



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

**CHINATAG**

**070-214**

**Implementing and Administering  
Security in a Microsoft  
Windows 2000 Network**

**Study Guide**

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

## TABLE OF CONTENTS

### List of Tables

### Introduction

### 1. Group Policy

- 1.1 The Structure of Group Policy Objects
  - 1.1.1 Physical Structure
  - 1.1.2 Logical Structure
- 1.2 Local and Active Directory Group Policy
  - 1.2.1 Local Group Policy
  - 1.2.2 Active Directory Group Policy
- 1.3 Group Policy Application Order
- 1.4 Delegating Group Policy Management
- 1.5 Filtering Group Policy Application
- 1.6 Configuring Client Computer Security Policy
- 1.7 Troubleshooting Group Policy Application

### 2. User Accounts and Security Groups

- 2.1 Types of User Accounts
  - 2.1.1 Local User Accounts
  - 2.1.2 Active Directory Domain User Accounts
  - 2.1.3 Built-In User Accounts
- 2.2 Creating User Accounts
  - 2.2.1 Creating Local User Accounts
  - 2.2.2 Creating Domain User Accounts
  - 2.2.3 Copying Domain User Accounts
  - 2.2.4 Security Identifiers (SIDs)
- 2.3 Security Groups
- 2.4 User Authentication
  - 2.4.1 The Local Logon Process
  - 2.4.2 Local Resource Access
  - 2.4.3 Workgroup Authentication
  - 2.4.4 Domain User Account Authentication

## 2.5 Domain Security Groups

### 2.5.1 Group Scopes

#### 2.5.1.1 Local Groups

#### 2.5.1.2 Global Groups

#### 2.5.1.3 Domain Local Groups

#### 2.5.1.4 Universal Groups

#### 2.5.1.5 Special Identity Groups

### 2.5.2 Using Security Groups to Set Permissions

## 2.6 Restricting Accounts, Users, and Groups

### 2.6.1 Account Policies

### 2.6.2 Managing User Rights

### 2.6.3 Restricted Groups

### 2.6.4 Security Policy Templates

#### 2.6.4.1 Standard Windows 2000 Security Templates

#### 2.6.4.2 Backward Compatible Security Templates

#### 2.6.4.3 Optional Component Files Templates

#### 2.6.4.4 Installation and Upgrade Security Templates

#### 2.6.4.5 Miscellaneous Security Templates

#### 2.6.4.6 Managing Security Templates

## 2.7 Account-Based Security

### 2.7.1 File System Permissions

#### 2.7.1.1 Cumulative Permissions

#### 2.7.1.2 The Deny Permission

#### 2.7.1.3 NTFS Permissions Inheritance

#### 2.7.1.4 Assigning Special Access Permissions

#### 2.7.1.5 Changing Permissions

#### 2.7.1.6 Copying and Moving Files and Folders

#### 2.7.1.7 Permissions Best Practices

#### 2.7.1.8 Troubleshooting Permission Problems

### 2.7.2 Share Service Security

#### 2.7.2.1 Administrative Shared Folders

#### 2.7.2.2 Combining Shared Folder Permissions and NTFS Permissions

### 2.7.3 Audit Policies

#### 2.7.3.1 Using an Audit Policy

#### 2.7.3.2 Using Event Viewer to View Security Logs

#### 2.7.3.3 Setting Up Auditing

### 2.7.4 Registry Security

#### 2.7.4.1 Editing the Registry

## 3. Certificate Services and Certificate Authorities

### 3.1 Encryption

#### 3.1.1 Secret Key Encryption

#### 3.1.2 Public Key Encryption

#### 3.1.3 Digital Signatures

### 3.2 Certificates

#### 3.3 Certificate Management

- 3.3.1 Certificate Enrollment
- 3.3.2 Certificate Expiration
- 3.3.3 Certificate Renewal
- 3.3.4 Certificate Revocation
- 3.3.5 Certificate and Key Recovery
- 3.3.6 Certificate Trust

