security settings this guide recommends. For instructions on how to use this tool to accomplish these tasks, see the information available in the Help Topics for the tool.

Although this guide is designed for enterprise customers, much of the guidance is appropriate for organizations of any size. To obtain the most value from this material, you will need to read the entire guide. However, it is possible to read individual portions of the guide to achieve specific aims. The “Chapter Summary” section in this overview briefly introduces the information in the guide. For further information about the security topics and settings related to Windows Vista, see the *Windows Vista Security Guide* and the companion guide, *Threats and Countermeasures*.

After deploying the appropriate security settings across your enterprise you can verify that the settings are in effect on each computer using the *Security Compliance Management Toolkit*. The toolkit includes Configuration Packs that match the recommendations in this guide for the EC and SSLF environments. The toolkit can be used with the Desired Configuration Management (DCM) feature in Microsoft® System Center Configuration Manager 2007 R2 to efficiently monitor compliance. In addition, you...
can quickly and easily run reports to demonstrate how your organization is meeting important compliance regulations. For further information about the toolkit, see the Security Compliance Management Toolkit Series on TechNet.

**Who Should Read This Guide**

The *Windows 7 Security Guide* is primarily for IT generalists, security specialists, network architects, and other IT professionals and consultants who plan application or infrastructure development and deployments of Windows 7 for both desktop and laptop client computers in an enterprise environment.

**Skills and Readiness**

The following knowledge and skills are required for the intended audience of this guide, which includes IT professionals who develop, deploy, and secure client computers running Windows 7 in enterprise organizations.

- MCSE on Windows Server 2003 or a later certification and two or more years of security-related experience, or equivalent knowledge.
- In-depth knowledge of the organization’s domain and AD DS environments.
- Experience with the Group Policy Management Console (GPMC).
- Experience in the administration of Group Policy using the GPMC, which provides a single solution for managing all Group Policy–related tasks.
- Experience using management tools including Microsoft Management Console (MMC), Gpupdate, and Gpresult.
- Experience deploying applications and client computers in enterprise environments.

**Guide Purpose and Scope**

The primary purposes of the guide are to enable you to:

- Use the solution guidance to efficiently create and apply tested security baseline configurations using Group Policy.
- Understand the reasoning for the security setting recommendations in the baseline configurations that are included in the guide, and their implications.
- Identify and consider common security scenarios, and how to use specific security features in Windows 7 to help you manage them in your environment.

The guide is designed to let you use only its relevant parts to meet the security requirements of your organization. However, readers will gain the most benefit by reading the entire guide.

This guide focuses on how to help create and maintain a secure environment for desktop and laptop computers that run Windows 7. The guide explains the different stages of how to secure two different environments, and what each security setting addresses for the desktop and laptop computers deployed in either one. The guide provides prescriptive information and security recommendations.

Client computers running Windows 7 in both the EC and SSLF environments were tested with computers running Windows Server 2008, Windows Server 2008 SP2, Windows Server 2003 R2, Windows Server 2003 SP2, Windows XP SP3, and Windows Vista SP2. These other computers were configured with security settings comparable to those on the Windows 7 computers to ensure that authentication and authorization functioned correctly. Other recent versions of Windows may also work if configured with similar settings but they have not been tested.
Microsoft Guidance and the FDCC

The Federal Desktop Core Configuration (FDCC) is a mandate from the Office of Management and Budget (OMB) that requires federal government computers running certain operating systems or applications to be configured in a specific way. The most recent memo from the OMB summarizes the requirements and the National Institute of Standards and Technology (NIST) publishes the mandated settings and resources to assist agencies with compliance on the FDCC Web site.

The FDCC settings for Windows XP and Windows Vista were developed in a collaborative effort involving the OMB, NIST, the Department of Defense (DoD), the Department of Homeland Security (DHS), and Microsoft. The FDCC settings for those two versions of Windows are similar to what is published in the security guides from Microsoft, but they are not identical. The FDCC includes some settings that are not prescribed in the Microsoft guidance, and requires different values for some settings that also appear in the guidance from Microsoft. This is to be expected because the scenarios targeted by the FDCC and the Microsoft security guides are not identical. As of the date of this publication there are no FDCC settings specified for Windows 7.

Chapter Summaries

The Windows 7 Security Guide consists of the following chapters:

Chapter 1: Implementing the Security Baseline
This chapter provides a set of procedures to implement prescribed security settings to enhance the default security of the client operating system. The streamlined procedures in this chapter offer a fast and efficient means for you to deploy the recommended security configuration settings and harden the default installation configuration of Windows 7–based client computers in your environment.

Chapter 2: Defend Against Malware
This chapter provides an overview of the security technologies in Windows 7, and recommendations on how to configure them when applicable.

Chapter 3: Protect Sensitive Data
This chapter discusses the features and services that are designed to protect data on client computers running Windows 7 in the Enterprise Client (EC) environment. The configuration of these features depends on your specific requirements and environment. This chapter provides you with a design process to identify how to configure the following features and services to better meet your data protection needs:

- BitLocker™ Drive Encryption
- BitLocker To Go
- Encrypting File System (EFS)
- Rights Management Services (RMS)
- Device management and installation

Chapter 4: Application Compatibility with Windows 7
This chapter includes simple procedures and recommendations that you can use to test the level of compatibility of your applications with Windows 7. The chapter also discusses some of the more common causes of application compatibility issues, and provides pointers to available resources that can help you to address them.
Style Conventions

This guide uses the following style conventions.

<table>
<thead>
<tr>
<th>Element</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold font</strong></td>
<td>Signifies characters typed exactly as shown, including commands, switches and file names. User interface elements also appear in bold.</td>
</tr>
<tr>
<td><em>Italic font</em></td>
<td>Titles of books and other substantial publications appear in <em>italic</em>. New terms when first mentioned also appear in <em>italic</em>.</td>
</tr>
<tr>
<td><code>&lt;Italic&gt;</code></td>
<td>Placeholders set in italic and angle brackets <code>&lt;filename&gt;</code> represent variables.</td>
</tr>
<tr>
<td><strong>Monospace font</strong></td>
<td>Defines code and script samples.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Alerts the reader to supplementary information.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>An important note provides information that is essential to the completion of a task.</td>
</tr>
<tr>
<td><strong>⚠️ Warning</strong></td>
<td>Alerts the reader to essential supplementary information that should not be ignored.</td>
</tr>
<tr>
<td>‡</td>
<td>This symbol denotes specific Group Policy setting modifications or recommendations.</td>
</tr>
<tr>
<td>§</td>
<td>This symbol denotes Group Policy settings that are new to Windows 7.</td>
</tr>
</tbody>
</table>

More Information

The following resources provide additional information about Windows 7 security-related topics on Microsoft.com:

- Federal Desktop Core Configuration (FDCC).
- Microsoft Assessment and Planning Toolkit.
- Security Compliance Management Toolkit Series.
- Threats and Countermeasures.

Support and Feedback

The Solution Accelerators – Security and Compliance (SA–SC) team would appreciate your thoughts about this and other solution accelerators.

Please direct questions and comments about this guide to secwish@microsoft.com.

We look forward to hearing from you.
Acknowledgments

The Solution Accelerators – Security and Compliance (SA–SC) team would like to acknowledge and thank the team that produced the Windows 7 Security Guide. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

**Development Team**

**Content Developers**
Kurt Dillard – kurtdillard.com
Richard Harrison – Content Master Ltd.

**Developers**
Gerald Herbaugh
Haikun Zhang – Beijing ZZZGroup Co. Ltd.
Jeff Sigman
José Maldonado
Michael Tan
ZhiQiang Yuan – Beijing ZZZGroup Co. Ltd.

**Editors**
John Cobb – Wadeware LLC
Steve Wacker – Wadeware LLC

**Product Manager**
Michelle Arney
Shruti Kala
Stephanie Chacharon – Xtreme Consulting Group Inc.

**Program Manager**
Tom Cloward

**Release Manager**
Cheri Ahlbeck – Aquent LLC
Karina Larson

**Test Manager**
Sumit Parikh

**Testers**
Jaideep Bahadur – Infosys Technologies Ltd.
Mansi Sharma – Infosys Technologies Ltd.
Raxit Gajjar – Infosys Technologies Ltd.

**Contributors and Reviewers**
Aaron Margosis, Alvaro Cano Fernandez, Blake Frantz – Center for Internet Security,
Chas Jeffries, Dan Fox, Daniel Taylor, Defense Information System Agency (DISA),
Derek Seaman – Lockheed Martin, Greg Cottingham, Guy Hunt, Juan Antonio Diaz Muñoz, Kathy Lambert, Lori Kingery, Mandy Tidwell, Mark Russinovich, Nate Morin, Rick

Solution Accelerators microsoft.com/technet/SolutionAccelerators

Note  At the request of Microsoft, the National Security Agency Information Assurance Directorate participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

Note  During the development of this Microsoft security guide and the associated security baseline settings, members of the Center for Internet Security community collaborated with Microsoft and provided comments that were incorporated into the published version.
Chapter 1: Implementing the Security Baseline

Microsoft works to improve and update the default security stance of its client operating system in every release. Windows® 7 builds on the significant security enhancements introduced in Windows Vista®, and includes additional security features that make Windows 7 the most secure client operating system that Microsoft has produced to date. This chapter demonstrates how to configure security settings to harden client computers running the default operating system that are joined to an Active Directory® Domain Services (AD DS) domain. Based on this infrastructure, you can use this guidance to enforce specific configuration changes to meet the network requirements of your environment.

This chapter provides a set of procedures to implement prescribed security settings to enhance the default security of Windows 7. The streamlined procedures in the chapter offer a fast and efficient means to deploy the recommended security configuration settings, and harden the default configuration of Windows 7–based client computers in your environment.

You can now harden the default operating system using only Group Policy objects (GPOs). Previous guidance from Microsoft required importing Security Template .inf files, and extensive manual modification of the Administrative Templates portion of several GPOs. Working with these files and templates is no longer necessary. All of the recommended Group Policy settings are documented in the Windows 7 Security Baseline Settings Excel® workbook that also accompanies this guide.

To deploy the guidance in this chapter, you need to:

- Create an organizational unit (OU) structure for your environment.
- Use the SCM tool to create the GPOs for your environment.
- Use the Group Policy Management Console (GPMC) to link and manage the GPOs.

⚠️ Warning ⚠️ It is essential to thoroughly test your OU and GPO designs before deploying them in a production environment.

The baseline GPOs that accompany this guide provide a combination of tested settings that enhance security for client computers running Windows 7 in the following two distinct security environments:

- **Enterprise Client (EC)**
- **Specialized Security – Limited Functionality (SSLF)**
Enterprise Client Environment

The Enterprise Client (EC) environment referred to in this chapter consists of a domain using AD DS in which computers running Windows Server® 2008, Windows Server® 2008, Windows Server® 2003 R2, or Windows Server® 2003 Service Pack 2 (SP2) and AD DS manage client computers that can run Windows 7, Windows Vista SP2 or Windows XP Professional SP3. The client computers are managed in this environment through Group Policy, which is applied to sites, domains, and OUs. Group Policy provides a centralized infrastructure within AD DS that enables directory-based change and configuration management of user and computer settings, including security and user data. The EC security baseline helps provide enhanced security that allows sufficient functionality of the operating system and applications for the majority of organizations.

Specialized Security – Limited Functionality Environment

The Specialized Security – Limited Functionality (SSLF) baseline in this guide addresses the demand to help create highly secure environments for computers running Windows 7. Concern for security is so great in these environments that a significant loss of functionality and manageability is acceptable.

⚠️ Warning  The SSLF security settings are not intended for the majority of enterprise organizations. The configuration for these settings has been developed for organizations where security is more important than functionality.

If you decide to test and deploy the SSLF configuration settings for the client computers in your environment, the IT resources in your organization may experience an increase in help desk calls related to the limited functionality that the settings impose. Although the configuration for this environment provides a higher level of security for data and the network, it also prevents some services from running that your organization may require. Examples of this include Remote Desktop Services, which allows users to connect interactively to desktops and applications on remote computers, and the Fax Service, which enables users to send and receive faxes over the network using their computers.

It is important to note that the SSLF baseline is not an addition to the EC baseline: the SSLF baseline provides a distinctly different level of security. For this reason, do not attempt to apply the SSLF baseline and the EC baseline to the same computers running Windows 7. Rather, for the purposes of this guide, it is imperative to first identify the level of security that your environment requires, and then decide to apply either the EC baseline or the SSLF baseline. To compare the setting differences between the EC baseline and SSLF baseline, see the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide.

⚠️ Important  If you are considering whether to use the SSLF baseline for your environment, be prepared to exhaustively test the computers and business applications in your environment after you apply the SSLF security settings to ensure that they do not prohibit required functionality for the computers and processes in your environment.

Specialized Security

Organizations that use computers and networks, especially if they connect to external resources such as the Internet, must address security issues in system and network design, and how they configure and deploy their computers. Capabilities that include process automation, remote management, remote access, availability 24 hours a day, worldwide access, and software device independence enable businesses to become more streamlined and productive in a competitive marketplace. However, these
capabilities also increase the exposure of the computers of these organizations to potential compromise.

In general, administrators take reasonable care to prevent unauthorized access to data, service disruption, and computer misuse. Some specialist organizations, such as those in the military, state and local government, and finance are required to protect some or all of the services, systems, and data that they use with a specialized security level. The SSLF baseline is designed to provide this level of security for these organizations. To preview the SSLF settings, see the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide.

Limited Functionality

The specialized security the SSLF baseline implements may reduce functionality in your environment. This is because it limits users to only the specific functions that they require to complete necessary tasks. Access is limited to approved applications, services, and infrastructure environments. There is a reduction in configuration functionality because the baseline disables many property pages with which users may be familiar.

The following sections in this chapter describe the areas of higher security and limited functionality that the SSLF baseline enforces:

- Restricted services and data access
- Restricted network access
- Strong network protection

Restricted Services and Data Access

Specific settings in the SSLF baseline can prevent valid users from accessing services and data if they forget or misspell passwords. In addition, these settings may lead to an increase in help desk calls. However, the security benefits that the settings provide help make it harder for malicious users to attack computers running Windows 7 in this environment. Setting options in the SSLF baseline that could potentially prevent users from accessing services and data include those that:

- Disable administrator accounts.
- Enforce stronger password requirements.
- Require more strict account lockout policy.
- Require more strict policy for the following User Rights Assignments settings: Log on as a Service and Log on as a Batch Job.

Note Setting details for both the EC and the SSLF baselines are available in the Windows 7 Security Guide Settings Excel workbook that accompanies this guide to provide you with another resource to compare setting values.

Restricted Network Access

Network reliability and system connectivity is paramount for successful business. Microsoft operating systems provide advanced networking capabilities that help to connect systems, maintain connectivity, and repair broken connections. Although this capability is beneficial to maintaining network connectivity, attackers can use it to disrupt or compromise the computers on your network.

Administrators generally welcome features that help to support network communications. However, in special cases, the primary concern is the security of data and services. In such specialized environments, some loss of connectivity is tolerated to help ensure data protection. Setting options in the SSLF baseline that increase network security but could potentially prevent users from network access include those that:

- Limit access to client systems across the network.
- Hide systems from browse lists.
• Control Windows Firewall exceptions.
• Implement connection security, such as packet signing.

**Strong Network Protection**

A common strategy to attack network services is to use a denial of service (DoS) attack. Such an attack prevents connectivity to data or services or overextends system resources and degrades performance. The SSLF baseline protects access to system objects and the assignment of resources to help guard against this type of attack. Setting options in the SSLF baseline that help to prevent DoS attacks, include those that:
• Control process memory quota assignments.
• Control object creation.
• Control the ability to debug programs.
• Control process profiling.

All of these security considerations contribute to the possibility that the security settings in the SSLF baseline may prevent applications in your environment from running or users from accessing services and data as expected. For these reasons, it is important to extensively test the SSLF baseline after you implement it and *before* you deploy it in a production environment.

**Security Design**

The security design this chapter recommends forms the starting point for the scenarios in this guide, as well as the mitigation suggestions for the scenarios. The remaining sections in this chapter provide design details about the core security structure:
• **OU Design for Security Policies**
• **GPO Design for Security Policies**

Microsoft strongly recommends that you perform your own testing in a lab environment before deploying new security policies to production computers. The settings recommended in this guide and stored as security baselines in the SCM tool have been thoroughly tested. However, your organization’s network has unique business applications that may be impacted by some of these settings. Therefore, it is extremely important to thoroughly test the settings before implementing them on any production computers.

**OU Design for Security Policies**

The Microsoft security guides for Windows, Office, and Internet Explorer use organizational units (OUs). An *OU* is a container within a domain that uses AD DS. An OU may contain users, groups, computers, and other OUs. If an OU contains other OUs, it is a parent OU. An OU within a parent OU is a child OU.

You can link a GPO to an OU, which will then apply the GPO’s settings to the users and computers that are contained in that OU and its child OUs. And to facilitate administration, you can delegate administrative authority to each OU.

OUs provide an effective way to segment administrative boundaries for users and computers. Microsoft recommends that organizations assign users and computers to separate OUs, because some settings only apply to users and other settings only apply to computers.

You can delegate control over a group or an individual OU by using the Delegation Wizard in the Microsoft® Management Console (MMC) Active Directory Users and Computers snap-in tool. See the "More Information" section at the end of this chapter for links to documentation about how to delegate authority.
One of the primary goals of an OU design for any environment is to provide a foundation for a seamless Group Policy implementation that applies to all client computers in AD DS. This ensures that the client computers meet the security standards of your organization. The OU design must also provide an adequate structure to accommodate security settings for specific types of users in an organization. For example, developers may require access to their computers that average users do not. Also, laptop users may have different security requirements than desktop users.

The following figure illustrates a simple OU structure that is sufficient for the Group Policy discussion in this chapter. This OU structure may differ from the requirements of your organization’s environment.

**Figure 1.1 Example OU structure for computers running Windows 7 and Windows Server 2008**

**Domain Root**

You should apply some security settings throughout the domain to control how the domain, as a whole, is configured. These settings are contained in GPOs that apply to the domain. Computers and Users are not managed in this container.
Domain Controllers OU
Domain controllers hold some of the most sensitive data in your organization — data that controls the security configuration itself. You apply GPOs at this level in the OU structure to configure and protect the domain controllers.

