SOLUTION**ACCELERATORS**

Act faster. Go further.

Windows® XP Security Guide

Security Compliance Management Toolkit

Version 3.2

Published: April 2003 | Updated: April 2010

For the latest information, see

microsoft.com/securitycompliance

Microsoft

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user's particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

Overview

Welcome to the *Windows XP Security Guide*. This guide is designed to provide you with the best information available to assess and counter security risks specific to computers running Windows® XP Professional Service Pack 3 (SP3) or later in your environment. The chapters in this guide provide detailed information about how to configure enhanced security settings and features in Windows XP Professional SP3 wherever possible to address identified threats in your environment. If you are a consultant, designer, or systems engineer who works in a Windows XP Professional SP3 environment, this guide was designed with you in mind.

Microsoft engineering teams, consultants, support engineers, partners, and customers have reviewed and approved the information in this guide 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.

Best practices to secure both client and server computers were developed by consultants and systems engineers who have implemented Windows XP Professional SP3, Windows Server® 2003 SP2, and Windows Server® 2008 in a variety of environments, and these best practices are detailed in this guide. Step-by-step security prescriptions, procedures, and recommendations are also provided to help you maximize security for computers in your organization that run Windows XP Professional SP3.

If you want more in-depth discussion of the concepts behind this material, see the companion guide, *Threats and Countermeasures*, as well as the *Microsoft Windows XP Resource Kit*, the *Microsoft Windows Server 2003 Resource Kit*, the *Microsoft Windows Security Resource Kit*, and Microsoft TechNet. For more information about all available Solution Accelerators, visit Solution Accelerators on TechNet.

This guide was originally created for Windows XP SP1. This updated version reflects the significant security enhancements in Windows XP SP3, and it was developed and tested with computers that run Windows XP Professional SP3. All references to Windows XP in this guide refer to Windows XP SP3 unless otherwise stated.

Executive Summary

Whatever your environment, you are strongly advised to be serious about security matters. Many organizations underestimate the value of their information technology (IT) environment, often because they exclude substantial indirect costs. If an attack on the servers in your environment is severe enough, it could significantly damage the entire organization. For example, an attack that makes your Web site unavailable and causes a major loss of revenue or customer confidence might lead to the collapse of your organization’s profitability. When you evaluate security costs, you should include the indirect costs that are associated with any attack in addition to the costs of lost IT functionality.

Vulnerability, risk, and exposure analysis with regard to security informs you of the tradeoffs between security and usability that all computer systems are subject to in a networked environment. This guide documents the major security-related countermeasures that are available in Windows XP Professional SP3 and later, the vulnerabilities that they address, and the potential negative consequences (if any) of each countermeasure's implementation.

The guide then provides specific recommendations for hardening computers that run Windows XP Professional SP3 or later. The *Windows XP 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 2003. The client computers in this environment include a mixture: some run Windows XP whereas others run Windows XP Professional SP3. For instructions about how to test and deploy the EC environment, see Chapter 1, "Implementing the Security Baseline." You can also use the Microsoft Excel® workbook Windows XP Security Baseline Settings to reference all of the recommended Group Policy settings for this environment.
- **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 XP Professional SP3. For instructions about how to test and deploy the SSLF environment, see Chapter 1, "Implementing the Security Baseline." You can also use the Excel workbook Windows XP Security Baseline Settings to reference all of the recommended Group Policy 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 XP Professional SP3 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 Security Compliance Manager (SCM) tool that accompanies the download for this toolkit. 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 Summaries" section in this overview briefly introduces the information in the guide. For further information about the security topics and settings related to Windows XP Professional SP3, see 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. You can use the toolkit with the Desired Configuration Management (DCM) feature in Configuration Manager 2007® (SP1) 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 *Security Compliance Management Toolkit* on TechNet.

Who Should Read This Guide

The *Windows XP 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 XP Professional SP3 for both desktop and laptop client computers in an enterprise environment. The guide is not intended for home users. This guide is for individuals whose job roles include the following:

- **IT generalist**. Users in this role handle security at every level in organizations ranging in size from 50 to 500 client computers. IT generalists focus on securing the computers that they manage quickly and simply.
- **Security specialist**. Users in this role focus on how to provide security across computing platforms within an organization. Security specialists require a reliable reference guide that addresses the security needs of every level of the organization that also offers proven methods to implement security countermeasures. Security specialists identify security features and settings and then provide recommendations on how their customers can most effectively use them in high risk environments.
- **IT operations, help desk, and deployment staff**. Users in IT operations focus on integrating security and controlling change in the deployment process, whereas deployment staff focuses on administering security updates quickly. Staffs in these roles also troubleshoot security issues related to applications that involve how to install, configure, and improve the usability and manageability of software. They monitor these types of issues to define measurable security improvements and a minimum of impact on critical business applications.
- **Network architect and planner**. Users in these roles drive the network architecture efforts for computers in their organization.
- **Consultant**. Users in this role work in organizations ranging in size from 50 to 5,000 or more client computers. IT consultants are aware of many kinds of security scenarios that span all the business levels of an organization. IT consultants from both Microsoft Services and partners take advantage of knowledge transfer tools for enterprise customers and partners.
- **Business analyst and business decision maker (BDM)**. Users in these roles have critical business objectives and requirements that need IT desktop or laptop support.

Note Users who want to apply the prescriptive guidance in this guide must, at a minimum, read and complete the steps to establish the EC environment in Chapter 1, "Implementing the Security Baseline."

Skills and Readiness

The following knowledge and skills are required for administrators and architects who develop, deploy, and secure computers running Windows XP Professional SP3 in an enterprise organization.

- MCSE 2000 or 2003 certification with more than two years of security-related experience or the equivalent.
- In-depth knowledge of the organization’s domain and Active Directory 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

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 XP Professional SP3 to help you manage them in your environment.

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

Guide Scope

This guide focuses on how to help create and maintain a secure environment for desktop and laptop computers that run Windows XP Professional SP3. 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 in the EC environment can run Windows XP Professional SP3. However, the computers that manage these client computers on the network must run Windows Server 2003 R2 or Windows Server 2003 SP2. Client computers in the SSLF environment can only run Windows XP Professional SP3.

The guide only includes the security settings available in the operating system that it recommends. For a thorough discussion of all the security settings in Windows XP Professional SP3, refer to the companion guide, *Threats and Countermeasures*.

Chapter Summaries

The *Windows XP Security Guide* consists of 3 chapters. Each chapter builds on the end-to-end solution process that is required to implement and secure Windows XP Professional SP3 or later in your environment.

Overview

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

Chapter 1: Implementing the Security Baseline

This chapter identifies the benefits to an organization of creating and deploying a security baseline. The chapter includes high-level security design recommendations that you can follow in preparation to implement either the EC baseline settings or the SSLF baseline settings. The chapter explains important security considerations for both the EC environment and the SSLF environment, and the broad differences between these environments.

You will need to run the .msi file for the SCM tool that accompanies the download for this toolkit to create, test, and deploy settings for either the EC environment or the SSLF environment. You can use this tool to customize baselines and generate GPO backup files for applying the settings to users and computers. For instructions on how to use this tool to accomplish these tasks, see the information available in the Help Topics for the tool.

Chapter 2: Additional Hardening Procedures

This chapter describes how you can implement additional countermeasures manually to further secure client computers running Windows XP Professional SP3.

Chapter 3: Software Restriction Policy for Windows XP Clients

This chapter provides a basic overview of software restriction policy, which provides administrators with a policy-driven mechanism to identify and limit the software that can run in their domain. Administrators can use a software restriction policy to prevent unwanted programs from running and prevent viruses, Trojan horses, or other malicious code from spreading.

Software restriction policies fully integrate with Active Directory and Group Policy, and you can use them in an environment without a Windows Server 2003 domain infrastructure when they are applied locally to client computers in the environment.

More Information

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

- Infrastructure Planning and Design.
- Microsoft Deployment.
- Microsoft Assessment and Planning Toolkit.
- *Microsoft Windows Security Resource Kit*.
- *Microsoft Windows Server 2003 Resource Kit*.
- Security Guidance.
- Solution Accelerators.
- *Threats and Countermeasures*.
- *Windows Server 2003 Security Guide*.
- Windows XP TechCenter.