#### 3.4 Uses for Certificates

#### 3.5 Installing Windows 2000 Certificate Services

- 3.5.1 Types of CAs
  - 3.5.1.1 Enterprise Root CA
  - 3.5.1.2 Enterprise Subordinate CA
  - 3.5.1.3 Stand-Alone Root CA
  - 3.5.1.4 Stand-Alone Subordinate CA
- 3.5.2 CA Security and Recovery
- 3.5.3 Cryptographic Service Providers
- 3.5.4 Issuing Certificates
- 3.5.5 Cryptographic Key Storage
- 3.5.6 Backing Up and Restoring CAs

#### 3.6 Computer Certificates

- 3.6.1 Certificate Templates
- 3.6.2 Deploying Computer Certificates
- 3.6.3 Deploying User Certificates
  - 3.6.3.1 Automated Deployment of User Certificates
  - 3.6.3.2 Manually Creating Certificates
  - 3.6.3.3 Moving Certificates

#### 3.7 Smart Card Certificates

- 3.7.1 Personal Identification Number
- 3.7.2 Types of Smart Card Certificates
- 3.7.3 Issuing Smart Cards
- 3.7.4 Smart Card Removal Behavior Policy
- 3.7.5 Troubleshooting Smart Card Certificates

#### 3.8 S/MIME Certificates

## 4. Authentication

#### 4.1 Windows 2000 Network Authentication

- 4.1.1 LAN Manager Authentication
- 4.1.2 NTLM Authentication
- 4.1.3 NTLM Version 2 Authentication

- 4.2 Creating a Secure Environment
- 4.3 Securing Macintosh Client Support
- 4.4 Trust Relationships
  - 4.4.1 Managing External Trust Relationships

## **5. IP Security**

- 5.1 IPSec Applications
- 5.2 Internet Key Exchange
  - 5.2.1 IKE in Windows 2000
  - 5.2.2 Distributing IKE Secret Keys
- 5.3 IPSec Within a Private Network
- 5.4 IPSec in Untrusted Networks
  - 5.4.1 Providing a Secret Key
  - 5.4.2 Creating IPSec Policy in Windows 2000
  - 5.4.3 IPSec Exceptions
- 5.5 IPSec on Web Servers
- 5.6 Troubleshooting IPSec

## **6. Remote Access and Security**

- 6.1 Installation and Configuration
  - 6.1.1 Routing and Remote Access Service Features
  - 6.1.2 Remote Access Client
  - 6.1.3 Remote Access Protocols
- 6.2 Remote Access Security
  - 6.2.1 Secure User Authentication
  - 6.2.2 Mutual Authentication
  - 6.2.3 Data Encryption
  - 6.2.4 Callback
  - 6.2.5 Caller ID
  - 6.2.6 Remote Access Account Lockout
  - 6.2.7 Managing RRAS Security Options
- 6.3 Managing Authentication
  - 6.3.1 Windows Authentication
  - 6.3.2 RADIUS Authentication and IAS
- 6.4 Securing RRAS Clients
  - 6.4.1 Remote Access Policies