Member Servers OU
This OU contains child OUs as described below. You should include settings that apply to all servers, but not to workstations, in the GPOs that you apply to this OU.

Server Role OUs
Microsoft recommends creating an OU for each server role that your organization uses. Each OU should contain only one type of server computer. You can then configure GPO settings and apply them to OUs that are specific to each role.

You can also choose to combine certain roles on the same server, if your organization requires it. For example, you may choose to combine the File and Print server roles. In this case, you can create an OU for these combined server roles called "File and Print Server," and then link the two role-specific GPO policies to that OU.

Important. Combining server roles on the same computer requires careful planning and testing to ensure that you do not negatively affect the overall security of the server roles that you combine.

Department OU
Security requirements often vary within an organization. For this reason, it may make sense to create one or more department OUs in your environment. This OU enables you to apply security settings from GPOs to computers and users in their respective department OUs.

Windows 7 Users OU
This OU contains the user accounts for the EC environment. The settings that you apply to this OU are described in detail in the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide.

Windows 7 Computers OU
This OU contains child OUs for each type of client computer running Windows 7 in the EC environment. This guide focuses on security guidance for desktop and laptop computers. For this reason, the engineers for this guide created the following computer OUs:

• Desktop OU. This OU contains desktop computers that constantly remain connected to the network. The settings applied to this OU are described in detail in the Windows 7 Security Baseline Settings Excel workbook.

• Laptop OU. This OU contains laptop computers for mobile users that are not always connected to the network. The Windows 7 Security Baseline Settings Excel workbook also provides details about the settings that apply to this OU.

GPO Design for Security Policies
A GPO is a collection of Group Policy settings that are essentially the files created by the Group Policy snap-in. The settings are stored at the domain level and affect users and computers contained in sites, domains, and OUs.

You can use GPOs to ensure that specific policy settings, user rights, and computer behavior apply to all client computers or users in an OU. Using Group Policy instead of a manual configuration process makes it simple to manage and update changes for many
computers and users. Manual configuration, which is inefficient because it requires a
technician to visit each client computer, is also potentially ineffective. This is primarily
because if the policy settings in domain-based GPOs are different than those applied
locally, the domain-based GPO policy settings will overwrite the locally applied policy
settings.

**Figure 1.2 GPO order of precedence**
The previous figure shows the order of precedence in which GPOs are applied to a
computer that is a member of the Child OU, from the lowest priority (1) to the highest
priority (5). Group Policy is applied first from the local security policy of each workstation.
After the local security policy is applied, GPOs are next applied at the site level, and then
at the domain level.

For computers running Windows Server 2008, Windows Server 2003 SP2 or later, and
Windows Vista SP1 or Windows XP Professional SP3 or later that are nested in several
OU layers, GPOs are applied in order from the parent OU level in the hierarchy to the
lowest child OU level. The final GPO is applied from the OU that contains the computer
account. This order of GPO processing for Group Policy—local security policy, site,
domain, parent OU, and child OU—is significant because settings in GPOs that are
applied later in the process will overwrite settings applied earlier. Different values for the
same setting configured in different GPOs are never combined. User GPOs are applied
in the same manner.

The following considerations apply when you design Group Policy:
- An administrator must set the order in which you link multiple GPOs to an OU, or
  Group Policy will be applied by default in the order it was linked to the OU, the order
  of precedence for the GPOs linked to the currently selected OU is shown in the Link
  Order list in the GPMC. If the same setting is configured in multiple policies, the
  policy that is highest on the policy list for the container will take precedence.
- You may configure a GPO with the **Enforced** option. However, if you select this
  option, other GPOs cannot override the settings that are configured in this GPO.
- Group Policy settings apply to users and computers, and are based on where the
  user or computer object is located in AD DS. In some cases, user objects may need
  policy applied to them based on the location of the computer object, not the location
  of the user object. The Group Policy loopback feature gives the administrator the
  ability to apply user Group Policy settings based on which computer the user is
  logged on to. The "Loopback Processing of Group Policy" article provides more
  information about this option.
- You may configure an Active Directory site, domain, or OU with the **Block policy
  inheritance** option. This option blocks GPO settings from GPOs that are higher in
  the Active Directory hierarchy unless they have the **Enforced** option selected. In
  other words, the **Enforced** option has precedence over the **Block policy
  inheritance** option.
Note  Administrators should only use the Enforced option and the Block policy inheritance option with utmost care because enabling these options can make troubleshooting GPOs difficult and cumbersome.

**Recommended GPOs**

To implement the OU design described above requires a minimum of the following GPOs:

- A policy for the domain.
- A policy to provide the baseline security settings for all domain controllers.
- A policy to provide the baseline security settings for all member servers.
- A policy for each server role in your organization.
- A policy for the Windows 7 Users OU.
- A policy for the Desktop OU.
- A policy for the Laptop OU.

The following figure expands on the preliminary OU structure to show the linkage between these GPOs and the OU design.
While the guide you are reading only covers a single product from Microsoft, the previous figure illustrates an environment that combines recommendations from the following security guides available in the Security Compliance Management Toolkit Series:

- Windows 7 Security Guide
- 2007 Microsoft Office Security Guide
- Internet Explorer 8.0 Security Guide

Presumably you network is running multiple versions of the Windows operating system and perhaps 2007 Office or Internet Explorer 2008. The combined example in the previous figure presents a notional AD DS design for OUs and Group Policy objects (GPOs). You will need to design your own OU hierarchy and Group Policy to fit the versions of Windows deployed in your environment, as well as settings for Microsoft Office or Internet Explorer as needed.
In the example in the previous figure, laptop computers are members of the Laptop OU. The first policy that is applied is the local security policy on the laptop computers. Because there is only one site in this example, no GPO is applied at the site level, which leaves the Domain GPO as the next policy that is applied. Finally, the Laptop GPO is applied.

Also in this figure, a File server is a member of the File Server OU. The first policy that is applied to the server is the local security policy. However, in general, little if any configuration of the servers is done by local policy. Security policies and settings should always be enforced by Group Policy.

Because there is only one File server in this example, no GPOs are applied at this level, which leaves the Domain GPO as the next policy that is applied to the servers. The Windows Server 2008 EC Baseline Policy is then applied to the Member Servers OU. Finally, any specific polices for the Web servers in the environment are applied to the Web Server OU.

As a precedence example, consider a scenario in which the policy setting for Allow logon through Terminal Services is set to apply to the following OUs and user groups:
• Member Servers OU – Administrators group
• Web Server OU – Remote Desktop Users and Administrators groups

In this example, logon through Terminal Services has been restricted to the Administrators group for servers in the Member Servers OU. However, a user whose account is in the Remote Desktop Users group can log on to a File server through Terminal Services because the File Servers OU is a child of the Member Servers OU and the child policy takes precedence.

If you enable the Enforced policy option in the GPO for the Member Servers OU, only users with accounts in the Administrators group can log on to the File server computer through Terminal Services. This is because the Enforced option prevents the child OU policy from overwriting the policy applied earlier in the process.

Using a GPO Created with the Security Compliance Manager Tool

The specific setting recommendations presented in this guide are available as pre-built baselines in the SCM tool. You can use these baselines created by Microsoft "as is", however most organizations will require some customization. When a baseline reflects your organization’s requirements, use the SCM tool to generate a GPO backup file. For more information about using the SCM tool, review the information available in the Help Topics for the tool. You can then use the Group Policy Management Consol (GPMC) to import the settings from the backed-up GPOs into your AD DS domain.

To import policy settings from a backed-up GPO into a GPO
1. In the GPMC console tree, expand Group Policy Objects in the forest and domain containing the GPO into which you want to import policy settings.
2. Right-click the GPO into which you want to import policy settings, and then click Import Settings.
3. When the Import Settings Wizard opens, follow the instructions in the wizard that opens, and then click Finish.
4. After the import operation completes, a summary will state whether the import succeeded. Click OK.

Using migration tables

Because some data in a GPO is domain-specific and might not be valid when copied directly to another domain, the GPMC provides migration tables. A migration table is a simple table that specifies a mapping between a source value and a destination value.
A migration table converts, during the copy or import operation, the references in a GPO to new references that will work in the target domain. You can use migration tables to update security principals and UNC paths to new values as part of the import or copy operation. Migration tables are stored with the file name extension .migtable, and are actually XML files. You do not need to know XML to create or edit migration tables; the GPMC provides the MTE for manipulating migration tables.

A migration table consists of one or more mapping entries. Each mapping entry consists of a source type, source reference, and destination reference. If you specify a migration table when performing an import or copy operation, each reference to the source entry is replaced with the destination entry when the policy settings are written into the destination GPO. Before you use a migration table, ensure that the destination references specified in the migration table already exist.

The following items can contain security principals and can be modified by using a migration table:

- Security policy settings of the following types:
  - User rights assignments.
  - Restricted groups.
  - System services.
  - File system.
  - Registry.
- Advanced folder redirection policy settings.
- The GPO Discretionary Access Control List (DACL), if it is preserved during a copy operation.
- The DACL on software installation objects, which is only preserved if the option to copy the GPO DACL is specified.

Also, the following items can contain UNC paths, which might need to be updated to new values as part of the import or copy operation, because servers in the original domain might not be accessible from the domain to which the GPO is being migrated:

- Folder redirection Group Policy settings.
- Software installation Group Policy settings.
- References to scripts, such as for logon and startup scripts, that are stored outside the source GPO. The script itself is not copied as part of the GPO copy or import operation, unless the script is stored inside the source GPO.

For more information about using the GPMC to import settings see the Group Policy Planning and Deployment Guide.

**Introducing the Local Policy Tool**

When you install the SCM tool, another utility called the Local Policy Tool (LPT) becomes available. This tool is designed to assist you with two optional tasks:

- Applying a security baseline to the local Group Policy of a computer.
- Exporting the local Group Policy of a computer to a group policy backup file.
- Updating the user interface of the Group Policy management tools.

You may want to apply the settings to the local Group Policy for stand-alone computers. You should update the user interface on the computers you will use to manage Group Policy so that you can view and manage the additional security settings discussed in this guide. The following sections discuss how to use the LPT to accomplish these tasks.

**Modifying Local Group Policy**

You can use the LPT to modify the local Group Policy of a computer by applying the security settings included in the GPOs described earlier. The LPT will apply the security
setting values recommended in this guide to modify the local policy. The tool does this by importing the settings from a GPO backup into the local Group Policy. Use the SCM tool to generate the GPO backup for the desired baseline.

**To apply a GPO backup file to the local Group Policy**

1. Log on as an administrator.
2. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
3. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.
   
   **Note** If prompted for logon credentials, type your user name and password, and then press **ENTER**.
4. At the command prompt, type `cscript LocalGPO.wsf /Path:<path>` and then press **ENTER** where `<path>` is the path to the GPO backup.
5. Completing this procedure modifies the local security policy settings using the values included in the GPO backup. You can use GPEdit.msc to review the configuration of the local Group Policy on your computer.

**To restore local Group Policy to the default settings**

1. Log on as an administrator.
2. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
3. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.
   
   **Note** If prompted for logon credentials, type your user name and password, and then press **ENTER**.
4. At the command prompt, type `cscript LocalGPO.wsf /Restore` and then press **ENTER**.

Completing this procedure restores all local policy settings to their default values.

**Exporting Local Group Policy to a GPO Backup**

You can use LPT to export a computer’s local Group Policy to a GPO backup file, which you can then apply to the local Group Policy of other computers or import into Active Directory.

**To export local Group Policy to a GPO backup file**

1. Log on as an administrator.
2. On the computer, click **Start**, click **All Programs**, and then click **LocalGPO**.
3. Right-click **LocalGPO Command Line**, and then click **Run as administrator** to open a command prompt with full administrative privileges.
   
   **Note** If prompted for logon credentials, type your user name and password, and then press **ENTER**.
4. At the command prompt, type `cscript LocalGPO.wsf /Path:<path> /Export` and then press **ENTER** where `<path>` is the path to the GPO backup.
5. Completing this procedure exports all local security policy settings to a GPO backup.

**Updating the Security Configuration Editor User Interface**

The solution presented in this guidance uses GPO settings that do not display in the standard user interface (UI) for the GPMC or the Security Configuration Editor (SCE) tool. These settings, which are all prefixed with **MSS:**, were developed by the Microsoft Solutions for Security group for previous security guidance.

For this reason, you need to extend these tools so that you can view the security settings and edit them as required. To accomplish this, the LPT automatically updates your computer while it creates the GPOs. Use the following procedure to update the SCE on the computers where you plan to manage the GPOs created with the SCM tool.

**To modify the SCE to display MSS settings**
Chapter 1: Implementing the Security Baseline

1. Ensure that you have met the following prerequisites:
   - The computer is joined to the domain using Active Directory where you created the GPOs.
   - The SCM tool is installed.
2. Log on as an administrator.
3. On the computer, click Start, click All Programs, and then click LocalGPO.
4. Right-click LocalGPO Command Line, and then click Run as administrator to open a command prompt with full administrative privileges.
   - Note: If prompted for logon credentials, type your user name and password, and then press ENTER.
5. At the command prompt, type cscript LocalGPO.wsf /ConfigSCE and then press ENTER.
   - Note: This script only modifies SCE to display MSS settings. This script does not create GPOs or OUs.

The following procedure removes the additional MSS security settings, and then resets the SCE tool to the default settings.

**To reset the SCE tool to the default settings**

1. Log on as an administrator.
2. On the computer, click Start, click All Programs, and then click LocalGPO.
3. Right-click LocalGPO Command Line, and then click Run as administrator to open a command prompt with full administrative privileges.
   - Note: If prompted for logon credentials, type your user name and password, and then press ENTER.
4. At the command prompt, type cscript LocalGPO.wsf /ResetSCE and then press ENTER.
   - Note: Completing this procedure reverts the SCE on your computer to the default settings. Any settings added to the default SCE will be removed. This will only affect the ability to view the settings with the SCE. Configured Group Policy settings remain in place.

**Domain Policy Settings**

A relatively small number of security settings are applied to the domain. These settings are applied through the Computer Configuration node in the Group Policy Object Editor. Within this node, the following setting groups appear in the Windows Settings subnode:

- **Password Policy Settings**
- **Account Lockout Policy Settings**

This section provides an overview of these two setting categories. For information about which specific settings are recommended for each role, review the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide. For detailed information about how each setting functions, the threats that each setting addresses, and the potential consequences of using each setting, read the companion guide, *Threats and Countermeasures*.

**Password Policy Settings**

Complex passwords that you change regularly help reduce the likelihood of a successful password attack. Password policy settings control the complexity and lifetime of passwords. You configure password policy settings using Group Policy at the domain level.

You can configure the password policy settings in the following location in the Group Policy Object Editor:

Solution Accelerators  microsoft.com/technet/SolutionAccelerators
How to Make Users Change Passwords Only When Required

In addition to these password policies, centralized control over all users is a requirement for some organizations. This section describes how to prevent users from changing their passwords except when they are required to do so.

Centralized control of user passwords is a cornerstone of a well-crafted Windows security scheme. You can use Group Policy to set minimum and maximum password ages. However, frequent password change requirements can enable users to circumvent the Enforce password history setting for your environment. Requirements for passwords that are too long may also lead to help desk calls from users who forget their passwords.

Users can change their passwords during the period between the minimum and maximum password age settings. However, the SSLF environment security design requires users to change their passwords only when prompted by the operating system after their passwords have reached the maximum age of 90 days. To achieve this level of control, administrators can disable the Change Password button in the Windows Security screen that appears when you press CTRL+ALT+DEL.

You can implement this configuration for an entire domain through Group Policy, or edit the registry to implement it for one or more specific users. For more information about this configuration, see "How To: Prevent Users from Changing a Password Except When Required in Windows Server 2003": Microsoft Knowledge Base article 324744.

Account Lockout Policy Settings

The account lockout policy is an AD DS security feature that locks a user account. The lock prevents users from logging on after a specified number of failed logon attempts occur within a specified period. Domain controllers track logon attempts and the number of allowed attempts, and the lockout period is based on the values configured for the account lockout settings.

These policy settings help prevent attackers from guessing user passwords, and they decrease the likelihood of successful attacks on your network environment. However, enabling account lockout policy can potentially result in more support issues for network users. Another drawback of configuring computers to automatically lock out accounts after a certain number of failed logons is that this could lead to a DoS condition. For example, some malware will attempt to connect to other computers using a list of account names collected previously and a dictionary of common passwords, if the account lockout threshold is configured this could cause the accounts of many users to be locked out.

You can minimize the risk of this type of DoS by configuring the account lockout duration to a relatively low value. Before you enable the following settings, ensure that your organization wants to accept this additional management overhead. For many organizations, an improved and less-costly solution is to automatically scan the Security event logs for domain controllers and generate administrative alerts when it appears that someone is attempting to guess passwords for user accounts.

You can configure the account lockout policy settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy
Computer Policy Settings

The security settings in this section apply to desktop and laptop computers in the domain. These settings are applied through the Computer Configuration node in the Group Policy Object Editor. Within this node, these settings appear in the Windows Settings and Administrative Templates subnodes in the Group Policy Object Editor.

The following sections discuss setting groups that appear within these subnodes:

• Audit Policy Settings
• User Rights Assignment Settings
• Security Options Settings
• Event Log Security Settings
• Windows Firewall with Advanced Security Settings
• Administrative Templates

This section provides an overview of these setting categories. For information about which specific settings are recommended for each role, review the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide. For detailed information about how each setting functions, the threats each setting addresses, and the potential consequences of using each setting, read the companion guide, Threats and Countermeasures.

Audit Policy Settings

An audit policy determines which security events to report to administrators so that there is a record of user or system activity in specified event categories. The administrator can monitor security-related activity, such as who accesses an object, when users log on to or log off from computers, or if changes are made to an Audit policy setting. For all of these reasons, we recommend that you form an Audit policy for an administrator to implement in your environment.

However, before you implement an Audit policy you must investigate which event categories to audit in your environment. The audit settings you choose within the event categories define your Audit policy. When you define audit settings for specific event categories, an administrator can create an Audit policy to meet the security needs of your organization.

If you do not configure audit settings, it will be difficult or impossible to determine what took place during a security incident. However, if you configure audit settings so that too many authorized activities generate events, the Security event log will fill up with too much data. The information in the following sections can help you decide what to monitor to facilitate the collection of relevant audit data for your organization.