Feedback

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

Please send your comments using the following resources:

- E-mail 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 XP 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

Authors and Experts

Bob Partridge – *Microsoft*

Haikun Zhang – *Minesage Co Ltd*

Hui Zeng – *Minesage Co Ltd*

Jose Maldonado – *Microsoft*

Kurt Dillard – *kurtdillard.com*

Michael Tan – *Microsoft*

Mike Danseglio – *Microsoft*

Richard Harrison – *Content Master*

Steve Clark – *Microsoft*

Steve Ryan – *Content Master*

Tony Quinn – *Microsoft*

ZhiQiang Yuan – *Minesage Co Ltd*

Product Managers

Bill Reid – *Microsoft*

Shruti Kala – *Microsoft*

Tony Bailey – *Microsoft*

Program Managers

Alison Woolford – *Content Master*

Bomani Siwatu – *Microsoft*

Vlad Pigin – *Microsoft*

Release Managers

Flicka Crandell – *Microsoft*

Karina Larson – *Microsoft*

Karl Seng – *Siemens Agency Services*

Test Manager

Sumit Parikh – *Microsoft*

Testers

Ankit Agarwal – *Infosys Technologies Ltd*

Ashish Java – *Infosys Technologies Ltd*

Avrojit Ray – *Infosys Technologies Ltd*

Dhanashri Dorle – *Infosys Technologies Ltd*

Mehul Mediwala – *Infosys Technologies Ltd*

Paresh Gujar – *Infosys Technologies Ltd*

Raxit Gajjar – *Infosys Technologies Ltd*

Rob Pike – *Microsoft*

Varun Rastogi – *Infosys Technologies Ltd*

Editors

John Cobb – *Wadeware LLC*

John Tobey – *Volt Information Sciences*

Kelly McMahon – *Content Master*

Reid Bannecker – *Volt Information Sciences*

Steve Wacker – *Wadeware LLC*

Contributors and Reviewers

Rich Benack, Shelly Bird, Susan Bradley, Duane Crider, Steve Dodson, Christine Duell, Mike Kaczmarek, Mark Kradel, Mike Lonergan, Joe Porter, Tom Shinder, Ben Smith, Josh Vincent, Jessica Zahn, Jeff Williams, Ignacio Avellaneda, Ganesh Balakrishnan, Nathan Buggia, Derick Campbell , Chase Carpenter, Bryan Chee, Jeff Cohen, Mike Danseglio, John Dwyer, Sean Finnegan, Karl Grunwald, Jesper Johansson**,** Joanne Kennedy, Jeff Newfeld, Rob Oikawa, and Jay Zhang, Roger Abell, *Arizona State University,* James Noyce, Jim Whitney, *Configuresoft, Volt Information Sciences,* Chrissy Lewis, *Siemens Business Services,* Frank Manning, *Volt Information Sciences*, David Mowers, Stacey Tsurusaki, *Volt Information Sciences*, and David Visintainer, *Volt Information Sciences.*

Note The United States Department of Commerce National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

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.

Chapter 1: Implementing the Security Baseline

Group Policy is a feature of the Active Directory® directory service that facilitates change and configuration management in Windows Server® 2008 and Windows Server® 2003 domains. However, you need to perform certain preliminary steps in your domain before you apply Group Policy to computers running Windows XP Professional Service Pack 3 (SP3) in your environment.

Group Policy settings are stored in Group Policy objects (GPOs) in the Active Directory database. The GPOs are linked to containers, which include Active Directory sites, domains, and organizational units (OUs). Because Group Policy is so closely integrated with Active Directory, it is important to have a basic understanding of Active Directory structure and the security implications of different design configuration options within it before you implement Group Policy. For more information about Active Directory design, see Chapter 1, "Windows Server 2003 Hardening Mechanisms" in the *Windows Server 2003 Security Guide*.

Group Policy is an essential tool for securing Windows XP Professional SP3. This chapter provides background information to help you implement Group Policy to apply and maintain a consistent security policy across a network from a central location.

To deploy this guidance, you need to:

- Create an organizational unit (OU) structure for your environment.
- Run the Security Compliance Manager (SCM) tool for this guide.
- 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 "Implementing the Security Policies" section in this chapter provides procedural details you can use to create and deploy the OU structure and security GPOs during both the test and production phases of the implementation.

The baseline GPOs that accompany this guide provide a combination of tested settings that enhance security for client computers running Windows XP Professional SP3 in the following two distinct environments:

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

Enterprise Client Environment

The Enterprise Client (EC) environment in this chapter consists of a domain using Active Directory, in which computers running Windows Server 2008, Windows Server 2003 R2, or Windows Server 2003 SP2 or later, manage client computers that can run 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 Active Directory that enables directory-based change and configuration management of user and computer settings, including security and user data.

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 XP Professional SP3. Concern for security is so great in these environments that a significant loss of functionality and manageability is acceptable. The Enterprise Client (EC) security baseline helps provide enhanced security that allows sufficient functionality of the operating system and applications for the majority of organizations.

⚠ **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 on 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 Terminal Services, which allows multiple 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 XP Professional SP3. 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. You can also use the Microsoft Excel® workbook Windows XP Security Baseline Settings to compare and evaluate the Group Policy settings.

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

Limited Functionality

The specialized security that 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

You can configure system services to one of three startup types: automatic, disabled, and manual. While the meanings of the first two types should be obvious, the third type does cause confusion sometimes. When a service is configured to manual startup, it will launch when a specific event occurs. For example, the Disk Management service launches when the Disk Management snap-in opens. In other cases, a service may launch another when specific conditions are met. The key thing to remember when modifying the configuration of a system service is that changing the default startup type from manual or automatic to any other value will probably cause the service, and consequently some Windows features, to behave differently or fail.

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 XP Professional SP3. 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 XP Security Baseline Settings workbook that also accompanies this guide. This provides another resource that you can use 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 over-extends 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.

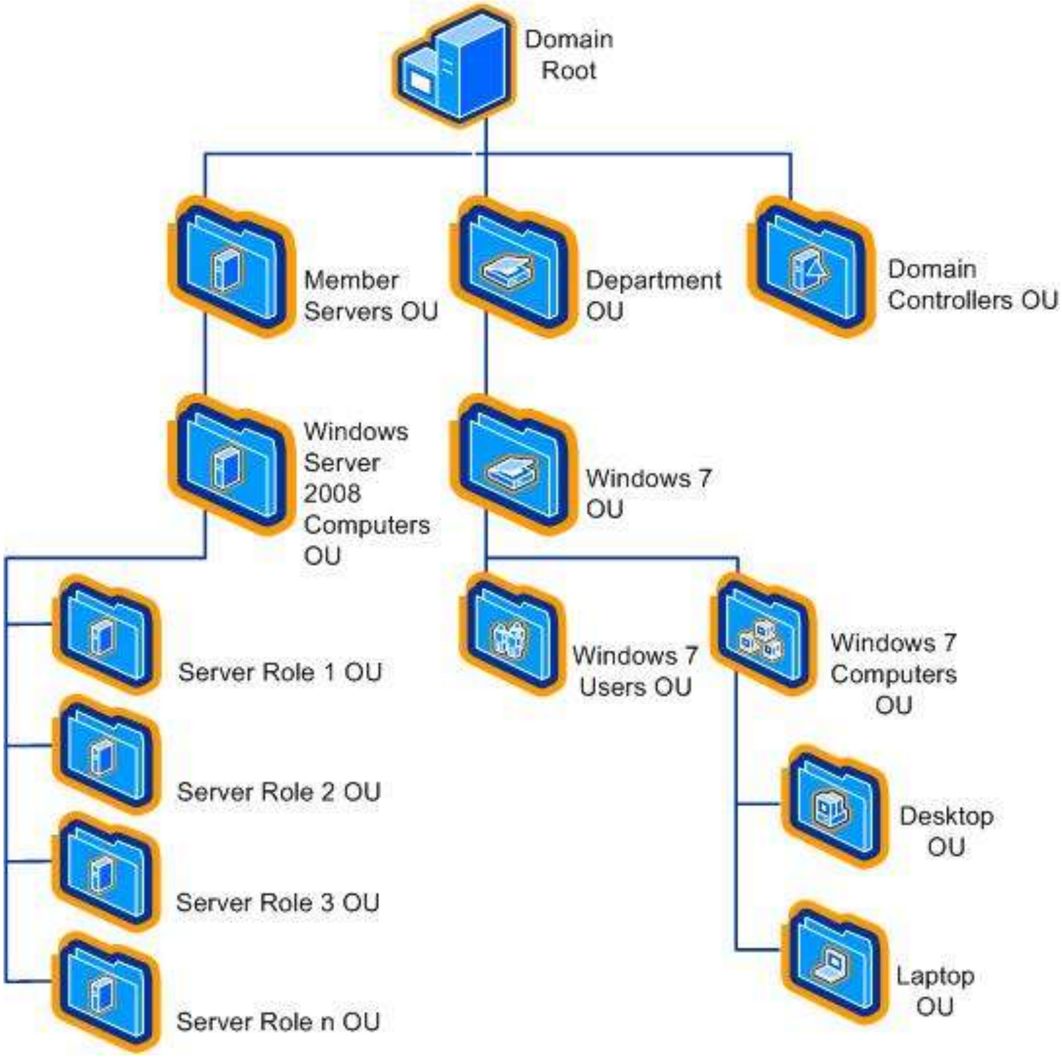


Figure 1.1 Example OU structure for computers running Windows 7 and Windows Server 2008

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.