#### 6.4.2 The Connection Manager Administration Kit

#### 6.5 Virtual Private Networks (VNP)

##### 6.5.1 VPN Protocols

##### 6.5.2 Configuring VPN Protocols

##### 6.5.3 Configuring Client VPN Settings

#### 6.6 Wireless Access

##### 6.6.1 Wireless Protocols

###### 6.6.1.1 The 802.11 Protocol

###### 6.6.1.2 The 802.11b Protocol

###### 6.6.1.3 The 802.11a Protocol

##### 6.6.2 Wireless Access Security

###### 6.6.2.1 Configuring Clients for Wireless Security

###### 6.6.2.2 802.1x Authentication

###### 6.6.2.3 802.1x Security Problems

###### 6.6.2.4 Troubleshooting 802.1x Connections

##### 6.6.3 Wired Equivalent Privacy

###### 6.6.3.1 WEP Security Problems

###### 6.6.3.2 Managing WEP on the Client

### **7. Implementing Server Security**

#### 7.1 Internet Security

##### 7.1.1 Types of Attack

##### 7.1.2 Methods of Attack

##### 7.1.3 Vectors for Attack

#### 7.2 Establishing Firewall Security

##### 7.2.1 Types of Firewalls

###### 7.2.1.1 Firewall Routers

###### 7.2.1.2 Proxies

###### 7.2.1.3 Internet Security and Acceleration (ISA) Server

#### 7.3 Securing Public Database Servers

##### 7.3.1 Proper Database Servers Placement

##### 7.3.2 Securing Microsoft SQL Server

#### 7.4 Securing Microsoft Exchange Server

##### 7.4.1 Open Relays

##### 7.4.2 Protecting an Exchange Server

###### 7.4.2.1 Protecting Exchange Server with a Relay Mail Server

###### 7.4.2.2 Protecting Exchange Server with a Strong Security Proxy

##### 7.4.3 Securing Credentials

#### 7.5 Securing Public Web Servers

##### 7.5.1 Establishing Security Settings

##### 7.5.2 Managing Directory Security Properties

- 7.5.3 IP Address and Domain Name Restrictions
- 7.5.4 Secure IIS
- 7.5.5 Web Authentication
  - 7.5.5.1 Anonymous Authentication
  - 7.5.5.2 Basic Authentication
  - 7.5.5.3 Digest Authentication
  - 7.5.5.4 Integrated Windows Authentication
  - 7.5.5.5 Certificate-based Authentication
- 7.5.6 Secure Sockets Layer (SSL)
  - 7.5.6.1 Obtaining and Installing SSL Certificates
  - 7.5.6.2 Authenticating Clients
  - 7.5.6.3 Installing a Client Certificate
  - 7.5.6.4 Client Certificate Mapping
  - 7.5.6.5 Certificate Trust Lists (CTLs)

## **8. Software Maintenance**

- 8.1 Service Packs and Hotfixes
  - 8.1.1 Installing Service Packs and Hotfixes
  - 8.1.2 Removing a Service Pack or Hotfix
  - 8.1.3 Slipstreaming Service Packs and Hotfixes
  - 8.1.4 Adding Service Packs and Hotfixes to a Network Installation Share
  - 8.1.5 Microsoft Software Update Services
    - 8.1.5.1 Windows Update
    - 8.1.5.2 Windows Update Catalog
    - 8.1.5.3 Automatic Updates
    - 8.1.5.4 Software Update Services
- 8.2 Remote Installation Services
  - 8.2.1 Setting up the RIS Server
  - 8.2.2 Client requirements for Remote Installation
  - 8.2.3 Creating a RIS Installation Image
  - 8.2.4 Installing Clients with RIS
- 8.3 Deploying Updates in the Enterprise
  - 8.3.1 Using Group Policy to Deploy Software
  - 8.3.2 Installing Multiple Hotfixes
- 8.4 Tools for Security Management
  - 8.4.1 The Microsoft Baseline Security Analyzer
  - 8.4.2 HFNetChk
  - 8.4.3 Microsoft Systems Management Server (SMS)

## **9. Intrusion Detection and Event Monitoring**

- 9.1 Detecting Network Intrusions
  - 9.1.1 Detecting Denial of Service Attacks
  - 9.1.2 Detecting Vulnerability Attacks

9.1.3 Detecting Impersonation Attacks

9.2 Implementing Decoy Servers

9.3 Event Analysis

9.4 Event Monitoring

9.5 Preserving Evidence

## LIST OF TABLES

TABLE 2.1:	Local Built-In Groups
TABLE 2.2:	System Groups for a Local Computer
TABLE 2.3:	Security Template Prefixes
TABLE 2.4:	Security Template Suffixes
TABLE 2.5:	Access Permissions Set by the Basic Security Template
TABLE 2.6:	Permission Inheritance Options
TABLE 2.7:	Troubleshooting Permission Problems
TABLE 2.8:	Shared Folder Permissions
TABLE 3.1:	CSP Encryption Algorithms
TABLE 3.2:	Standard PKI Certificate Stores
TABLE 3.3:	The Windows 2000 Certificate Templates
TABLE 6.1:	Remote Access Policy Conditions
TABLE 6.2:	Additional RADIUS Remote Access Policy Conditions
TABLE 8.1:	Network Services Required by RIS
TABLE 8.2:	HFNetChk Options

