Security

Chapter 3 - Secure Configuration

This section provides detailed procedures for making security configuration changes to the standard install base of Windows 2000 in support of the Evaluated Configuration. Tables are provided describing the security objective and the configuration actions necessary to meet that objective. Actions are described for Windows 2000 Professional (Stand-alone and Domain Member), Server (Stand-alone and Domain Member), and Domain Controller configurations.

If a Domain Security Policy is to be applied for all computers across a Domain, the settings defined for Windows 2000 Professional and Server must be used to comprise the requirements for the Domain Security Policy, as applicable. The Domain Controller settings defined in the document tables apply only to a Domain Controller Security Policy.

Section 5 of this document provides the procedures for automating most of the security settings defined in this section by applying pre-defined security configuration templates. For convenience, a Windows 2000 Security Configuration Checklist is provided in Appendix E of this document.

Windows 2000 Security Policies

This subsection explains the various security policy tools and their order of precedence with respect to application of security policies. By default, Group Policies are inherited and cumulative, and affect all computers in an Active Directory container. Group Policies are administered through the use of Group Policy Objects (GPOs), which are data structures attached in a specific hierarchy to selected Active Directory Objects, such as Sites, Domains, or Organizational Units (OUs).

These GPOs, once created, are applied in a standard order: LSDOU, which stands for (1) Local, (2) Site, (3) Domain, (4) OU, with the later policies being superior to the earlier applied policies. Local Group Policy Objects are processed first, and then domain policy. If a computer is participating in a domain and a conflict occurs between domain and local computer policy, domain policy prevails. However, if a computer is no longer participating in a domain, local Group Policy object is applied.

When a computer is joined to a domain with the Active Directory and Group Policy implemented, a Local Group Policy Object is processed. Note that LGPO policy is processed even when the Block Policy Inheritance option has been specified.

Account policies (i.e., password, lockout, Kerberos) are defined for the entire domain in the default domain Group Policy Object (GPO). Local policies (i.e., audit, user rights, and security options) for Domain Controllers (DCs) are defined in the default Domain Controllers GPO. For DCs, settings defined in the default DC GPO have higher precedence than settings defined in the default Domain GPO. Thus, if a user privilege were configured (for example, Add workstations to domain) in the default Domain GPO, it would have no impact on the DCs in that domain.

Options exist that allow enforcement of the Group Policy in a specific Group Policy Object so that GPOs in lower-level Active Directory containers are prevented from overriding that policy. For example, if there is a specific GPO defined at the domain level and it is specified that the GPO be enforced, the policies that the GPO contains apply to all OUs under that domain; that is, the lower-level containers (OUs) cannot override that domain Group Policy.

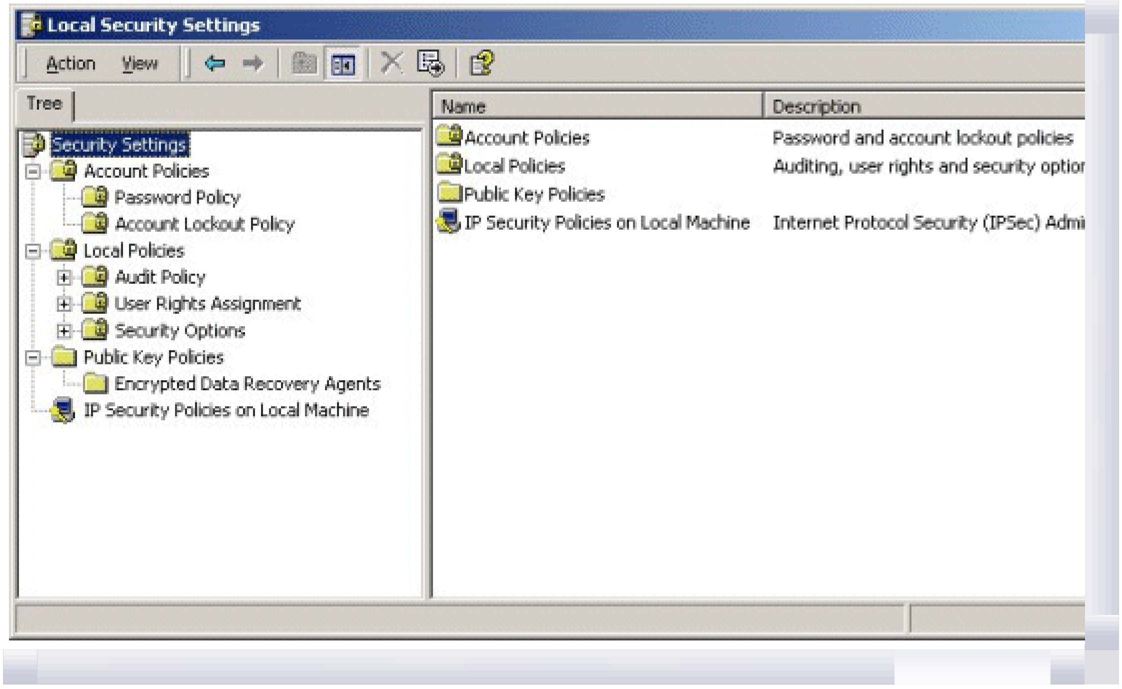
> **Note** The Account Policies security area receives special treatment in how it takes effect on computers in the domain. All DCs in the domain receive their account policies from GPOs configured at the domain node **regardless of where the computer object for the DC is.** This ensures that consistent account policies are enforced for all domain accounts. All non-DC computers in the domain follow the normal GPO hierarchy for getting policies for the local accounts on those computers. By default, member workstations and servers enforce the policy settings configured in the domain GPO for their local accounts, but if there is another GPO at lower scope that overrides the default settings, then those settings will take effect.

Local Security Policy

A Local Security Policy is used to set the security requirements on the local computer. It is primarily used for stand-alone computers or to apply specific security settings to a Domain member. Within an Active Directory managed network the Local Security Policy settings have the least precedence.

To open the Local Security Policy:

1. Log on to the computer with administrative rights.
2. In a Windows 2000 Professional computer, **Administrative Tools** is not displayed as a Start menu option by default. To view the **Administrative Tools** menu option in Windows 2000 Professional, click **Start**, point to **Settings**, and select **Taskbar and Start Menu**. In the **Taskbar and Start Menu Properties** window, click the **Advanced** tab. Check the **Display Administrative Tools** checkbox in the **Start Menu Settings** dialog box. Click the **OK** button to complete the setting.
3. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the Local Security Settings console.

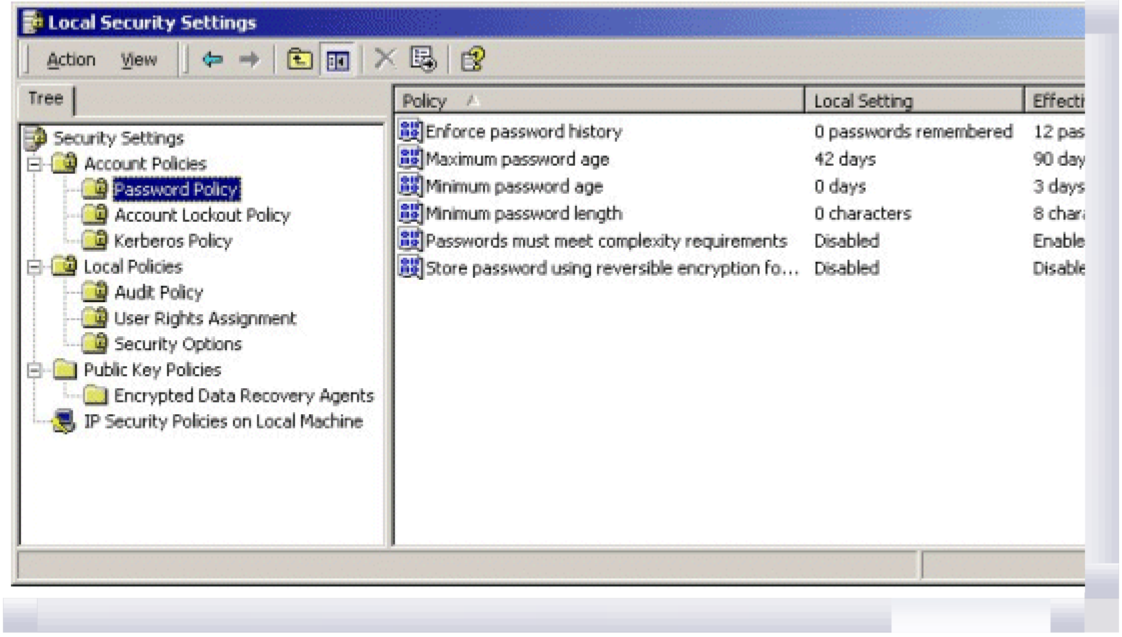


- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Public Key Policies
    - Encrypted Data Recovery Agents
  - IP Security Policies on Local Machine

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security optior
Public Key Policies	
IP Security Policies on Local Machine	Internet Protocol Security (IPSec) Admi

If your browser does not support inline frames, click here to view on a separate page.

Note Local Security Policies display Local Settings for the computer and the Effective Settings resulting from the addition of Domain level security policy settings. Domain level security policy settings take precedence over any local settings, as shown below.



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
    - Kerberos Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Public Key Policies
    - Encrypted Data Recovery Agents
  - IP Security Policies on Local Machine

Policy	Local Setting	Effecti
Enforce password history	0 passwords remembered	12 pas
Maximum password age	42 days	90 day
Minimum password age	0 days	3 days
Minimum password length	0 characters	8 chara
Passwords must meet complexity requirements	Disabled	Enable
Store password using reversible encryption fo...	Disabled	Disable

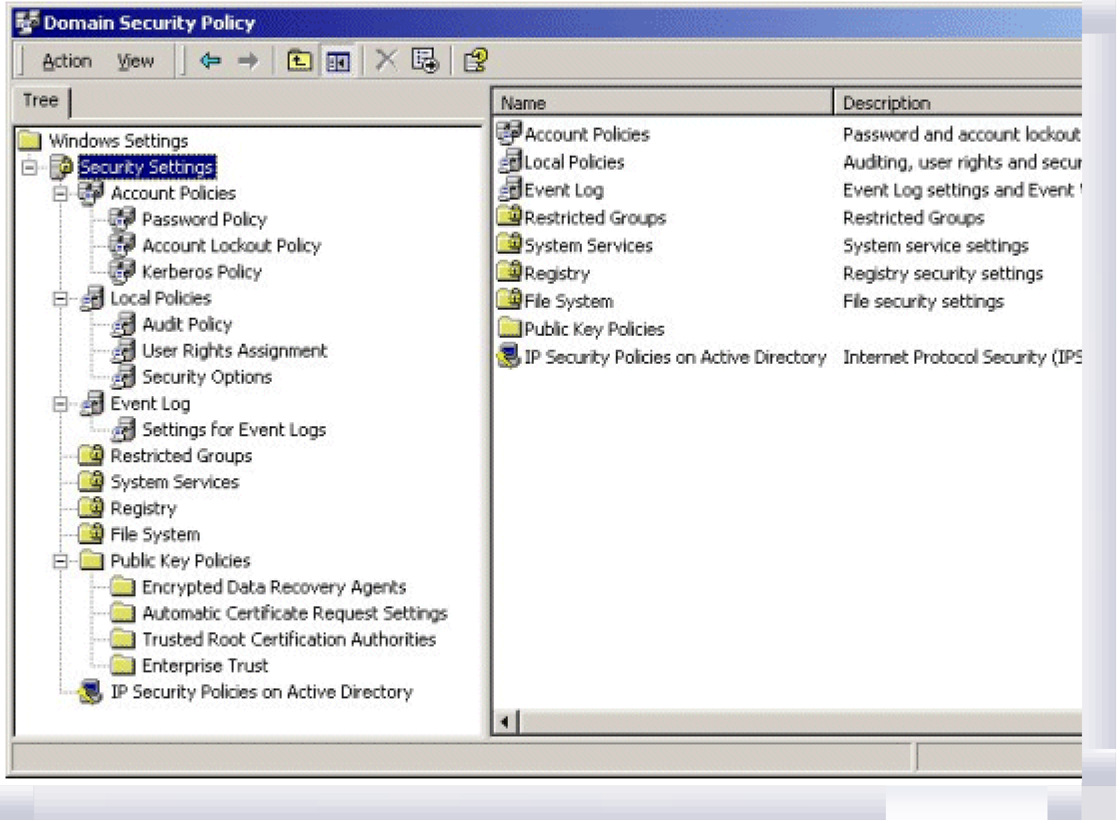
If your browser does not support inline frames, click here to view on a separate page.

Domain Security Policy

A Domain Security Policy is used to set and propagate security requirements for all computers in the Domain. The Domain Security Policy overrides Local Security Policy settings for all computers within the Domain.

To open the Domain Security Policy:

1. Log on to the Domain Controller with administrative rights.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Security Policy**. This opens the Domain Security Policy console.



Name	Description
Account Policies	Password and account lockout
Local Policies	Auditing, user rights and secur
Event Log	Event Log settings and Event \
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
Public Key Policies	
IP Security Policies on Active Directory	Internet Protocol Security (IPS

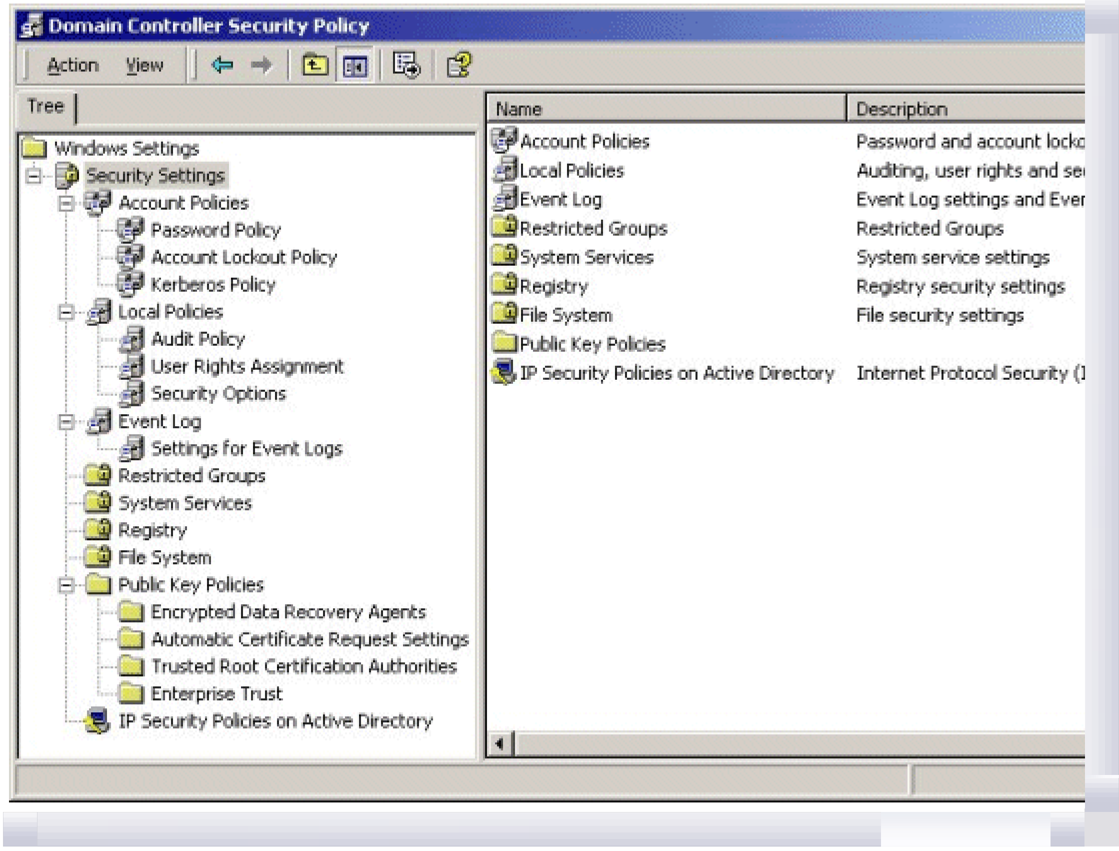
If your browser does not support inline frames, click here to view on a separate page.