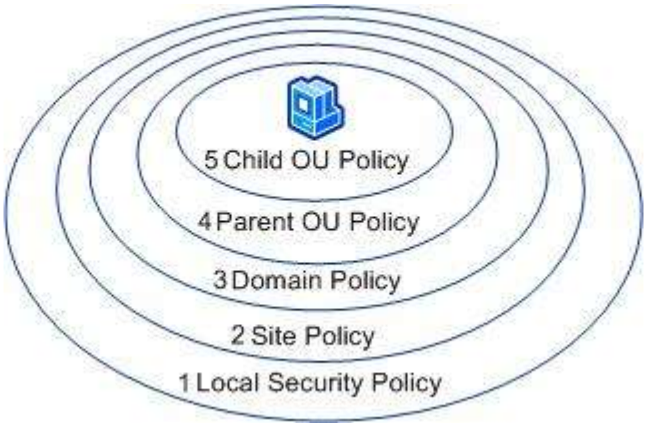


Figure 1.2 GPO order of precedence

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.

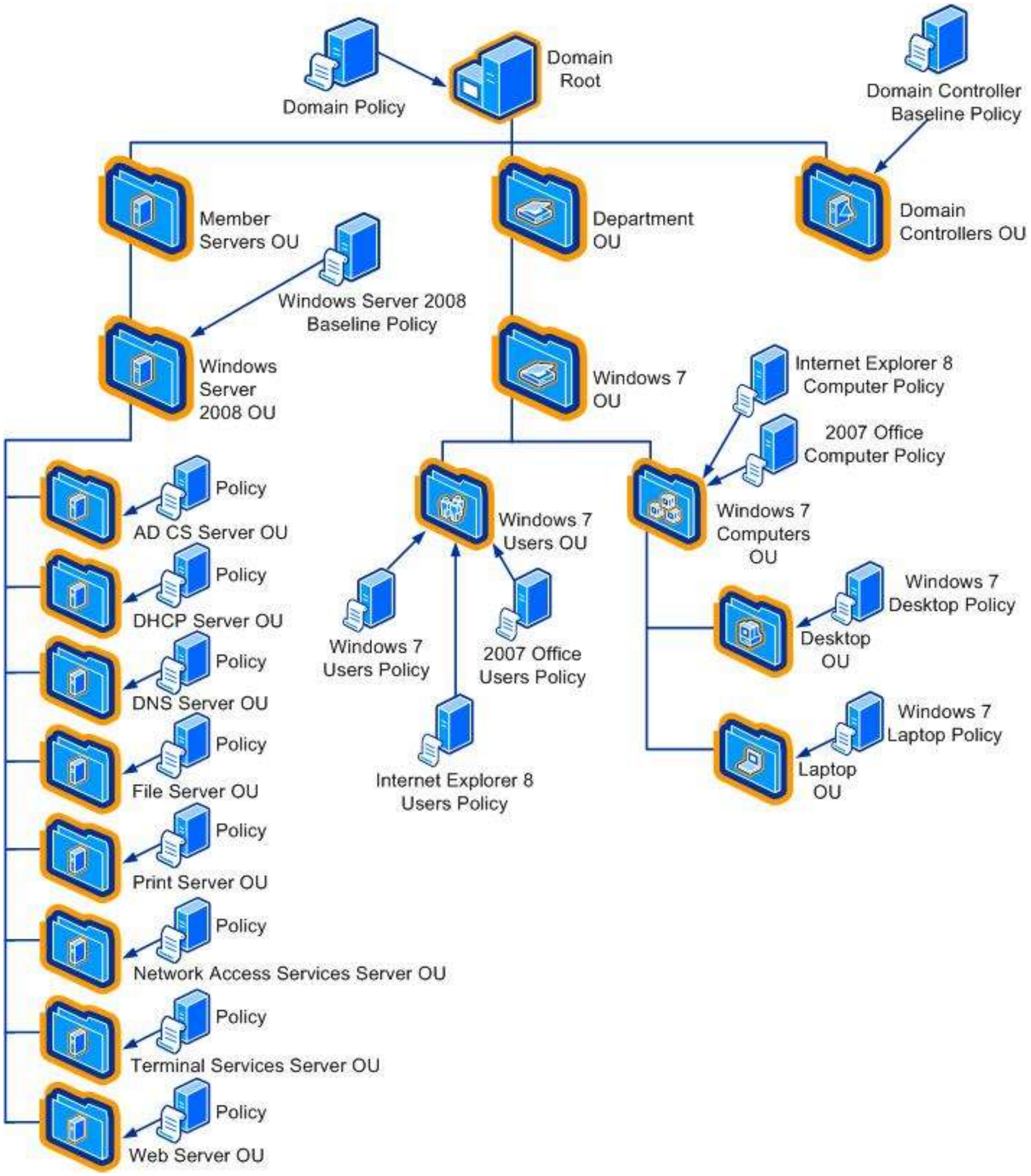


Figure 1.3 Example OU structure and GPO links for computers running Windows 7 and Windows Server 2008

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 Server 2008 Security Guide*
- *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

Security Templates

Security Templates are text files that contain security setting values. They are subcomponents of GPOs, The policy settings that are contained in Security Templates can be modified in the MMC Group Policy Object Editor snap-in, and they are located under the **Computer Configuration\Windows Settings\Security Settings** folder. You can also modify these files with the MMC Security Templates snap-in or with a text editor such as Notepad. Microsoft recommends using the Group Policy Object Editor snap-in to manage policy settings in Security

Templates that are in GPOs, and that you use the Security Templates snap-in to manage policy settings in stand-alone Security Templates.

Some sections of the template files contain specific access control lists (ACLs) that are defined by the Security Descriptor Definition Language (SDDL). For details about how to edit security templates and SDDL, see the "More Information" section at the end of this chapter.

Administrative Templates

Additional security settings are available in Unicode-based files that are called Administrative Templates. These files contain registry settings that affect Windows XP Professional SP3 and its components, along with other applications such as Microsoft Office 2003. Administrative Templates may include computer settings as well as user settings. Computer settings are stored in the HKEY_LOCAL_MACHINE registry hive. User settings are stored in the HKEY_CURRENT_USER registry hive

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 than 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

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.

More Information

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

- Achieving Autonomy and Isolation with Forests, Domains, and Organizational Units.
- *Best Practice Active Directory Design for Managing Windows Networks*.
- Enterprise Management with the Group Policy Management Console.
- Gpresult for more information about the Group Policy Results tool.
- Gpupdate for information about the Group Policy Update utility.
- Loopback Processing of Group Policy.
- *Microsoft Windows XP Professional Resource Kit*.
- *Step-by-Step Guide to Understanding the Group Policy Feature Set*.
- "Using Administrative Template Files with Registry-Based Group Policy" white paper.
- Windows Server Group Policy.

Chapter 2: Additional Hardening Procedures

This chapter describes some additional countermeasures that you can implement manually to secure client computer running Windows® XP for each of the security environments that are defined in this guide.

Disable Automatic Execution of Windows Error Reporting

Some organizations may feel that system debuggers such as the Windows Error Reporting tool that is included with Windows could be exploited by knowledgeable attackers. For instructions about how to disable the Windows Error Reporting, see "How to disable Dr. Watson for Windows": Microsoft Knowledge Base article 188296.

Disable SSDP/UPNP: Disable SSDP/UPNP

Some organizations also may feel that the Universal Plug and Play features that are included with subcomponents of Windows XP Professional SP3 should be completely disabled. Although the **Universal Plug and Play host** service is disabled in this guide, other applications, such as Windows Messenger, use the **Simple Service Discovery Protocol (SSDP) discovery service** process to identify network gateways or other network devices. You can ensure that no applications use the SSDP and UPnP features that are included with Windows XP Professional SP3 by adding a REG_DWORD registry value called **UPnPMode** to the **HKEY_LOCAL_MACHINE\Software\Microsoft\DirectPlayNATHelp\DPNHUPnP\** registry key, and then setting its value to **2**.

For more information, see "Traffic Is Sent After You Turn Off the SSDP Discover Service and Universal Plug and Play Device Host": Microsoft Knowledge Base article 317843.

Securing the File System

The NTFS file system has been improved with each new version of Microsoft Windows®. The default permissions for NTFS are adequate for most organizations. The settings that are discussed in this section are for organizations that use laptops and desktops in the Specialized Security – Limited Functionality (SSLF) environment defined in this guide.

File system security settings can be modified through Group Policy. You can configure the file system settings in the following location in the Group Policy Object Editor:

Computer Configuration\Windows Settings\Security Settings\File System

Caution: Ensure to thoroughly test any changes to the default file system security settings in a lab environment before deploying them in a large organization. There have been cases in which file permissions have been altered to a point that required the affected computers to be completely rebuilt.

The default file permissions in Windows XP Professional SP3 are sufficient for most situations. However, if you are not going to block membership of the **Power Users** group with the Restricted Groups feature or if you are going to enable the **Network access: Let Everyone permissions apply to anonymous users** setting, you may want to apply the optional permissions that are described in the next paragraph. These optional permissions are very specific, and they apply additional restrictions to certain executable tools that a malicious user with elevated privileges may use to further compromise the system or network.

Note that these permission changes do not affect multiple folders or the root of the system volume. It can be very risky to change permissions in that manner, and doing so can often cause system instability. All of the files are located in the **%SystemRoot%\System32\** folder, and they are all given the following permissions: **Administrators: Full Control, System: Full Control**.