Windows 7 includes the same nine audit policy categories present in previous versions of Windows, and adds an additional setting category called Global Object Access Auditing.

You can configure the Audit policy settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration

The following list provides a brief description of each setting category:

• Account Logon. The Account Logon audit category generates events for credential validation. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are
authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on.

- **Account Management.** The Account Management audit category helps you track attempts to create new users or groups, rename users or groups, enable or disable user accounts, change account passwords, and enable auditing for Account Management events. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user and group accounts.

- **Detailed Tracking.** The Detailed Tracking audit category determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Enabling **Audit process tracking** will generate a large number of events, so it is typically set to **No Auditing**. However, this setting can provide a great benefit during an incident response from the detailed log of the processes started and the time when they were launched.

- **DS Access.** The DS Access audit category applies only to domain controllers. For this reason, the DS Access audit category and all related subcategories are configured to **No Auditing** for both environments discussed in this guide.

- **Logon/Logoff.** This audit category generates events that record the creation and destruction of logon sessions. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource.

  If you configure the **Audit logon events** setting to **No auditing**, it is difficult or impossible to determine which user has accessed or attempted to access organization computers.

- **Object Access.** By itself, this policy setting will not cause auditing of any events. It determines whether to audit the event of a user who accesses an object—for example, a file, folder, registry key, or printer—that has a specified system access control list (SACL), effectively enabling auditing to take place.

  A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:
  - The security principal (user, computer, or group) to be audited.
  - The specific access type to be audited, called an access mask.
  - A flag to indicate whether to audit failed access events, successful access events, or both.

  If you configure the **Audit object access** setting to **Success**, an audit entry is generated each time that a user successfully accesses an object with a specified SACL. If you configure this policy setting to **Failure**, an audit entry is generated each time that a user fails in an attempt to access an object with a specified SACL.

  Organizations should define only the actions they want enabled when they configure SACLs. For example, you might want to enable the **Write and Append Data auditing** setting on executable files to track when they are changed or replaced, because computer viruses, worms, and Trojan horses typically target executable files. Similarly, you might want to track when sensitive documents are accessed or changed.

- **Policy Change.** The Policy Change audit category determines whether to audit every incident of a change to user rights assignment policies, Windows Firewall policies, Trust policies, or changes to the Audit policy itself. The recommended settings would let you see any account privileges that an attacker attempts to elevate—for example, by adding the **Debug programs** privilege or the **Back up files and directories** privilege.
• **Privilege Use.** The Privilege Use audit category determines whether to audit each instance of a user exercising a user right. If you configure this value to **Success**, an audit entry is generated each time that a user right is exercised successfully. If you configure this value to **Failure**, an audit entry is generated each time that a user right is exercised unsuccessfully. This policy setting can generate a very large number of event records.

• **System.** The System audit category allows you to monitor system events that succeed and fail, and provides a record of these events that may help determine instances of unauthorized system access. System events include starting or shutting down computers in your environment, full event logs, or other security-related events that affect the entire system.

• **Global Object Access Auditing.** This policy setting category allows you to configure a global system access control list (SACL) on the file system or Registry for an entire computer. This setting is new in Windows 7 and is ignored by previous version of Windows.

You can use **Advanced Audit Policy Configuration** in Windows 7 to easily configure the audit policy settings using Group Policy. However, this is not the case in Windows Vista. Although the audit subcategories were introduced in Windows Vista, they cannot be configured individually in Windows Vista because the subcategories are not exposed in the Group Policy Object Editor.


We recommend configuring only the necessary audit subcategories that your organization requires.

**Note** Descriptions of every audit policy subcategory is not provided in this guide. The companion guide, **Threats and Countermeasures**, includes detailed descriptions of each of the 50 audit policy subcategories.

**User Rights Assignment Settings**

In conjunction with many of the privileged groups in Windows 7, you can assign a number of user rights to certain users or groups that typical users do not have. To set the value of a user right to **No one**, enable the setting but do not add any users or groups to it. To set the value of a user right to **Not Defined**, do not enable the setting. You can configure the user rights assignment settings in Windows 7 at the following location in the Group Policy Object Editor:

    Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

**Security Options Settings**

The security option settings applied through Group Policy on computers running Windows 7 in your environment can enable or disable capabilities and features, such as floppy disk drive access, CD-ROM drive access, and logon prompts. You also can use these settings to configure various other settings, such as those that control digital signing of data, administrator and guest account names, and how driver installation works. You can configure the security option settings in the following location in the Group Policy Object Editor:

    Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
Not all of the settings that are included in this section exist on all types of systems. Therefore, the settings that comprise the Security Options portion of Group Policy that are defined in this section may need to be manually modified on systems in which these settings are present to make them fully operable. Alternatively, the Group Policy templates can be edited individually to include the appropriate setting options to make the prescribed settings take full effect.

MSS Settings

There are setting recommendations in this guide that use registry value entries that do not display by default through the Security Configuration Editor (SCE), the Group Policy Editor, or the Group Policy Management Console (GPMC). These settings are all prefixed with MSS:. They were originally developed by the Solutions Accelerators – Security and Compliance team (previously known as Microsoft Solutions for Security) for the Windows XP Security Guide. These settings are included in the security template portion of Group Policy, rather than the Administrative Templates portion. If the policy is removed, these settings are not automatically removed with it. They must be manually changed with a registry editing tool such as Regedt32.exe.

These additional settings are added to the SCE by modifying the Sceregvl.inf file (located in the %windir%\inf folder) and reregistering the Scecli.dll file. The original security settings as well as the additional ones appear under Local Policies\Security Options in the snap-ins and tools recommended in this guide. The SCE is used to define security templates that can be applied to individual computers or any number of computers through Group Policy. Security Templates can contain password policies, lockout policies, Kerberos protocol policies, Audit policies, event log settings, registry values, service startup modes, service permissions, user rights, group membership restrictions, registry permissions, and file system permissions. The SCE appears in a number of MMC snap-ins and administrator tools including the Security Templates snap-in, the Security Configuration and Analysis snap-in, the Group Policy Editor, Local Security Settings, Domain Controller Security Policy, and Domain Security Policy.

You should update the Sceregvl.inf file and reregister Scecli.dll as described in the "Introducing the Local Policy Tool" section earlier in this chapter.

Potential Issues with SMB Signing Policies

When Server Message Block (SMB) signing policies are enabled and a SMB version 1 client establishes a non-guest session or a non-anonymous session with a server, the client enables security signatures for the server. Later sessions then inherit the security signature sequence that is already established.

To improve security, Windows 7, Windows Vista, and Windows Server 2008 prevent server authenticated connections from being maliciously downgraded to a guest session or to an anonymous session. However, this improved security does not work as intended when the domain controller is running Windows Server 2003 and the client computers are running Windows Vista SP1 or Windows Server 2008. Specifically, this applies if the policies in the following locations are enabled on a domain controller that is running Windows Server 2003:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)
- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)

The following policies are enabled on a member computer running Windows Vista with SP1 or Windows Server 2008 in the same domain:

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)
Reducing the Use of NTLM Authentication

NT LAN Manager (NTLM) authentication is ubiquitous on many corporate networks even though more secure authentication protocols have been available in Windows for many years. There are new security policies in Windows 7 and Windows Server 2008 to help you analyze and restrict NTLM authentication usage in your IT environment. Exploiting these features requires data gathering, analysis of NTLM traffic, and a methodical process with which to restrict the traffic so that stronger authentication protocols, such as Kerberos, will be used. Reducing the usage of the NTLM protocol requires both knowledge of deployed application requirements on NTLM and strategies and steps necessary to configure infrastructures to use other protocols.

The first step in restricting the NTLM protocol on your network is to understand which computers and applications in your organization are using the NTLM protocol for authentication. You can find this information by enabling certain security policies for auditing on computers running Windows 7. By reviewing the event logs, you can determine which applications can be configured to successfully use a stronger authentication protocol and also determine computers or domains that can function without the NTLM protocol. Once you understand how NTLM is being used on your network you can use new Group Policy settings in Windows 7 and Windows Server 2008 to restrict NTLM protocol usage on clients, servers, and domain controllers. These policies can be configured on computers running Windows 7 and Windows Server 2008, which can affect NTLM usage on computers running earlier versions of Windows. For more information, see Introducing the Restriction of NTLM Authentication.

Event Log Security Settings

The event log records events on the system, and the Security log records audit events. You can use the event log container of Group Policy to define attributes that are related to the Application, Security, and System event logs, such as maximum log size, access rights for each log, and retention settings and methods. You can configure the event log settings in the following location in the Group Policy Object Editor:

Administrative Templates\Windows Components\Event Log Service

Windows Firewall with Advanced Security Settings

The firewall included with Windows 7 is very similar in structure to the firewall in Windows Vista. The firewall in Windows 7 allows for precise control of its configuration via the Windows Firewall with Advanced Security settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings \Windows Firewall with Advanced Security

To control these settings, within the Windows Firewall with Advanced Security section of the Group Policy Object Editor, click the Windows Firewall Properties link. In the Windows Firewall with Advanced Security dialog box, you can specify settings for the Domain, Private, and Public profiles. For each profile, you can specify general settings in the State section and then, in the Settings section, you can click the Customize button.
to specify customized settings. This section includes an overview of each of the profiles that you can configure in the Windows Firewall with Advanced Security dialog box.

In Windows Vista, firewall policy is based on the network connection "type," which could be one of four options — such as Home, Work, Public, or Domain.

While this helped to solve a number of security issues related to the firewall in Windows XP with SP1, there were still some scenarios that could present problems for computer users and support staff. For example, if a user connected to the Internet through a "Home" network, and then used virtual private networking to access to a corporate network. In such a case, because the network type (and thus the firewall settings) had already been set based on the first network to which the user connected, the firewall settings appropriate for accessing the corporate network could not be applied.

Windows 7 addresses these scenarios by supporting multiple active firewall policies. This enables a computer to obtain and apply a domain firewall profile regardless of other active networks on the computer. This functionality allows IT professionals to simplify connectivity and security policies by maintaining a single set of rules for both local and remote clients.

**Domain Profile**

This profile applies when a computer is connected to a network and authenticates to a domain controller in the domain to which the computer belongs. The recommended Windows Firewall with Advanced Security configuration for the EC environment includes firewall rules that allow for Remote Desktop and Remote Assistance communications to occur. Furthermore, local administrators of computers in the EC environment can configure local firewall rules to permit additional communications to a computer.

In the SSLF environment, all inbound communications are blocked by default and local firewall rules are ignored by computers. Additions or modifications to firewall rules must be configured using the Group Policy Object Editor.

**Important** The prescribed firewall settings for the SSLF environment greatly limit inbound connections to your computers. You should extensively test this firewall configuration in your environment to ensure all applications work as expected.

To see which rules are defined for the Domain Profile, within the Windows Firewall with Advanced Security section of the Group Policy Object Editor, click the Inbound Rules link.

**Private Profile**

This profile only applies if a user with local administrator privileges assigns it to a network that was previously set to use the Public profile. We recommend only changing the profile to Private for a trusted network. The recommended Windows Firewall with Advanced Security configuration for the EC environment includes firewall rules that allow for Remote Desktop communications to occur. Furthermore, local administrators of computers in the EC environment can configure local firewall rules to permit additional communications to a computer. In the SSLF environment, all inbound communications are blocked by default and local firewall rules are ignored by computers. Additions or modifications to firewall rules must be configured using the Group Policy Object Editor.

To see which rules are defined for the Private Profile, within the Windows Firewall with Advanced Security section of the Group Policy Object Editor, click the Inbound Rules link.

**Public Profile**

This profile is the default network location type when the computer is not connected to a domain. Public profile settings should be the most restrictive because the computer is connected to a public network where security cannot be as tightly controlled as within an IT environment. In both the EC and SSLF environments, all inbound communications are
blocked by default and no firewall rules exist that allow for additional communications to a computer. Furthermore, local firewall rules are ignored by computers in both environments described in this guide. Additions or modifications to firewall rules that apply to the Public Profile must be configured using the Group Policy Object Editor.

**Computer Configuration\Administrative Templates**

The following setting groups for the computer policy contain settings that this guide prescribes. The settings appear in the **Computer Configuration\Administrative Templates** subnode of the Group Policy Object Editor.

- Network
  - BranchCache
  - Network Connections
- System
  - Logon
  - Group Policy
  - Power Management
  - Remote Assistance
  - Remote Procedure Call
  - Internet Communication Management\Internet Communication Settings
- Windows Components
  - Autoplay Policies
  - Credential User Interface
  - Event Log Service
  - HomeGroup
  - Remote Desktop Services
  - Windows Explorer
  - Windows Remote Shell
  - Windows Update

**Windows Update**

Administrators use Windows Update settings to manage how updates and hotfixes are applied on Windows 7–based workstations. Updates are available from Windows Update. Alternatively, you can set up an intranet Web site to distribute updates and hotfixes in a similar manner with additional administrative control.

*Windows Server Update Services* (WSUS) is an infrastructure service that builds on the success of the Microsoft Windows Update and Software Update Services (SUS) technologies. WSUS manages and distributes critical Windows updates that resolve known security vulnerabilities and other stability issues with Windows operating systems. WSUS eliminates manual update steps with a dynamic notification system for critical updates that are available to Windows–based client computers through your intranet server. No Internet access is required from client computers to use this service. This technology also provides a simple and automatic way to distribute updates to your Windows–based workstations and servers.

Windows Server Update Services also offers the following features:

- **Administrator control over content synchronization within your intranet.** This synchronization service is a server-side component that retrieves the latest critical updates from Windows Update. As new updates are added to Windows Update, the
server running WSUS automatically downloads and stores them, based on an administrator-defined schedule.

- **An intranet-hosted Windows Update server.** This easy-to-use server acts as the virtual Windows Update server for client computers. It contains a synchronization service and administrative tools for managing updates. It services requests for approved updates from client computers that are connected to it through the HTTP protocol. This server can also host critical updates that are downloaded from the synchronization service and refer client computers to those updates.

- **Administrator control over updates.** The administrator can test and approve updates from the public Windows Update site before deployment on their organization’s intranet. Deployment takes place on a schedule that the administrator creates. If multiple servers are running WSUS, the administrator controls which computers access particular servers that run the service. Administrators can enable this level of control with Group Policy in an Active Directory environment or through registry keys.

- **Automatic updates on computers (workstations or servers).** Automatic Updates is a Windows feature that can be set up to automatically check for updates that are published on Windows Update. WSUS uses this Windows feature to deploy administrator approved updates from an update server located on the intranet.

**Note:** If you choose to distribute updates through another method, such as Microsoft System Center Configuration Manager, this guide recommends that you disable the **Configure Automatic Updates** setting.

There are several Windows Update settings. A minimum of three settings is required to make Windows Update work: **Configure Automatic Updates**, **No auto-restart for scheduled Automatic Updates installations**, and **Reschedule Automatic Updates scheduled installations**. A fourth setting is optional and depends on the requirements of your organization: **Specify intranet Microsoft update service location**.