Domain Controller Security Policy

A Domain Controller Security Policy is used to set and propagate security requirements for Domain Controllers. The Domain Controller Security Policy applies strictly to all Domain Controllers within the applicable Domain and is not overwritten by the Domain Security Policy.

To open the Domain Controller Security Policy:

1. Log on to the Domain Controller with administrative rights.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Domain Controller Security Policy**. This opens the Domain Controller Security Policy console.



Name	Description
Account Policies	Password and account locko
Local Policies	Auditing, user rights and se
Event Log	Event Log settings and Ever
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings
Public Key Policies	
IP Security Policies on Active Directory	Internet Protocol Security (I

If your browser does not support inline frames, click here to view on a separate page.

Organizational Unit Group Policy Objects

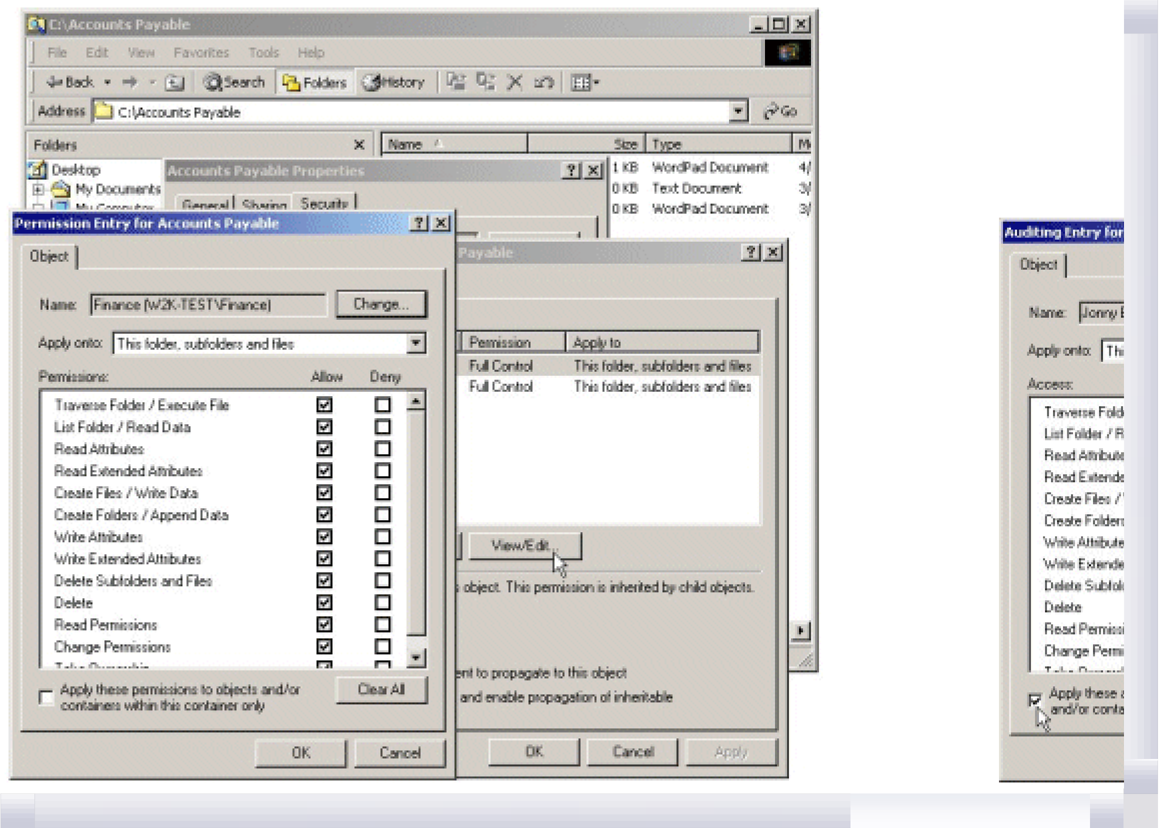
This document will not cover the implementation of OU GPOs. However, it should be noted that an OU GPO may override security policy settings implemented by the previously discussed policy interfaces. For example, if a policy that is set for the domain is incompatible with the same policy configured for a child OU, the child does not inherit the domain policy setting. Instead, the setting in the child OU is applied. This can be avoided by selecting the No Override option when creating an OU GPO. The **No Override** option forces all child containers to inherit the parent's policies even if those policies conflict with the child's policies, and even if **Block Inheritance** has been set for the child. The **No Override** check box is located by clicking the **Options** button on the GPO's **Properties** dialog box.

Additional Security Configuration Interfaces

For ease of discussion and implementation, this document focuses on managing security settings through the interfaces describe above, Windows 2000 Security Policies. However, additional tools are available, and may be addressed in cases where stand-alone policy interfaces do not provide a capability to address specific security management options. These tools include several of the standard Windows 2000 management interfaces, as well as the Security Configuration Tool Set which can not only be used to apply specific security setting, but also to test the operating systems for compliance with established policy requirements. Details on using each of these interfaces can be found in the Windows 2000 Evaluated Configuration Administrator's Guide.

Windows Explorer

Windows Explorer can be used to configure permission and audit settings on specific files and folders. Shares and share permissions can also be set through the **Windows Explorer** interface, as illustrated below.



C:\Accounts Payable
File Edit View Favorites Tools Help
Back Search Folders History
Address C:\Accounts Payable
Folders
Desktop
My Documents
Accounts Payable Properties
General Sharing Security
Auditing Entry for

Name	Size	Type
	1 KB	WordPad Document
	0 KB	Text Document
	0 KB	WordPad Document

Permission Entry for Accounts Payable

Object

Name: Finance (W2K-TEST\Finance) Change...

Apply onto: This folder, subfolders and files

Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□
Create Folders / Append Data	☑	□
Write Attributes	☑	□
Write Extended Attributes	☑	□
Delete Subfolders and Files	☑	□
Delete	☑	□
Read Permissions	☑	□
Change Permissions	☑	□

□ Apply these permissions to objects and/or containers within this container only

Clear All

OK Cancel

Permission	Apply to
Full Control	This folder, subfolders and files
Full Control	This folder, subfolders and files

View/Edit...

object. This permission is inherited by child objects.

ent to propagate to this object

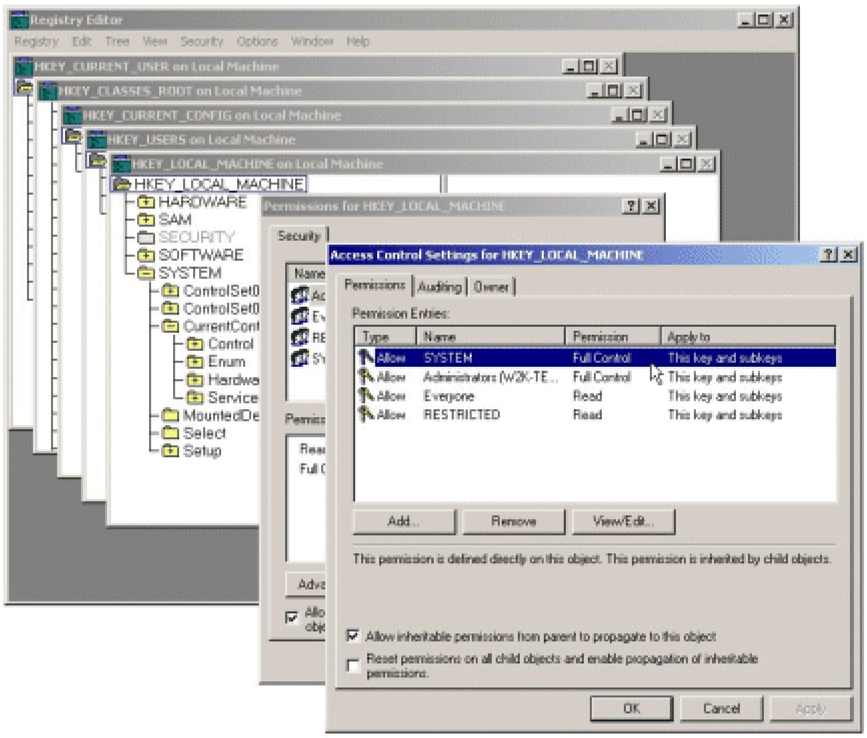
and enable propagation of inheritable

OK Cancel Apply

If your browser does not support inline frames, click here to view on a separate page.

Registry Editors

Two Registry editors are available with Windows 2000; **Regedit.exe** and **Regedt32.exe**. Of the two, **Regedt32.exe** is the only one that supports editing of permission and audit settings for Registry key objects. In the Evaluated Configuration, only Regedt32.exe should be used.



Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_CURRENT_USER on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_USERS on Local Machine
HKEY_LOCAL_MACHINE on Local Machine
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet0
ControlSet0
CurrentCont
Control
Enum
Hardwa
Service
MountedDe
Select
Setup
Permissions for HKEY_LOCAL_MACHINE
Security

Access Control Settings for HKEY_LOCAL_MACHINE

Permissions | Auditing | Owner

Permission Entries:

Type	Name	Permission	Apply to
Allow	SYSTEM	Full Control	This key and subkeys
Allow	Administrators (W2K-TE...	Full Control	This key and subkeys
Allow	Everyone	Read	This key and subkeys
Allow	RESTRICTED	Read	This key and subkeys

Add... Remove View/Edit...

This permission is defined directly on this object. This permission is inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

□ Reset permissions on all child objects and enable propagation of inheritable permissions.

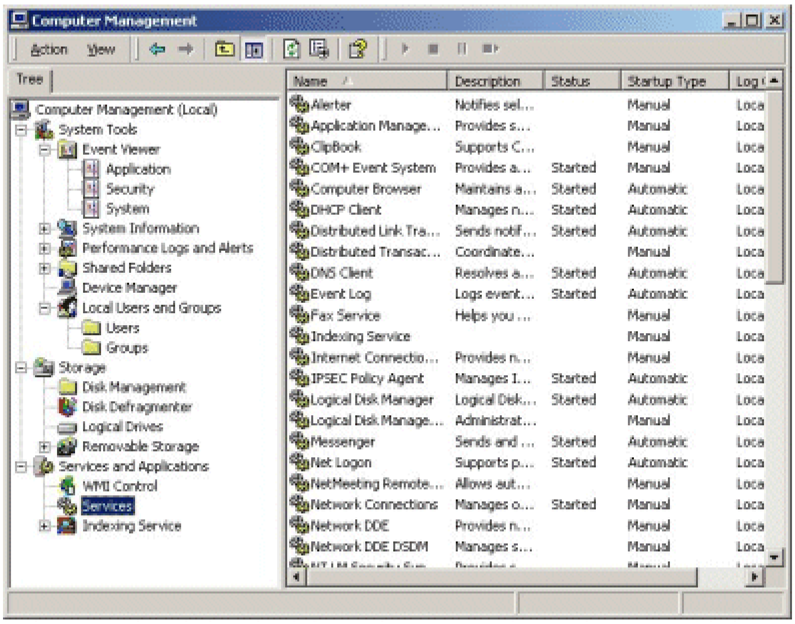
OK Cancel Apply

If your browser does not support inline frames, click here to view on a separate page.

> **Warning** Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows 2000 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Computer Management Interface

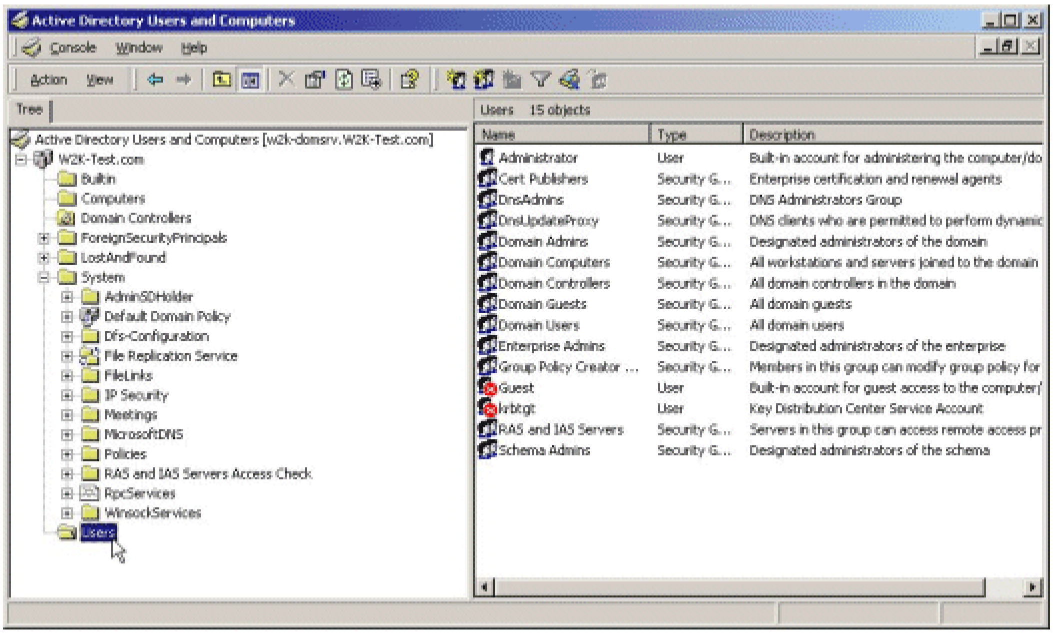
The **Computer Management** interface is available on all Windows 2000 operating systems. It supports management of audit logs, share assignments and permissions, system services, as well as user and groups accounts. On Domain Controllers the user and group accounts are managed from **Active Directory Users and Computers** interface instead of the **Computer Management** interface.



Name	Description	Status	Startup Type	Log (
Alerter	Notifies sel...		Manual	Loca
Application Manage...	Provides s...		Manual	Loca
ClipBook	Supports C...		Manual	Loca
COM+ Event System	Provides a...	Started	Manual	Loca
Computer Browser	Maintains a...	Started	Automatic	Loca
DHCP Client	Manages n...	Started	Automatic	Loca
Distributed Link Tra...	Sends notif...	Started	Automatic	Loca
Distributed Transac...	Coordinate...		Manual	Loca
DNS Client	Resolves a...	Started	Automatic	Loca
Event Log	Logs event...	Started	Automatic	Loca
Fax Service	Helps you ...		Manual	Loca
Indexing Service			Manual	Loca
Internet Connectio...	Provides n...		Manual	Loca
IPSEC Policy Agent	Manages I...	Started	Automatic	Loca
Logical Disk Manager	Logical Disk...	Started	Automatic	Loca
Logical Disk Manage...	Administrat...		Manual	Loca
Messenger	Sends and ...	Started	Automatic	Loca
Net Logon	Supports p...	Started	Automatic	Loca
NetMeeting Remote...	Allows aut...		Manual	Loca
Network Connections	Manages o...	Started	Manual	Loca
Network DDE	Provides n...		Manual	Loca
Network DDE DSDM	Manages s...		Manual	Loca

Active Directory Users and Computers

The **Active Directory Users and Computers** interface is used to create and manage users, computers, and other Active Directory objects for a domain and is only available on Domain Controllers.