- regedit.exe
- arp.exe
- at.exe
- attrib.exe
- cacls.exe
- debug.exe
- edlin.exe
- eventcreate.exe
- eventtriggers.exe
- ftp.exe
- nbtstat.exe
- net.exe
- net1.exe
- netsh.exe
- netstat.exe
- nslookup.exe
- ntbackup.exe
- rcp.exe
- reg.exe
- regedt32.exe
- regini.exe
- rexec.exe
- route.exe

- rsh.exe
- sc.exe
- secedit.exe
- subst.exe
- systeminfo.exe
- telnet.exe
- tftp.exe
- tlntsvr.exe

Advanced File and Folder Permissions

You can set file and folder permissions with more control than the default permissions in the **Permissions** dialog box. To do so, right-click the file, choose **Properties**, and then on the <*File Properties*> page, click **Advanced**. The following table describes these advanced file permissions.

Table 2.1 Advanced File Permissions and Descriptions

Advanced permission name	Description
Traverse Folder/Execute	Allows or denies user requests to move through folders to reach other files or folders, even if the user has no permission to traverse folders (applies to folders only).
List Folders/Read Data	Allows or denies user requests to view file names and subfolder names within the specified folder. It only affects the contents of that folder and does not affect whether the folder on which you are setting the permission will be listed (applies to folders only).
Read Attributes	Allows or denies the ability to view data in files (applies to files only).
Read Extended Attributes	Allows or denies user requests to view the attributes of a file or folder, such as read-only and hidden. Attributes are defined by NTFS.
Create Files/Write Data	Create Files allows or denies creating files within the folder (applies to folders only). Write Data allows or denies the ability to make changes to the file and overwrite existing content (applies to files only).
Create Folders/Append Data	Create Folders allows or denies user requests to create folders within a specified folder (applies to folders only). Append Data allows or denies the ability to make changes to the end of the file but not to change, delete, or overwrite existing data (applies to files only).
Write Attributes	Allows or denies user requests to make changes to the end of the file, but not to change, delete, or overwrite existing data (applies to files only).
Write Extended Attributes	Allows or denies user requests to change the attributes of a file or folder, such as read-only or hidden. Attributes are defined by NTFS.

Advanced permission name	Description
Delete Subfolders and Files	Allows or denies the ability to delete subfolders and files, even if the Delete permission has not been assigned on the subfolder or file (applies to folders).
Delete	Allows or denies user requests to delete subfolders and files, even if the Delete permission has not been assigned on the subfolder or file (applies to folders).
Read Permissions	Allows or denies user requests to read the permissions of files or folders, such as Full Control, Read, and Write.
Change Permissions	Allows or denies user requests to change permissions of files or folders, such as Full Control, Read, and Write.
Take Ownership	Allows or denies taking ownership of the file or folder. The owner of a file or folder can always change permissions on it, regardless of any existing permissions that protect the file or folder.

The following three additional terms are used to describe the inheritance of permissions that are applied to files and folders:

- **Propagate** refers to the propagation of inheritable permissions to all subfolders and files. Any child objects of an object inherit the parent object's security settings, provided the child object is not protected from accepting permission inheritance. If there is a conflict, the explicit permissions on the child object will override the permissions that are inherited from the parent object.
- **Replace** refers to the replacement of existing permissions on all subfolders and files with inheritable permissions. The parent object's permission entries will override any security settings on the child object, regardless of the child object's settings. The child object will have identical access control entries as the parent object.
- **Ignore** refers to not allowing permissions on a file or folder (or key) to be replaced. Use this configuration option if you do not want to configure or analyze security for this object or any of its child objects.

More Information

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

- "How to disable Dr. Watson for Windows": Microsoft Knowledge Base article 188296.
- "Traffic Is Sent After You Turn Off the SSDP Discover Service and Universal Plug and Play Device Host": Microsoft Knowledge Base article 317843.

Chapter 3: Software Restriction Policy for Windows XP Client Computers

Software restriction policy provides administrators with a way to identify software and control its ability to run on local computers. This feature can help protect computers that run Windows® XP Professional against known conflicts and safeguard them against malicious software, such as viruses and Trojan horse programs. Software restriction policy integrates fully with the Active Directory® directory service and Group Policy. You can also use it on stand-alone computers. Software restriction policy requires an administrator to define the applications that are allowed to run on the client computers in your environment and to determine the restrictions that the policy will apply to the client computers.

When you implement software restriction policy, the first decision you must make is whether to configure the default security level to **Unrestricted** or **Disallowed**. If the default security level is set to **Unrestricted**, then all software is allowed to run and you must configure additional rules to block specific applications. The more secure approach is to configure the default security level to **Disallowed**, which does not allow any software to run, and then configure additional rules to allow specific applications. You can apply software restriction policy to multiple computers through domain–based Group Policy or to individual computers through local Group Policy.

Important: It is important to thoroughly test all of the policy settings discussed in this guide before you deploy them to production systems, especially software restriction policy settings. Mistakes in the design or implementation of this feature can cause considerable user frustration.

Software restriction policy provides a number of ways to identify software, as well as a policy–based infrastructure to enforce rules on how the identified software may run. Computer users must comply with the guidelines that are established in the software restriction policy by the administrator in their environment.

You can use software restriction policy to accomplish the following:

- Control what software may run on the client computers in your environment.
- Restrict user access to specific files on multi-user computers.
- Decide who may add trusted publishers to client computers.
- Define whether the policies affect all users or a subset of users on the client computers.
- Prevent executable files from running on your local computers based on policies that are set at a computer, OU, site, or domain level.

Software Restriction Policy Architecture

Software restriction policy provides the following powerful features:

- **Policy enforcement that is either domain–based or local computer–based**. Administrators create the policy and then define which applications are trusted and which are not. The policy is enforced at run time and users do not receive prompts that allow them to choose whether to run executable files.
- **Policy that applies to more than just binary executable files**. The definition of what constitutes software is ambiguous. Software restriction policy provides control over Microsoft Visual Basic® Scripting Edition (VBScript), JScript®, and other scripting languages. It also integrates with the Windows Installer feature to provide control over which packages can be installed on client computers. This feature includes an application programming interface (API) that you can use to coordinate the policy runtime with other runtimes.
- **Policy that is scalable**. Because it is implemented through Group Policy, software restriction policy can be effectively implemented and managed across domains that consist of tens of thousands of computers.
- **Policy that is flexible**. Administrators have the flexibility to prohibit unauthorized scripts, to regulate Microsoft ActiveX® controls, and to tightly lock down client computers.
- **Policy that enables strong cryptography to identify software**. Software restriction policy can identify software using hashes or digital signatures.

Software restriction policy implementation includes three phases:

1. The administrator or a delegated authority creates the policy with the Microsoft Management Console (MMC) Group Policy snap-in for the Active Directory container site, domain, or OU. Microsoft recommends creating a separate Group Policy object (GPO) for software restriction policy.

   Note: To create a new software restriction policy for a local stand-alone computer, you must be a member of the **Administrators** group on the local computer. To configure these policy settings, click **Windows Settings**, **Security Settings**, and then **Software Restriction Policy**.

2. The computer-level policy is downloaded and takes effect after you start the computer. User policies take effect when the user logs on to the system or domain. To update the policy, execute the **gpupdate.exe /force** command.
3. When a user starts an executable file such as an application or script, the policy determines whether it can run according to its precedence rules.

Unrestricted or Disallowed Settings

A software restriction policy consists of two parts:

- A default rule that specifies which programs may run.
- An inventory of exceptions to the default rule.

You can set the default rule that is used to identify software to either **Unrestricted** or **Disallowed**—which allow you to either run or not run all software, respectively. If you set the default rule to **Unrestricted**, an administrator can define exceptions or a set of programs that are not allowed to run. Use the **Unrestricted** default setting in an environment with loosely managed client computers. For example, you can restrict users' ability to install a program that will conflict with existing programs by creating a rule to block it.

A more secure approach is to set the default rule to **Disallowed** and then allow only a specific set of programs to run. The **Disallowed** default setting requires an administrator to define all the rules for each application and ensure that users have the correct security policy settings on their computers to access the applications that they are allowed to run. The **Disallowed** default setting is the more secure approach for organizations that want to protect client computers running Windows XP Professional SP3.

Four Rules to Identify Software

Rules in a software restriction policy identify one or more applications and specify what software is allowed to run. The enforcement engine in Windows XP Professional SP3 queries the policy's rules before applications are allowed to run. To create a rule, you need to identify applications and then categorize them as exceptions to the **Disallowed** default setting. Each rule can include comments to describe its purpose.

A software restriction policy uses the following four rules to identify software:

- **Hash Rule**. Uses a cryptographic fingerprint of the executable file.
- **Certificate Rule**. Uses a digitally signed certificate from a software publisher for the .exe file.
- **Path Rule**. Uses the local, Universal Naming Convention (UNC), or registry path of the .exe file location.
- **Zone Rule**. Uses the Internet Zone where the executable file originated (if it was downloaded using Microsoft Internet Explorer®).