You can configure the following prescribed computer settings in the following location within the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components \Windows Update
```

Configuring Windows Update is essential to the security of the computers in your environment because it helps ensure that the client computers receive security updates from Microsoft soon after they are available.

**Note**  Windows Update depends on several services, including the Remote Registry service and the Background Intelligence Transfer Service.

### More Information

The following resources provide additional information about Windows 7 security-related topics on Microsoft.com:

- [Back Up, Restore, Copy, and Import](#) page on the Windows Server TechCenter.
- [Enterprise Management with the Group Policy Management Console](#).
- "Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled": Microsoft Knowledge Base article 950876.
- "How To: Prevent Users from Changing a Password Except When Required in Windows Server 2003": Microsoft Knowledge Base article 324744.
- [Introducing the Restriction of NTLM Authentication](#).
• "Loopback Processing of Group Policy": Knowledge Base article 231287.
• Migrating GPOs Across Domains with GPMC.
• Best Practices for Delegating Active Directory Administration.
• "Security guidance configuration support": Microsoft Knowledge Base article 885409 that includes detailed information about the potential impact some settings may have on previous Windows versions.
• Threats and Countermeasures.
• Windows 7 Security Enhancements.
• Well-known security identifiers in Windows operating systems.
• Windows Firewall.
• Windows Server Update Services (WSUS).
Chapter 2: Defend Against Malware

Malicious software (also called malware), is any program or file that is harmful to a computer user. Examples of malware include computer viruses, worms, Trojan horse programs, rootkits, and spyware that can gather information about a computer user without their permission.

Windows® 7 builds on the technologies introduced in Windows Vista®. These technologies include several new ones that you can use to help enhance your protection against malware on computers running Windows 7 in your environment. You can use these features and services in addition to the settings prescribed in the Group Policy objects (GPOs) in the previous chapter, some of which also help to provide protection against malware.

Windows® Internet Explorer® 8 is available in Windows 7. This version of Internet Explorer includes several significant security enhancements that help prevent the installation of unwanted software, and technologies that help guard against unauthorized transmission of personal data that greatly increase browser security and privacy protection. Also new in this version of the browser is the option to completely remove it from a Windows 7 installation if required. For these reasons, all the details of how to take full advantage of the new security capabilities in Internet Explorer 8 are available in the Internet Explorer 8 Security Compliance Management Toolkit.

This chapter provides overviews of the security technologies in Windows 7, and recommendations on how to configure them when applicable. You can implement these recommendations in the appropriate GPOs described in Chapter 1, "Implementing the Security Baseline." However, it is important to note that many of the settings for these technologies require information specific to your environment. For this reason, most of the recommended values for these additional settings are not included in the GPOs described in the previous chapter.

All of these technologies are by default configured to provide enhanced protection for computers running Windows 7 in the Enterprise Client (EC) environment. However, there are some new Group Policy settings that you can use to help customize the behavior and functionality of these technologies to provide even better protection against malware for your environment.

**Note** For each major section in the chapter, specific Group Policy settings are highlighted to document the default configuration for a new installation of Windows 7. Specific setting modifications or recommendations are denoted with the ‡ symbol. For more details on these setting values, see the Windows 7 Security Baseline Settings workbook that accompanies this guide.
Windows 7 Defense Technologies

Windows 7 includes the following new and enhanced technologies that provide improved defense against malware:

• Action Center
• User Account Control (UAC)
• Biometric Security
• Windows Defender
• Malicious Software Removal Tool
• Windows Firewall
• AppLocker

In addition to these protection technologies, it is important to understand that logging in as a standard user account is still a highly recommended security practice.

Also Microsoft strongly recommends installing a real-time antivirus scanning solution such as Forefront Client Security to help protect your computer against new threats as they are developed. If your organization is using a defense-in-depth strategy you may wish to evaluate using additional scanning services that are available from Microsoft as part of Windows 7 or as additional downloaded services.

Even with all these protection technologies in place, if you are not protecting who has the ability to gain administrative level access to your computers, you are exposing all computers users in your environment to risk.

Action Center

In Windows Vista, security configuration options are accessed from the Security Center in Control Panel. In Windows 7, the Security Center has been absorbed into the new Action Center. The Action Center has security configurations as well as options for other administrative tasks such as backup, troubleshooting, diagnostics, and Windows Update tasks. The scope of security messages that you can turn on or off in the Action Center appears in the Change Action Center settings dialog box in Figure 2.1.
Figure 2.1 The Change Action Center settings dialog box
In addition to reporting issues of users running Windows 7, the Action Center also controls how such issues are reported to Microsoft to discover potential solutions. The reporting options available to you appear in Figure 2.2.

Figure 2.2 The Action Center Problem Reporting Settings dialog box

Solution Accelerators  
microsoft.com/technet/SolutionAccelerators
Any user can view reporting information sent to Microsoft using the following steps:
5. Open the main Action Center window.
6. Click Maintenance.
7. Under Check for solutions to problem reports, click View reliability history.
8. In the list of reliability details, double-click any item to view its technical details.

Items listed under Informational events usually detail changes to the computer's software and hardware configuration.

For more information about reporting problems and your privacy, see the Privacy Statement for the Windows Error Reporting Service.

Using Group Policy to Mitigate Risk for the Action Center

You can review and configure the available UAC settings in two locations in the Group Policy Object Editor:

Computer Configuration\Windows Components\Windows Error Reporting

The following table provides security setting information specific to this technology in Windows 7.

Table 2.1 Windows Action Center Settings

<table>
<thead>
<tr>
<th>Policy object</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Windows Error Reporting</td>
<td>If this setting is enabled, Windows Error Reporting will not send any problem information to Microsoft. In addition, solution information will not be available in the Action Center Control Panel.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

User Configuration\Start Menu and Taskbar\

The following table provides security setting information specific to this technology in Windows 7.

Table 2.2 Windows Action Center Settings

<table>
<thead>
<tr>
<th>Policy object</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove the Action Center icon</td>
<td>Prevents the Action Center in the system control area from displaying. If you enable this setting, the Action Center icon will not display in the system notification area. If you disable or do not configure this setting, the Action Center icon will display in the system notification area.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

User Account Control

Windows Vista introduced User Account Control (UAC) to make it easier to use an account that does not have administrative privileges. UAC consists of several technologies: the Protected Administrator (PA) account, UAC elevation prompts, registry virtualization, file system virtualization, and Windows Integrity levels. While using an account configured as a PA is somewhat more secure than using an unprotected administrator account, it is even more secure to use a standard user account for daily activities. Many tasks that could only be done by administrators in previous versions of Windows can be completed by standard users in Windows Vista. The risk of malware installing unauthorized software or making unapproved system changes is reduced by the performing day-to-day tasks with an account that only has standard user privileges.
In Windows 7, you can configure the type and frequency of UAC notifications. There are four basic levels that you can configure using the UAC settings option in the Action Center:

- **Always notify me when**: This option causes UAC to always notify you when you install software or make any changes to Windows settings.
- **Default – Notify me only when programs try to make changes to my computer**: This option causes UAC to notify you when programs make changes, but not if you make changes to Windows settings. This is the default setting in Windows 7.
- **Notify me only when programs try to make changes to my computer (do not dim my desktop)**: This option causes UAC to notify you only when programs make changes, but turns off Secure Desktop, which dims the desktop while the UAC prompt displays.
- **Never notify me when**: This option causes UAC to not notify the user if programs try to install software or make changes to the computer or if the user attempts to make administrator level changes to Windows settings. This option is not recommended.

When UAC technology was first introduced, frequent notifications caused some users to disable them. In Windows 7, the number of elevation prompts has been lowered by making it possible for standard users to perform more tasks. Also, when a using a PA account some programs included with Windows 7 are able to automatically elevate without displaying a prompt.

- We recommend maintaining the Windows 7 default setting of **Notify me only when programs try to make changes to my computer** as a minimum requirement, and to consider increasing the notification frequency to **Always notify** in environments where client computers are often connected to public networks or if security is a high priority. Using a less secure value increases the likelihood of malware making undesirable changes to the computer.

The **Administrator Approval Mode** feature in UAC provides limited protection for computers running Windows 7 and Windows Vista Service Pack 1 (SP1) from some types of malware. Most programs and tasks included with Windows 7 will function as expected with standard user privileges. When users need to perform administrative tasks, such as installing new software or modifying certain system settings, they are first prompted for consent before they can complete such tasks. However, this mode does not provide the same level of protection as a standard user account, and it does not guarantee that malicious software already on the client computer cannot tamper with the elevated software. This mode also does not guarantee that the elevated software itself will not attempt malicious actions after it is elevated.

**Risk Assessment**

Users with administrative privileges log on with their administrative capabilities enabled. This could allow administrative tasks to occur accidentally or maliciously without the knowledge of the individual, as in the following examples:

- A user unknowingly downloads and installs malware from a malicious or infected Web site.
- A user is tricked into opening an e-mail attachment that contains malware, which runs and possibly installs itself on the computer.
- A removable drive is inserted into the computer and the **AutoPlay** feature then attempts to run the malicious software automatically.
- A user installs unsupported applications that can affect the computers performance or reliability.
Risk Mitigation

We recommend that all users log on using a standard user account for everyday tasks. While UAC can be used to elevate privileges by providing credentials for an administrator account, you should instead open a separate desktop session for the administrator account using Fast User Switching. Also, ensure that UAC is enabled to prompt the user when an attempt is made to perform a task that requires administrative privileges.

Mitigation Considerations

UAC can help mitigate the risks described in the previous "Risk Assessment" section. However, it is important to consider the following:

• If you have in-house application developers, we recommend requesting that they download and review the "Windows Vista Application Development Requirements for User Account Control Compatibility" article. This document describes how to design and develop UAC–compliant applications.

• Applications that are not compliant with UAC can cause problems with the default UAC protection levels. For this reason, it is important to test applications with UAC before you deploy them. For more information about application compatibility testing, see Chapter 4, "Application Compatibility with Windows 7" later in this guide.

• The administrative credential and privilege escalation requests of UAC increase the number of steps required to complete many administrative tasks. You should evaluate the affect of the increased steps on your administrative staff. If the additional UAC prompts significantly affect these users, you can configure the UAC policy setting Behavior of the elevation prompt for administrators in Admin Approval Mode to the option Elevate without prompting. However, changing this weakens the computer's security configuration and raises the risk of legacy malware in your environment.

• A user who has administrative privileges operating as a PA can disable Administrator Approval Mode, disable UAC from prompting for credentials to install applications, and change the elevation prompt behavior. For this reason, you cannot guarantee your UAC policies are in place if you allow users to have access to administrative privileges on the computers in your organization.

• We recommend assigning two accounts for administrative staff. For everyday tasks, staff should use a standard level account. When specific administrative tasks are required, staff should log on with an administrative level account, perform the tasks, and then log off to return to the standard user account.

• The Group Policy settings for this guide disable a standard user’s ability to elevate privileges, note that this is the default behavior for computers that belong to an Active Directory domain. This is the recommended approach because it enforces that administrative tasks can only be performed by accounts that have specifically been set up at the administrative level.

• If an application is incorrectly identified as an administrative or user application, Windows might start the application under the wrong security context. For example, with an "administrator" or "standard" token.
# Mitigation Process

Start the mitigation process by investigating the full capabilities of UAC. For more information, see [Understanding and Configuring User Account Control in Windows Vista](#) and [Getting Started with User Account Control on Windows Vista](#).

## To use this mitigation process

1. Identify the number of users who are able to carry out administrative tasks.
2. Identify how often administrative tasks are required.
3. Determine if administrators should be able to perform administrative tasks by simply agreeing to the UAC prompt, or if they should be required to enter specific credentials to perform administrative tasks.
4. Determine if standard users should have the ability to elevate privileges to perform administrative tasks. The policy settings applied as part of this guide specifically block the ability for standard users to elevate their privileges.
5. Identify how application installations should be handled.
6. Configure the UAC Group Policy settings to suit your requirements.

## Using Group Policy to Mitigate Risk for UAC

You can review and configure the available UAC settings in the following location in the Group Policy Object Editor:

```
Computer Configuration\Windows Settings\Security Settings\Local Policy\Security Options\User Account Control\
```

The following table provides security setting information specific to this technology in Windows 7.

## Table 2.3 Windows UAC Settings

<table>
<thead>
<tr>
<th>Policy object</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Control: Admin Approval Mode for the built-in Administrator account</td>
<td>This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account.</td>
<td>Disabled</td>
</tr>
<tr>
<td>User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop</td>
<td>This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user.</td>
<td>Disabled</td>
</tr>
<tr>
<td>User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode</td>
<td>This policy setting controls the behavior of the elevation prompt for administrators.</td>
<td>Prompt for consent for non-Windows binaries</td>
</tr>
<tr>
<td>User Account Control: Behavior of the elevation prompt for standard users</td>
<td>This policy setting controls the behavior of the elevation prompt for standard users.</td>
<td>Prompt for credentials on the secure desktop</td>
</tr>
<tr>
<td>User Account Control: Detect application installations and prompt for elevation</td>
<td>This policy setting controls the behavior of application installation detection for the computer.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Policy object</td>
<td>Description</td>
<td>Windows 7 default</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>User Account Control: Only elevate executable that are signed and validated</td>
<td>This policy setting enforces public key infrastructure (PKI) signature checks for any interactive applications that request elevation of privilege. Enterprise administrators can control which applications are allowed to run by adding certificates to the Trusted Publishers certificate store on local computers.</td>
<td>Disabled</td>
</tr>
<tr>
<td>User Account Control: Only elevate UIAccess applications that are installed in secure locations</td>
<td>This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system.</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Run all Administrators in Admin approval Mode</td>
<td>This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer.</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Switch to the secure desktop when prompting for elevation</td>
<td>This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop.</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Account Control: Virtualize file and registry write failures to per-user locations</td>
<td>This policy setting controls whether application write failures are redirected to defined registry and file system locations.</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the **Explain** tab of the setting in the Group Policy Object Editor.

**Biometric Security**

Windows 7 includes the Windows Biometric Framework that exposes fingerprint readers and other biometric devices to higher-level applications in a uniform way, and offers a consistent user experience for discovering and launching fingerprint applications. Previous versions of Windows have supported the use of fingerprint sensors to log on to the computer, and many laptops now come with fingerprint sensors, but third-party drivers and software are required to use them. This support is now part of the Windows 7 operating system and all that is required is the driver for the reader hardware.

**Risk Assessment**

The standard password verification methods have a number of problems that can lead to security risks in your environment. If you only employ a password only authentication mechanism, users may write passwords down, passwords can be overheard, users can forget them, and simple passwords may become subject to brute force attacks that can guess them.
To strengthen your password security, require multifactor authentication by adding a device such as a smartcard as part of the process. This requires users to provide something *that they know* (a password) and *something that they have* (the smartcard). This improves on the password only verification approach. However, smartcards and smartcard devices may still be susceptible to theft, loss, or possibly even unauthorized altering.

**Risk Mitigation**

Adopting the Biometric support in Windows 7 allows an organization to implement an additional layer of verification by requiring users to provide *something that that is a part of them*. This helps to mitigate the risks associated with password and smart card based approaches. While the Biometric support in Windows 7 can support many different types of biometric authentication, the availability and low cost of fingerprint readers make this form of biometric authentication the most likely to be adopted in many organizations.

Fingerprint identification offers the following advantages:

- Fingerprints normally remain constant throughout life.
- No two fingerprints have ever been found to be the same (not even those of identical twins).
- Fingerprint scanners have become more affordable.
- The scanning process is fast and simple.
- The reliability of the scan is high, which is to say that it has a low false acceptance rate (FAR) compared to other forms of biometric scanning, such as face recognition or voice analysis.

This form of identification also has some disadvantages:

- Users with injured fingers may be unable to authenticate.
- Researchers have shown that it’s possible to trick some fingerprint recognition systems into granting access when a fraudulent data is presented.
- A user’s age or job responsibilities may prevent reliable fingerprint scanning.

**Mitigation Considerations**

If your organization intends to adopt a biometric verification mechanism, such as fingerprint scanning, as part of your Windows 7 deployment there are a number of considerations to plan for in advance:

- Biometric systems typically require that personal indefinable information is stored on the computer that performs the authentication. This can cause privacy issues for an organization to manage.
- Many modern laptop computers now come with built-in fingerprint readers to make deployment of biometrics simpler however the sophistication and accuracy of these built-in devices may not be as robust and precise of dedicated solutions. You can compare the quality of systems by examining various metrics such as false rejection rate, false acceptance rate, crossover error rate, failure to enroll rate, and throughput rate.
- If your environment includes areas where users or computers are exposed to situations where clean hands may be difficult to maintain or where gloves are required, fingerprint scanners cannot be used. Such difficulties could be overcome by using systems that rely on other physiological data like retinas, faces, or hand geometry.
- Users should be required to provide an additional piece of unique data along with the biometric evidence such as a passphrase, PIN, or smartcard. It is possible to fool some biometric devices by impersonating users. For example, a group of Japanese researchers demonstrated using imitation fingers made of gelatin to bypass some systems. For more information, see [Impact of Artificial "Gummy" Fingers on Fingerprint Systems](#).
Mitigation Process

The specifics of each organization's biometric deployment are unique to their particular environment. However, there are a number of stages that need to be addressed to ensure that the solution meets your needs and helps to improve your organization's authentication process. To effectively use the Biometrics, consider the following process.

To use this mitigation process

1. Investigate the various biometric verification mechanisms to determine which solution best meets your organization's needs.
2. Review your organization's privacy policy documentation and ensure privacy issues introduced by biometrics are addressed.
3. Determine the physical hardware requirements for the biometric solution and establish a timeline to deploy those requirements.
4. Determine the infrastructure requirements for the biometric solution, such as Public Key infrastructure or client software deployment requirements.
5. Identify employees who may have trouble utilizing the biometric system and find alternatives for them. Establish an alternate authentication processes for these users such as usernames with a password or smartcards with a PIN.
6. Educate users ahead of time about the biometric authentication system and the alternate processes for those who cannot use the new system.
7. Conduct a pilot program that encompasses a wide range of users to identify and resolve problems before the full deployment is undertaken.
8. Enroll users into the biometric system by following the manufacturer's instructions for scanning and verifying their biometric data.
9. Train users on how to use the system, assist any users who encounter difficulties.
10. Anticipate the possibility that some users will strongly resist using a biometric system, plan to allow such users to utilize an alternate authentication process.

Using Group Policy to Mitigate Risk for Biometrics

You can review and configure the available biometrics settings in the following location in the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Biometrics
```

The following table provides security setting information specific to this technology in Windows 7.

### Table 2.4 Biometric Control Settings

<table>
<thead>
<tr>
<th>Policy object</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow the use of biometrics</td>
<td>If you enable (or do not configure) this policy setting, the Windows Biometric Service users can run applications that require biometrics on Windows.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Allow users to log on using biometrics</td>
<td>This policy setting determines whether users can log on or elevate UAC permissions using biometrics. By default, local users can log on to the local computer.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Allow domain users to log on using biometrics</td>
<td>This policy setting determines whether domain users can log on or elevate UAC permissions using biometrics. By default, domain users cannot use biometrics to log on.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>
Policy object | Description | Windows 7 default
---|---|---
Timeout for fast user switching events | This policy setting specifies the number of seconds a pending fast-user switch event remains active before the switch is initiated. By default, a fast user switch event is active for 10 seconds before it becomes inactive. | Not configured

This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor.

**Windows Defender**

Windows Defender is an antispyware service that was initially available as an optional download for Windows® XP. This service has now been integrated into Windows® and runs automatically by default. This service can help protect your computer against spyware and other potentially unwanted software. Spyware can be installed on your computer without your knowledge any time you connect to the Internet, and it can infect your computer when you install some programs using removable media. Windows Defender offers both real-time scanning protection and a scheduled full scanning option.

The dialog in Figure 2.3 displays the recommended settings for a computer running Windows 7 with Windows Defender enabled.

![Figure 2.3 Configuring Windows Defender automatic scanning options](image)

When a program tries to modify a protected area in Windows 7, Windows Defender prompts the user to either allow or reject the change in an effort to guard against spyware installation.

You can configure Windows Defender via Group Policy settings in Windows 7 to control a variety of Windows Defender behavior. The Group Policy settings described in the following sections do not contain any settings that modify the default behavior of Windows Defender. This is because the values for these settings are likely to be specific to the requirements of your environment.
Microsoft SpyNet Community

Microsoft® SpyNet is an online community dedicated to helping a computer user choose how to respond to potential spyware threats. The community also helps stop the spread of new spyware infections.

When Windows Defender detects software or changes by software not yet classified as security risks, you can see how other members of the community are responding to the alert. In turn, actions you take help other members choose how to respond. Your actions also help Microsoft choose which software to investigate for potential threats. You can choose to send basic or additional information about detected software. Additional information helps improve how Windows Defender works. For example, the technology can include the location of detected items on your computer if harmful software has been removed. In these cases, Windows Defender will automatically collect and send the information to the community. For more information on the type of information that is sent in Microsoft SpyNet reports, see the Windows Defender Privacy Policy.

Risk Assessment

Spyware presents a number of serious risks to an organization that must mitigate them to ensure that its data and computers are not compromised. The most common identifiable risks that spyware create for organizations include:

- Sensitive business data that could be exposed to unauthorized users.
- Employee personal information that could be exposed to unauthorized users.
- Computer compromise by an unauthorized attacker.
- Lost productivity because of spyware that affects computer performance and stability.
- Support cost increases because of spyware infections.
- A potential blackmail risk to your organization if an infection exposes sensitive data.