Users 15 objects

Name	Type	Description
Administrator	User	Built-in account for administering the computer/do
Cert Publishers	Security G...	Enterprise certification and renewal agents
DnsAdmins	Security G...	DNS Administrators Group
DnsUpdateProxy	Security G...	DNS clients who are permitted to perform dynamic
Domain Admins	Security G...	Designated administrators of the domain
Domain Computers	Security G...	All workstations and servers joined to the domain
Domain Controllers	Security G...	All domain controllers in the domain
Domain Guests	Security G...	All domain guests
Domain Users	Security G...	All domain users
Enterprise Admins	Security G...	Designated administrators of the enterprise
Group Policy Creator ...	Security G...	Members in this group can modify group policy for
Guest	User	Built-in account for guest access to the computer/
krbtgt	User	Key Distribution Center Service Account
RAS and IAS Servers	Security G...	Servers in this group can access remote access pr
Schema Admins	Security G...	Designated administrators of the schema

If your browser does not support inline frames, click here to view on a separate page.

Microsoft Security Configuration Tool Set

The Microsoft Security Configuration Tool Set consists of a set of Microsoft Management Console (MMC) snap-ins designed to provide a capability for security configuration and analysis of Windows 2000 operating systems. The Security Configuration Tool Set allows administrators to configure security on Windows 2000 operating systems, and then perform periodic analysis of the systems to ensure that the configuration remains intact or to make necessary changes over time.

Account Policies

Account policies are the rules that control three major account authentication features: password configuration, account lockout, and Kerberos authentication.

- **Password policy.** For local user accounts, determines settings for passwords such as enforcement, and lifetimes.
- **Account lockout policy.** For local user accounts, determines when and for whom an account will be locked out of the system.
- **Kerberos policy.** Kerberos authentication is the primary authentication mechanism used in an Active Directory domain.

Account policies can be applied to user accounts in domains, organizational units, trees, and so forth, and there is a hierarchical structure to these policies:

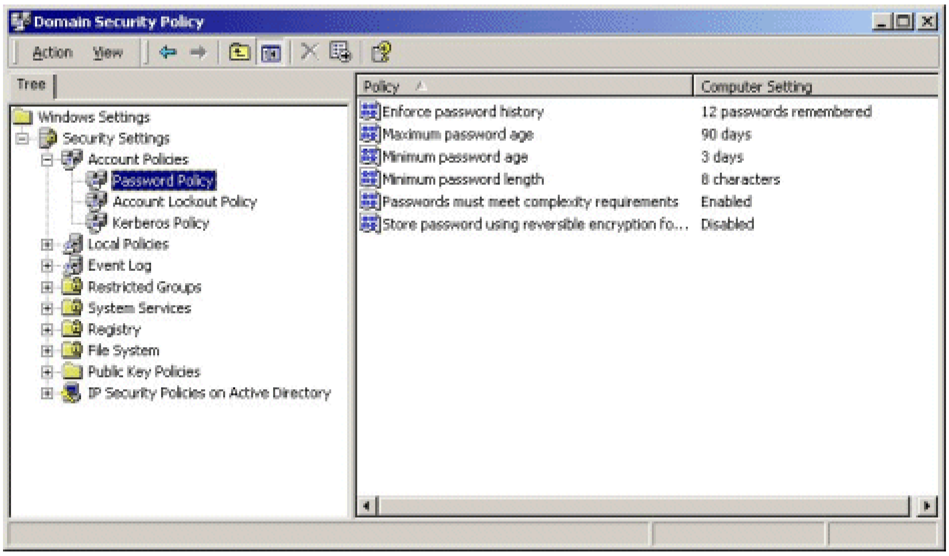
- Domain policies take precedence over Active Directory object policies.
- Organization unit policies take precedence over Domain policies.
- Root domain policies take precedence over all policies.

See the Windows 2000 Evaluated Configuration Administrator's Guide for additional information on setting account policies.

Set the Password Policy

View and edit current password policy settings as follows:

1. Open the applicable Security Policy
2. Expand Security Settings.
3. Within Security Settings, expand Account Policies to reveal the Password, Account Lockout, and Kerberos policies.
4. Click on the **Password Policy** object. The right-hand details pane will reveal the configurable Password Policy settings.



Policy	Computer Setting
Enforce password history	12 passwords remembered
Maximum password age	90 days
Minimum password age	3 days
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption fo...	Disabled

If your browser does not support inline frames, click here to view on a separate page.

5. Set the Password Policy as recommended or required in Table 3.1.

Table 3.1 Password Policy Settings

Password Policies	Professional	Server	DC	Required	Recommended
Set the Password History Requirements **Security Objective**: Set limit on how often passwords may be reused. **Procedure:** a. Double click on the Enforce password history policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the Define this policy setting box.	✓	✓	✓		✓

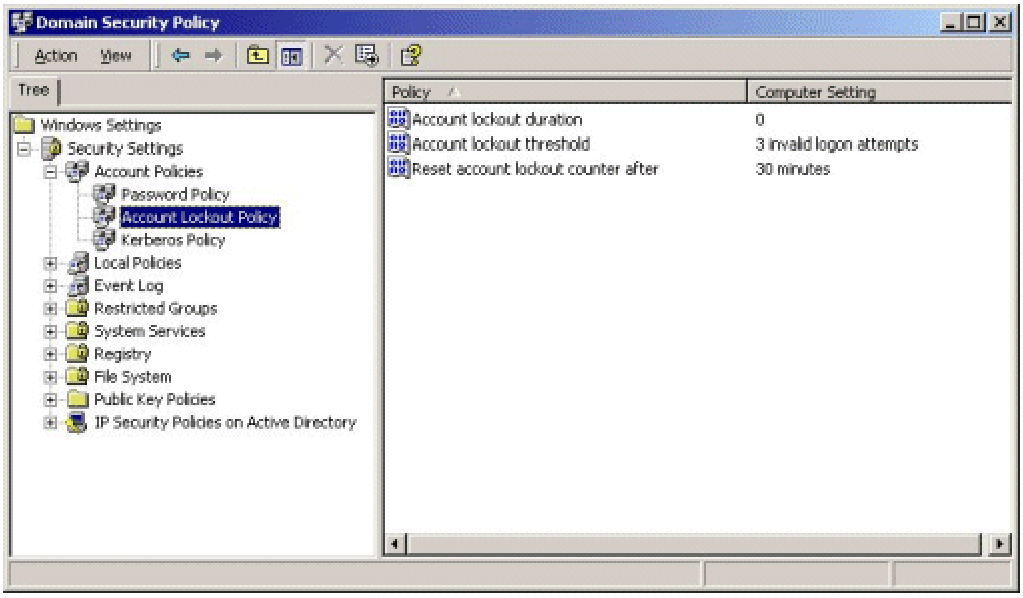
c. Change the number in the passwords remembered field (maximum is 24) to reflect the number of passwords the system will remember. A recommended setting is 24 passwords remembered.					
Set the Maximum Password Age **Security Objective**: Set the length of time users can keep their passwords before they have to change it. **Procedure:** a. Double click on the **Maximum password age** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **days** field to the desired number. A recommended setting is 42 days. **Note** The ST requires that a password expiration time be able to be set, but does not specify an expiration period. A Maximum Password Age must be set if a Minimum Password Age is used.	✓	✓	✓		✓
Set the Minimum Password Age **Security Objective**: Set the length of time users must keep a password before they can change it. **Procedure**: a. Double click on the **Minimum password age** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **days** field to the desired number. A recommended setting is 2 days. **Note** The ST requires that the administrator be able to set a minimum password age, but does not specify the length of time users must keep a password before they can change it. A Minimum Password Age must be set if a Maximum Password Age is used.	✓	✓	✓		✓
Set the Minimum Password Length **Security Objective:** Set the minimum number characters required for user passwords. **Procedure:** a. Double click on the **Minimum password length** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the	✓	✓	✓	✓	

Define this policy setting box. c. Change the number in the **characters** field to eight (8). **Note** The ST requires that passwords be set to a minimum of 8 characters.					
Set the Password Complexity Requirements **Security Objective:** Requires the use of complex (strong) password. This policy will impose a requirement for a combination of alphanumeric, special, and upper and lower case characters in a password. **Procedure:** a. Double click on the **Passwords must meet complexity requirements** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Select the **Enabled** radio button. **Note** The ST does not specify password complexity requirements.	✓	✓	✓		✓
Do Not Enable Reversible Encryption for Passwords **Security Objective:** Not recommended. **Procedure:** Verify the default setting is "Disabled."	✓	✓	✓	✓	

Set the Account Lockout Policy

View current Account Lockout Policy settings and edit as follows:

1. Open the applicable Security Policy.
2. Expand Security Settings.
3. Within Security Settings expand Account Policies to reveal the Password, Account Lockout, and Kerberos policies.
4. Click on the **Account Lockout Policy** object. The right-hand details pane will reveal the configurable Account Lockout Policy settings.



Policy	Computer Setting
Account lockout duration	0
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

If your browser does not support inline frames, click here to view on a separate page.

5. Set the Account Lockout Policy as recommended or required in Table 3.2.

Table 3.2 Account Lockout Policy Settings

Account Lockout Policies	Professional	Server	DC	Required	Recommended
Set Account Lockout Duration **Security Objective:** Once an account is locked for invalid password attempts, this setting keeps the account locked for a specified period of time (or until an administrator unlocks the account) before resetting. **Procedure:** a. Double click on the **Account lockout duration** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. It is recommended that the policy be set to lock the account indefinitely by changing the number in the **minutes** field to zero (0). This will require an administrator to unlock the account. **Notes** The ST requires that a lockout duration be set. To meet the strength of function requirement, the value must be set to 1 minute or greater. The value can also be set to 0, which then requires the administrator to unlock the account. The Account lockout duration policy is linked to the Reset account lockout counter after policy. If the Account lockout duration policy is set to 0, the Reset account lockout counter after policy can be set to any value. If the Account lockout duration policy is set to a value other than 0, the Reset account lockout counter after policy will be automatically set to an equal value by default.	✓	✓	✓	✓	
Set Account Lockout Threshold **Security Objective:** Set the number of invalid login attempts that are allowed before an account is locked out. **Procedure:** a. Double click on the **Account lockout threshold** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **invalid login attempts** field to the desired number. It is required that it not be set at a value greater than 5. **Note** The ST requires that a limit on the number of unsuccessful authentication attempts be set, but does not specify the limit. To meet the strength of function requirement, the value must be set	✓	✓	✓	✓	

at a value not greater than 5. Setting the **Account lockout threshold** will require that the **Reset account lockout counter after** and the **Account lockout duration** value settings be set. By default, they will be set to 30.					
Set the Account Lockout Reset Counter **Security Objective:** Every time a logon attempts fails, the value of a threshold that tracks the number of bad logon attempts is raised. This policy determines how long the lockout threshold is maintained before being reset. **Procedure:** a. Double click on the **Reset account lockout counter after** policy object in the right-hand details pane to open the corresponding Security Policy Setting dialog window. b. For Domain-level policies, check the **Define this policy setting** box. c. Change the number in the **minutes** field to the desired number. It is recommended that the reset counter be set to a minimum of 30 minutes. **Note** The **Reset account lockout counter after** setting is linked to the **Account lockout duration** setting. If the **Reset account lockout counter after** setting is set to a value of 30 or less, the **Account lockout duration** setting will be automatically set to 30 by default. If the **Reset account lockout counter after** setting is set to a value of 31 or greater, the **Account lockout duration** will be automatically set to an equal value by default.	✓	✓	✓	✓	

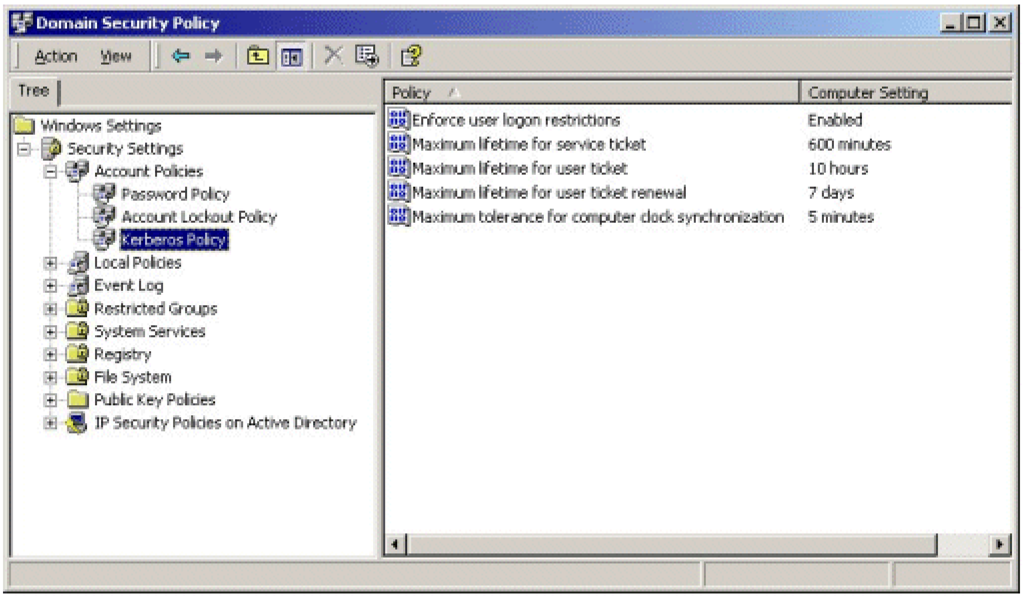
Access the Kerberos Policy Settings

View current Kerberos Policy settings and allow editing.

1. Open the Domain Security Policy or the Domain Controller Security Policy, as applicable.

   Note The Kerberos Policy Settings are not available through a Local Security Policy tool. Domain members can inherit this policy from the Domain Security Policy.

2. Expand Security Settings.
3. Within Security Settings expand Account Policies to reveal the Password, Account Lockout, and Kerberos policies.
4. Click on the **Kerberos Policy** object. The right-hand details pane will reveal the configurable Kerberos Policy settings.



Policy	Computer Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

If your browser does not support inline frames, click here to view on a separate page.

5. Set the Kerberos Policy as recommended or required in Table 3.3.

Table 3.3 Kerberos Policy Settings

Kerberos Policies	Professional	Server	DC	Required	Recommended
Enforce User Logon Restrictions **Security Objective:** Validates every logon request by checking the user rights policy to see if the user has permission to log on locally or to access the computer from the network. **Procedure:** Default settings are adequate. Verify the setting is "Enabled."	✓	✓	✓	✓	
Set the Maximum Lifetime for Service Ticket **Security Objective:** Sets the maximum duration for which a service ticket is valid. **Procedure:** Default settings are adequate. Verify that ticket expiration is set to "600 minutes."	✓	✓	✓		✓
Set the Maximum Lifetime for User Ticket **Security Objective:** Sets the maximum duration for which a user ticket is valid. **Procedure:** Default settings are adequate. Verify that ticket expiration is set to "10 hours."	✓	✓	✓		✓
Set the Maximum Lifetime for User Ticket Renewal **Security Objective:** Sets the renewal period for expired tickets. **Procedure:** Default settings are adequate. Verify that the ticket renewal expires in "7 days."	✓	✓	✓		✓
Set the Maximum Tolerance for Computer Clock Synchronization **Security Objective:** Sets the maximum tolerance for synchronization between	✓	✓	✓	✓	

computers in the Domain. **Procedure**: Default settings are adequate. Verify that the maximum tolerance is set to "5 minutes."					