The Hash Rule

A *hash* is a digital fingerprint that uniquely identifies a software program or executable file even if the program or executable file is moved or renamed. Administrators can use a hash to track a particular version of an executable file or program that they may not want users to run.

With a hash rule, software programs remain uniquely identifiable because the hash rule match is based on a cryptographic calculation that involves the contents of the file. The only file types that are affected by hash rules are those that are listed in the **Designated File Types** section of the details pane for **Software Restriction Policies**.

Hash rules work effectively in a static environment. If software in your environment is upgraded, the hash needs to be recalculated for each updated executable file. Hash rules work well in environments that experience infrequent software changes or upgrades.

A hash rule consists of the following three pieces of data, separated by colons:

- The MD5 or SHA-1 hash value
- The file length
- The hash algorithm ID number

Digitally signed files use the hash value that is contained in the signature, which may be MD5 or SHA-1. Executable files that are not digitally signed use an MD5 hash value.

Hash rules are formatted as follows:

```
[MD5 or SHA1 hash value]:[file length]:[hash algorithm id]
```

The following hash rule example is for a 126-byte file with contents that match the MD5 hash value (7bc04acc0d6480af862d22d724c3b049) and the hash algorithm (denoted by the hash algorithm identifier 32771):

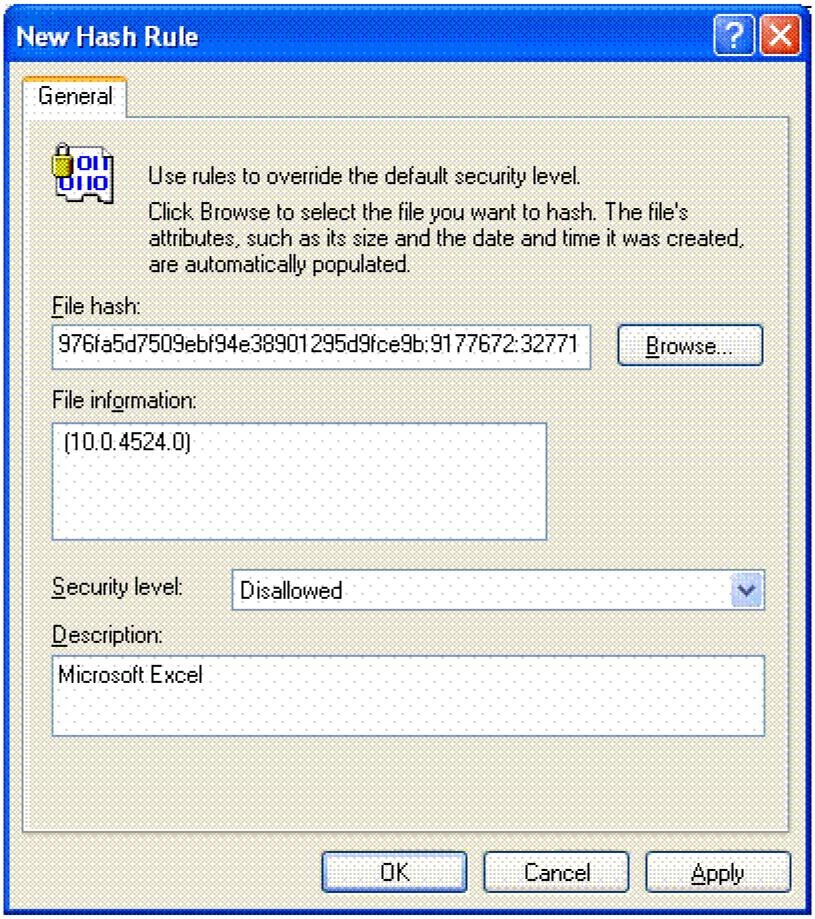
7bc04acc0d6480af862d22d724c3b049:126:32771

Each file that the administrator wants to restrict or allow needs to contain a hash rule. When software is updated, the administrator must create a new hash rule for each application because the hash values for the original executable files will not match those of the new files.

Complete the steps in the following procedure to create a hash rule for an executable file.

To create a hash rule for an existing executable file

1. On the Group Policy Object Editor tool bar, click **Windows Settings**, **Security Settings**, **Software Restriction Policy**, and then right-click **Additional Rules**.
2. Click **New Hash Rule** on the shortcut menu.



Use rules to override the default security level.

Click Browse to select the file you want to hash. The file's attributes, such as its size and the date and time it was created, are automatically populated.

File hash: 976fa5d7509ebf94e38901295d9fce9b:9177672:32771

File information: (10.0.4524.0)

Security level: Disallowed

Description: Microsoft Excel

Figure 3.1 The New Hash Rule dialog box

3. Click **Browse** to select the file for which you want to create a hash rule. In this example, the executable file is **Excel.exe**. The new file hash value displays in the **File Hash:** box, and the application version displays in the **File Information:** box.
4. Select the default security level setting that you want for this rule. The options are:
   - **Disallowed**
   - **Unrestricted**

The Certificate Rule

A certificate rule specifies that a software publisher's certificate (used for code-signing) must exist before a program is allowed to run. For example, an administrator can require signed certificates for all scripts and ActiveX controls. Allowable sources that comply with the certificate rule include:

- A commercial certificate authority (CA), such as VeriSign.
- A Windows Server® 2003 or Windows Server® 2008 public key infrastructure (PKI).
- A self-signed certificate.

A certificate rule is a strong software identification method because it uses signed hashes in the signature of the signed file to match files, regardless of name or location. Unfortunately, few software vendors use code-signing technology, and even those that do typically sign a small percentage of the executable files that they distribute. For these reasons, certificate rules are generally used for a few specific application types such as ActiveX controls or internally developed applications. For example, this guide recommends that organizations digitally sign scripts that are used to manage computers and users so that all unsigned scripts can be blocked. A hash rule can be used to identify exceptions to a certificate rule.

Enabling Certificate Rules

Certificate rules are not enabled by default. Complete the steps in the following procedure to enable certificate rules.

To enable certificate rules

1. Use the Group Policy Object Editor to open the GPO.
2. In the console tree, click **Security Options**.
3. In the details pane, double-click **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies**.
4. To make the certificate rules available, click **Enabled**.

For detailed instructions about how to digitally sign files, see the *Step-by-Step Guide to Digitally Signing Files with Test Certificates* section in the appendix of the Using Software Restriction Policies to Protect Against Unauthorized Software.

Many commercial Web sites have their software code-signed by a commercial certification authority (CA). These certificates are usually valid from one to several years. When you use certificate rules, be aware that the certificates carry expiration dates. You may be able contact the software publisher to find out more information about the expiration period for a published certificate. When you receive a certificate from a commercial CA or software publisher, you can export it to a file to create a certificate rule.

To export a certificate using Internet Explorer 7

1. On the main toolbar of the browser, click **Tools**, and then select **Internet Options**.
2. On the **Internet Options** dialog, click the **Content** tab, and then click **Certificates**.
3. Scroll right and click the **Trusted Publishers** tab.
4. Select the desired certificate and click **Export** to start the Certificate Export Wizard.
5. Use the wizard to export the certificate in the *DER encoded binary X.509* format.

Note: The procedure for exporting certificates in Internet Explorer 6 is slightly different, to do so follow the instructions for exporting certificates in DER encoded binary X.509 format in the "Installing and Removing Trusted Certificates" section Chapter 6, "Digital Certificates" of the *Microsoft Internet Explorer 6 Resource Kit*.

The Path Rule

A path rule specifies either a folder or a fully qualified path to a program. When a path rule specifies a folder, it matches any program that is contained in that folder and any programs that are contained in subfolders of that folder. Path rules support both local and UNC paths.

The administrator must define all directories from which a specific application can launch in the path rule. For example, if a desktop shortcut is used to launch an application, the path rule must specify both the executable file and the shortcut paths to run the application. If a user attempts to run an application with only a partial path rule, the **Software Restricted** warning displays.

Many applications use the *%ProgramFiles%* variable to install files on the hard drive of Windows XP Professional SP3–based computers. Unfortunately, some applications are hard-coded to copy files to the **C:\Program Files** subdirectory, and will do so even if this variable is set to another directory on a different drive. Remember this limitation when you create and test path rules.

Using Environment Variables in Path Rules

You can define a path rule to use environment variables. Because path rules are evaluated in the client environment, environment variables allow an administrator to adapt a rule to a particular user's environment.

The following two examples show instances of how to apply environment variables to a path rule.

- "%UserProfile%" matches **C:\Documents and Settings\<*User*>** and all subfolders under this directory.
- "%ProgramFiles%\<*Application*>" matches **C:\Program Files\<*Application*>** and all subfolders under this directory.

Note: Environment variables are not protected by access control lists (ACLs). There are two types of environment variables, **User** and **System**. Users who are able to start a command prompt can redefine the **Users** environment variable to a different path. Only users in the **Administrators** group can change the **System** environment variable.

Although the two preceding examples are very useful, you may want to consider other available environment variables. For a complete list, see the Command shell overview.