# Implementing and Administering Security in a Microsoft Windows 2000 Network

**Exam Code: 070-214**

## **Certifications:**

**Microsoft Certified (MCP)**

**Microsoft Certified Systems Administrator (MCSA)**

**Microsoft Certified Systems Engineer (MCSE)**

**Elective**

**Elective**

## **Prerequisites:**

None

## **About This Study Guide**

This Study Guide is based on the current pool of exam questions for the 070-214 - Implementing and Administering Security in a Microsoft Windows 2000 Network. As such it provides all the information required to pass the Microsoft MCSE 070-214 exam and is organized around the specific skills that are tested in the exam. Thus, the information contained in this Study Guide is specific to the 070-214 exam and does not represent a complete reference work. This Study Guide also includes the information required to answer questions related to the implementing and administering security in networks with Windows NT 4.0 and Windows 98 that may be asked during the exam. Topics covered in this Study Guide includes Implementing, Managing, and Troubleshooting Baseline Security: Configuring security templates, registry and file system permissions, account policies, audit policies, user rights assignment, security options, system services, restricted groups, and event logs, deploying security templates, troubleshooting security template problems, configuring additional security based on computer roles, and configuring additional security for client-computer operating systems by using Group Policy; Implementing, Managing, and Troubleshooting Service Packs and Security Updates: Determining the current status of service packs and security updates, Installing service packs and security updates, managing service packs and security updates, and troubleshooting the deployment of service packs and security updates; Implementing, Managing, and Troubleshooting Secure Communication Channels: configuring IPSec to secure communication between networks and hosts, configuring IPSec authentication, appropriate encryption levels, and the appropriate IPSec protocol, deploying and managing IPSec certificates, troubleshooting IPSec, implement security for wireless networks, configuring public and private wireless LANs, wireless encryption levels, and wireless network connection settings on client computers, configuring Server Message Block (SMB) signing to support packet authentication and integrity, deploying and manage SSL certificates, obtaining public and private certificates, installing certificates for SSL, and renewing certificates, and configuring SSL to secure communication channels; Configuring, Managing, and Troubleshooting Authentication and Remote Access Security: configuring and troubleshooting authentication in mixed Windows client-computer environments, configuring the interoperability of Kerberos authentication with UNIX computers, configuring authentication for extranet scenarios, trust relationships and members of non-trusted domain authentication, configuring and troubleshooting authentication for Web users, configuring authentication for secure remote access, configuring and troubleshooting virtual private network (VPN) protocols, and managing client-

computer configuration for remote access security; Implementing and Managing a Public Key Infrastructure (PKI) and Encrypting File System (EFS): installing and configuring Certificate Authority (CA) hierarchies, installing and configuring the root, intermediate, and issuing CA, configuring certificate templates. Considerations include LDAP queries, HTTP queries, and third-party CAs, configuring the publication of Certificate Revocation Lists (CRLs), configuring public key Group Policy, configuring certificate renewal and enrolment, and deploying certificates to users, computers, and CAs, managing Certificate Authorities (CAs), enrolling and renewing certificates, revoking certificates, managing and troubleshooting Certificate Revocation Lists (CRLs), backing up and restoring the CA, manage client-computer and server certificates, publishing certificates through Active Folder, issuing certificates using MMC, Web enrolment, programmatic, or auto enrolment using Windows XP, and recovering KMS-issued keys, and manage and troubleshoot EFS; and Monitoring and Responding to Security Incidents: configuring and managing auditing, managing audit log retention., analyzing security events, responding to security incidents, isolating and containing the incident, implementing counter measures and restoring services.