Local Policies

Local Policies determine the security options for a user or service account. Local policies are based on the computer a user is logged into, and the rights the user has on that particular computer. Local Policies can be used to configure:

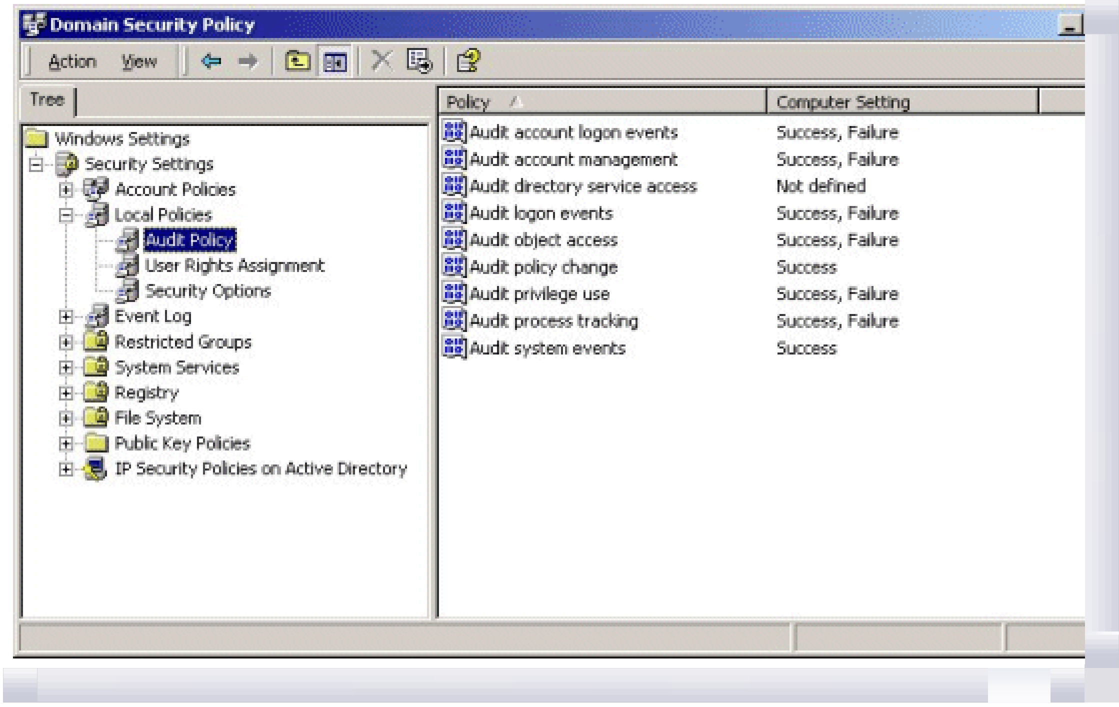
- **Audit policy.** Determines which security events are logged into the Security log on the computer (i.e., successful attempts, failed attempts or both). The Security log is part of Event Viewer.
- **User rights assignment.** Determines which users or groups have logon or task privileges on the computer.
- **Security options.** Enables or disables security settings for the computer, such as digital signing of data, Administrator and Guest account names, floppy drive and CD ROM access, driver installation, and logon prompts.

> **Note** Local policies, by definition, are local to a computer. When these settings are imported to a Group Policy object in Active Directory, they will affect the local security settings of any computer accounts to which that Group Policy object is applied. Therefore, it is important to note the order of precedence for security policies. Security policies associated with Group Policy (Organizational Units) override policies established at the local level. Policies from the domain override locally defined policies. In either case, user account rights may no longer apply if there is a local policy setting that overrides those privileges. This is important because the behavior of Microsoft Windows 2000 can be quite different from the behavior in Microsoft Windows NT. For example, when password policies are configured for the Domain group policy (as they are by default), they affect every computer in that domain. This means that the local account databases (on individual workstations) in the domain have the same password policy as the domain itself.

Set Event Audit

Enable auditing of security related events:

1. Open the applicable Security Policy.
2. Expand Security Settings.
3. Within Security Settings, expand Local Policies to reveal the Audit, User Rights Assignment, and Security Options policies.
4. Click on the **Audit Policy** object. The right-hand details pane will reveal the configurable Audit Policy settings



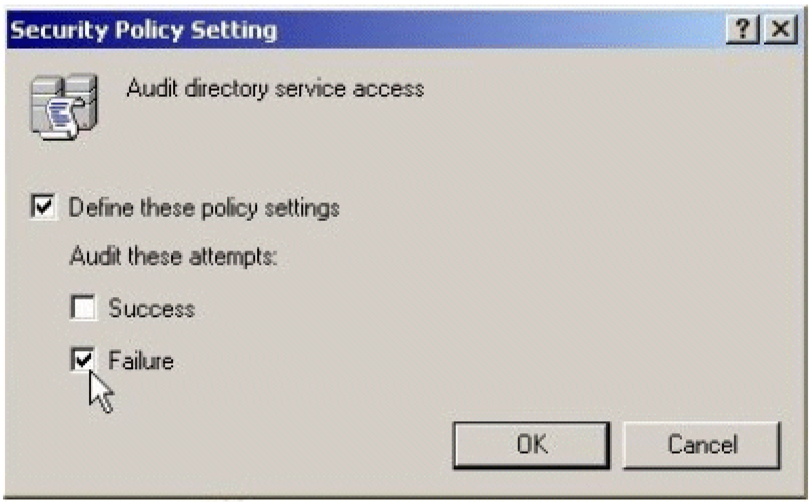
Windows Settings
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Public Key Policies
IP Security Policies on Active Directory

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not defined
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success

If your browser does not support inline frames, click here to view on a separate page.

5. To set auditing of a security event, double click on the desired audit policy in the right-hand details pane. This will open the Security Policy Setting dialog window.

6. For Domain-level policies, check the **Define these policy settings** box, and check success or failure of the event as shown below.



Security Policy Setting

Audit directory service access

☑ Define these policy settings

Audit these attempts:

□ Success

☑ Failure

If your browser does not support inline frames, click here to view on a separate page.

7. Follow these procedures to set auditing of event categories as defined in Table 3.4.

Table 3.4 Audit Policy Settings

Audit Policies			**Professional**	**Server**	**DC**	**Required**	**Recommended**
Audit Event Categories	Success	Failure					
Audit Account Logon Events	✓	✓	✓	✓	✓		✓
Audit Account Management	✓	✓	✓	✓	✓		✓
Audit Directory Service Access	✓	✓	✓	✓	✓		✓
Audit Logon Events	✓	✓	✓	✓	✓		✓
Audit Object Access	✓	✓	✓	✓	✓		✓
Audit Policy Change	✓		✓	✓	✓		✓
Audit Privilege Use	✓	✓	✓	✓	✓		✓
Audit Process Tracking	✓	✓	✓	✓	✓		✓
Audit System Events	✓		✓	✓	✓		✓

Notes

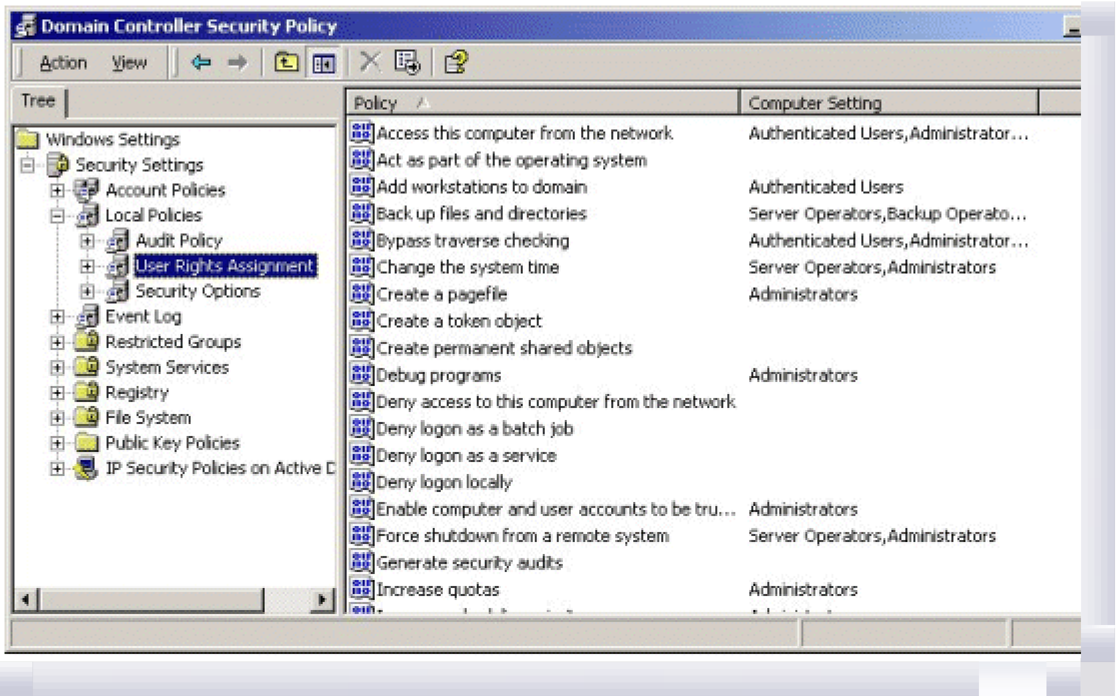
1. The Evaluated Configuration must include the "ability" to provide specific audit information. However, it is not required that the audit information be generated.
2. Setting an **Audit Object Access** policy only enables the capability to audit objects. To collect object access audit events, an auditing SACL must be set on each specific object for which access attempts are to be logged. The same applies if setting the **Audit Directory Service Access** policy.
3. Appendix B – Audit Categories and Events, provides a matrix of Windows 2000 audit events, applicable ST requirements, and recommended audit settings.
4. "Account logon events" are generated where the account resides, such as on a Domain. "Logon events" are generated where the logon attempt occurs.

Modify Logon Rights and Privileges

Modify Logon Rights and Privileges for user accounts and services:

1. Open the applicable Security Policy.
2. Expand Security Settings.
3. Within Security Settings, expand Local Policies to reveal the Audit, User Rights Assignment, and Security Options policies.

4. Click on the **User Rights Assignment** object. The right-hand details pane will reveal the configurable user rights policy settings.



Policy	Computer Setting
Access this computer from the network	Authenticated Users,Administrator...
Act as part of the operating system	
Add workstations to domain	Authenticated Users
Back up files and directories	Server Operators,Backup Operato...
Bypass traverse checking	Authenticated Users,Administrator...
Change the system time	Server Operators,Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	
Enable computer and user accounts to be tru...	Administrators
Force shutdown from a remote system	Server Operators,Administrators
Generate security audits	
Increase quotas	Administrators

If your browser does not support inline frames, click here to view on a separate page.

5. To set a user Logon Right or Privilege, double click on the desired policy in the right-hand details pane. This will open the Security Policy Setting dialog window.

6. For Domain-level policies, check the **Define these policy settings** box.

7. To remove a Logon Right or Privilege for an account, click on the account name to highlight it and click the **Remove** button.

8. To add a Logon Right or Privilege to an account, click the **Add** button and browse the appropriate account directory for the desired account.

9. There are several default assignments of user rights and privileges that the administrator should or must (see recommended or required columns in Table 3.5) change to maintain the evaluated configuration.

Note The Power Users account does not exist on a Domain Controller. Therefore modifications affecting user rights and privileges for the Power Users group cannot be done manually from a Domain Controller. Also note that although the Power Users group does not reside on the Domain Controller, there may still exist references to this group in the Domain Controller's local policy, which remain after the computer is upgraded from a Server to a Domain Controller.

Table 3.5 User Rights and Privileges

User Rights and Privilege Assignment			**Profession**
Logon Right	Default	Modified	
Access this computer from the network ***(Professional/Server)***	Administrators Backup Operators Power Users Users Everyone	Administrators Backup Operators Power Users Users Authenticated Users	✓
Access this computer from the network ***(Domain Controller)***	Administrators Authenticated Users Everyone	Administrators Authenticated Users	
Log on Locally ***(Professional)***	Administrators Backup Operators Power Users Users Machinename\Guest	Administrators Backup Operators Power Users Users	✓

Log on Locally ***(Server)***	Administrators Backup Operators Power Users Users Machinename\Guest Machinename\TsInternetUser	Administrators Backup Operators Power Users Users **Note** The Machinename\TsInternetUser account is removed because Windows 2000 Terminal Server is not part of the Evaluated Configuration.	
Log on Locally ***(Domain Controller)***	Administrators Account Operators Backup Operators Print Operators Server Operators TsInternetUser	Administrators Account Operators Backup Operators Print Operators Server Operators **Note** The TsInternetUser account is removed because Windows 2000 Terminal Server is not part of the Evaluated Configuration.	
Privilege	**Default**	**Modified**	
Add Workstations to the Domain ***(Domain Controller)***	Authenticated Users	Remove the Authenticated Users account. Do not grant this privilege to other users. **Note** Domain Administrators have this privilege by default.	
Increase Quotas ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	
Increase Scheduling Priority ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	
Load and Unload Device Drivers ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	
Manage Auditing and Security Log ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	
Modify Firmware Environment ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	
Profile System Performance ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	
Shut Down the	Administrators	Administrators	✓

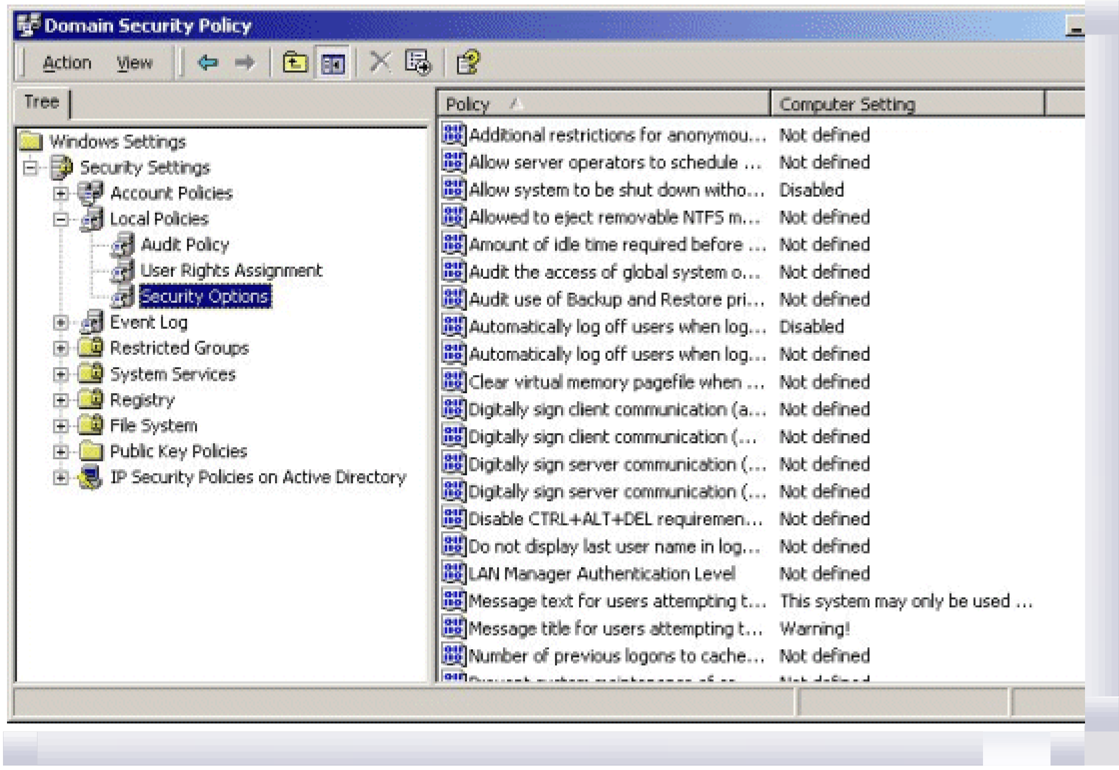
System ***(Professional)***	Backup Operators Power Users Users	Backup Operators Power Users Authenticated Users	
Take Ownership of Files and Objects ***(Domain Controller – in the Domain Security Policy)***	(Not Defined)	Administrators	

Note Appendix C – User Rights and Privileges, provides a matrix of Windows 2000 user rights and privileges, applicable ST requirements, and the recommended/required modifications.