Using Wildcards in Path Rules

A path rule can incorporate the "?" and "*" wildcards. The following examples show wildcards that are applied to different path rules:

- **\\DC – ??\login$** matches **\\DC – 01\login$**, **\\DC – 02\login$**, and so on.
- ***\Windows** matches **C:\Windows**, **D:\Windows**, **E:\Windows**, and all subfolders under each directory.
- **C:\win*** matches **C:\winnt**, **C:\windows**, **C:\windir**, and all subfolders under each directory.
- ***.vbs** matches any application that has this extension in Windows XP Professional SP3.
- **C:\Application Files*.*** matches all application files in the specific subdirectory.

Registry Path Rules

Many applications store paths to their installation folders or application directories in the Microsoft Windows registry. Some applications can be installed anywhere on the file system. To locate them, you can create a path rule to look up their registry keys.

These locations may not be easily identified using specific folder paths, such as **C:\Program Files\Microsoft Platform SDK**, or environment variables, such as **%ProgramFiles%\Microsoft Platform SDK**. However, if the program stores its application directories in the registry, you can create a path rule that will use the value that is stored in the registry, such as:

> **%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PlatformSDK\Directories\Install Dir%**

This type of path rule, called a registry path rule, is formatted as follows:

> *%<Registry Hive>\<Registry Key Name>\<Value Name>%*

Note: Any registry path rule suffix should not contain a \ character immediately after the last % sign in the rule. The registry hive name must be written completely; abbreviations will not work.

When the default rule is set to **Disallowed**, four registry path rules are set up so that the operating system has access to system files. These registry path rules are created as a safeguard—so that you do not lock yourself and all other users out of the system—and are set to **Unrestricted**. These rules should only be modified or deleted by advanced users. The registry path rule settings are:

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

Path Rule Precedence

When there are multiple path rules that match, the most specific rule takes precedence over the others. The following set of paths is ordered from highest precedence (most specific match) to lowest precedence (most general match):

- Drive:\Folder1\Folder2\FileName.Extension
- Drive:\Folder1\Folder2\*.Extension
- *.Extension
- Drive:\Folder1\Folder2\
- Drive:\Folder1\

Zone Rule

You can use a zone rule to identify software that is downloaded from any of the following zones that are defined in Internet Explorer:

- Internet
- Intranet
- Restricted Sites

- Trusted Sites
- My Computer

The current version of the Internet zone rule applies only to Windows Installer (*.msi) packages. Also, this rule does not apply to software that is downloaded through Internet Explorer. All other file types that are affected by zone rules are listed in the Designated File Types table later in this chapter. One list of designated file types is shared by all zone rules.

Rule Recommendations

Use the information in the following table to determine which type of rule is best suited for an application’s users and environment.

Table 3.1 Determining the Best Rule for a Given Application

Task	Recommended rule
Allow or disallow a specific program version.	**Hash rule** Browse to the file to create a hash rule.
Identify a program always installed in the same place.	**Path rule with environment variables** %ProgramFiles%\Internet Explorer\iexplore.exe
Identify a program that can be installed anywhere on client computers.	**Registry path rule** %HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\InoculateIT\6.0\Path\HOME%
Identify a set of scripts on a central server.	**Path rule** \\SERVER_NAME\Share
Identify a set of scripts on a set of servers. For example, DC01, DC02, and DC03.	**Path rule with wildcard** \\DC??\Share
Disallow all .vbs files, except those in a login script directory.	**Path rule with wildcard** *.VBS set to **Disallowed** \\LOGIN_SRV\Share\*.VBS set to **Unrestricted**
Disallow a file installed by a virus that is always called Flcss.exe.	**Path rule** Flcss.exe set to **Disallowed**
Identify a set of scripts that can be run anywhere.	**Certificate rule** Use a certificate to digitally sign the scripts.
Allow software to be installed from trusted Internet zone sites.	**Zone rule** Set **Trusted Sites** to **Unrestricted**.

Software Restriction Policy Precedence Rules

Rules are evaluated in a specific order. The rules that more specifically match a program take precedence over rules that more generally match the same program. If two identical rules with differing security levels are established for the same software, the rule with the highest security level takes precedence. For example, if two hash rules—one with the security level **Disallowed** and one with the security level **Unrestricted**—are applied to the same software program, the rule with the security level **Disallowed** takes precedence, and the program will not run. The following list defines the precedence order for the rules, from the most specific to the least specific:

1. Hash rule
2. Certificate rule
3. Path rule
4. Zone rule
5. Default rule

Software Restriction Policy Options

This section discusses the various enforcement options that influence the way a software restriction policy functions. These options alter the way Microsoft Authenticode® trust settings are enforced for digitally signed files. There are two enforcement options: Dynamic-link library (DLL) checking and Skip Administrators.

DLL Checking

Most programs consist of an executable file and many supporting DLLs. By default, software restriction policy rules are not enforced on DLLs. This default setting is recommended for most customers for the following three reasons:

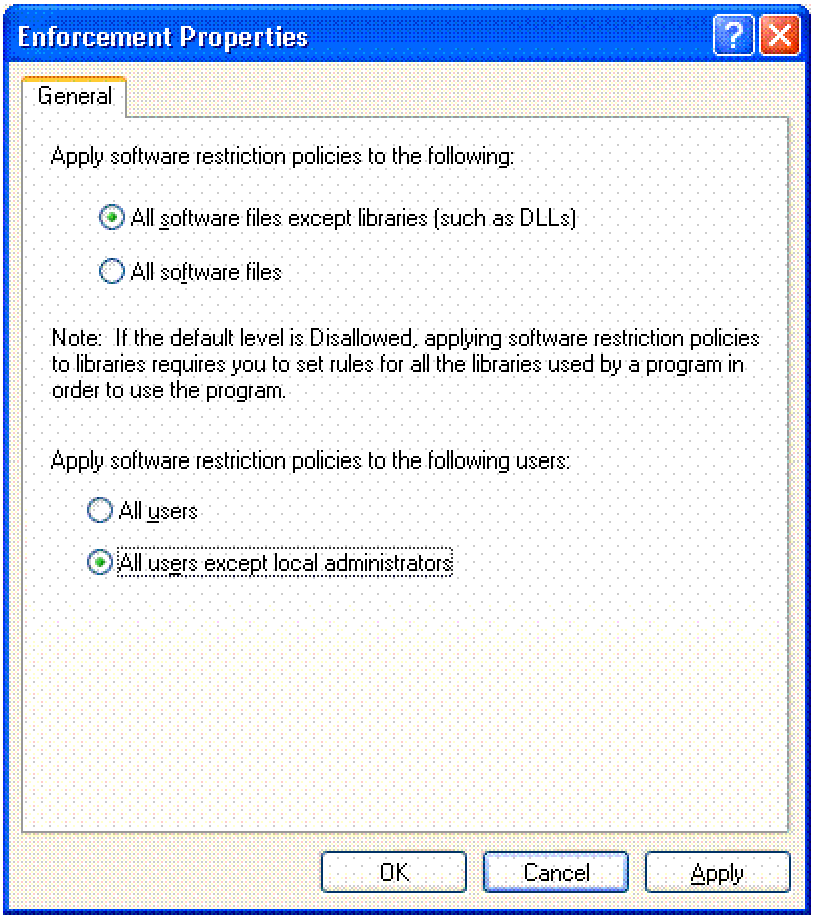
- If the main executable file is disallowed the program is prevented from running, so there is no need to disallow the constituent DLLs.
- DLL checking degrades system performance because it has to check all libraries that are linked to the application. For example, if a user runs 10 programs during a logon session, the software restriction policy evaluates each program. With DLL checking turned on, the software restriction policy evaluates each DLL load within each program. If each program uses 20 DLLs, this configuration would result in 10 executable program checks plus 200 DLL checks—which would require the software restriction policy to perform 210 evaluations. A program such as Internet Explorer consists of an executable file (iexplore.exe) and many supporting DLLs.
- If the default security level is set to **Disallowed**, the system is forced to not only identify the main executable file before it is allowed to run but also all of the .exe file's constituent DLLs, which places added burden on the system.

Because viruses primarily target executable files, some specifically target DLLs. Therefore, DLL checking is the recommended option when you want the highest possible assurance for the programs running in your environment.

To ensure that a program does not contain a virus, you can use a set of hash rules that identify the executable file and all of its constituent DLLs.

To turn off the DLL Checking option

- When you edit a software restriction policy, in the **Enforcement Properties** dialog box, select **All software files except libraries (such as DLLs)** as shown in the following figure:



Apply software restriction policies to the following:

● All software files except libraries (such as DLLs)

○ All software files

Note: If the default level is Disallowed, applying software restriction policies to libraries requires you to set rules for all the libraries used by a program in order to use the program.

Apply software restriction policies to the following users:

○ All users

● All users except local administrators

Figure 3.2 The Enforcement Properties dialog box for file and user enforcement options

Skip Administrators

You may want to disallow programs from running for most users but allow administrators to run all of them. For example, an administrator may have a shared computer that multiple users connect to through Terminal Server. The administrator may want users to run only specific applications on the computer, but allow members in the local **Administrators** group to run anything. Use the **Skip Administrators** enforcement option to achieve this functionality.