Risk Mitigation

Windows Defender is designed to mitigate risks related to spyware. Regular updates for the technology are provided automatically via Windows Update or you can use Microsoft Windows Server Update Services (WSUS).

In addition to the spyware protection that Windows Defender offers, Microsoft also strongly recommends installing an antivirus package that is capable of extending your spyware protection to detect viruses, Trojan horse programs, and worms. For example, products such as Microsoft Forefront™ Client Security provide unified malware defense for business desktops, laptops, and server operating systems.

Mitigation Considerations

Windows Defender is enabled by default in Windows 7. The technology is designed to be as unobtrusive as possible to users under normal conditions. However, consider the following recommendations as part of deploying Windows 7 for your organizations:

- Test the interoperability of any third-party real-time spyware or antivirus scanners that you may want to use in your organization.
- Design a system to manage signature definition update deployments if your organization manages a large number of computers.
- Train users in some of the common tricks that spyware programs employ to socially engineer a user into running a malicious program.
- Adjust the scheduled scan time to suit the needs of your organization. The default time is 2:00 A.M. daily. If the computer is not able to perform the scan at this time, the user is later notified and asked to run a scan. If the scan does not occur within the next two days, it will occur approximately 10 minutes after the computer is next started. In Windows 7, the scan runs as a low priority process to minimize its effect...
on the client's performance as much as possible. The low priority scan has a much lower performance affect than it did on users running Windows XP.

- Windows Defender is not designed as an enterprise class antispyware application. It does not provide centralized reporting, monitoring, or a control mechanism. If additional reporting or control is required, you will need to investigate additional products such as Microsoft Forefront Client Security.
- Determine a policy for your organization to report possible spyware to the Microsoft SpyNet online community.

**Mitigation Process**

Windows Defender is a default part of Windows 7. For this reason, no additional steps are required to activate Windows Defender. However, there are a few additional steps that we recommend considering to ensure that your organization stays protected.

**To use this mitigation process**

1. Investigate antispyware capabilities of Windows 7 and Windows Defender.
2. Investigate the Group Policy settings for Windows Defender.
3. Evaluate additional antivirus protection for your organization and determine if it provides antispyware capabilities as well as antivirus protection.
4. Plan the optimal update process for the computers in the organization. Mobile computers may need a different update configuration than desktop computers.
5. Provide training to enable users to identify suspicious computer activity.
6. Provide training to support staff to use Windows Defender tools to help resolve support calls.