Modify Security Options

Modify predefined security related Registry settings:

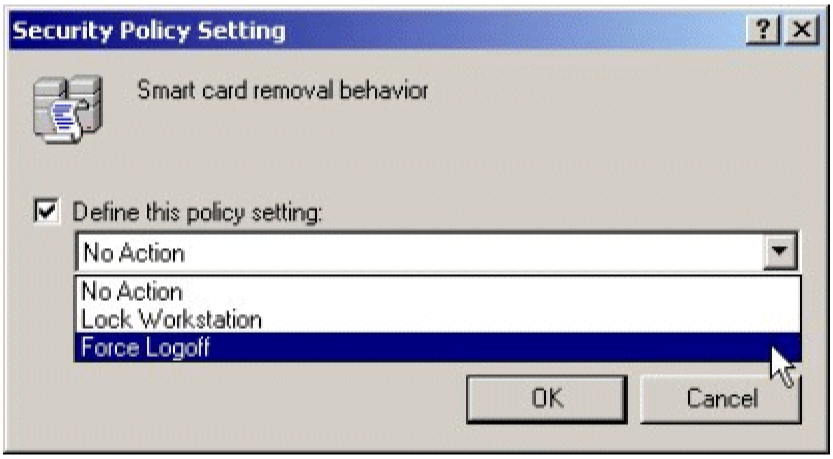
1. Open the applicable Security Policy.
2. Expand Security Settings.
3. Within Security Settings, expand Local Policies to reveal the Audit, User Rights Assignment, and Security Options policies.
4. Click on the **Security Options** object. The right-hand details pane will reveal the configurable security options.



Policy	Computer Setting
Additional restrictions for anonymou...	Not defined
Allow server operators to schedule ...	Not defined
Allow system to be shut down witho...	Disabled
Allowed to eject removable NTFS m...	Not defined
Amount of idle time required before ...	Not defined
Audit the access of global system o...	Not defined
Audit use of Backup and Restore pri...	Not defined
Automatically log off users when log...	Disabled
Automatically log off users when log...	Not defined
Clear virtual memory pagefile when ...	Not defined
Digitally sign client communication (a...	Not defined
Digitally sign client communication (...	Not defined
Digitally sign server communication (...	Not defined
Digitally sign server communication (...	Not defined
Disable CTRL+ALT+DEL requiremen...	Not defined
Do not display last user name in log...	Not defined
LAN Manager Authentication Level	Not defined
Message text for users attempting t...	This system may only be used ...
Message title for users attempting t...	Warning!
Number of previous logons to cache...	Not defined

If your browser does not support inline frames, click here to view on a separate page.

5. To set a Security Option, double click on the desired policy in the right-hand details pane. This will open the Security Policy Setting dialog window.
6. For Domain-level policies, check the **Define these policy settings** box.
7. Input to the **Security Policy Setting** dialog boxes for selected security options will vary depending on the configuration requirements of the option. For example some security options may require selection from a drop down menu or a text input as shown below.



Security Policy Setting

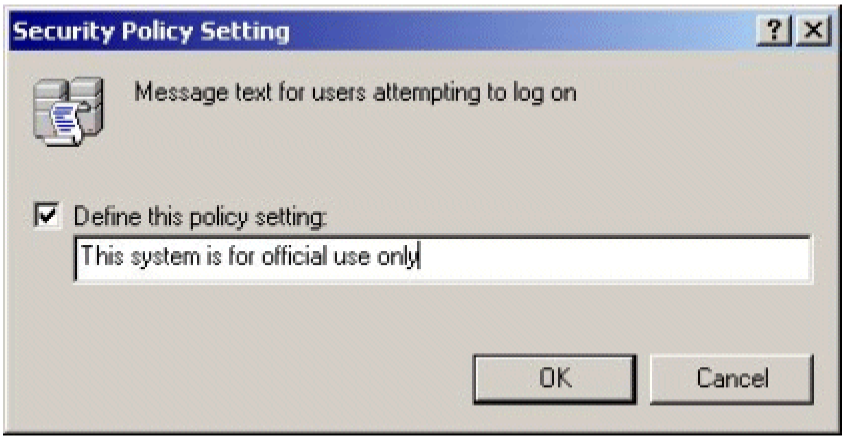
Smart card removal behavior

☑ Define this policy setting:

No Action

No Action
Lock Workstation
Force Logoff

If your browser does not support inline frames, click here to view on a separate page.



Security Policy Setting

Message text for users attempting to log on

☑ Define this policy setting:

This system is for official use only

If your browser does not support inline frames, click here to view on a separate page.

8. Modify the Security Options as shown in Table 3.6.

Table 3.6 Security Option Settings

Security Options	Professional	Server	DC	Required	Recommended
Set Additional Restrictions for Anonymous Connections **Security Objective:** Disable ability of anonymous user to enumerate SAM accounts and shares. **Procedure:** a. Double click on Additional restrictions for anonymous connections in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select Do not allow enumeration of SAM accounts and shares. d. Click the **OK** button.	✓	✓	✓	✓	
Allow server operators to schedule tasks (domain controllers only) **Security Objective:** Determines if Server Operators are allowed to submit jobs by means of the AT schedule facility. By default, a user must be an administrator in order to submit jobs by means of the AT scheduler. Enabling this security policy			✓	✓	

setting allows members of the Server Operators group to submit AT schedule jobs on Domain Controllers without having to make them Administrators. **Procedure:** Do not enable this feature. The AT schedule facility is not part of the Evaluated Configuration. **Note** The Domain level policy default is “**Not Defined**.” It is recommended that the policy be set to **Disabled**.					
Disable Shutdown Without Logon **Security Objective:** Disable the ability to shut down the computer without first authenticating to the system. **Procedure:** a. Double click on Allow system to be shut down without having to log on in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Disabled** radio button and click the **OK** button.	✓	✓	✓	✓	
Restrict Ability to Eject Removable NTFS Media **Security Objective:** Ensure integrity of ACL settings on data contained in removable media by allowing only authorized administrators the capability of removing the media from the computer. **Procedure:** a. Double click on **Allowed to eject removable NTFS media** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select **Administrators** and click the **OK** button.	✓	✓	✓		✓
Amount of idle time required before disconnecting a session **Security Objective:** Determines the amount of continuous idle time that must pass in a Server Message Block (SMB) session before the session is disconnected due to inactivity. Administrators can use this policy to control when a computer disconnects an inactive SMB session. If client activity resumes, the session is automatically reestablished. This policy is defined for servers by default in Local Computer Policy with a default value of 15 minutes. This policy is not defined on workstations. For this policy setting, a value of 0 means to disconnect an idle session as quickly as reasonably possible. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Audit the Access of Global System Objects **Security Objective:** Enable the capability	✓	✓	✓		✓

to audit access of global system objects. When this policy is enabled, it causes system objects such as mutexes, events, semaphores, and DOS Devices to be created with a default system access control list (SACL). If the Audit object access audit policy is also enabled, then access to these system objects will be audited. **Procedure:** a. Double click on **Audit the access of global system objects** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note** In the evaluated configuration, these objects must be auditable, however, enforcing this audit capability is optional. To audit these objects, the administrator must set this option. This setting will generate a large amount of audit information. Therefore, it should only be enabled where there is a strict audit management process in place for reviewing, archiving, and clearing the audit logs on a regular basis. The maximum log size should also be edited to support an increase in the number of events being logged.					
Audit the Use of Backup and Restore Privilege **Security Objective:** Enable the capability to create audit event entries whenever the **Backup files and directories** or the **Restore files and directories privileges** are used. By default, the use of backup and restore privileges are not audited. When the **Audit privilege use** audit policy is enabled and this security option is set, the use of the Backup and Restore privileges will be audited. **Procedure:** a. Double click on **Audit use of Backup and Restore privilege** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note** In the evaluated configuration, these objects must be auditable, however, enforcing this audit capability is optiona. To audit these objects, the administrator must set this option. This setting will generate a large amount of audit information. Therefore, it should only be enabled where there is a strict audit management process in place for reviewing, archiving, and clearing the audit logs on a regular	✓	✓	✓		✓

basis. The maximum log size should also be edited to support an increase in the number of events being logged.					
Automatically Log Off Users When Logon Time Expires **Security Objective:** Force a user log off of the network when that user remains logged on beyond the allowed hour range. **Procedure:** a. Double click on Automatically log off users when logon time expires in the right-hand details pane. b. Check the Define these policy settings box. c. Select the **Enabled** radio button and click the **OK** button. **Note** This Security Option can only be set at the Domain Controller.			✓		✓
Automatically Log Off Users When Logon Time Expires (Local) **Security Objective:** Force a user log off of the local computer when that user remains logged on beyond the allowed hour range. **Procedure:** Double click on **Automatically log off users when logon time expires (local)** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓		✓
Clear Virtual Memory Page File When System Shuts Down **Security Objective:** Removes the virtual memory pagefile when the system is shut down. The pagefile is reinitialized the next time a user logs in. The purpose is to ensure that any information that may remain within the page file is not available to the next user that logs on to the machine. **Procedure:** a. Double click on Clear virtual memory pagefile when system shuts down in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓	✓	
Digitally sign client communications (always) **Security Objective:** Determines whether the computer will always digitally sign client communications. The Windows 2000 Server Message Block (SMB) authentication protocol supports mutual authentication, which closes a “man-in-the-middle” attack, and supports message	✓	✓	✓	✓	

authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Enabling this option requires the Windows 2000 SMB client to perform SMB packet signing. If this policy is disabled, it does not require the SMB client to sign packets. This policy is disabled by default. For the Evaluated Configuration, this policy option may be disabled and the following security option, **"Digitally sign client communications (when possible)"** may be enabled. Since the Evaluated Configuration operating environment is a closed network with all computers configured to the same requirements, communications will use SMB signing (see note below). **Procedure:** a. Double click on **Digitally sign client communications (always)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Disabled** radio button and click the **OK** button. **Note** In order to use SMB signing, it must be either enabled or required on both the SMB client and the SMB server. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing will use the packet signing protocol during all subsequent sessions. If SMB signing is required on a server, then a client will not be able to establish a session unless it is at least enabled for SMB signing.					
Digitally sign client communications (when possible) **Security Objective:** If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) client to perform SMB packet signing when communicating with an SMB server that is enabled or required to perform SMB packet signing. See "**Digitally sign client communications (always)**" for additional details. **Procedure:** a. Double click on Digitally sign client communications (when possible) in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note** **See note** for Digitally sign client communications (always).	✓	✓	✓	✓	
Digitally sign server communications (always)	✓	✓	✓	✓	

Security Objective: If this policy is enabled, it requires the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is disabled by default. See "**Digitally sign client communications (always)**" for additional details. **Procedure:** a. Double click on **Digitally sign server communications (always)** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Disabled** radio button and click the **OK** button. **Note See note for** Digitally sign client communications (always).					
Digitally sign server communications (when possible) **Security Objective:** If this policy is enabled, it causes the Windows 2000 Server Message Block (SMB) server to perform SMB packet signing. This policy is disabled by default on workstation and server platforms in Local Computer Policy. This policy is enabled by default on Domain Controllers.. See "**Digitally sign client communications (always)**" for additional details. **Procedure:** a. Double click on Digitally sign server communications (when possible) in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button. **Note See note for** Digitally sign client communications (always).	✓	✓	✓	✓	
Disable CTRL+ALT+DEL Required for Logon **Security Objective: DO NOT ENABLE THIS OPTION.** Enabling this option will disable the trusted path mechanism. The purpose of the trusted path mechanism is to prevent spoofing of user login sessions. The default setting of this option is Disabled on a Windows 2000 computer, although a policy tool may show it as Not Defined. **Procedure:** Verify that the **Disable CTRL+ALT+DEL requirement for logon** option in the right hand details pane is **set to Not Defined or is Disabled**.	✓	✓	✓	✓	
Do Not Display Last User Name on Logon Screen **Security Objective:** By default, the Windows 2000 login interface displays the user ID of the last user that logged onto the computer. Enabling this option removes the name of the last user from the login session. As a result, an intruder	✓	✓	✓		✓

attempting to break into the computer locally would not only need to guess the password, but would also need to guess a correct user ID. **Procedure:** a. Double click on **Do not display user name in the logon screen** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.					
LAN Manager Authentication Level **Security Objective:** This Security Option is used to set the Windows Challenge/Response authentication level. It is used to establish which challenge/response authentication protocol is used for network logons. The choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted as per the following selection options: • **Send LM & NTLM responses**: Clients use LM and NTLM authentication, and never use NTLMv2 session security; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send LM & NTLM - use NTLMv2 session security if negotiated**: Clients use LM and NTLM authentication, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLM response only**: Clients use NTLM authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only**: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only\refuse LM**: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM (accept only NTLM and NTLMv2 authentication). • **Send NTLMv2 response only\refuse LM & NTLM**: Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it; DCs refuse LM and NTLM (accept only NTLMv2 authentication). The default setting for servers is **Send LM & NTLM responses**. LM authentication allows clear text passwords. Security weaknesses found with the NTLM protocol allow password crackers to decrypt NTLM-protected	✓	✓	✓		✓

authentication. To counteract this, NTLM version 2 was developed. NTLMv2 introduces additional security features, including • **Unique session keys per connection**. Each time a new connection is established, a unique session key is generated for that session. This way a captured session key will serve no useful purpose after the connection is completed. • **Session keys protected with a key exchange**. The session key can't be intercepted and used unless the key pair used to protect the session key is obtained. • **Unique keys generated for the encryption and integrity of session data**. The key that's used for the encryption of data from the client to the server will be different from the one that's used for the encryption of data from the server to the client. **Procedure:** a. Double click on **LAN Manager Authentication level** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. From the drop-down menu, select **Send NTLMv2 response only\refuse LM & NTLM** and click the **OK** button.					
Implement an Authorized Usage Warning **Security Objective:** Configure the interactive logon screen to display a logon banner with a title and warning. **Procedure:** a. To set a message title, double click on **Message title for users attempting to log on** in the right-hand details pane. This will open the Security Policy Setting dialog window. b. For Domain-level policies, check the **Define these policy settings** box. c. Enter the title for the logon message (for example, “Warning”) and click **OK**. d. To set the message, double click on **Message text for users attempting to log on** in the right-hand details pane. This will open the Security Policy Setting dialog window. e. For Domain-level policies, check the **Define these policy settings** box. f. Enter the message text and click **OK**. **Note** The Evaluated Configuration must allow for the ability to set a banner, it is not required that one be set.	✓	✓	✓		✓
Disable Caching of Logon Information **Security Objective:** Windows 2000 has	✓	✓	✓	✓	