Although there is an overlap of material in this Study Guide and the Chinatag 070-210, 070-215, 070-216, 070-217, 070-218, and 070-220 Study Guides, the relevant information from those Study Guides are included in this Study Guide. This is thus the only Study Guide you will require to pass the MCSE 070-214 exam.

### **Intended Audience**

This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 070-214 - Implementing and Administering Security in a Microsoft Windows 2000 Network. The information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex and require an understanding of material provided for the MCSA / MCSE exam: 070-210 - Installing, Configuring, and Administering Microsoft Windows 2000 Professional and the MCSA / MCSE exam 070-215 - Installing, Configuring, and Administering Microsoft Windows 2000 Server.

### **How To Use This Study Guide**

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup. Although there is a fair amount of overlap between this Study Guide, the Chinatag 070-210 Study Guide, the Chinatag 070-215 Study Guide, the Chinatag 070-216 Study Guide, the Chinatag 070-217 Study Guide, the Chinatag 070-218 Study Guide and the Chinatag 070-220 Study Guide. We would not advise skimming over the information that seems familiar. Instead, read over it again to refresh your memory.
- Perform all labs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

**Note:** Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

## 1. Group Policy

Group Policy is the primary configuration management tool for Microsoft Windows networks. It determines which software is available to users, the appearance of the desktop, and what operating system features are enabled. Because of this, you can use Group Policy as a security mechanism. Group Policy can restrict dangerous operating system features to prevent well-meaning users from accidentally damaging their computers configurations. It can also limit access to configuration tools and software that malicious users can use to hack into other computers and carry out a wide variety of attacks. However, because Group Policy is primarily a central configuration management tool rather than a security feature, it has a number of security limitations.

Group Policy is a package of settings files, scripts, and installation files that create a specific computer configuration for groups of users or computers based on their memberships in organizational units (OUs), or their locations at specific sites, campuses, or facilities. Group Policy can also be used to configure special requirements for specific computers. Group Policy settings are stored in Group Policy Objects (GPOs). GPOs are packages of files that are interpreted on the client computers to which the GPO is linked. GPOs are stored as folders and files in the Domain Controller's *SYSVOL* share and are automatically replicated among Domain Controllers. These GPOs must be linked to Active Directory containers, i.e., domains, organizational units, and/or sites, to take effect.

A business' organizational structure creates a natural environment for the deployment of software and the configuration of computers. Users within a specific OU are likely to require access to the same software applications and network resources, while users within another OU might require access to a different set of software applications and network resources. Windows 2000 domains can also be used to enforce security boundaries between departments in organizations where security is of paramount concern. Domains, OUs, and sites are all Active Directory containers.

Whether these divisions are modeled as domains or OUs, the application of Group Policy remains the same: you configure a Group Policy Object (GPO), then you link the GPO to an Active Directory container to apply the Group Policy settings to all the computers within that container when they are booted and to all users within that container when they log on to the network.

### Active Directory Containers

Active Directory containers are Active Directory objects that can contain other Active Directory objects such as users, computers, and other subordinate Active Directory containers.

Using this deployment mechanism, administrators can use Group Policy as an automated means of:

- Controlling desktop configurations;
- Deploying software applications; device drivers; and software updates and patches;
- Managing the options and features of software applications; and
- Deploying startup and logon scripts to map network drives and printers and perform other repetitive tasks.

A specific GPO can be linked to a number of Active Directory objects. You can link a GPO to a domain or OU:

- When you create a GPO from within an Active Directory object's **Properties** dialog box, the Windows 2000 creates a link between the GPO and the Active Directory object;

- By using the **Active Directory Users And Computers** management console in **Administrative Tools**, you can manually link a GPO to an Active Directory object on the **Group Policy** tab in the Active Directory object's **Properties** dialog box.

You can link a GPO to a site by using the **Sites And Services** management console in **Administrative Tools**.