**Using Group Policy to Mitigate Risk for Windows Defender**

You can review and configure the available Windows Defender settings in the following location in the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\Windows Defender
```

The following table provides security setting information specific to this technology in Windows 7.

**Table 2.5 Windows Defender Control Settings**

<table>
<thead>
<tr>
<th>Policy object</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn on definition updates through both WSUS and Windows Update</td>
<td>This setting allows you to configure Windows Defender to check and install definition updates from Windows Update when a locally managed WSUS server is not available.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Turn on definition updates through both WSUS and the Microsoft Malware Protection Center</td>
<td>This setting allows you to configure Windows Defender to check and install definition updates from both Windows Update and the Microsoft Malware Protection Center when a locally managed Windows Server Update Services (WSUS) server is not available.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>
This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor.

### Malicious Software Removal Tool

The Microsoft Windows Malicious Software Removal Tool (MSRT) is a small executable program designed to help identify and remove selected high risk malware from Windows computers. Every month, Microsoft releases a new version of the tool through Microsoft Update, Windows Update, WSUS, and the Microsoft Download Center. When the tool runs, it scans your computer in the background and produces a report if it detects any infections. This tool does not install in the operating system it is scanning and it does not have any Group Policy settings that it uses in Windows. The reporting log for MSRT is stored at %SystemRoot%\Debug\mrt.log.

The MSRT is not designed to serve as an enterprise-class antivirus application. It does not provide centralized reporting, monitoring, or a control mechanism. If additional...
reporting or control is required, you will need to investigate additional products such as Microsoft Forefront Client Security.

**Risk Assessment**

We recommend running a real-time antivirus scanner on all the computers in your organization in addition to the protection services provided in Windows 7. However, even with these protection measures installed, there are two risks that can still apply to organizations:

- If the installed real-time antivirus scanner does not detect a specific instance of malware.
- If the malware manages to disable the installed real-time antivirus scanner.

For these situations, the MSRT does provide an additional layer of security to help detect and remove common malicious software. The complete list of malware removed by the MSRT is described in [Malware Families Cleaned by the Malicious Software Removal Tool](https://microsoft.com).

**Risk Mitigation**

To help mitigate these risks, we recommend that you configure your client computers to run Automatic Updates so that the MSRT will download and run them as soon as they are released. The MSRT is designed to mitigate risks related to malicious software that Microsoft identifies as particularly prevalent or high risk to Windows users.

**Mitigation Considerations**

If you are considering whether to use this tool in your environment, the following list highlights some considerations to help ensure a successful deployment:

- The Malicious Software Removal Tool (MSRT) is approximately 9 MB in size, which can affect an organization’s Internet connection if a large number of client computers attempt to download the tool at the same time.
- The tool is primarily intended for noncorporate users who do not have an existing, up-to-date antivirus product installed on their computers. However, you also can deploy the tool in an enterprise environment to enhance existing protection and as part of a defense-in-depth strategy. To deploy the tool in an enterprise environment, you can use one or more of the following methods:
  - Windows Server Update Services
  - SMS Software Package
  - Group Policy–based computer startup script
  - Group Policy–based user logon script

For enterprise environments, we recommend reviewing "Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment"; Knowledge Base article 891716.

- The MSRT provides no real-time protection so Microsoft also strongly recommends installing an antivirus package that is capable of extending your protection to detect viruses, Trojan horse programs, and worms in real time. For example, products such as Microsoft Forefront Client Security provide unified malware defense for business desktops, laptops, and server operating systems.
- Typically, when you run the Windows Malicious Software Removal Tool, the tool creates a randomly named temporary directory in the root of the drive with the most free disk space on your computer, which is typically the root or system drive. This directory will contain several files and includes the Mrtstub.exe file. Most of the time, this folder is deleted automatically after the tool has finished running or after the computer next restarts. But sometimes this folder may not be deleted automatically.
In these cases, you can delete this folder manually with no adverse effect on the computer.

**Mitigation Process**

To effectively use the Malicious Software Removal Tool, use the following process.

**To use this mitigation process**

1. Investigate the Malicious Software Removal Tool capabilities.
   
   For more information, see the Malicious Software Removal Tool Web page.

2. Assess the need for the tool in your environment.

3. Determine the most appropriate method of deploying the tool in your organization.

4. Identify the systems in your organization that can benefit from the protection that the tool offers.

5. Deploy the tool via the selected deployment method.

**Windows Firewall**

A personal firewall is a critical line of defense against many kinds of malware. Like the firewall functionality available since the release of Windows XP Professional SP2, the firewall in Windows 7 is turned on by default to help protect the user’s computer as soon as the operating system is operational.

Windows Firewall in Windows 7 uses the same approach as that in Windows Vista and includes both inbound and outbound filtering to help protect users by restricting operating system resources that behave unexpectedly. Windows 7 also uses the same Windows Firewall with Advanced Security console user interface that was introduced in Windows Vista. This interface centralizes inbound and outbound traffic filtering, and IPsec server and domain isolation settings in the user interface to simplify configuration and reduce policy conflicts.

Windows Firewall with Advanced Security supports the following environment profiles:

- **Domain Profile.** This profile applies when a computer is connected to a network and authenticates to a domain controller in the domain to which the computer belongs.

- **Public Profile.** This profile is the default network location type when the computer is not connected to a domain. Public profile settings should be the most restrictive because the computer is connected to a public network where security cannot be as tightly controlled as within an IT environment.

- **Private Profile.** This profile only applies if a user with local administrator privileges assigns it to a network that was previously set to Public. We recommend only doing this for a trusted network.

In Windows Vista, only one network profile can be active on the computer at a time. However, in Windows 7, you can make multiple per-network adapter profiles active at once. If there are multiple network adapters connected to different networks, each network adapter applies the firewall profile that is the most appropriate for the type of network to which it is connected: Private, Public, or Domain. For example, if you are at a coffee shop with a wireless hotspot and connect to your corporate domain network by using a VPN connection, the Public profile continues to protect the network traffic that does not go through the tunnel, and the Domain profile protects the network traffic that goes through the tunnel. This also addresses the issue of a network adapter that is not connected to a network as this unidentified network will be assigned the Public profile, and other network adapters on the computer will continue to use the profile that is appropriate for the network to which they are attached.
Risk Assessment

A network connection is a vital requirement in modern business. However, this connection has also become a major target for attackers. The threats associated with connectivity need to be mitigated to ensure that data or computers are not compromised. The most commonly identifiable threats to an organization from network-based attacks include:

- A computer that is compromised by an unauthorized attacker who could then gain administrative level access to that computer.
- Network scanner applications that an attacker can use to remotely determine open network ports to launch an attack.
- Sensitive business data that could be exposed to unauthorized users if a Trojan horse program can open an unauthorized network connection from a client computer to an attacker.
- Mobile computers that may be exposed to network attacks while outside the organization's network firewall.
- Computers on an internal network that could be exposed to a network attack from a compromised computer that connects directly to the internal network.
- A potential blackmail risk to your organization if an attacker successfully compromises internal computers.

Risk Mitigation

The firewall in Windows 7 provides protection to the client computer out of the box. The firewall blocks most unsolicited inbound traffic until a change is made either by an administrator or by Group Policy.

Windows Firewall also includes outbound network traffic filtering, and out of the box this rule is set to "Allow" for all outgoing network traffic. You can use Group Policy settings to configure these rules in the Windows 7 firewall to ensure that client security settings remain constant.

Mitigation Considerations

There are a few issues to consider if you are planning to use the firewall in Windows 7:

- Test the interoperability of applications that are required on your organization's computers. Each application should have a record of the network port requirements to help ensure only the required ports are opened through the Windows Firewall.
- Like Windows Vista, the Windows 7 firewall supports the Domain, Private, and Public profiles to provide a fine level of control to protect a client computer when a user operates it outside of the organization's network defenses.
- Evaluate the logging capacities of the Windows Firewall to determine its ability to integrate into your existing enterprise reporting or monitoring solutions.
- By default Windows Firewall blocks remote control or remote management of Windows 7–based computers. Microsoft has created a number of rules specifically for such remote tasks in the Windows Firewall. If you want your organization's computers to support these remote tasks, enable the required rules for each profile that the task requires. For example, you may choose to enable the Remote Desktop rule for the Domain profile to allow your help desk to support users on the organization's network. However, you also may choose to leave it disabled for the Public and Private profiles to reduce the attack surface of your computers when they are off your network.
Mitigation Process
Windows 7 includes Group Policy settings and management UI that assist you with configuring the functionality available in the Windows Firewall. The advanced security settings for Windows 7 do apply to Windows Vista computers, but they do not apply on client computers running Windows XP or to Windows XP Mode virtual machine images.
If you plan to modify the default behavior of the Windows Firewall, we recommend using the Windows Firewall with Advanced Security Group Policy settings to manage client computers running Windows Vista or Windows 7.
You can review and configure the new Group Policy settings and management snap-in available for Windows Firewall in the following location in the Group Policy Object Editor:

   Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security

We recommend enabling Windows Firewall with Advanced Security for all three profiles. In addition to the advanced firewall rules, Windows Firewall also supports connection security rules. Connection security involves authenticating two computers before they start communications, and securing information sent between the two computers. Windows Firewall with Advanced Security incorporates IPsec technology to support key exchange, authentication, data integrity, and optionally, data encryption.
For more information, see the IPsec Web page on Microsoft TechNet.
The Windows 7 Security Baseline Settings workbook that accompanies this guide describes all of the prescribed Windows Firewall with Advanced Security settings, and indicates which settings require environment-specific information.

AppLocker
Windows 7 includes and updated and improved version of Software Restriction Policies called AppLocker. This feature is easier to use and provides new capabilities and extensions that reduce administrative overhead and help administrators control how users can access and use files, such as executable files, scripts, Windows Installer files, and dynamic-link library (DLL) files. You can use AppLocker with domain Group Policy or on the local machine with the Local Security Policy snap-in.

Risk Assessment
Whenever a user installs an unauthorized application on a company computer, there are risks associated with that process. At a minimum, the installation process modifies the attack surface of the computer and creates the risk of starting additional services or opening firewall ports. But even if these concerns prove not to be the case, now there is an additional application installed on the computer to maintain to help ensure that it does not become a target of an application layer attack seeking to exploit a vulnerably that the application itself introduced.
Finally, it is possible that the application is malicious in intent and was installed either by mistake or intentionally by the user, which can then launch an attack on other systems after the computer connects to the organizations network.

Risk Mitigation
AppLocker enables administrators to implement a set of application control policies that can significantly reduce an organization’s risk to attacks that can result from unauthorized applications being installed on the computers you manage. AppLocker allows you to mitigate risks associated with application installations by allowing you to do the following:
• Define rules based on file attributes derived from the digital signature, including the publisher, product name, file name, and file version. For example, you can create
rules based on the publisher attribute that is persistent through updates, or you can create rules for a specific version of a file.

- Assign a rule to a security group or an individual user.
- Create exceptions to rules. For example, you can create a rule that allows all Windows processes to run except Registry Editor (Regedit.exe).
- Use audit-only mode to deploy the policy and understand its impact before enforcing it.
- Import and export rules. The import and export affects the entire policy. For example, if you export a policy, all of the rules from all of the rule collections are exported, including the enforcement settings for the rule collections. If you import a policy, the existing policy is overwritten.
- Simplify creating and managing AppLocker rules by using AppLocker PowerShell cmdlets.

**Mitigation Considerations**

If you are considering whether to use this tool in your environment, the following list highlights some considerations to help ensure a successful deployment:

- It is important to thoroughly test all of the application control policies before you deploy them to a production environment. Mistakes in the design or implementation of this feature can cause considerable disruption to a user’s productivity.
- Plan to spend time evaluating the application usage models for your organization using the audit-only feature of AppLocker to ensure you fully understand the scope of applications your users need before implementing restrictions.
- Consider a staged roll out plan starting with users who have a high risk usage pattern of application installation or on computers that contain sensitive data.

**Mitigation Process**

AppLocker appears under the Application Control Policies node in the Group Policy Editor. Windows 7 still supports Software Restriction Policies as well.

**Note:** AppLocker is not available in the consumer editions of Windows 7.

**Using Group Policy to Mitigate Risk with AppLocker**

You can review and configure the available AppLocker settings in the following location in the Group Policy Object Editor:

`Computer Configuration\Windows Settings\Security Settings\Application Control Policies`

This guide does not provide recommendations on which applications to consider blocking on the client computers you manage, as this is obviously specific to the requirements of each organization. For more information about how to plan for and deploy AppLocker policies in your organization, see the [AppLocker Technical Documentation for Windows 7 and Windows Server 2008 R2](https://technet.microsoft.com/en-us/library/bb730886.aspx).

**Software Restriction Policies**

The Software Restriction Policies provided in Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 are still available and supported in Windows 7. Administrators can still use these policies as a way to identify application software and control its ability to run on local computers. However, due to the significant usability enhancements provided by AppLocker in Windows 7, we recommend replacing Software Restriction Policies with AppLocker policies. For this reason, they are not covered in this guide. For more information about how to design and implement these policies, see "[Using Software Restriction Policies to Protect Against Unauthorized Software](https://technet.microsoft.com/en-us/library/bb730886.aspx)" on TechNet.
More Information

The following resources provide additional information about enhanced security features and technologies in Windows 7 on Microsoft.com:

- [AppLocker Technical Documentation for Windows 7 and Windows Server 2008 R2](#).
- "Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment": Knowledge Base article 891716.
- [Impact of Artificial "Gummy" Fingers on Fingerprint Systems](#).
- [Internet Explorer 8 Security Compliance Management Toolkit](#).
- [IPsec](#).
- [Forefront Client Security](#).
- [Getting Started with User Account Control on Windows Vista](#).
- [Malicious Software Removal Tool](#).
- [Malware Families Cleaned by the Malicious Software Removal Tool](#).
- [Privacy Statement for the Windows Error Reporting Service](#).
- [Windows Defender](#).
- [Windows Defender Privacy Policy](#).
- [Windows Firewall](#).
- [Windows Server Group Policy](#).
- [Windows Server Update Services (WSUS)](#).
- "Windows Vista Application Development Requirements for User Account Control Compatibility" article.
- [Understanding and Configuring User Account Control in Windows Vista](#).
- [User Account Control](#).
- [Using Software Restriction Policies to Protect Against Unauthorized Software](#).
Chapter 3: Protect Sensitive Data

Effective technology features and services to help counter the risk of data theft or exposure was a primary customer request for Microsoft to include in Windows Vista®. In Windows® 7, these features have been enhanced and extended.

Microsoft has developed both new and enhanced features and services to help organizations better protect the data that resides on their client computers. The features and services this chapter discusses are designed to protect data on client computers running Windows 7 in the Enterprise Client (EC) environment. The configuration of these features depends on the specific requirements of your environment. This chapter provides you with a design process to identify how to configure the following features and services to better meet your data protection needs:

- Optimize cryptographic randomization
- BitLocker™ Drive Encryption
- Encrypting File System (EFS)
- Rights Management Services (RMS)
- Device management and installation

You can use BitLocker, EFS, RMS, and device management and installation to help protect sensitive data in the enterprise. However, each technology and method performs specific functions to help secure data. In fact, all these technologies and methods are complimentary elements of data protection, and Microsoft highly recommends using them as part of an enterprise’s overall security strategy. You can use each one separately or together, depending on the security needs of your organization. The following table provides examples of how these technology features and services work to protect data in different scenarios within an enterprise.

Table 3.1 Data Protection Technology Comparison in Windows 7

<table>
<thead>
<tr>
<th>Scenario</th>
<th>BitLocker</th>
<th>EFS</th>
<th>RMS</th>
<th>Device management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop data protection</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Branch office server data protection</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local single-user file and folder protection</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Desktop data protection</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Removable drive protection</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared computer file and folder protection</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Remote file and folder protection</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Untrusted network administrator protection</td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>
Optimize Cryptographic Randomization

If a Trusted Platform Module (TPM) is installed and enabled Windows 7 will use it to provide seed material for the Windows Random Number Generator (RNG). The RNG is used to generate cryptographic keys for various applications. The randomness of cryptographic keys will be improved when generated in this manner rather than purely in software. For this reason, it is recommended that you access your PC’s BIOS and enable the TPM hardware.

By default, Windows 7 gathers RNG seed material from the TPM at boot time, and every 40 minutes thereafter. There are three configuration items can be used to control this behavior, the default values are ideal for most scenarios therefore you may not need to configure any of them.

The setting TpmBootEntropy is managed in the Boot Configuration Data (BCD). When set to false it disables boot-time entropy gathering from the TPM on a TPM-enabled machine. The default value is true on a normal boot and false in Safe Mode and Safe Mode With Networking. This option is available both on BIOS and EFI systems. For more information about managing settings stored in the BCD, see Boot Configuration Data in Windows Vista and BCDEdit Commands for Boot Environment.

The refresh interval determines how frequently (in minutes) entropy is periodically gathered from the TPM. When it is set to zero, no entropy is gathered in this way. This value does not affect boot-time entropy gathering from the TPM. Care must be taken when changing this value because configuring a smaller interval can reduce the Mean Time To Failure of some vendor TPM implementations. This setting is stored in the HKey_Local_Machine registry hive as a DWORD value called TpmRefreshEntropyIntervalInMinutes, located at \Software\Policies\Microsoft\Cryptography\RNG. The default value is 40, valid values range from 0 to 40.

You can also specify the number of millibits of entropy per byte of output from the TPM RNG. This setting is stored in the HKey_Local_Machine registry hive as a DWORD value called TpmEntropyDensityInMillibitsPerByte, located at \System\CurrentControlSet\Control\Cryptography\RNG. The default value is 8000, valid values range from 1 to 8000.

### Scenario

<table>
<thead>
<tr>
<th>Scenario</th>
<th>BitLocker</th>
<th>EFS</th>
<th>RMS</th>
<th>Device management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote document policy enforcement</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect content in transit</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect content during collaboration</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Protect against data theft</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Note** For each of these areas in the chapter, specific Group Policy settings are highlighted to document the default configuration for a new installation of Windows 7. Specific setting modifications or recommendations are denoted with the ✓ symbol. For more details on these setting values, see the Windows 7 Security Baseline Settings workbook.
Chapter 3: Protect Sensitive Data

**BitLocker Drive Encryption**

BitLocker Drive Encryption in Windows 7 has been improved to allow you to protect data on all hard drives on a client computer, including removable data drives such as USB flash drives and IEEE 1394 drives.

When enabled for operating system (OS) drives BitLocker Drive Encryption can lock the normal boot sequence until the user provides the credentials required by BitLocker. While it is possible to use a USB flash drive to hold the decryption keys, the maximum protection is obtained when a Trusted Platform Module (TPM 1.2) is used to protect the encryption keys and prevent software-based attacks on system integrity or security of data stored on the drives. You can configure the TPM to perform a preboot check of the boot components on the hard disk to ensure that they have not changed.

For more information about TPM technology, refer to the specifications and materials maintained on the [Trusted Computing Group](https://www.trustedcomputinggroup.org) Web site. If no TPM is available, BitLocker can still help protect the data, but no system integrity validation is performed.

BitLocker is available in the Windows 7 Enterprise and Ultimate editions of the operating system for client computers.

The options available to you in BitLocker map to the following key user scenarios:

- Protecting operating system drives.
- Protecting fixed data drives.
- Protecting removable data drives.

   The details of these scenarios are provided in the following sections of this chapter.

- **Note** BitLocker is also available to protect disk drives on Windows Server® 2008 and later. However, this scenario is not covered as part of this guide.

- **Note** Although you can save a Windows Virtual PC virtual hard disk (VHD) file on a file system that is protected by BitLocker, you cannot use the VHD for native boot or enable BitLocker on the volume(s) that are contained inside a VHD.

**Protecting Operating System and Fixed Data Drives**

In this scenario you can use BitLocker to protect all fixed drives on a computer whether they contain the operating system files or additional data files. This is the recommended configuration to ensure that all data on the system is protected by BitLocker.

**Risk Assessment**

One of the primary risks that BitLocker is designed to mitigate is data theft from stolen or lost mobile computers. When an attacker gains physical access to a computer, the potential consequences include the following unauthorized acts:

- The attacker can log on to Windows 7 and copy files.
- The attacker can restart the client computer into an alternate operating system to:
  - View file names.
  - Copy files.
  - Read the contents of the hibernation file or paging file to discover plaintext copies of in-process documents.
  - Read the contents of the hibernation file to discover plaintext copies of software private keys.

Even if files are encrypted using EFS, a careless user might move or copy a file from an encrypted location to an unencrypted location, which could leave the file information formatted in plaintext. Uninformed IT staff might also neglect to encrypt hidden folders, where applications keep backup copies of in-process files. There are also operational...
risks, such as unauthorized personnel tampering and modification of system and boot files, which may prevent normal system operation.

**Risk Mitigation**

To mitigate these risks, configure the computer to use BitLocker encryption to require an integrity check of boot components and pre-boot authentication prior to granting access to an encrypted operating system drive. In addition, ensure to protect the operating system and data files.

**Mitigation Considerations**

When used on operating system drives and fixed data drives BitLocker can mitigate the risks defined in the previous "Risk Assessment" section. However, before you use BitLocker, it is important to consider the following requirements and best practices for this data protection feature:

- In order to use BitLocker in the optimal configuration, the motherboard on the client computer must provide a TPM 1.2 chip that includes a Trusted Computing Group–compliant BIOS implementation. The recommended configuration is to require a user-configured PIN to unlock the system. Optionally, you can also use a startup key on a USB flash drive with a machine-readable key written to it.

- The hard drive must contain at least two partitions: the operating system partition and the active system partition. The operating system partition is where the Windows operating system files are installed that will be encrypted. The active system partition must remain unencrypted so that the computer can start, and this partition must be at least 100 MB in size. By default in Windows 7, the system partition is automatically created, is not be given a letter, and is hidden from users. If your computer does not have a separate, active system partition, the partitions on the drive will be modified during BitLocker setup.

- If you use BitLocker with a USB key or a PIN, you must establish procedures to address lost keys and forgotten PINs.

- BitLocker does have a small effect on system performance, but this is typically unnoticeable. However, if system performance is critical, you may want to test the configuration to ensure that the BitLocker overhead does not significantly affect user productivity.

- Depending on the computer vendor, TPM management tools may require manual steps to configure the TPM device state and a BIOS administrator password during the build process, which may prevent fully automated or scripted system deployments and upgrades.

- To use a startup key to unlock the operating system drive during the boot sequence, the computer BIOS must be able to read USB drives in the preboot environment.

- BitLocker may have an impact on your software distribution procedures if software or system updates are distributed overnight remotely, and you restart computers without the users present. The following examples illustrate this potential impact:
  - If a computer has a protector type of TPM and a PIN or a TPM and a startup key, and at 2:00 A.M. you deploy a software update to the computer that requires the computer to restart, the computer will not restart without the PIN or startup key.
  - If you currently use Wake-on-LAN or a BIOS auto-power on feature to start computers for maintenance purposes, these computers also will be affected by a TPM and PIN or startup key protector.

- OEM-distributed BIOS/TPM firmware updates may affect BitLocker-enabled computers. A BIOS update may cause the TPM to register a change in the pre-boot components and result in the TPM going into recovery. If this is a concern, BitLocker should be suspended prior to the update being installed and then resumed post-update.
• Although it is unlikely, application updates may affect BitLocker-enabled computers. If, during installation or updating, the updates make changes to the boot manager or files that BitLocker measures, this will cause a system boot failure and force the computer into recovery mode. Before installing or updating applications that affect the Windows 7 boot environment, test them on BitLocker-enabled computers.

• All domain controllers in the domain must be running Windows Server® 2003 Service Pack 2 (SP2) or later.

  Note  Windows Server 2003 requires you to extend the schema to support storing BitLocker recovery information in Active Directory® Directory Services (AD DS).

Mitigation Process

Use the following risk mitigation process to assess how best to configure BitLocker to help protect sensitive data on the client computers that you manage.

To use this mitigation process

1. Investigate BitLocker technology and capabilities.

   Note  For more information about BitLocker, see BitLocker Drive Encryption on Microsoft TechNet and the Windows BitLocker Drive Encryption Design and Deployment Guides.

2. Assess the need for BitLocker in your environment.

3. Confirm that the hardware, firmware, and software that your organization uses meet BitLocker requirements.

4. Identify the systems in your organization that require BitLocker protection.

5. Identify the level of protection your systems require. A PIN or USB key containing encryption keys can be required to start the operating system. The operating system will not start without these keys.

6. Install necessary drivers on a test system.

7. Use Group Policy objects (GPOs) to configure BitLocker on test systems.

8. After a successful test, install the drivers and configure BitLocker on production systems.

9. Use Group Policy to control options for enabling and managing BitLocker.

Using Group Policy to Mitigate Risk for BitLocker

There are two Group Policy templates that we recommend using to manage the configuration of BitLocker. These templates allow you to manage TPM configuration separately from the rest of BitLocker. The following table outlines the Group Policy settings available for BitLocker in the VolumeEncryption.admx template. You can configure these settings in the following location in the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption

In Windows 7 there are three levels of policy settings organized under this path:

• Fixed Data Drives
• Operating System Drives
• Removable Data Drives
At the global settings level the following Group Policy settings are available.
§ Denotes Group Policy settings that are new in Windows 7.

**Table 3.2 Global BitLocker Drive Encryption Settings**

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store BitLocker recovery information in Active Directory Domain Services</td>
<td>Manages the AD DS backup of BitLocker recovery information. This policy only applies to computers running Windows Server 2008 or Windows Vista.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Choose default folder for recovery password</td>
<td>Specifies the default path that is displayed when the BitLocker setup wizard prompts the user to enter the location of a folder in which to save the recovery password.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Choose how users can recover BitLocker-protected drives</td>
<td>Controls whether the BitLocker setup wizard can display and specifies BitLocker recovery options.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Choose drive encryption method and cipher strength</td>
<td>Configures the algorithm and cipher strength used by BitLocker. BitLocker uses a default encryption method of AES 128-bit with Diffuser.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Provide the unique identifiers for your organization</td>
<td>Allows you to associate unique organizational identifiers to a new drive that is enabled with BitLocker.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Prevent memory overwrite on restart</td>
<td>Controls computer restart performance at the risk of exposing BitLocker secrets.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Validate smart card certificate usage rule compliance</td>
<td>Allows you to associate an object identifier from a smart card certificate to a BitLocker-protected drive.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor.

The following table outlines the Group Policy settings available for the TPM in the TPM.admx template. You can configure these settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\System\Trusted Platform Module Services**

**Table 3.3 Trusted Platform Module Settings**

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn on TPM backup to Active Directory Domain Services</td>
<td>Manages the AD DS backup of Trusted Platform Module (TPM) owner information.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Configure the list of blocked TPM</td>
<td>Manages the Group Policy list of TPM commands blocked by Windows.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>
Chapter 3: Protect Sensitive Data

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore the default list of blocked TPM commands</td>
<td>Manages enforcement of the computer’s default list of blocked TPM commands.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Ignore the local list of blocked TPM commands</td>
<td>Manages enforcement of the computer’s local list of blocked TPM commands.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor.

**Fixed Data Drives Settings**

Settings specific to fixed drives that contain user or application data but not operating system data are contained in the following location in the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives

The following table outlines the Group Policy settings that are available for BitLocker in the VolumeEncryption.admx template. At the Fixed Data Drives settings level, the following Group Policy settings are available.

**Table 3.4 Fixed Data Drives Settings**

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ Configure use of smart cards on fixed data drives</td>
<td>Specifies whether smart cards can be used to authenticate user access to the BitLocker-protected fixed data drives on the computer.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Deny write access to fixed drives not protected by BitLocker</td>
<td>Determines whether BitLocker protection is required for fixed data drives to be writable on the computer.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Allow access to BitLocker-protected fixed data drives from earlier versions of Windows</td>
<td>Configures whether fixed data drives formatted with the FAT file system can be unlocked and viewed on computers running Windows Server 2008, Windows Vista, Windows XP SP3, or Windows XP SP2 operating systems.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Configure use of passwords for fixed data drives</td>
<td>Specifies whether a password is required to unlock BitLocker-protected fixed data drives. It also specifies password length and complexity requirements.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Choose how BitLocker-protected fixed drives can be recovered</td>
<td>Allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor.
Operating System Drives Settings

For settings that are specific to drives that contain operating system data, you can use the settings in the following location within the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives

At the Operating System Drives settings level, the following Group Policy settings are available.

Table 3.5 BitLocker Operating System Drives Settings

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ Require additional authentication at startup</td>
<td>Configures whether BitLocker allows or requires additional authentication each time the computer starts and whether you are using BitLocker with or without a TPM.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Require additional authentication at startup (Windows Server 2008 and Windows Vista)</td>
<td>Controls whether the BitLocker setup wizard can set up an additional authentication method that is required each time the computer starts.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Allow enhanced PINs for startup</td>
<td>Configures whether BitLocker can use enhanced startup PINs.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Configure minimum PIN length for startup</td>
<td>Minimum length for TPM startup PINs. This policy setting is applied when you turn on BitLocker. The startup PIN must have a minimum length of 4 digits and can have a maximum length of 20 digits.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Choose how BitLocker-protected operating system drives can be recovered</td>
<td>Controls how BitLocker-protected operating system drives are recovered in the absence of the required startup key information.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Configure TPM platform validation profile</td>
<td>Configures how the computer’s TPM security hardware secures the BitLocker encryption key.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the setting’s Explain tab in the Group Policy Object Editor.

Your security policies must effectively support BitLocker password and key management. These policies should be comprehensive enough to secure the information, but not make BitLocker difficult to support. The following list includes policy examples:

- Always require backup of recovery passwords in AD DS.
- Always require backup of TPM owner information in AD DS.
- Use recovery keys and recovery passwords as a backup recovery method.
- If you are using TPM and a PIN or USB startup keys, change them on a regular scheduled basis.
- On TPM-enabled computers, use a BIOS administrator password to prohibit access.
- Ensure that users do not store key material, such as USB startup keys, with the computer.
- Save recovery keys to a central location for support and disaster recovery purposes.
- Backup recovery material to secure offline storage.

Solution Accelerators  
microsoft.com/technet/SolutionAccelerators
Protecting Removable Data Drives

In this scenario you can use BitLocker to protect removable data disk drives, such as external USB, IEEE 1394 drives, SD cards, or USB flash drives. BitLocker To Go is a new technology in Windows 7 that allows organizations to use removable drives in a manner that protects the data on the drives from unauthorized access, even if the drive is lost or stolen.

Risk Assessment

Removable drives present a significant risk to an organization’s sensitive data. Such devices have become so affordable and available that it is possible for huge amounts of sensitive data to be quickly copied and removed in a very short time.

In addition, laptop computers and removable USB flash drives are often exposed to threats such as theft and loss while they are in transit. Both of these scenarios could lead to sensitive data falling into unauthorized hands.

Risk Mitigation

To mitigate this risk, organizations have gone to many lengths, including banning the devices, disabling USB and IEEE 1394 ports, and configuring computers to protect the boot sequence so that the system will only start when authorized. In addition, they have taken steps to ensure to protect the operating system and data files.

BitLocker To Go provides a robust protection layer that means that even if an attacker gains physical access to the drive, such a situation no longer has to mean that the attacker has access to the data stored on the drive. Using Group Policy, organizations can require removable drives to use BitLocker To Go to protect a drive before data can be copied to it.

Mitigation Considerations

BitLocker can mitigate the risks defined in the previous "Risk Assessment" section. However, before using BitLocker on removable data drives, it is important to consider the following requirements and best practices for this data protection feature:

• BitLocker To Go does not require a TPM chip.
• Drives encrypted with BitLocker To Go can be configured to require either a password or smart card, if you specify smart cards, ensure that all computers where the removable drives will be accessed have smart card readers available.
• BitLocker does have a small effect on system performance, but this is typically unnoticeable. However, if system performance is critical, you may want to test the configuration to ensure that the BitLocker overhead does not significantly affect user productivity.
• Note that drives can be accessed as read only devices from computers running Windows XP or Windows Vista. Older versions of Windows will see a second partition on the device that is normally hidden on Windows 7. This is known as the discovery drive, it contains the BitLocker To Reader application. Users can unlock the encrypted drive with this application by providing a password or recovery password. You can configure the Group Policy setting Allow access to BitLocker-protected removable data drives from earlier versions of Windows to control whether or not the discovery drive is created and BitLocker To Go is installed on removable drives when BitLocker protection is turned on for the drive. For more information, see Best Practices for BitLocker in Windows 7.
• All domain controllers in the domain must be running Windows Server 2003 SP2 or later.
  Note Windows Server 2003 requires you to extend the schema to support storing BitLocker recovery information in AD DS.
Mitigation Process

Use the following risk mitigation process to assess how best to configure BitLocker to help protect sensitive data on removable data drives on the client computers that you manage.

To use this mitigation process
1. Investigate BitLocker technology and capabilities.
   Note: For more information about BitLocker, see BitLocker Drive Encryption on Microsoft TechNet and the Windows BitLocker Drive Encryption Design and Deployment Guides.
2. Assess the need for BitLocker on removable data drives in your environment.
3. Confirm that the hardware and software that your organization uses meets BitLocker requirements for removable data drives.
4. Identify the systems in your organization that require BitLocker protection on removable data drives.
5. Test required removable drive devices including USB Flash drives.
6. Use GPOs to configure BitLocker on removable data drive settings on the test systems.
7. Train users how to correctly use BitLocker on removable data drives for their environment.
8. After successful testing, configure BitLocker for removable data drives on production systems.

To remove BitLocker encryption from a removable data drive access BitLocker Drive Encryption in Control Panel.

Using Group Policy to Mitigate Risk for BitLocker on Removable Data Drives

The following table outlines the Group Policy settings that are available for BitLocker To Go in the VolumeEncryption.admx template. You can configure these settings in the following location in the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
```

At the global settings level, the following Group Policy settings are available.