the capability to cache logon information. If the Domain Controller cannot be found during logon and the user has logged on to the system in the past, it can use those credentials to log on. The CachedLogonsCount Registry valued determines how many user account entries Windows 2000 saves in the logon cache on the local computer. If the value of this entry is 0, Windows 2000 does not save any user account data in the logon cache. In that case, if the user’s Domain Controller is not available and a user tries to log on to a computer that does not have the user's account information, Windows 2000 displays the following message: **The system cannot log you on now because the domain <Domain-name> is not available.** If the Administrator disables a user’s domain account, the user could still use the cache to log on by disconnecting the net cable. To prevent this, Administrators should disable the caching of logon information. This results in a somewhat longer logon time, but prevents hackers from tapping logon information from short-term memory. **Procedure:** a. Double click on Number of previous logons to cache (in case domain controller is not available in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. In the **Cache:** text box, set the number of logons to 0 and click the **OK** button.					
Prevent System Maintenance of Computer Account Passwords **Security Objective:** Determines whether the computer account password should be prevented from being reset every week. As a part of Windows 2000 security, ***computer account*** passwords are changed automatically every seven days. If this policy is enabled, the machine is prevented from requesting a weekly password change. If this policy is disabled, a new password for the computer account will be generated every week. This policy is disabled by default. **Procedure:** Do not enable this policy. Verify that local policies are set to **Disabled** and that Domain policies are either **Disabled** or **Not defined**.	✓	✓	✓		✓
Prevent Users from Installing Print Drivers **Security Objective:** Determines whether members of the Users group are prevented from installing print drivers. If this policy is enabled, it prevents users from installing printer drivers on the local machine. This prevents users from “Adding Printers” when the device driver does not exist on	✓	✓	✓	✓	

the local machine. If this policy is disabled, then a member of the Users group can install printer drivers on the computer. By default, this setting is enabled on servers and disabled on workstations. **Procedure:** Do not change the defaults for servers and stand-alone computers. For Domain policies: a. Double click on **Prevent users from installing print drivers** in the right-hand details pane. b. For Domain-level policies, check the **Define these policy settings** box. c. Select the **Enabled** radio button and click the **OK** button.					
Prompt User to Change Password Before Expiration **Security Objective:** Determines how far in advance Windows 2000 should warn users that their password is about to expire. By giving the user advanced warning, the user has time to construct a sufficiently strong password. By default, this value is set to 14 days. **Procedure:** None. The default setting is adequate.	✓	✓	✓		✓
Recovery Console: Allow Automatic Administrative Logon **Security Objective:** By default, the Recovery Console requires that a password be provide the for the Administrator account before accessing the system. If this option is enabled, the Recovery Console does not require a password and will automatically log on to the system. By default, this setting is disabled, although a policy tool may show it as Not Defined. **Procedure:** Do not enable this option. **Note** The Windows 2000 Recovery Console is not part of the Evaluated Configuration; it is therefore recommended that security policies be set to enforce disabling of this option.	✓	✓	✓	✓	
Recovery Console: Allow Floppy Copy and Access to All Drives and Folders **Security Objective:** Enabling this option enables the Recovery Console SET command, which allows the following Recovery Console environment variables to be set: • **AllowWildCards** - Enable wildcard support for some commands (such as the DEL command). • **AllowAllPaths** - Allow access to all files and folders on the computer. • **AllowRemovableMedia** - Allow files to be copied to removable media, such as a floppy disk. • **NoCopyPrompt** - Do not prompt when overwriting an existing file. By default, the SET command is disabled	✓	✓	✓		✓

and all these variables are not enabled, although a policy tool may show it as Not Defined.. **Procedure:** Do not enable this option. **Note** The Windows 2000 Recovery Console is not part of the Evaluated Configuration; it is therefore recommended that security policies be set to enforce disabling of this option.					
Rename Administrator Account **Security Objective:** Used to change the name that is associated with the security identifier (SID) for the account "Administrator." This reduces the chances of administrator exploit attempts by forcing a potential hacker to not only have to guess the password, but also the user ID associated with the Administrator account. **Procedure:** Double click on **Rename administrator account** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. In the text box, enter the new name for the Administrator account and click the **OK** button.	✓	✓	✓		✓
Rename Guest Account **Security Objective:** Used to change the name that is associated with the security identifier (SID) for the account "Guest." This reduces the chances of anonymous exploit attempts by forcing a potential hacker to not only have to guess the password, but also the user ID associated with the Guest account. **Procedure:** Double click on **Rename guest account** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. In the text box, enter the new name for the Guest account and click the **OK** button. **Note** The Guest account must be disabled in the evaluated configuration (see Table 4-8).	✓	✓	✓		✓
Restrict CD-ROM Access to Locally Logged-On User Only **Security Objective:** Determines whether a CD-ROM is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable CD-ROM media. If no one is logged on interactively, the CD-ROM may be shared over the network. If this policy is disabled, then the local user and remote users can access the CD-ROM simultaneously. **Procedure:**	✓	✓	✓	✓	

Double click on **Restrict CD-ROM access to locally logged-on user only** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. Select the **Enabled** radio button and click the **OK** button.					
Restrict Floppy Access to Locally Logged-On User Only **Security Objective:** Determines whether removable floppy media is accessible to both local and remote users simultaneously. If enabled, this policy allows only the interactively logged-on user to access removable floppy media. If no one is logged on interactively, the floppy media may be shared over the network. If this policy is disabled, then the local user and remote users can access the floppy media simultaneously. **Procedure:** Double click on **Restrict floppy access to locally logged-on user only** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. Select the **Enabled** radio button and click the **OK** button.	✓	✓	✓	✓	
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always) **Security Objective:** Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic must be either signed or encrypted. If this policy is disabled, signing and encryption are negotiated with the domain controller. By default, this policy is disabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Secure Channel: Digitally Encrypt Secure Channel Data (When Possible) **Security Objective:** Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords)	✓	✓	✓		✓

is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic should be encrypted. If this policy is disabled, outgoing secure channel traffic will not be encrypted. By default, this option is enabled. **Procedure:** Do not change the default setting.					
Secure Channel: Digitally Sign Secure Channel Data (When Possible) **Security Objective:** Determines whether the computer will always digitally encrypt or sign secure channel data. When a Windows 2000 system joins a domain, a computer account is created. Thereafter, when the system boots, it uses the password for that account to create a secure channel with the domain controller for its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as passwords) is encrypted, but the channel is not integrity checked and not all information is encrypted. If this policy is enabled, all outgoing secure channel traffic should be signed. If this policy is disabled, no outgoing secure channel traffic will be signed. By default, this option is enabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Secure Channel: Require Strong (Windows 2000 or Later) Session Key **Security Objective:** If this policy is enabled, all outgoing secure channel traffic will require a strong (Windows 2000 or later) encryption key. If this policy is disabled, the key strength is negotiated with the DC. This option should only be enabled if all of the DCs in all trusted domains support strong keys. By default, this value is disabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Send Unencrypted Password to Connect to Third-Party SMB Servers **Security Objective:** If this policy is enabled, the Server Message Block (SMB) redirector is allowed to send clear-text passwords to non-Microsoft SMB servers that do not support password encryption during authentication. By default, this option is disabled. **Procedure:** Do not change the default setting.	✓	✓	✓		✓
Shut Down the System Immediately if Unable to Log Security Audits **Security Objective:** Determines whether the system should shut down if it is unable to log security events. If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be	✓	✓	✓		✓

logged when the security audit log is full and the retention method specified for the security log is either **Do Not Overwrite Events** or **Overwrite Events by Days**. If the security log is full and an existing entry cannot be overwritten and this security option is enabled, the following blue screen error will occur: **STOP: C0000244 {Audit Failed}** **An attempt to generate a security audit failed.** To recover, an administrator must log on, archive the log (if desired), clear the log, and reset this option as desired. By default, this policy is disabled. **Procedure:** Double click on **Shut down system immediately if unable to log security audits** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. Select the **Enabled** radio button and click the **OK** button. **Note** Use this security policy on servers and Domain Controllers only after implementing strict procedures for archiving and clearing the audit logs on a regular basis. **Note** The ST requires the system to be able to prevent auditable events from occurring, except those taken by the administrator, if the audit log is full. If the administrator desires this functionality, this option must be enabled.					
Smart Card Removal Behavior **Security Objective:** Determines what should happen when the smart card for a logged-on user is removed from the smart card reader. The options are: • No Action • Lock Workstation • Force Logoff By default, **No Action** is specified. If **Lock Workstation** is specified, then the workstation is locked when the smart card is removed allowing users to leave the area, take their smart card with them, and still maintain a protected session. If Force Logoff is specified, then the user is automatically logged off when the smart card is removed. **Procedure:** Double click on **Smart card removal behavior** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. From the drop-down menu, select **Lock Workstation** and click the **OK** button. **Note** The integration of smart card technology is not part of the	✓	✓	✓		✓

Evaluated Configuration.					
Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links) **Security Objective:** Determines the strength of the default discretionary access control list (DACL) for objects. Windows 2000 maintains a global list of shared system resources such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects with what permissions. If this policy is enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create. By default, this option is enabled locally on Windows 2000 Professional and Server, but is not defined in the Domain Security Policy. **Procedure:** Double click on **Strengthen default permissions of global system objects (e.g. Symbolic Links)** in the right-hand details pane. For Domain-level policies, check the **Define these policy settings** box. Select the **Enabled** radio button and click the **OK** button. For stand-alone computers/domain members, verify that this security option is enabled in the local policy.	✓	✓	✓	✓	
Unsigned Driver Installation Behavior **Security Objective:** Determines what should happen when an attempt is made to install a device driver (by means of the Windows 2000 device installer) that has not been certified by the Windows Hardware Quality Lab (WHQL). The options are: • **Silently succeed** • **Warn but allow installation** • **Do not allow installation** The default setting is to **Warn but allow installation**. **Procedure:** Double click on **Unsigned driver installation behavior** in the right-hand details pane. For local policies, make sure the behavior is set to **Warn but allow installation**. For Domain-level policies, check the **Define these policy settings** box. From the drop-down menu, select **Warn but allow installation** and click the **OK** button.	✓	✓	✓		✓
Unsigned Non-Driver Installation Behavior **Security Objective:** Determines what	✓	✓	✓		✓

should happen when an attempt is made to install any non-device driver software that has not been certified. The options are: ● **Silently succeed** ● **Warn but allow installation** ● **Do not allow installation** The default setting is to **Silently succeed**. **Procedure:** Double click on **Unsigned non-driver installation behavior** in the right-hand details pane. For local policies, make sure the behavior is set to **Warn but allow installation**. For Domain-level policies, check the **Define these policy settings** box. From the drop-down menu, select **Warn but allow installation** and click the **OK** button.					

Additional Security Settings

The additional security settings described in this subsection are not available in the security policy GUIs and must therefore be configured through the Registry Editor. Instructions for using the Registry editor are available in the Windows 2000 Evaluated Configuration Administrator's Guide.

Information on how to edit the Registry is also available through the **Help** tool in **Regedit.exe**. For example, for instructions on adding a key to the Registry:

1. Click the **Start** button and select **Run...**
2. Within the **Run** dialog window's text box, type **regedt32** and click the **OK** button to open the **Registry Editor** (Regedt32.exe).
3. From the editor's **Help** menu, select **Contents**.
4. In the right-hand pane of the Registry Editor's Help tool, click on the "**Add and delete information in the registry**" hyperlink.
5. The pane will change to provide a list of help topics for adding and deleting information in the Registry. Click on the "**Add a key to the registry**" hyperlink to obtain the detailed instructions.

Warning Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows 2000 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Required Registry Settings

The Registry settings described in this subsection are required in order to conform to Evaluated Configuration requirements. All numerical values are shown in decimal, unless otherwise noted.

Disable DirectDraw

The DirectDraw feature exists to enable high-performance multimedia applications. It does this by providing applications with the most direct path possible to the 2-D graphics hardware on a system. The DirectDraw feature is not part of the Evaluated Configuration and must be disabled.

Disable DirectDraw by editing the Registry and changing the Timeout value to 0 as shown below.

Key Path: **HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers**	**Format**	**Value**
Key: DCI **Value Name:** Timeout	REG_DWORD	0

Remove OS/2 and POSIX subsystems

The OS/2 and POSIX subsystems were not included in the evaluated configuration, and should therefore be removed. To remove OS/2 and POSIX support from Windows 2000, edit the Registry and delete the value as shown below.

Key Path: **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager**	**Format**	**Value**

Key: SubSystems **Value Name:** Optional	REG_MULTI_SZ	Delete the value

Disable unnecessary devices

For the Evaluated Configuration, it is necessary to disable all of the devices listed below by editing the Registry and changing the **Start** value to 4 as shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services		**Format**	**Value**
Key: audstub	**Value Name:** Start	REG_DWORD	4
Key: mnmdd	**Value Name:** Start	REG_DWORD	4
Key: ndistap	**Value Name:** Start	REG_DWORD	4
Key: ndiswan	**Value Name:** Start	REG_DWORD	4
Key: ndproxy	**Value Name:** Start	REG_DWORD	4
Key: parvdm	**Value Name:** Start	REG_DWORD	4
Key: pptpminiport	**Value Name:** Start	REG_DWORD	4
Key: ptilink	**Value Name:** Start	REG_DWORD	4
Key: rasacd	**Value Name:** Start	REG_DWORD	4
Key: rasl2tp	**Value Name:** Start	REG_DWORD	4
Key: raspti	**Value Name:** Start	REG_DWORD	4
Key: wanarp	**Value Name:** Start	REG_DWORD	4

Protect kernel object attributes

This step is necessary to ensure that the object manager may change attributes of a kernel object in the object table for the current process if and only if the previous mode of the caller is kernel mode. To enable this capability edit the Registry to create and set the value of the Registry entry shown below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Control	**Format**	**Value**
Key: Session Manager **Value Name:** EnhancedSecurityLevel	REG_DWORD	1

Restrict Null Session Access

Null sessions are a weakness that can be exploited through the various shares that are on the computer. Modify null session access to shares on the computer adding **RestrictNullSessAccess**, a Registry value that toggles null session shares on or off to determine whether the Server service restricts access to clients logged on to the system account without username and password authentication. Setting the value to 1 restricts null session access to unauthenticated users to all server pipes and shares except those listed in the **NullSessionPipes** and **NullSessionShares** entries.

Key Path: HKLM\SYSTEM\ CurrentControlSet\Services\LanmanServer	**Format**	**Value**
Key: parameters **Value Name:** RestrictNullSessAccess	REG_DWORD	1

Restrict null session access over named pipes

Restricting such access helps prevents unauthorized access over the network. To restrict null session access over named pipes and shared directories, edit the Registry and delete the values as shown in the table below.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer	**Format**	**Value**
Key: parameters **Value Names:** NullSessionPipes NullSessionShares	REG_MULTI_SZ	Delete all values

Service Pack 3 Registry entries

Service Pack 3 introduces a number of new registry entries that can be configured to enhance the security provided by the operating system.