## 1.1 The Structure of Group Policy Objects

### 1.1.1 Physical Structure

Group Policy is implemented by a number of components called Group Policy client-side extensions. Each extension interprets the specific files stored in the GPO in Active Directory that pertain to it and makes various changes to the client based on the settings contained in the GPO. The various Group Policy client-side extensions manage:

- Folder redirection;
- Disk quotas;
- Scripts;
- Security;
- Encrypting File System (EFS) recovery;
- Application management;
- Internet Explorer settings;
- Registry settings; and
- IP security.

The Group Policy client-side extension that manages registry settings to modify the behavior of the operating system is configured through *.adm* files, which contain information about registry keys, their available settings, and their location within the Group Policy namespace. Two *.adm* files are especially important: *Inetres.adm*, which controls Internet Explorer registry settings, and *System.adm*, which controls Windows settings. *Conf.adm*, which controls NetMeeting configuration, is also included by default. Administrators can also create their own *.adm* files. These files are stored within each GPO's *\ADM* folder in *SYSVOL*. In the case of Local GPOs, all Group Policy files, including *.adm* files, are stored within the *%SystemRoot%\system32\GroupPolicy* folder.

Group Policy folders within a Domain Controller's *SYSVOL* directory are named using an automatically generated **globally unique identifier** (GUID). Each GUID is unique among Domain Controllers anywhere in the world. Therefore, when two organizations and their Active Directory directories merge, their Group Policy folders will not cause conflicts because they have different identifiers.

### 1.1.2 Logical Structure

By default, every GPO has two components:

- A **Computer Configuration** component, which is applied to every user of a computer when the computer is booted, and before anyone logs on. You can use this component to manage how a computer will behave no matter who is logged on.

- A **User Configuration** component, which is applied, based on the identity of the logged on user, and it applies only to that user. You can use this component to manage how specific users are allowed to operate computers, regardless of which computer they log on to. If a User Configuration setting conflicts with a Computer Configuration setting, the Computer Configuration setting takes precedence unless the User Configuration policy has been flagged, indicating that it is not to be overridden.

Both Computer Configuration and User Configuration policies have three major divisions:

- A **Software Settings** component, which contains settings extensions provided primarily by independent software vendors for software installation.
- A **Windows Settings** component, which contains settings that apply to Windows 2000, as well as startup/shutdown scripts in Computer Configuration or logon/logoff scripts in User Configuration. This, which contains most of the settings that are security specific.
- An **Administrative Templates** component, which can be extended by administrators using *.adm* files, and contains settings that modify the behavior of Internet Explorer, Windows Explorer, and other programs.

To optimize speed with which GPOs are loaded, and to minimize network traffic, it is recommended that you separate your GPOs into those that affect computer configuration and those that affect user configuration and disable the unnecessary portion by clicking the **Properties** button on the **Group Policy** tab and selecting the **Disable Computer Configuration Settings** or the **Disable User Configuration Settings** check box. This practice will separate User Configuration settings from Computer Configuration settings and will speed the application of Group Policy because, if a policy contains both sets of settings, it must be loaded twice, and for each load, half of the policy will not apply.

## 1.2 Local and Active Directory Group Policy

### 1.2.1 Local Group Policy

A local GPO is a GPO that is stored locally on the client computer rather than downloaded from a Domain Controller. Because local GPOs are stored locally, they are always available, even when the computer has no connection to the network or is not a member of a domain. When Windows 2000 starts, local GPOs are applied first. Local GPOs are normally used to control settings on computers that are not part of a domain or are unable to contact the domain, but they can be used on any computer regardless of its domain membership. After local Group Policy settings are applied, computers that are members of a domain then download GPOs from Domain Controllers based on the computer's membership in a domain, site, or OU, and apply those settings. Because local GPOs are applied first, their settings are frequently overridden by domain Group Policy settings.

### 1.2.2 Active Directory Group Policy

Every GPO has two components:

- A **Computer Configuration** portion that is applied before anyone logs on.
- A **User Configuration** portion that is applied based on the identity of the logged on user.