Table 3.6 BitLocker on Removable Data Drive Settings

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ Control use of BitLocker on removable drives</td>
<td>Controls the use of BitLocker on removable data drives.</td>
<td>Not configured</td>
</tr>
<tr>
<td>$ Configure use of smart cards on removable data drives</td>
<td>Specifies whether smart cards can be used or required to authenticate user access to BitLocker-protected removable data drives on a computer.</td>
<td>Not configured</td>
</tr>
<tr>
<td>$ Deny write access to removable drives not protected by BitLocker</td>
<td>Configures whether BitLocker protection is required for a computer to write data to a removable data drive. This setting also determines whether drives configured with BitLocker in other organizations are granted write access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Policy setting</td>
<td>Description</td>
<td>Windows 7 default</td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>§ Allow access to BitLocker-protected removable data drives from earlier versions of Windows</td>
<td>Configures whether removable data drives formatted with the FAT file system can be unlocked and viewed on computers running Windows Server 2008, Windows Vista, Windows XP SP3, or Windows XP SP2 operating systems. This setting also determines whether the BitLocker To Go Reader is applied to drives.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Configure use of passwords for removable data drives</td>
<td>Specifies whether a password is permitted or required to unlock BitLocker-protected removable data drives. This setting also specifies password length and complexity requirements.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Choose how BitLocker-protected removable drives can be recovered</td>
<td>Allows you to control how BitLocker-protected removable data drives are recovered in the absence of the required credentials.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the **Explain** tab of the setting in the Group Policy Object Editor.
Encrypting File System

You can use Encrypting File System (EFS) to encrypt files and folders to help protect data from unauthorized access. EFS is integrated into the NTFS file system and its operation is completely transparent to applications. When a user or program attempts to access an encrypted file, the operating system automatically attempts to acquire a decryption key for the content, and then silently performs encryption and decryption on behalf of the user. Users who have authorized keys are able to access and work with encrypted files just as they would with any other file, whereas other users are denied access.

In Windows 7, the architecture of EFS now supports elliptic curve cryptography (ECC). This enables EFS to be compliant with Suite B encryption requirements as defined by the National Security Agency to meet the needs of United States government agencies for protecting classified information. Suite B compliance requires the use of AES, SHA, and ECC cryptographic algorithms for data protection.

Suite B does not allow the use of RSA cryptography, but EFS in Windows 7 supports a new "mixed-mode" operation of ECC and RSA algorithms. This provides backward compatibility with EFS files created using algorithms supported in previous versions of Windows. This backward compatibility might be useful to organizations that use RSA and also want to use the ECC algorithm to prepare for Suite B compliance.

Note: We recommend using BitLocker and EFS in combination to maximize data protection.

Risk Assessment

Unauthorized access to data can compromise business processes and profitability. Especially where multiple users have access to the same system or mobile computer systems, data is at risk of compromise. The risk area that EFS is designed to mitigate is data theft or compromise due to lost or stolen mobile computers, or due to exposure of sensitive data by an insider. Shared computers might also be subject to this data risk.

When an attacker gains physical access to a computer with unencrypted data, the potential consequences include the following unauthorized acts:

- The attacker may restart the computer and escalate their user privilege to local Administrator to access the user’s data. An attacker also could download tools to mount a brute-force attack to obtain the user’s password, so that they can log on as the user to access the user’s data.
- The attacker could attempt to log on to a computer running Windows 7 to copy all available data to a removable device, and then send it via e-mail, copy it over the network, or transmit it using FTP to a remote server.
- The attacker could restart the computer into an alternate operating system and copy files directly from the hard drive.
- The attacker could connect the computer into another network, start the stolen computer, and then log on to it remotely.
- If a user caches their network files in Offline Files, an attacker can use them to escalate privilege to Administrator/LocalSystem, and then inspect the contents of the Offline Files cache.
- An attacker could restart the computer using an alternative operating system, read the contents of the paging file, and discover plaintext copies of in-process documents.
- A curious coworker could open sensitive files owned by other users of a shared computer.
Risk Mitigation

To mitigate these potential data compromise risks, you can encrypt data when it is stored on the hard drive. Improvements in the EFS technology in Windows 7 help you to mitigate the following risks and enforce security:

• Use EFS to prevent an attacker from reading encrypted files through another operating system by requiring the attacker to obtain a key that is capable of decrypting the content. You can store such a key on a smart card for added security.
• Enforce the strength of encryption that EFS uses through Group Policy.
• Thwart an attacker who attempts to access a user’s data using a brute-force password attack by storing the user’s EFS keys on a smart card, or by using BitLocker in combination with EFS to deny the attacker access to the user’s password hashes and cached credentials.
• Prevent an attacker from accessing a user’s confidential data by enforcing encryption of the user’s Documents folder through Group Policy. Alternatively, you can enforce encryption of other locations or the user’s entire data partition through a logon script.
• Use EFS to provide encryption on multiple drives and network shares.
• Use EFS to protect the contents of the system paging file and the Offline Files cache.

Mitigation Considerations

You can use EFS in Windows 7 to mitigate the risks described in the previous Risk Assessment section. However, before deploying EFS, consider the following:

• You must implement tested procedures for key management and data recovery requirements. In the absence of reliable and well-defined procedures, critical data may become inaccessible if keys are lost.
• Under normal operation, the overhead due to EFS is not noticeable. However, if system performance is critical, you must perform thorough testing to ensure that EFS does not adversely affect performance.
• If your organization needs to become Suite B compliant, you will need to adopt the ECC algorithm to prepare your systems with the required encryption standards.
• If you enable EFS on a volume, you cannot also compress files on the same volume.
• If necessary, deploy and test additional scripts to encrypt sensitive file locations.
• Users and IT staff must be properly trained to avoid issues, such as:
  • File copies or file moves from an encrypted location to an unencrypted location, which could leave the files formatted as plaintext files.
  • Failure to encrypt hidden folders where applications maintain backup copies of in-process files.
• Thoroughly test your EFS configuration to ensure that encryption is set on all sensitive file locations, including Documents, the Desktop, and temporary folders.
Mitigation Process

Use the following risk mitigation process to assess how best to configure EFS to help protect sensitive data on the client computers that you manage.

To use this mitigation process
1. Investigate EFS technology and capabilities.
   Note: For more information, see the "Best practices for the Encrypting File System" article on Microsoft.com.
2. Assess the need for EFS in your environment.
3. Investigate the configuration of EFS using Group Policy.
4. Identify the computer systems and users that require EFS.
5. Identify the level of protection that you require. For example, does your organization require using smart cards with EFS?
6. Configure EFS as appropriate for your environment using Group Policy.

Specific Mitigation Steps for EFS

To use Group Policy to manage EFS, there are several security settings in this location:

Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System

To add or create a Data Recovery Agent (DRA), right-click Encrypting File System, and then click Properties to open the Encrypting File System Properties dialog box.

![Encrypting File System Properties dialog box General tab](Figure 3.1 The Encrypting File System Properties dialog box General tab)
The ECC option of "Allow" detailed in Figure 3.1 sets EFS to "mixed-mode" operation so that the computer can use both RSA and ECC algorithms. If your environment requires Suite B compliance, select the "Require" option, and then select the ECC certificate key size as displayed in Figure 3.2.

![Figure 3.2 The Encrypting File System Properties Certificates dialog box](image)

**Certificates tab**

It is important to note that these policy settings apply only when a file or folder is initially encrypted. If a file or folder was encrypted before this setting was configured, the user will still have access to the file or folder and they will still be encrypted by using the algorithm that was enforced at that time. Selecting **Require** does not enforce the use of AES for the file encryption key; it only enforces the use of an ECC algorithm.

There are also four Group Policy templates that include EFS settings, which are listed in the following table.

**Table 3.7 EFS Group Policy Settings**

<table>
<thead>
<tr>
<th>Template and setting</th>
<th>Path and description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupPolicy.admx</td>
<td>Computer Configuration\ Administrative Templates\ System\Group Policy</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

**EFS recovery policy processing**

Determines when encryption policies are updated.
<table>
<thead>
<tr>
<th>Template and setting</th>
<th>Path and description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>EncryptFilesOnMove.admx</td>
<td>Do not automatically encrypt files moved to encrypted folders</td>
<td>Not configured</td>
</tr>
<tr>
<td></td>
<td>Computer Configuration\Administrative Templates\System\</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prevents Windows Explorer from encrypting files that are moved to an encrypted folder.</td>
<td></td>
</tr>
<tr>
<td>OfflineFiles.admx</td>
<td>Encrypt the Offline Files cache</td>
<td>Not configured</td>
</tr>
<tr>
<td></td>
<td>Computer Configuration\Administrative Templates\Network\Offline Files\</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This setting determines whether offline files are encrypted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> On Windows XP SP3, these files are encrypted with the system key whereas on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Vista SP1 or later, they are encrypted with the user’s key.</td>
<td></td>
</tr>
<tr>
<td>Search.admx</td>
<td>Allow indexing of encrypted files</td>
<td>Not configured</td>
</tr>
<tr>
<td></td>
<td>Computer Configuration\Administrative Templates\Windows Components\Search\</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This setting allows encrypted items to be indexed by Windows Search.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> There may be data security issues if encrypted files are indexed and the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>index is not adequately protected by EFS or another means.</td>
<td></td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the **Explain** tab of the setting in the Group Policy Object Editor.
Rights Management Services

Rights Management Services (RMS) is designed to provide security and usage policy enforcement for sensitive e-mail, documents, Web content, and other types of information. RMS provides information security by encrypting information persistently. When a file or e-mail message is transmitted through the enterprise or the Internet using RMS, only those who are authenticated and explicitly authorized to access it can do so. RMS consists of the following three components:

- **RMS server.** Windows 7 requires Windows Rights Management Services for Windows Server 2003 or later.
- **RMS client.** The client is built in to Windows 7.
- **RMS platform or application.** This is a platform or application that is designed to encrypt and control usage of the information it manages.

**Note:** While the RMS client is built in to Windows 7 a separate client access license must be purchased to use it.

Risk Assessment

RMS can help mitigate the risk to organizations that unauthorized personnel may be able to view sensitive information. Such information may have been distributed or made available to unauthorized users either in error or maliciously. Specific examples of this type of risk include:

- Unauthorized users who sniff the network, access USB flash and portable hard drives, or access insufficiently protected server shares and storages.
- Authorized users who send sensitive information to unauthorized recipients inside or outside the organization.
- Authorized users who copy or move sensitive data to unauthorized locations or applications, or from an authorized device to an unauthorized device, such as a removable storage device.
- Authorized users who accidently provide access to sensitive information to unauthorized recipients via peer-to-peer (P2P) technologies or instant messaging.
- Authorized users who print sensitive files, and the printed documents are discovered by unauthorized users who distribute, copy, fax, or distribute them via e-mail.

Risk Mitigation

To effectively protect information that users share and collaborate on regardless of the mechanism they use, we recommend securing the information directly via RMS. In this way, RMS seamlessly protects the information as it is transmitted between hosts, devices, and shares.

Mitigation Considerations

You can use RMS to mitigate the risks described in the previous “Risk Assessment” section. However, before deploying RMS, consider the following:

- RMS requires Windows Rights Management Services for Windows Server 2003 or later, as the RMS server, and rights-enabled applications installed on the client computer.
- Microsoft Office SharePoint® Server 2007 or later is required if you want to make use of SharePoint-RMS integration (where RMS protects documents and information that reside on SharePoint sites).
- If you want to take advantage of the optional smart card integration of the RMS solution, ensure that each client computer that you use to access the content is compatible with the smart cards.

Solution Accelerators  
microsoft.com/technet/SolutionAccelerators
To use Web-based applications such as Outlook® Web Access (OWA) with RMS, the Rights Management Add-on for Internet Explorer is required.

IT staff will require training to successfully deploy, support, and troubleshoot RMS.

**Mitigation Process**

Use the following risk mitigation process to assess how best to configure RMS to help protect sensitive data on the client computers that you manage.

**To use this mitigation process**

1. Investigate RMS technology and capabilities.
   
   **Note** For more information about RMS, see the Windows Rights Management Services Technology Center.

2. Assess the need for RMS in your environment.

3. Identify support of applications and services for RMS.

4. Assess potential RMS deployment architectures, such as:
   - Single server (or single cluster)
   - Single certification, single license
   - Single certification, multiple license
   - Multiple certification, single license
   - Multiple certification, multiple license

5. Identify information that you want to secure using RMS.

6. Identify users and groups that require access to specific information.

7. Configure RMS to allow only required access to information.

**Managing RMS Using Group Policy**

The Group Policy settings to configure RMS are not part of the Windows 7 installation. RMS is primarily a server-based solution, so configuring the behavior of the services should be performed on the RMS server.

In addition, RMS-aware applications may have individual settings that govern how they handle RMS protected content.
Device Management and Installation

The ability of users to add new Plug and Play (PnP) hardware on their client computers, such as USB key drives or other removable storage devices, creates significant security issues for IT administrators. Not only can these types of devices make client computers harder to maintain when users use them to install unsupported hardware, they also can pose threats to data security.

A number of changes have been introduced in Group Policy to help enhance what administrators can do to manage attempts to install unsupported or unauthorized devices. However, it is important to understand that a device is installed for a computer not for a particular user. After a user installs a device, it is typically available to all users of that computer. Windows 7 and Windows Vista support user-level access controls for read and write access to installed devices. For example, you can allow full read and write access to an installed device, such as a USB flash drive to one user account, but only allow read access to another user account on the same computer.

For more information about device management and installation and how you can configure Group Policy to manage it, see the Step-By-Step Guide to Controlling Device Installation Using Group Policy.

Risk Assessment

Unauthorized addition or removal of devices is a high security risk because these actions can enable an attacker to run malicious software, remove data, and add unwanted data. Specific examples of this type of risk include:

• Authorized users may copy sensitive files from an authorized device to an unauthorized removable storage device, either intentionally or unintentionally. This may include copying from an encrypted location to an unencrypted location on a removable device.
• Attackers might log on to the computers of authorized users, and then copy data to a removable storage device.
• Attackers could use a removable storage device or network share with malicious software to use an AutoRun script to install malicious software on an unattended client computer.
• Attackers could install an unauthorized key-logging device, which they could use to record user account details to launch an attack.

Risk Mitigation

To mitigate these risks, we recommend protecting the computer systems you manage against the installation and use of unauthorized devices. You can use Group Policy settings to control the use of PnP devices, such as USB flash drives and other removable storage devices.
Mitigation Considerations
You can use Group Policy in Windows 7 to mitigate the risks described in the previous “Risk Assessment” section by using the Device Installation settings. However, before deploying device management and installation settings to the client computers in your environment, take into account the following mitigation considerations:

- Restricting devices may block legitimate file sharing or mobile users from working most effectively.
- Restricting devices can prevent you from using a USB key as part of the BitLocker drive encryption process. For example, if the Removable Disks: Deny write access policy setting is in effect for a user, even if that user is an administrator, the BitLocker setup program cannot write its startup key to a USB flash drive.
- Some devices identify themselves with both a “removable storage” and a “local storage” ID. For example, some startup USB flash drives may do this. Therefore, it is important to thoroughly test your GPOs to ensure that the correct devices are restricted and allowed.

Mitigation Process
Use the following risk mitigation process to assess how best to configure device management and installation to help protect sensitive data on the client computers that you manage.

To use this mitigation process
1. Investigate the device management and installation capabilities of Windows 7.
   - Note For more information, see the Step-By-Step Guide to Controlling Device Installation Using Group Policy.
2. Assess the need for device management and installation in your environment.
3. Investigate the Group Policy settings for device management and installation.
4. Identify removable devices that you require in your environment and record the required Hardware or Compatibility IDs for these devices.
5. Identify the computer systems and users that require removable devices.
6. Configure Group Policy to enable installation of specifically required device classes.
7. Configure Group Policy to enable installation of devices on computer systems that specifically require this capability.