Prevent interference of the session lock from application generated input

Service Pack 3 introduces a Registry key value that can be used to prevent application generated keyboard/mouse input messages from interfering with the session lock. The keys name is BlockSendInputResets and as with most policy settings the key resides in:

HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop (Policy) and

HKCU\Control Panel\Desktop (User)

Policy takes precedence over the User applied setting. The key will be REG_SZ to be consistent with other related keys and will be interpreted as a Boolean value with any non –zero value meaning the key is set and the feature active. A zero value or the key not existing will maintain the current functionality.

When this key is set only 'real' (mouse or keyboard) input will reset the screensavers timer. Currently there are 3 cases where 'injected' will reset the time.

- Input injected via SendInput – This is the case where an app is intentionally trying to simulate input and will be blocked.
- Window activation – When a new window becomes active the counter is reset. This will be blocked unless the screensaver is already active.
- Calls to SystemParametersInfo() that set SPI_SETSCREENSAVETIMEOUT, SPI_SETSCREENSAVEACTIVE, SPI_SETLOWPOWERTIMEOUT, SPI_SETLOWPOWERACTIVE, SPI_SETPOWEROFFTIMEOUT, SPI_SETPOWEROFFACTIVE. These will no longer result in the timer being reset if BlockSendInputResets is set. This should not have an effect on user experience, as a user setting these values will result in 'real' input from their mouse movement and keystrokes.

To enable this capability, edit the following Registry key value as shown in the table below. The key path will need to be created, under the **HKCU\Software\Policies \Microsoft** key, along with the necessary value.

Key Path: (Policy) **HKCU\Software\Policies\Microsoft\Windows\Control Panel**	**Format**	**Value**
Key: Desktop **Value Name:** BlockSendInputResets	REG_SZ	1

Note It is important to note that the appropriate screen saver settings must be set in conjunction with this key for the feature to make sense. The necessary screen saver settings are:

- A selected screen saver
- Password protection
- A screen saver timeout period

If the screensaver is not properly configured this feature will essentially have no effect on the machines overall security. Procedures for setting a password protected screen saver are available in the "Enable Automatic Screen Lock Protection" subsection.

Generate an audit event when the audit log reaches a percent full threshold

Service Pack 3 includes a feature for generating a security audit in the security event log when the security log reaches a configurable threshold. To enable this capability create the key value shown in the table below with a value setting that will designate the percent value that will cause the event to be recorded in the security log. The value shown in the table below is a recommendation and can be configured to an appropriate value based on local operational needs. For example, if set as shown below, and the security log size reaches the percent shown (90), the security log will show one event entry for eventID 523 with the following text: "The security event log is 90 percent full."

Key Path: **HKLM\SYSTEM\CurrentControlSet\Services\Eventlog**	**Format**	**Value**
Key: Security **Value Name:** WarningLevel	REG_DWORD	90

Recommended Registry Settings

The Registry settings described in this subsection are recommended in order to establish a more secure operating system configuration.

Harden the TCP/IP stack against denial of service attacks

Denial of service attacks are network attacks aimed at making a computer or a particular service on a computer unavailable to network users. The following Registry TCP/IP-related values help to increase the resistance of the Windows 2000 TCP/IP Stack in Windows 2000 against denial of service network attacks. Some of the key values listed below will need to be added the specified Registry key. Additional details can be found in Microsoft Knowledge Base Article Q315669, "HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000."

Key Path: **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip**	**Format**	**Value**
Key: Parameters **Value Name:** DisableIPSourceRouting	REG_DWORD	2
Key: Parameters **Value Name:** EnableDeadGWDetect	REG_DWORD	0
Key: Parameters **Value Name:** EnableICMPRedirect	REG_DWORD	0
Key: Parameters **Value Name:** EnablePMTUDiscovery	REG_DWORD	0
Key: Parameters **Value Name:** EnableSecurityFilters	REG_DWORD	1
Key: Parameters **Value Name:** KeepAliveTime	REG_DWORD	300,000
Key: Parameters **Value Name:** PerformRouterDiscovery	REG_DWORD	0
Key: Parameters **Value Name:** SynAttackProtect	REG_DWORD	2
Key: Parameters **Value Name:** TcpMaxConnectResponseRetransmissions	REG_DWORD	2
Key: Parameters **Value Name:** TcpMaxConnectRetransmissions	REG_DWORD	3
Key: Parameters **Value Name:** TCPMaxPortsExhausted	REG_DWORD	5

Key Path: **HKLM\SYSTEM\CurrentControlSet\Services\NetBT**	**Format**	**Value**
Key: Parameters **Value Name:** NoNameReleaseOnDemand	REG_DWORD	1

Make screensaver password protection immediate

The grace period allowed for user movement before screensaver lock is considered is set to a default of 5 seconds. An entry to the registry can be made to adjust the length of the delay. To make password protection effective immediately, it is "recommended" that the value of this entry be set to 0. To set this value, edit the Registry key as shown in the table below and create the value name ScreenSaverGracePeriod with a value of 0.

Key Path: **HKLM\Software\Microsoft\Windows NT\CurrentVersion**	**Format**	**Value**
Key: Winlogon **Value Name:** ScreenSaverGracePeriod	REG_SZ	0

Review time service authentication

Review the key shown in the table below to ensure the "type" value is set to NT5DS. This ensures the Evaluated Configuration is operating with authenticated time service.

Key Path: **HKLM\SYSTEM\CurrentControlSet\Services\W32Time**	**Format**	**Value**
Key: Parameters **Value Name:** type	REG_SZ	Nt5DS

Disable LMHash creation

Windows 2000-based servers can authenticate computers running all previous versions of Windows. However, previous versions of Windows do not use Kerberos for authentication, so Windows 2000 supports LAN Manager (LM), Windows NT (NTLM) and NTLM version 2 (NTLMv2). The LM hash is relatively weak compared to the NTLM hash and therefore prone to rapid brute force attack. For the Evaluated Configuration LM authentication is not required and can therefore be disabled to ensure greater security. Windows 2000 Service Packs 2 and higher provide a registry setting to disable the storage of the LM hashes. Additional details can be found in Microsoft Knowledge Base article Q299656 "New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager". To set this value, edit the Registry key as shown in the table below and create the key name NoLMHash.

Key Path: **HKLM\SYSTEM\CurrentControlSet\Control\Lsa**	**Format**	**Value**
Key: NoLMHash **Value Name:** A value name is not necessary	N/A	N/A

Disable autorun

Autorun begins reading from a drive as soon as media is inserted in it. As a result, the setup file of programs and the sound on audio media starts immediately. To prevent a possible malicious program from starting when media is inserted, create the following Registry value to disable autorun on all drives.

Key Path: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies		**Format**	**Value**
Key: Explorer	**Value Name:** NoDriveTypeAutoRun	REG_DWORD	255

Review Service Pack 3 Registry entries

Service Pack 3 introduces a number of new registry entries that can be configured to enhance the security provided by the operating system.

LDAP BIND command request settings

This value is used to determine the LDAP server (ldapagnt.lib) handling of LDAP bind command requests as follows.

1. (default) or not defined: The AD's LDAP agent always supports LDAP client request for LDAP traffic signing when handling a LDAP bind command request which specifies a SASL authentication mechanism.
2. The AD's LDAP agent only supports SASL in a LDAP bind command request unless the incoming request is already protected with TLS/SSL. It rejects the LDAP bind command request if other types of authentication are used. If the LDAP bind command request does not come in via TLS/SSL, it requires the LDAP traffic signing option in the client security context.

To set this value, edit the Registry key as shown in the table below and create the value name LdapServerIntegrity with a value of 2.

Key Path: HKLM\System\CurrentControlSet\Services\NTDS		**Format**	**Value**
Key: Parameters	**Value Name:** LdapServerIntegrity	REG_DWORD	2

Generate administrative alert when the audit log is full

To add Alerter service recipients for Windows 2000 based computers, edit the Registry (using Regedt32.exe) as shown in the table below. The Value entry will be the name of each recipient (user name or computer name) that is to receive the administrative alerts. Each recipient should be on a separate line in the **Data** dialog box.

Key Path: HKLM\SYSTEM\CurrentControlSet\Services\Alerter		**Format**	**Value**
Key: Parameters	**Value Name:** AlertNames	REG_MULTI_SZ	As explained above

> **Note** Administrative alerts rely on both the Alerter and Messenger services. Make sure that the Alerter service is running on the source computer and that the Messenger service is running on the recipient computer.

Audit Log Management

Management options for event logs, including the security log, can be configured for all computers in a domain by using the Even Log folder within the Domain Security Policy or a specific Group Policy object associated with domains, OUs, and sites (Domains). The Event Log folder does not appear in the Local Security Policy object.

For domain members, the management options for local audit can be configured using the Event Viewer Snap-In. From the Event Viewer, the applicable Properties interface is selected to set the management options for a particular log, such as the Security log.

These interfaces allow for viewing, sorting, filtering, and searching the event logs as well as setting the maximum log size or clearing the log. The user must have access to the event log file in order to successfully view it. To view the contents of the security log, the user must be logged on as a member of the Administrator's group. No special privilege is required to use the Event Viewer itself. Security is enforced by the ACL on the log and certain registry settings.

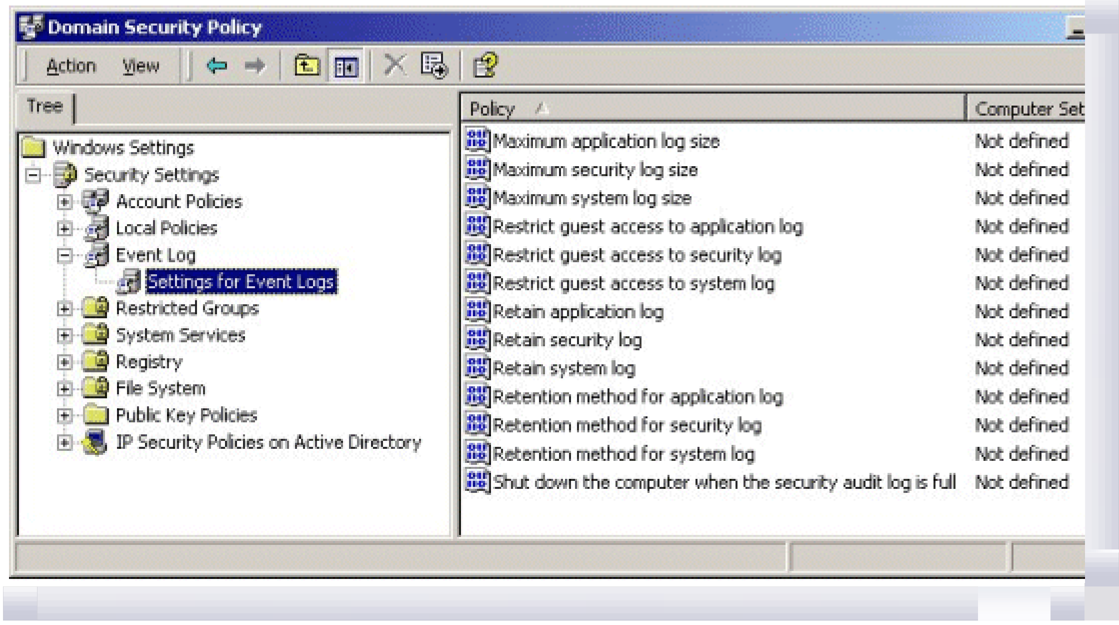
Access the Settings for Event Logs

View current settings for event logs and allow editing.

Procedure for Domain and Domain Controller Policies:

1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand Security Settings.
3. Within Security Settings, expand Event Log to reveal the Settings for Event Logs policy.

4. Click on the **Settings for Event Logs** object. The right-hand details pane will reveal the configurable audit log management settings.

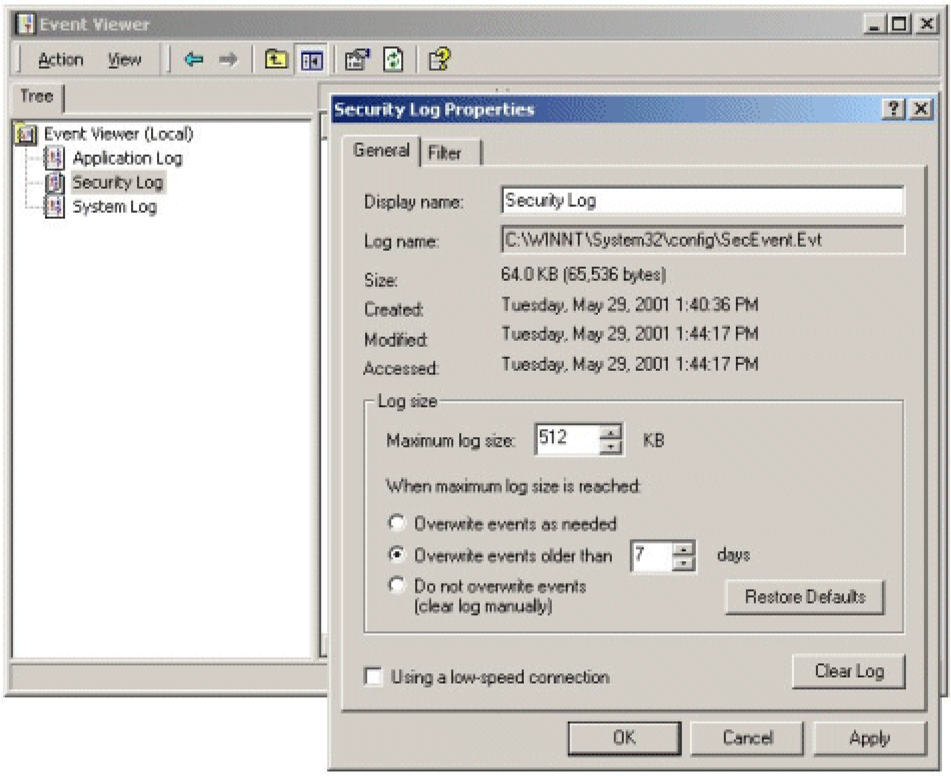


Policy	Computer Set
Maximum application log size	Not defined
Maximum security log size	Not defined
Maximum system log size	Not defined
Restrict guest access to application log	Not defined
Restrict guest access to security log	Not defined
Restrict guest access to system log	Not defined
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	Not defined
Retention method for security log	Not defined
Retention method for system log	Not defined
Shut down the computer when the security audit log is full	Not defined

If your browser does not support inline frames, click here to view on a separate page.

Procedure for Standalone Workstations and Servers:

1. Open the Event Viewer, Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer**.
2. Right-click on the **Security Log** object and select **Properties**. The **Security Log Properties** window will appear revealing the configurable audit log management settings.



Display name: Security Log

Log name: C:\WINNT\System32\config\SecEvent.Evt

Size: 64.0 KB (65,536 bytes)

Created: Tuesday, May 29, 2001 1:40:36 PM

Modified: Tuesday, May 29, 2001 1:44:17 PM

Accessed: Tuesday, May 29, 2001 1:44:17 PM

Log size

Maximum log size: 512 KB

When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

If your browser does not support inline frames, click here to view on a separate page.

Set the Audit Policies as required or recommended in Table 3.8.