After Windows applies local Group Policy to computers in a domain when they start, it downloads the Computer Configuration portion of any GPOs from Active Directory that apply to them. It then applies the

Computer Configuration portion of all GPOs before displaying the logon prompt. When users log on, the process is repeated for the User Configuration portion of the same set of GPOs.

### 1.3 Group Policy Application Order

By default, **Local Group Policy** is applied first, followed by **site-linked** GPOs; and then **domain-linked** and **OU-linked** GPOs. Domain-linked and OU-linked GPOs are downloaded and applied in hierarchical order from parent to child within the Active Directory structure. Unless a GPO is specifically set not to allow overrides, Group Policy settings automatically override the same Group Policy settings applied by earlier GPOs. Therefore, it is good practice to construct Group Policy settings that are more specific and more restrictive as you descend through the Active Directory container hierarchy.

In the Properties dialog box for an Active Directory object, you can change the order in which GPOs are applied to the object by modifying their order in the Group Policy list. GPOs listed lowest are applied first followed. Thus, the GPOs at the bottom of the list have the least effect because they are overridden by the settings in GPOs listed above them. To change the order in which GPOs are applied, select a specific GPO and then use the **Up** and **Down** buttons to move it to the position you want.

You can flag a GPO to allow no overrides from subsequently applied GPOs. This feature is extremely useful for enforcing security within a single GPO. By containing security-related Group Policy settings within a single GPO and setting that GPO to disable policy override, you need not worry about the application order of GPOs or about other GPOs that might apply to a specific Active Directory object. To prevent subsequent GPOs from overriding a GPO, click the **Options** button on the **Group Policy** tab of the Active Directory object's **Properties** dialog box, and select the **No Override** check box.

The administrator can also modify the application order of GPOs for any Active Directory container. By modifying the application order, administrators can prioritize certain GPOs to ensure that their settings will override other GPOs, or flag a GPO to prevent its settings from being overridden no matter when it is applied.

### 1.4 Delegating Group Policy Management

In large organizations, administrative control over Group Policy can be delegated on a per-domain or per-OU basis. When administrative control is delegated for portions of Active Directory, you must restrict administrators from modifying GPOs that are outside of their authority. Because an administrator must have both **Read** and **Write** access to modify a GPO, you can restrict access by changing permissions to remove **Write** access for GPOs outside an administrator's authority.

### 1.5 Filtering Group Policy Application

Users are normally assigned to a single OU. User policies are also assigned on a per-OU basis. However, some users within the OU, such as power users or subordinate administrators, might require different security settings. To separate users within an OU so that different GPOs are applied to them, you can either create subordinate OUs, applying the various GPOs to those subordinate OUs rather than to the parent OU, or you can filter the application of a Group Policy setting by using permissions.

A GPO can be applied to a user only if the user has **Read and Apply Group Policy** permissions to the object. By default, **Authenticated Users** inherit these rights for all GPOs. You can prevent the application

of a GPO to a user or group of users by creating a specific **Deny Access Control Entry** in the Group Policy Object's access control list (ACL). ACLs are used to determine which users can access a specific secured resource such as a file or folder.

However, while Group Policy filtering is effective, it is best practice to create additional subordinate OUs and control the assignment of GPOs through links to those additional Active Directory objects. It is recommended that you use Group Policy filtering only in those cases when you cannot apply Group Policy the way you want using additional Active Directory container objects and linking, such as when the GPO is far up the Active Directory hierarchy and you do not have administrative rights to move the GPO to a more appropriate location.

It is crucial that you test Group Policy application whenever you create or modify a GPO, or when you suspect that your GPO is not completely effective. To do this, create a test user account within the OU top which the GPO is applied and then log on to your computer using the test user account to test the effectiveness of the GPO.