If the software restriction policy is created in a GPO that is linked to an object in Active Directory, Microsoft recommends to deny the **Apply Group Policy** permission on the GPO to the **Administrators** group and to not use the **Skip Administrators** option. This method consumes less network bandwidth because GPO settings that do not apply to administrators are not downloaded.

Note: Software restriction policy defined in local security policy objects cannot filter user groups, and would therefore require use of the **Skip Administrators** option.

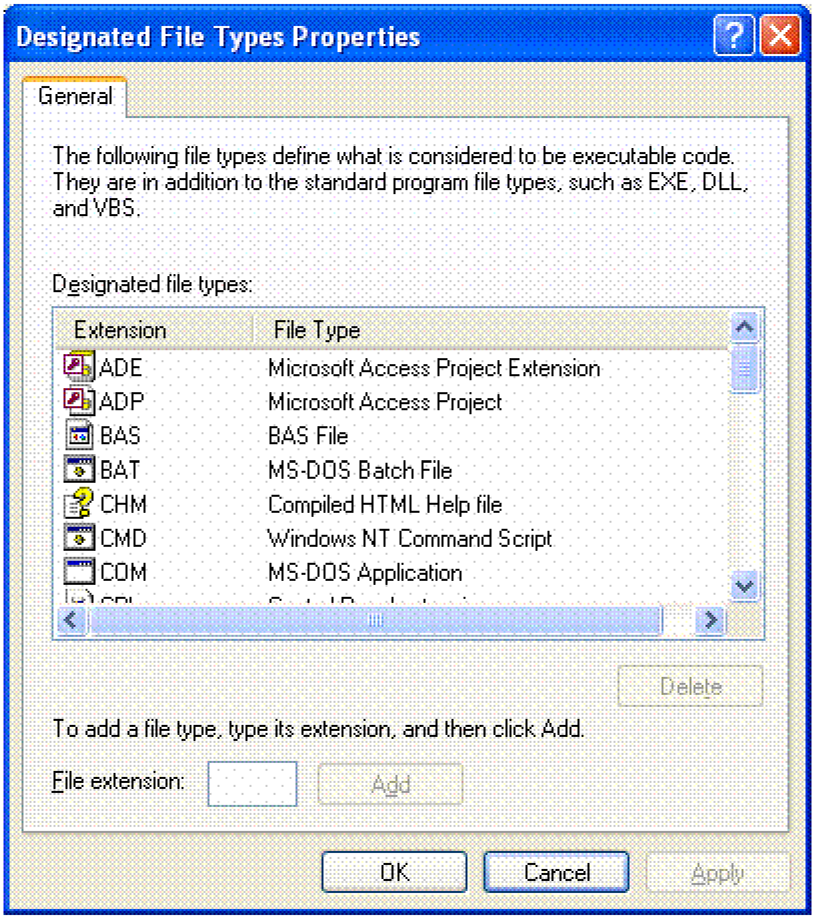
To turn on the Skip Administrators option

- In the **Enforcement Properties** dialog box (shown in Figure 3.2), select **All users except local administrators**.

Defining Executables

The **Designated File Types Properties** dialog box in the following figure lists the file types that are governed by software restriction policy. These file types are considered executable files. For example, a screen saver file (.scr), is considered an executable file because it loads as a program when you double-click it in Windows Explorer.

Software restriction policy rules only apply to the file types listed in the **Designated File Types Properties** dialog box. If your environment uses a file type that you want to apply rules to, add it to the list. For example, for Perl script files you may choose to add .pl and other file types associated with the Perl engine to the **Designated file types:** list under the **General** tab of the **Designated File Types Properties** dialog box.



The following file types define what is considered to be executable code. They are in addition to the standard program file types, such as EXE, DLL, and VBS.

Designated file types:

Extension	File Type
ADE	Microsoft Access Project Extension
ADP	Microsoft Access Project
BAS	BAS File
BAT	MS-DOS Batch File
CHM	Compiled HTML Help file
CMD	Windows NT Command Script
COM	MS-DOS Application

To add a file type, type its extension, and then click Add.

File extension:

Figure 3.3 The Designated File Types Properties dialog box

For the GPO design that is defined in this guide, the file types .mdb and .lnk are removed and .ocx is added. The following table lists the designated file types.

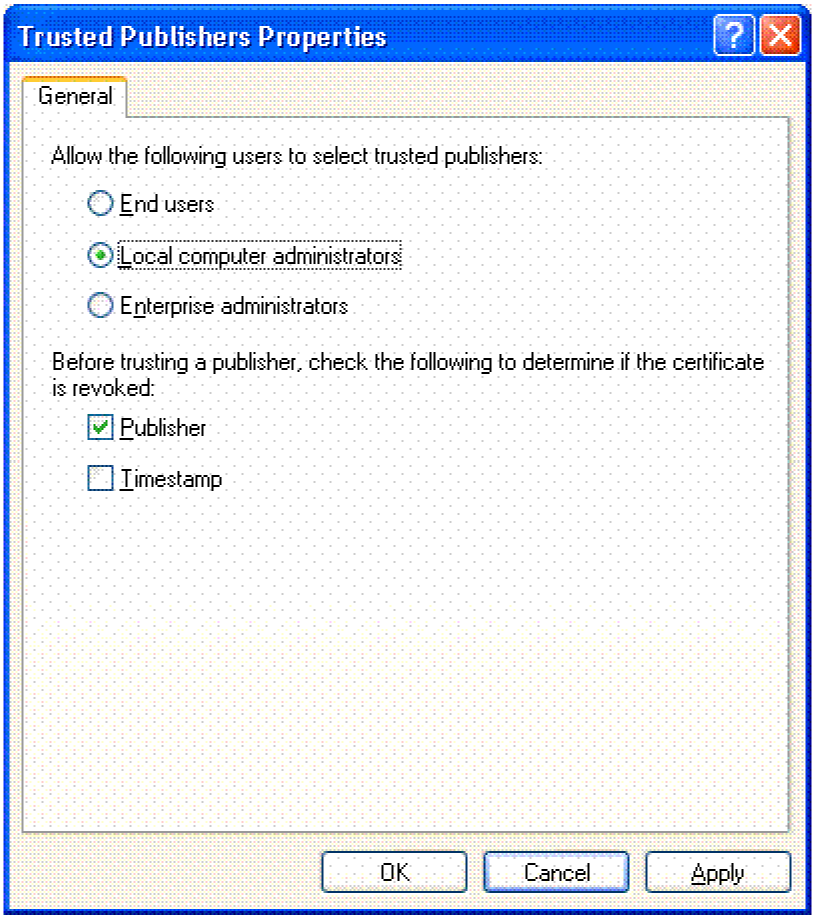
Table 3.2 Designated File Types

File extension	Description
.ade	Microsoft Access Project extension
.adp	Microsoft Access Project
.bas	Visual Basic Class Module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Windows NT command script
.com	MS-DOS application
.cpl	Control Panel extension
.crt	Security certificate
.exe	Application
.hlp	Windows Help file
.hta	HTML application
.inf	Setup Information file
.ins	Internet Communication setting
.isp	Internet Communication setting
.js	JScript file
.jse	JScript Encoded Script file
.mde	Microsoft Access MDE Database
.msc	Microsoft Common Console document
.msi	Windows Installer Package
.msp	Windows Installer Patch
.mst	Visual Test Source file
.ocx	ActiveX Control
.pcd	Photo CD Image
.pif	Shortcut to MS-DOS program
.reg	Registry entry
.scr	Screen Saver
.sct	Windows Script Component
.shs	Shell Scrap Object
.url	Internet Shortcut (Uniform Resource Locator)
.vb	Visual Basic file
.vbe	VBScript Encoded Script file
.vbs	VBScript Script file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Scripting Host Setting file

Trusted Publishers

You can use the **Trusted Publishers Properties** dialog box to configure which users can select trusted publishers. You can also determine which, if any, certificate revocation checks are performed before you trust a publisher. With certificate rules enabled, software restriction policy will check a certificate revocation list (CRL) to ensure that the software's certificate and signature are valid. However, this process may decrease performance when signed programs are started.

The options on the **General** tab of the **Trusted Publishers Properties** dialog box shown in the following figure allow you to configure settings that are related to ActiveX controls and other signed content.



Allow the following users to select trusted publishers:

○ End users

● Local computer administrators

○ Enterprise administrators

Before trusting a publisher, check the following to determine if the certificate is revoked:

☑ Publisher

□ Timestamp

Figure 3.4 The Trusted Publisher Properties dialog box

The following table shows trusted publisher options that are related to ActiveX controls and other signed content.

Table 3.3 Trusted Publisher Tasks and Settings

Setting name	Task
Enterprise administrators	Use to allow only enterprise administrators to make decisions about signed active content.
Local computer administrators	Use to allow local computer administrators to make all decisions about signed active content.
End users	Use to allow users to make decisions about signed active content.
Publisher	Use to ensure that the certificate the software publisher uses has not been revoked.
Timestamp	Use to ensure that the certificate the organization uses to time stamp the active content has not been revoked.