Using Group Policy to Control Device Installation
To manage device management and installation, we recommend using the DeviceInstallation.admx Group Policy template. The following table outlines the Group Policy settings available in this template. You can configure these settings in the following location in the Group Policy Object Editor:

    Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions

Table 3.8 USB Device Management and Installation Settings

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow administrators to override Device Installation Restriction policies</td>
<td>Allows administrators to override Device Installation Restriction policies.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

Solution Accelerators  
microsoft.com/technet/SolutionAccelerators
<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
</table>
| Allow installation of devices that match any of these device IDs | This setting specifies a list of Plug and Play hardware IDs and compatible IDs that describe devices that can install, unless the following settings specifically prevent the setting from taking effect:  
  Prevent installation of devices that match these device IDs  
  Prevent installation of devices for these device classes  
  Prevent installation of removable devices.  
  Only use this setting when the setting for Prevent installation of devices not described by other policy settings is enabled. | Not configured    |
| Allow installation of devices using drivers that match these device setup classes | This setting specifies a list of device setup class globally unique identifiers (GUIDs) describing devices that users can install, unless specifically prevented by the following policy settings:  
  Prevent installation of devices that match these device IDs  
  Prevent installation of devices for these device classes  
  Prevent installation of removable devices.  
  Only use this setting when the Prevent installation of devices not described by other policy settings setting is enabled. | Not configured    |
<p>| Display a custom message title when device installation is prevented by a policy setting | This setting allows you to display a custom message title in the notification balloon when a device installation is attempted and a policy setting prevents the installation. | Not configured    |
| Display a custom message when installation is prevented by policy settings | This setting allows you to display a custom message to users in the notification balloon when a device installation is attempted and a policy setting prevents it. | Not configured    |</p>
<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
</table>
| Prevent installation of devices not described by other policy settings | This setting allows you to prevent the installation of devices that are not specifically described by any other policy setting. If you enable this policy setting, Windows cannot install or update the device driver for any device not described by the following settings:  
**Allow installation of devices that match any of these device IDs**  
**Allow installation of devices for these device classes.** | Not configured     |
| Prevent installation of devices that match any of these device IDs | This setting specifies a list of Plug and Play hardware IDs and compatible IDs for devices that Windows cannot install.  
**Note** This policy setting takes precedence over any other policy setting that allows Windows to install a device. | Not configured     |
| Prevent installation of devices using drivers that match these device setup classes | This setting specifies a list of device setup class GUIDs for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device. | Not configured     |
| Prevent installation of removable devices         | This setting allows you to prevent Windows from installing removable devices. A device is considered removable when the driver for the device to which it is connected indicates that the device is removable.  
**Note** This policy setting takes precedence over any other policy setting that allows Windows to install a device.  
For this policy to apply, the drivers for the device must correctly identify that the device is removable. For more information, see the [Step-By-Step Guide to Controlling Device Installation Using Group Policy](microsoft.com/technet/SolutionAccelerators). | Not configured     |
| § Time (in seconds) to force reboot when required for policy changes to take effect | This setting determines the amount of time (in seconds) that the system will wait to restart in order to enforce a change in device installation restriction policies. If you disable or do not configure this setting, the system will not force a restart.  
**Note** If a restart is not forced, the access right will not take effect until the system is restarted. | Not Configured     |

This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor.
## Using Group Policy to Control Device Usage

In addition to helping you control the installation of devices, Windows 7 allows you to control the level of access users have to particular device classes after they have been installed. There are two other templates described in the following tables that contain settings that can affect the behavior of devices. The RemovableStorage.admx template contains the following settings for removable storage devices that are located in the following location in the Group Policy Object Editor:

```
Computer Configuration\Administrative Templates\System\Removable Storage Access
```

### Table 3.9 Device Settings

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Removable Storage classes: Deny all access</td>
<td>This setting configures access to all removable storage devices classes.</td>
<td>Not configured</td>
</tr>
<tr>
<td>All Removable Storage: Allow direct access in remote sessions</td>
<td>This setting grants standard user accounts access to removable storage devices in remote sessions. The default configuration does not allow this access for remote sessions.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ CD and DVD: Deny execute access</td>
<td>This setting denies execute access to the CD and DVD removable storage class. The default setting allows execute access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>CD and DVD: Deny read access</td>
<td>This setting denies read access to the CD and DVD removable storage class. The default setting will allow read access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>CD and DVD: Deny write access</td>
<td>This setting denies write access to the CD and DVD removable storage class. The default setting will allow write access to this device class.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Custom Classes: Deny read access</td>
<td>This setting denies read access to custom device classes. The default setting allows read access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Custom Classes: Deny write access</td>
<td>This setting denies write access to custom device classes. The default setting allows write access to this device class.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Floppy Drives: Deny execute access</td>
<td>This setting denies execute access to the Floppy Drives removable storage class, including USB Floppy Drives. The default setting allows execute access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Floppy Drives: Deny read access</td>
<td>This setting denies read access to floppy drives. The default setting allows read access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Floppy Drives: Deny write access</td>
<td>This setting denies write access to floppy drives. The default setting allows write access to this device class.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Removable Disks: Deny execute access</td>
<td>This setting denies execute access to removable disks. The default setting allows execute access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Policy setting</td>
<td>Description</td>
<td>Windows 7 default</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Removable Disks: Deny read access</td>
<td>This setting denies read access to removable drives. The default setting allows read access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Removable Disk: Deny write access</td>
<td>This setting denies write access to removable drives. The default setting allows write access to this device class.</td>
<td>Not configured</td>
</tr>
<tr>
<td>§ Tape Drives: Deny execute access</td>
<td>This setting denies execute access to the Tape Drive removable storage class. The default setting allows execute access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Tape Drives: Deny read access</td>
<td>This setting denies read access to tape drives. The default setting allows read access.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Tape Drives: Deny write access</td>
<td>This setting denies write access to tape drives. The default setting allows write access to this device class.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>
| Time (in seconds) to force reboot | This setting determines the amount of time (in seconds) that the system waits to restart in order to enforce a change in access rights to removable storage devices. If you disable or do not configure this setting, the system will not force a reboot.  
**Note** If the restart is not forced, the access right will not take effect until the system is restarted. | Not configured    |
| § WPD Devices: Deny execute access | This setting denies execute access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. The default setting allows execute access.                           | Not configured    |
| WPD Devices: Deny read access    | This setting denies read access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. The default setting allows read access.                                    | Not configured    |
| WPD Devices: Deny write access   | This setting denies write access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices. The default setting allows write access.                                | Not configured    |

This table provides a simple description for each setting. For more information about a specific setting, see the **Explain** tab of the setting in the Group Policy Object Editor.
Using Group Policy to Control AutoPlay and AutoRun

The Autoplay.admx template contains the following settings that affect the AutoPlay and AutoRun behavior for removable storage devices and removable media in Windows 7. You can find the settings for this template in the following location in the Group Policy Object Editor:

Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies

Table 3.10 AutoPlay Policy Settings

<table>
<thead>
<tr>
<th>Policy setting</th>
<th>Description</th>
<th>Windows 7 default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default behavior for AutoRun</td>
<td>This setting configures the default behavior for AutoRun commands. By default, Windows Vista and Windows 7 prompt the user to confirm whether the AutoRun command can run.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Don't set the always do this checkbox</td>
<td>If you enable this setting, the &quot;Always do this...&quot; checkbox in the Autoplay dialog does not appear by default when the dialog displays.</td>
<td>Not configured</td>
</tr>
<tr>
<td>Turn off Autoplay</td>
<td>This setting allows you to disable the Autoplay feature for the CD, DVD-ROM, and removable drives, or all drives. Disabling Autoplay helps to prevent the spread of malicious software that uses autorun scripts on removable drives and network shares.</td>
<td>Not configured ‡</td>
</tr>
<tr>
<td>§ Turn off Autoplay for non-volume devices</td>
<td>If you enable this setting, Autoplay is disabled for non-volume devices, such as Media Transfer Protocol (MTP) devices. If you disable or do not configure this setting, Autoplay remains enabled for non-volume devices.</td>
<td>Not configured</td>
</tr>
</tbody>
</table>

This table provides a simple description for each setting. For more information about a specific setting, see the Explain tab of the setting in the Group Policy Object Editor. These settings also appear under the user configuration at the following location:

User Configuration\Administrative Templates\Windows Components\AutoPlay Policies

If the device management and installation settings conflict, the settings for computer configuration take precedence over user configuration settings.

Note Some policy settings specify the use of device setup class globally unique identifiers (GUIDs), and others use Plug and Play device setup class GUIDs. For more information, see How Setup Selects Drivers.
More Information

The following resources provide additional information about enhanced security features and technologies to help protect sensitive data in Windows 7 on Microsoft.com:

- **BCDEdit Commands for Boot Environment.**
- **Best Practices for BitLocker in Windows 7.**
- **Best practices for the Encrypting File System.**
- **BitLocker Drive Encryption.**
- **BitLocker Drive Encryption Overview.**
- **Boot Configuration Data in Windows Vista.**
- **How Setup Selects Drivers.**
- **Office 2003 Policy Template Files and Deployment Planning Tools.**
- **Step-By-Step Guide to Controlling Device Installation Using Group Policy.**
- **The Encrypting File System.**
- **Trusted Computing Group.**
- **Windows BitLocker Drive Encryption Design and Deployment Guides.**
- **Windows Rights Management Services Technology Center.**
- **Windows Vista Security and Data Protection Improvements:** "Data Protection."
Chapter 4: Application Compatibility with Windows 7

The Windows Vista® operating system introduced a number of significant changes in the way it handles applications extending down to the kernel level to provide a more secure application platform than Windows® XP. However, these changes introduced application compatibility issues, and to resolve them required modifying many applications to make them function properly on computers running Windows Vista.

The application model of Windows® 7 is built on the same basic architecture as Windows Vista. Most applications remain compatible between these operating systems. This alone makes adopting Windows 7 less challenging than migrating from Windows XP to Windows Vista. If your organization is like many that remain standardized on Windows XP, you may need to transition to updated versions of your key applications, but the availability of Windows Vista–compatible application versions, and well-proven shims will make this task more manageable.

However, there is a possibility that older applications may not work properly with some of the new security technologies built into Windows 7. Technologies such as User Account Control (UAC) and Windows Resource Protection (WRP) can cause older applications to fail.

The Microsoft Deployment Toolkit (MDT) 2010 contains comprehensive application compatibility guidance to enable IT professionals to test applications for compatibility with Windows 7, and mitigate compatibility issues discovered during the testing process. For more information about this subject, see the Application Compatibility Feature Team Guide.

This chapter includes simple procedures that you can use to test the compatibility level of your applications with Windows 7. The chapter also discusses some of the more common causes of application compatibility issues, and provides pointers to available resources that can help you to address them.

Application Compatibility Testing

This section provides guidance on how to test and evaluate application compatibility with Windows 7. It includes two scenarios that you can use to test application compatibility with the operating system. The scenarios are designed to help you test an application on a computer running Windows 7.

To test an application on a computer running Windows 7

1. Install Windows 7 on a test computer, and then log on to the computer as an administrator.

2. Install the application that you want to test on the computer. If a prompt appears requesting permission to install the application, click Permit to continue the installation. If the installation succeeds, go to Step 6.

   **Note** This step is not necessary if you use a Microsoft Installer (.msi) file to install the application.

   **Warning** If the application installer offers to automatically launch the new program do not allow it to do so because it will execute with the same elevated privileges used to conduct the installation.
3. If the application installation fails and no installation permission prompt displayed, right-click the installer .exe file, click the option to Run this program as administrator, and then retry the installation. If the installation succeeds, go to Step 7.

4. If you receive any errors related to the operating system version, application registration, or file copy, right-click the installer .exe file, click Compatibility, and then choose the Windows XP Professional SP3 compatibility mode.

5. Repeat Step 2. If you still cannot install the application, go to Step 8.

6. Log on as a user without administrative privileges to the test computer running Windows 7.

7. Start the application. If the application does not start properly or displays errors, enable the Windows XP Professional SP3 compatibility mode for the application .exe file, and then try to run it again on the operating system.

8. If the application starts successfully, run the full suite of tests you would typically use to test it on a computer running Windows XP Service Pack 3 (SP3). If the application passes all major functionality tests, the application will run properly with Windows 7.

9. If the application does not install and start successfully, stops responding, produces an error, or fails any major functionality test, it may be one of the applications that is subject to compatibility issues with Windows 7. Refer to other resources in this chapter to further investigate and test the application.

If you complete these steps and determine that the application performs properly, you can assume that it will work with Windows 7.

**Known Application Compatibility Issues**

This section describes technologies, enhancements, and changes in Windows 7 that are known to cause application compatibility issues. Where possible, this section also includes potential ways to mitigate them.

**Important** Test all third-party applications that you plan to use in your environment with Windows 7 to ensure that they work properly with the operating system.

**Security Enhancements**

The following security enhancement features in Windows Vista and Windows 7 may cause compatibility issues with third-party applications developed for earlier versions of Windows:

- **User Account Control.** This feature in Windows Vista and Windows 7 provides a method of separating standard user privileges and tasks from those that require administrator access. User Account Control (UAC) increases security by improving the computer experience for users running standard user accounts. Users can perform more tasks and enjoy higher application compatibility without the need to log on to their client computers with administrative-level privileges. This helps reduce the effects of malware, incidences of unauthorized software installation, and unapproved system changes.

  One of the most useful features of UAC is its ability to virtualize portions of the registry and file system when applications running with limited privileges attempt to write data to system-wide locations. UAC can introduce problems in applications that are not compliant with these enhancements. For this reason, it is important to test applications with UAC enabled before you deploy them.

- **Windows Resource Protection.** Introduced in Windows Vista, WRP is the new name for Windows File Protection, which protects registry keys and folders as well as key system files. WRP is designed to help improve the overall security and stability of the operating system. Applications that attempt to make changes to these protected areas may not operate properly with Windows 7. In these cases, you must modify the
applications so that they function as intended. For more information about this feature and its implications for application compatibility, see About Windows Resource Protection on MSDN®.

- **Protected Mode.** This feature of Windows® Internet Explorer® 7 and later helps protect computers running Windows from the installation of malware and other harmful software by running with less privileged, more secure rights. When Internet Explorer is in Protected Mode, the browser can only interact with specific areas of the file system and registry.

Although Protected Mode helps maintain the integrity of client computers running Windows, it can affect the proper operation of older Internet and intranet Web applications. You may need to modify such Web applications to run them in a more restrictive environment. By default Protected Mode is not enabled in Internet Explorer® 8 when accessing sites located in the Intranet zone or the Trusted sites zone.

### Operating System Changes and Innovations

The following operating system changes and innovations in Windows 7 may cause compatibility issues with third-party applications:

- **New system APIs.** Application programming interfaces (APIs) expose layers of the Windows Vista SP1 operating system differently than in previous versions of Windows. Antivirus and firewall software are examples of applications that rely on these new APIs to properly monitor and safeguard both Windows Vista and Windows 7. To resolve this, upgrade applications that perform these functions to versions that are compatible with Windows Vista SP1.

- **Windows 7 64-Bit.** Windows 16-bit applications and 32-bit drivers are not supported in the Windows 64-bit environment. Automatic registry and system file redirection is only available for the 32-bit applications. For these reasons, 64-bit applications must comply with the full Windows 7 and Windows Vista application standards.

- **Operating system versions.** Many older applications check for specific versions of Windows. When third-party applications cannot detect a specific operating system version, many of them stop responding. In some cases you can resolve this situation by manually configuring the compatibility mode for the application to an older version of Windows.

Most operating system versioning requirements related to compatibility issues are addressed by new functionality built into Windows 7. Features such as the Program Compatibility Assistant can usually resolve these types of issues automatically. For more information about the Program Compatibility Assistant and other tools and resources, see the next section of this chapter.

The Windows 7 and Windows Server 2008 R2 Application Quality Cookbook on MSDN provides additional information about these security enhancements and operating system changes and innovations in Windows 7. This resource also provides test approaches and possible remedies for most of these compatibility issues.
Tools and Resources

This section provides brief overviews and pointers to several features and technologies available for Windows 7 that are designed to help you address application compatibility issues.

**Program Compatibility Assistant**

This feature automatically specifies an appropriate "compatibility mode" for applications designed to run with previous versions of Windows®. When Windows 7 detects applications that need to run in compatibility modes for Windows® 2000, Windows XP Professional SP3, or later versions of Windows, the operating system directs the applications to be updated automatically to run on Windows 7 without further user intervention.

For more information, see the [Program Compatibility Assistant: frequently asked questions](https://microsoft.com/technet/SolutionAccelerators) page of the Windows Help and Support Web site.

**Program Compatibility Wizard**

The Program Compatibility Wizard is included with Windows 7 to assist you when a program written for an earlier version of Windows does not run correctly. The wizard will help you specify compatibility settings for the program, which will resolve application compatibility issues for many older programs.

To open the Program Compatibility Wizard, click the **Start** button, click **Control Panel**, click **Programs**, and then click **Use an older program with this version of Windows**.

For more information, see the [Make older programs run in this version of Windows](https://microsoft.com/technet/SolutionAccelerators) page of the Windows Vista Help and Support Web site.

**Warning** Do not run the Program Compatibility Wizard on older antivirus programs, disk utilities, or other system programs because it might cause data loss or create a security risk. Instead, use only versions of these programs and utilities designed specifically to work with your version of the operating system.

**Microsoft Application Compatibility Toolkit**

Microsoft has released a suite of tools and documentation to help you identify and manage your organization's applications. The Microsoft Application Compatibility Toolkit (ACT) 5.5 is designed to help you reduce the cost and time involved to resolve application compatibility issues to let you more quickly deploy Windows 7.

ACT 5.5 can help you prepare to use Windows 7 by providing a detailed inventory of your existing applications, managing critical applications, and determining the extent of your application environment that may require special attention in preparation for Windows 7 deployments. The toolkit has been specifically updated to support the security features in Windows 7.

You can use the ACT features to:

- Verify an application's compatibility with a new version of the Windows operating system, or a Windows Update, including a risk assessment.
- Become involved in the ACT Community by sharing your risk assessment with other ACT users.
- Test your Web applications and Web sites for compatibility with new releases and security updates to Internet Explorer.

For more information about the toolkit, see [Microsoft Application Compatibility Toolkit (ACT) Version 5.5](https://microsoft.com/technet/SolutionAccelerators).
**Windows XP Mode**

If you cannot make your application compatible with Windows 7 using ACT 5.5 or the other application compatibility tools in the operating system, Windows 7 offers another option called *Windows XP Mode*. This feature provides a method to install and seamlessly run Windows XP applications directly from a Windows 7–based PC. Windows XP Mode uses Windows Virtual PC virtualization technology to provide a virtual Windows XP environment for incompatible Windows XP applications. After installing the application, the user simply uses the application directly from the Windows 7 desktop. There is no need for the user to know that the application is in fact running inside a Windows XP virtual machine.

Windows XP Mode is an optional download available in the Professional, Ultimate and Enterprise editions of Windows 7, and provides a 32-bit Windows XP Professional SP3 environment that is preloaded on the virtual hard disk. While this option does provide an excellent compatibility solution, it also introduces a second operating system that must be configured to the required level of security for your organization. By default this Windows XP virtual machine is configured to use shared networking, or Network Address Translation (NAT). This is good because it ensures that unsolicited inbound network traffic never reaches the virtual machine, however it also changes the way Internet Explorer automatically detects the location of web servers. When running under Windows XP Mode and accessing sites over a NAT Internet Explorer may assign some external sites to the Internet Zone, therefore you should also lock down to match the restrictive settings specified for the Restricted Sites Zone. You can then add trustworthy web sites to the Trusted Sites Zone. To start using Windows XP Mode, download it from the [Windows XP Mode and Windows Virtual PC](http://microsoft.com/technet/SolutionAccelerators) page. Refer to the [Windows XP Security Guide](http://microsoft.com/technet/SolutionAccelerators) for information about settings that you can use to harden the Windows XP Mode environment. To obtain the *Windows XP Security Guide*, download it with the [Windows XP Security Compliance Management Toolkit](http://microsoft.com/technet/SolutionAccelerators).

**More Information**

The following resources provide additional information about Windows 7 application compatibility-related topics on Microsoft.com:

- [Application Compatibility and User Account Control](http://microsoft.com/technet/SolutionAccelerators).
- [Introduction to the Protected Mode API](http://microsoft.com/technet/SolutionAccelerators).
- [Make older programs run in this version of Windows](http://microsoft.com/technet/SolutionAccelerators) in Windows Vista Help and Support.
- [Microsoft Application Compatibility Toolkit (ACT) Version 5.5](http://microsoft.com/technet/SolutionAccelerators).
- [Microsoft Virtualization](http://microsoft.com/technet/SolutionAccelerators).
- [Program Compatibility Assistant: frequently asked questions](http://microsoft.com/technet/SolutionAccelerators).
- [Windows 7 Upgrade Adviser](http://microsoft.com/technet/SolutionAccelerators).