### 1.6 Configuring Client Computer Security Policy

Group Policy is most appropriately used to prevent users from reconfiguring the operation of their computers. In most enterprises, workers usually use a relatively small set of software applications, defined by the kind of work they perform. Group Policy can be used to restrict the number of software applications that are available to a group of users as defined by their job requirements. Group Policy implements this restriction by matching the name of the software application against an allowed list. However, restricting access to certain software applications does not prevent a user from downloading a similar program and running it to obtain the same functionality.

You can use Group Policy to control the behavior of **Internet Explorer**. Group Policy restrictions for Internet Explorer are contained in two places in the Group Policy namespace:

- *\User Configuration\Windows Settings\Internet Explorer Maintenance*, which controls home page and other URLs, Security Zone settings, content rating settings, and other such "pre-deployment" settings; and
- *\User Configuration\Administrative Templates\Windows Components\Internet Explorer*, which allows you to disable components of the Internet Explorer user interface, such as menu items, Properties dialog boxes, and options.

To fully secure Internet browsing, you should use Group Policy to direct your internal users through a **proxy server** that can check the HTTP protocol for errors and restricting access to sites that are dangerous. The primary security purpose of controlling Internet Explorer settings is to prevent users from bypassing the proxy server to browse the Web directly. For organizations whose security policy does not require a proxy server, you can control Internet Explorer security settings to prevent users from changing security zone restrictions that could enable dangerous content like **ActiveX** controls from Web sites that you do not trust.

### 1.7 Troubleshooting Group Policy Application

Users can encounter a number of relatively routine problems when working with Group Policy. Typical problems with Group Policy application include:

- Unexpected or unintended results;

- Incomplete application of policy; and
- Lack of policy application.

In a properly functioning network, these problems usually occur because multiple GPOs are being applied and it is not obvious which policy has priority for a specific setting. Other possible causes are a client computer that cannot resolve the name of a Domain Controller or that does not have proper access to a GPO or *SYSVOL* share. Typical solutions to Group Policy problems include:

- Verifying that the client has properly configured DNS settings and can resolve the name of the Domain Controller responsible for storing the Group Policy;
- Verifying that the user or computer account is contained within the Active Directory container that is linked to the GPO;
- Verifying that a previously applied policy is not set to **No Override**; and
- Verifying that the user has **Read and Apply** permissions for the GPO.

Also, larger networks are likely to experience Group Policy problems due to replication of GPOs, while more complex Active Directory structures can take significantly more time to analyze when an attempt is made to determine which specific GPO contains a particular setting.

You can solve most of these Group Policy problems by:

- Confirming that replication is occurring correctly and that the Group Policy is the same across Domain Controllers;
- Ensuring that individual GPOs are kept small so that they replicate quickly among sites;
- Ensuring that the user has **Read and Apply** permissions for the GPO using *Userenv.log*;
- Verifying that Windows 2000 is not attempting to apply a Windows NT 4 policy to the client; and
- Refreshing all types of Group Policy extensions by rebooting the computer and logging on again.

In addition, several side effects can occur in the Group Policy application of networks that are in the process of a migration from Windows NT 4 domains to Windows 2000 domains. These include the following:

- If the computer is running Windows NT 4, it receives Windows NT 4 system policy rather than the Windows 2000 Computer Configuration portion of Group Policy;
- If Windows NT 4 based Domain Controllers manage a user account, that user account receives Windows NT 4 system policy rather than the Windows 2000 User Configuration portion of a GPO, regardless of the client operating system; and
- If Active Directory manages the user account, the user receives the User Configuration portion of a GPO no matter which operating system is installed on the client computer.

To avoid problems, you should upgrade all user accounts to Active Directory as quickly as possible by upgrading resource domains to Windows 2000. Update Windows NT Backup Domain Controllers (BDCs) to Windows 2000 as quickly as possible after that. Also, do not upgrade the Windows NT clients to Windows 2000 until all Domain Controllers have been upgraded to Windows 2000. Finally, use *Regini.exe* to clean the registry of the computer that has residual system policy problems as Windows NT 4 system policy permanently alters the registry of Windows NT computers.