Software Restriction Policy Design and Deployment

This section describes how to administer software restriction policy with Group Policy snap-ins, things to consider when you edit a policy for the first time, and how to apply a software restriction policy to a group of users. A variety of issues that relate to software restriction policy deployment are also discussed.

Integration with Group Policy

You can administer software restriction policy with Group Policy snap-ins to a set of client computers as well as to all the users that log on to the computers. The policy is applied to the Desktop OU and the Laptop OU that are defined in this guide.

Domain

The administrator should create a separate GPO for the software restriction policy. This method provides a way to disable the Group Policy without disrupting other policies that are applied to the object if unexpected problems should arise.

Local

A local policy should be configured for the stand-alone client computers in your environment.

Designing a Policy

This section describes the steps to follow when you design and deploy a software restriction policy. Policy design requires you to make several decisions, all of which are described in the following table.

Table 3.4 Important Policy Design Considerations

Decision	Factors to consider
Laptops or workstations	Investigate the needs of mobile users in your environment to determine if laptops require a different policy than that for desktops. Laptops tend to need more flexibility than desktops.
Server shares, logon scripts, and home drives	You will need to define a path rule for any applications that start from a server share or home directory. You can add logon script files to the path rule. If a script calls any other script, also add the executable locations to the path rule.
GPO or local security policy	In this guide a GPO is used for the design. However, consider the effects that local policy will have on your design.
User or computer policy	This design applies all settings at the computer level.
Default security level	Microsoft recommends configuring the default setting to **Disallowed**, and then configuring the rest of the policy accordingly. The **Unrestricted** default setting is also available.

Decision	Factors to consider
Additional rules	You will need to apply additional operating system path rules as needed when you use the **Disallowed** default policy. In the **Disallowed** configuration, the four rules are created automatically.
Policy options	If you use a local security policy and do not want the policy to apply to administrators on the client computers in your environment, select the policy enforcement option **Skip Administrators**. If you want to check DLLs as well as executable files and scripts, select the policy enforcement option **DLL Checking**. If you want to establish rules for file types that are not in the default list of designated file types, use the option to add them as needed to the **Designated File Types Properties** dialog box. If you want to change who can make decisions about whether ActiveX controls and other signed content can be downloaded, select the check box for **Publisher** under the **General** tab of the **Trusted Publishers Properties** dialog box.
Applying the policy to a site, domain, or OU	The policy will reside under the OU in which the desktops and laptops are located.

Note: Although this guide recommends to enforce software restriction policy at the computer level, in many cases enforcement at the user level makes sense. For example, an organization with shared computers, such as Terminal Server application servers or call center workstations, may want to allow certain users to run a suite of applications, but block all other users.

Best Practices

Microsoft recommends creating a separate GPO for software restriction policy, so that if you need to disable the policy in an emergency it will not affect the rest of your domain or local policy. Also, if you accidentally lock down a workstation with software restriction policy in the design phase of your OU, restart the computer in **Safe mode**, log on as a local administrator, and then modify the policy. Software restriction policy is not applied when you start Windows in **Safe mode**. After you start the computer in **Safe mode**, run Gpupdate.exe and then restart it.

For the best security, use ACLs in conjunction with software restriction policy and do not give users administrative privileges. Users may try to rename or move disallowed files or overwrite unrestricted files to circumvent software restriction policy. Use ACLs to deny users access to perform either of these actions. Users who are members of the local **Administrators** group can bypass your software restriction policy. Therefore, Microsoft recommends not giving users administrative privileges whenever feasible.

Login scripts are usually located under SYSVOL on the domain controller or a centralized server. The domain controller often changes with each login. If your default rule is set to **Disallowed**, be sure to create rules that identify the locations of your logon scripts. If the logon servers have similar names, consider the use of wildcards to locate them, or use the logon script name with unrestricted settings.

Important: Test new software restriction policy settings thoroughly in test environments before you apply them to your domain. New policy settings may act differently than originally expected. Thorough testing diminishes the chance of encountering a problem when you deploy software restriction policy settings on your network.

Stepping Through the Process

Use the following information to guide you through the process of software restriction policy design and applying the design as a GPO to laptops and desktops in your environment.

Step 1: Create a GPO for the OU

Locate the OU you created for desktops or laptops in your environment. If you are working on a stand-alone client computer, the policy settings are located in the Local Computer Policy. In this policy, click **Properties**, and then create a new GPO. Name the policy according to your organization's naming convention. Remember, this policy will only be used to enforce software restrictions.

Step 2: Set the Software Restriction Policy

Right-click the GPO and click **Edit**. Traverse the tree until you locate **Windows Settings\Security Settings\Software Restriction Policy**. The first time you edit the policy you will see the following message:

> No Software Security Policies are defined.

This message warns that you will define default values when you create a policy. These default values can override policy settings from other software restriction policies. Because no software restriction policy settings have been set yet, use the default settings to start. Right-click the **Actions** menu, and select **New Software Restriction Policies**.

Step 3: Set Up the Path Rules

After you determine which applications and scripts the workstations will use, you can set up the path rules. Some programs launch other programs to perform tasks, and the software applications in your environment may depend on one or more programs that support other programs. Inventory and installation documentation about the currently installed software is very useful for tracking path rules. An example of a workstation design might include the following guidelines:

- Applications = *\Program Files
- Shared Group Applications = g:\Group Applications
- Logon script = Logon.bat
- Desktop Shortcuts = *.lnk
- Approved VBS Scripts =*.vbs

Step 4: Set the Policy Options

The following options include the recommended policy settings for the design that is defined in this guide. These options alter the enforcement behavior scope or the Authenticode trust settings for digitally signed files.

- **Enforcement**. If the computer is part of the domain, ensure that the **Domain Admins** group is automatically added to the **Administrators** group.
- **Apply to Users**. Includes all users except local Administrators. Use of this option delays the launch of each application. To compensate for this delay, the design configures the policy to not check DLLs.

- **Apply to Files**. Includes all software files except libraries (such as DLLs). Use of this option delays the launch of each application. To compensate for this delay, the design configures the policy to not check DLLs.
- **Designated file types**. For the GPO design that is defined in this guide, .ocx files were added to the list and .mdb and .lnk file types were removed. You could add custom application file type extensions as needed to make them subject to the same rules.
- **Trusted Publishers**. For the GPO design that is defined in this guide, the **Administrators** group was enabled and the option for **Trusted Publisher Properties: Local Computer Administrators** was selected.

Before you trust a publisher, select the **Check: Publisher** option when you design the GPO to ensure the policy will validate certificates.

Step 5: Apply the Default Settings

It is a best practice to configure the policy to the default **Unrestricted** setting. This method ensures that the policy is properly initialized before software restrictions are applied. After you review the policy settings, reset the default setting to **Disallowed**.

Step 6: Test the Policy

If the computer is part of a domain, move the computer into the OU container where the policy is applied. Restart the test computer and log on to it. The test plans should have instructions about how each of the applications should work when the policy is applied. Run the applications to ensure they have full functionality and that you can access all of their features. After you have validated the functionality of the applications, simulate an attack on the applications to ensure that the policy has no security vulnerabilities.

If the computer is a stand-alone client, log on to the test computer and follow your test plan. After you have validated the applications, launch the simulated attack again to ensure that the policy has no security vulnerabilities.

Deploying Software Restriction Policy

After the policy is thoroughly tested, apply it to the desktop or laptop OU in your environment. If it is for a stand-alone client computer, apply it to the Local Computer Settings on the client. Open the MMC Computers and Users snap-in and traverse the directory until you reach the OU container for the desktops or laptops. Then, create the new GPO with the Group Policy Object Editor. Edit the properties and apply the appropriate policy settings based on the information in the following tables to the **Software Restriction Policy** under **Windows Settings\Security Settings**.

Table 3.5 Security Levels

Default rule in UI	Description	Setting
Disallowed	Software will not run, regardless of the access rights of the user.	Use this default rule

Table 3.6 Additional Rules

Path rule	Setting
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\SystemRoot%	Unrestricted

Path rule	Setting
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\SystemRoot%\*.exe	Unrestricted
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\SystemRoot%\System32\*.exe	Unrestricted
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\ProgramFilesDir%	Unrestricted
*.vbs	Disallowed
G:\Group Applications	Unrestricted
Logon.bat or Logon script	Unrestricted
*\Program Files	Unrestricted

Table 3.7 Enforcement on Files and Users

Enforcement options	Recommendation
Apply software restriction policies to the following:	All software files except DLLs.
Apply software restriction policies to the following users:	All users except local administrators.

Table 3.8 Designated File Types

File types	Recommendation
Designated file types properties	Remove .mdb and .lnk file types and add .ocx.

Table 3.9 Trusted Publishers

Trusted publishers	Recommendation
Allow the following user groups to select trusted publishers:	**Local Computer Administrators**
Determine if the certificate is revoked.	Select the **Publisher** option.

More Information

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

- Chapter 6, "Digital Certificates" of the *Microsoft Internet Explorer 6 Resource Kit.*
- Command shell overview.
- Using Software Restriction Policies to Protect Against Unauthorized Software.
- Windows Server 2003 Group Policy.