Table 3.8 Audit Management Settings

Audit Management and Configuration	Professional	Server	DC	Required	Recommended

Set Maximum Application Log Size **Security Objective:** Specifies the maximum size for the Application event log. The default is 512KB, and the maximum size is 4GB (4,194,240KB). Requirements for the Application log size vary depending the function of the platform and the need for historical records of application related events. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Maximum application log size** in the right-hand details pane. b. Check the Define this policy setting box. c. Enter the desired value for the application log size in the text box. For most environments, the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. d. Click the **OK** button.			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: a. In the **Application Log Properties** window, under the **General** tab, enter the desired value for the application log size in the **Maximum log size:** text box. For most environments the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. b. Click the **OK** button.	✓	✓			✓
Set Maximum Security Log Size **Security Objective:** Specifies the maximum size for the Security event log. The default is 512KB, and the maximum size is 4GB. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Maximum security log size** in the right-hand details pane. b. Check the Define this policy setting box. c. Enter the desired value for the security log size in the text box. The log retention method for the security log should be set to not overwrite events, therefore a larger log size should be			✓		✓

set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. d. Click the **OK** button.					
Procedure for Standalone Windows 2000 Professional and Server: a. In the **Security Log Properties** window, under the **General tab**, enter the desired value for the application log size in the **Maximum log size**: text box. The log retention method for the security log should be set to not overwrite events, therefore a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. b. Click the **OK** button.	✓	✓			✓
Set Maximum System Log Size **Security Objective:** Specifies the maximum size for the System event log. The default is 512KB, and the maximum size is 4GB. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Maximum system log size** in the right-hand details pane. b. Check the Define this policy setting box. c. Enter the desired value for the system log size in the text box. For most environments the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared, including the amount of disk space that is available. d. Click the **OK** button.			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: a. In the **System Log Properties** window, under the **General** tab, enter the desired value for the system log size in the **Maximum** log size: text box. For most environments the default setting is adequate. However, if the log retention method is set to not overwrite events, a larger log size should be set based on the amount of expected activity and the frequency with which the logs will be manually reviewed, archived, and cleared. b. Click the **OK** button.	✓	✓			✓
Restrict Guest Access to the Application Log			✓		✓

Security Objective: Prevent anonymous access to the Application event log. If this policy is enabled, guests are prevented from access to the Application event log. By default, this policy is disabled locally on all Windows 2000 operating systems. **Procedure for Domain and Domain Controller Policies**: a. Double click on **Restrict guest access** to application log in the right-hand details pane. b. Check the **Define these policy** settings box. c. Select the Enabled radio button and click the **OK** button. **Procedure for Standalone Workstations and Servers:** Not available on standalone workstations and servers.					
Restrict Guest Access to the Security Log **Security Objective:** Prevent anonymous access to the Security event log. If this policy is enabled, guests are prevented from access to the Security event log. By default, this policy is disabled locally on all Windows 2000 operating systems. A user must possess the **Manage auditing and security log** user right in order to access the security log. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Restrict guest access to security log** in the right-hand details pane. b. Check the Define these policy settings box. c. Select the **Enabled** radio button and click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** Not available on standalone workstations and servers.			✓		✓
Restrict Guest Access to the System Log **Security Objective:** Prevent anonymous access to the System event log. If this policy is enabled, guests are prevented from access to the System event log. By default, this policy is disabled locally on all Windows 2000 operating systems. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Restrict guest access to system log** in the right-hand details pane. b. Check the Define these policy settings box. c. Select the **Enabled** radio button and click the **OK** button. **Procedure for Standalone Windows 2000 Professional and Server:** Not			✓		✓

available on standalone workstations and servers.					
Retain Application Log **Security Objective:** Determines the number of days' worth of events that should be retained for the Application log if the retention method for the application log is set to **Overwrite events by days** in a Domain policy, or if the **Overwrite events older than** option is selected in the **Application Log Properties** window of a standalone workstation or server. Set this value **only if** the log is archived at scheduled intervals and make sure that the maximum Application log size is large enough to accommodate the interval. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of "**Not defined**."			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: Do not change the default number of days (7) set in the **Overwrite events older than** option of the **Application Log Properties** window.	✓	✓			✓
Retain Security Log **Security Objective:** Determines the number of days' worth of events that should be retained for the Security log if the retention method for the application log is set to **Overwrite events by days** in a Domain policy, or if the **Overwrite events older than** option is selected in the **Security Log Properties** window of a standalone workstation or server. Set this value **only if** the log is archived at scheduled intervals and make sure that the maximum Security log size is large enough to accommodate the interval. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of "**Not defined**."			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: Do not change the default number of days (7) set in the **Overwrite events older than** option of the **Security Log Properties** window.	✓	✓			✓
Retain System Log **Security Objective:** Determines the number of days' worth of events that should be retained for the System log if the retention method for the application log is set to **Overwrite events by days** in a Domain policy, or if the **Overwrite events older than** option is selected in the **System Log Properties** window of a standalone workstation or server. Set this value **only if** the log is archived at scheduled intervals and make sure that the maximum System log size is large enough to accommodate the interval. **Procedure for Domain and Domain Controller Policies:** Do not change the			✓		✓

default setting of “**Not defined**.”					
Procedure for Standalone Windows 2000 Professional and Server: Do not change the default number of days (7) set in the **Overwrite events older than** option of the **System Log Properties** window.	✓	✓			✓
Retention Method for Application Log **Security Objective:** Determines how Application logs that have reached their maximum size will be handled by the operating system. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of **“Not defined.”**			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: Do not change the **Overwrite events older than** (7 days) option of the **System Log Properties** window.	✓	✓			✓
Retention Method for Security Log **Security Objective:** Determines how Security logs that have reached their maximum size will be handled by the operating system. **Procedure for Domain and Domain Controller Policies:** a. Double click on **Retention method for Security log** in the right-hand details pane. b. Check the Define these policy settings box. c. Select the **Do not overwrite events (clear log manually)** radio button and click the **OK** button.			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: a. In the Security Log Properties window, under the General tab, select the Do not overwrite events (clear log manually) radio button. b. Click the OK button.	✓	✓			✓
Retention Method for System Log **Security Objective:** Determines how System logs that have reached their maximum size will be handled by the operating system. **Procedure for Domain and Domain Controller Policies:** Do not change the default setting of “**Not defined**.”			✓		✓
Procedure for Standalone Windows 2000 Professional and Server: Do not change the **Overwrite events older than** (7 days) option of the **System Log Properties** window.	✓	✓			✓
Shut Down the Computer when the Security Log is Full **Security Objective:** Determines whether the system should shut down if it is unable to log security events. If this policy is	✓	✓	✓		✓

enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method specified for the security log is either **Do Not Overwrite Events** or **Overwrite Events by Days.** **Procedure**: Use the Shut down system immediately if unable to log security audits security option instead of this policy setting. This policy setting is not available in standalone workstations and servers. **Note** The ST requires the system to be able to prevent auditable events from occurring, except those taken by the administrator, if the audit log is full. If the administrator desires this functionality, this option must be enabled.					

Default Group Accounts

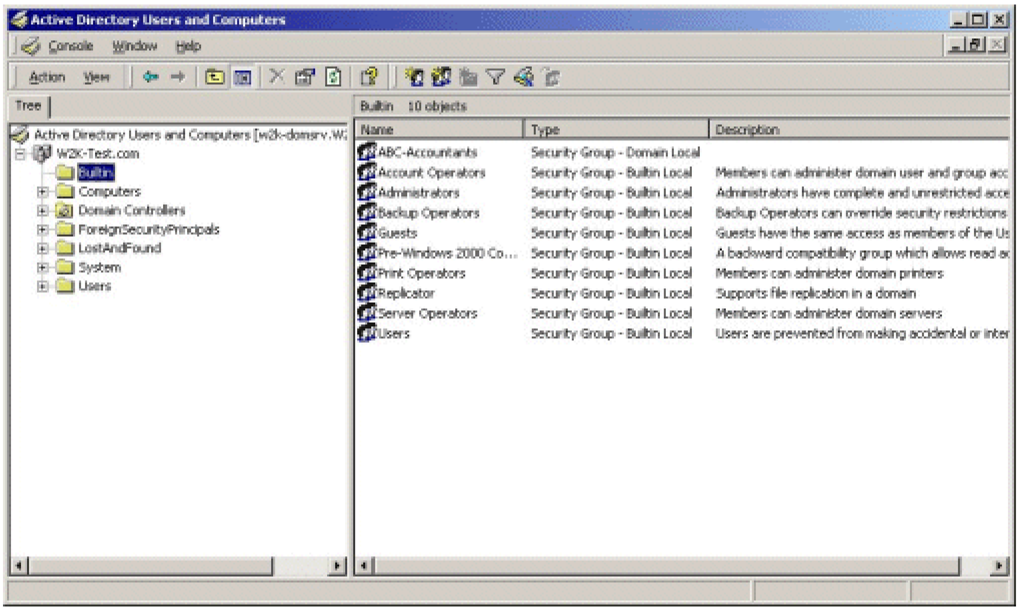
This subsection discusses required and recommended changes to default group memberships for the built-in groups found in default Windows 2000 operating system installations. These built-in groups have a predefined set of user rights and privileges as well as group members. The four built-in groups are defined as follows:

- **Global Groups.** When a Windows 2000 domain is established, built-in global groups are created in the Active Directory store. Global groups are used to group common types of user and group accounts for use throughout the entire domain.
- **Domain Local Groups.** Domain local groups provide users with privileges and permissions to perform tasks specifically on the domain controller and in the Active Directory store.
- **Local Groups.** Stand-alone Windows 2000 Servers, member servers, and Professional workstations have built-in local groups. These built-in local groups provide members with the capability to perform tasks only on the specific computer to which the group belongs.
- **System Groups.** System groups do not have specific memberships that can be modified. Each is used to represent a specific class of users or to represent the operating system itself. These groups are created within Windows 2000 operating systems automatically, but are not shown in the group administration GUIs.

> **Note** Appendix D – User and Group Accounts, provides a complete description of the default group account settings to be maintained in the evaluated configuration, including additional details, applicable ST requirements, and recommended changes.

Review / Modify Group Account Memberships for a Domain

1. To access group accounts within a Domain, log in with an administrative account on the Domain Controller.
2. Open Start, point to Administrative Tools, and then click Active Directory Users and Computers.
3. In the console tree, double-click the domain node.
4. Group accounts are found in the **Builtin** and **Users** containers.



Active Directory Users and Computers [w2k-domsrv.W2
- W2K-Test.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - System
  - Users

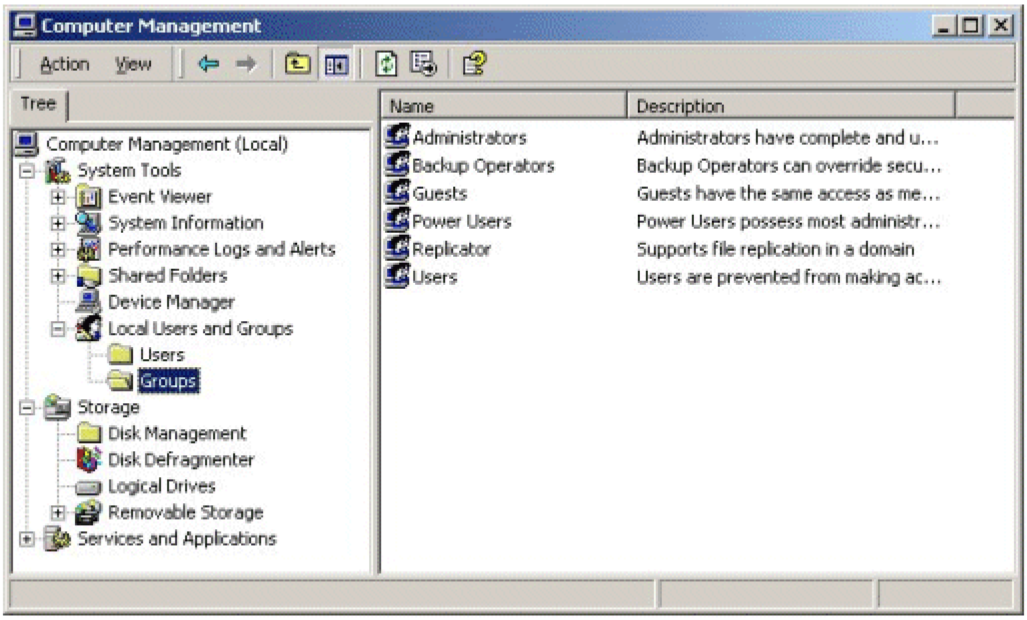
Builtin 10 objects

Name	Type	Description
ABC-Accountants	Security Group - Domain Local	
Account Operators	Security Group - Builtin Local	Members can administer domain user and group acc
Administrators	Security Group - Builtin Local	Administrators have complete and unrestricted acce
Backup Operators	Security Group - Builtin Local	Backup Operators can override security restrictions
Guests	Security Group - Builtin Local	Guests have the same access as members of the Us
Pre-Windows 2000 Co...	Security Group - Builtin Local	A backward compatibility group which allows read ac
Print Operators	Security Group - Builtin Local	Members can administer domain printers
Replicator	Security Group - Builtin Local	Supports file replication in a domain
Server Operators	Security Group - Builtin Local	Members can administer domain servers
Users	Security Group - Builtin Local	Users are prevented from making accidental or inter

If your browser does not support inline frames, click here to view on a separate page.

Review / Modify Group Account Memberships for a Standalone

1. To access group accounts within a Standalone or individual Domain Member computer, log in with an administrative account.
2. Open Start, point to Administrative Tools, and then click Computer Management.
3. In the console tree, double-click on **Local Users and Groups**.
4. Group accounts are found in the **Groups** container.



Computer Management (Local)
- System Tools
  - Event Viewer
  - System Information
  - Performance Logs and Alerts
  - Shared Folders
  - Device Manager
  - Local Users and Groups
    - Users
    - Groups
- Storage
  - Disk Management
  - Disk Defragmenter
  - Logical Drives
  - Removable Storage
- Services and Applications

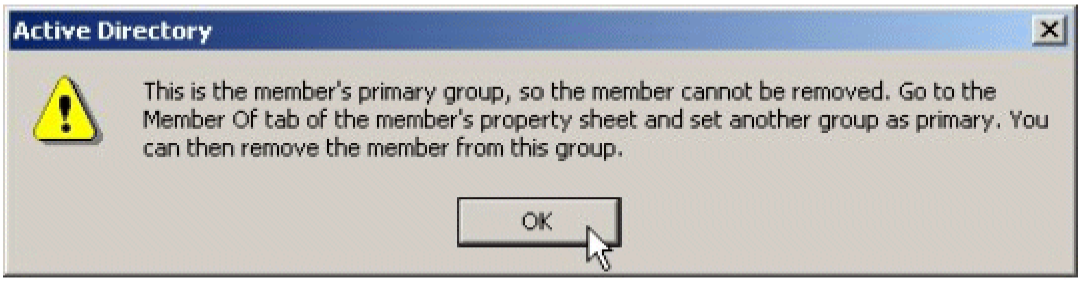
Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Guests	Guests have the same access as me...
Power Users	Power Users possess most administr...
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac...

If your browser does not support inline frames, click here to view on a separate page.

Note Set Group Memberships as required or recommended in Table 3.9.

Change the Primary Group Membership of an Account

Some of the required group membership changes identified in the table below call for removing an account from a specific group. Within a domain, accounts must have a primary group assignment. It may therefore be necessary to first change the account's primary group membership that is set by default when a computer is joined to a domain. If an attempt is made to remove an account from its primary group, the action will be denied and the following message will appear:

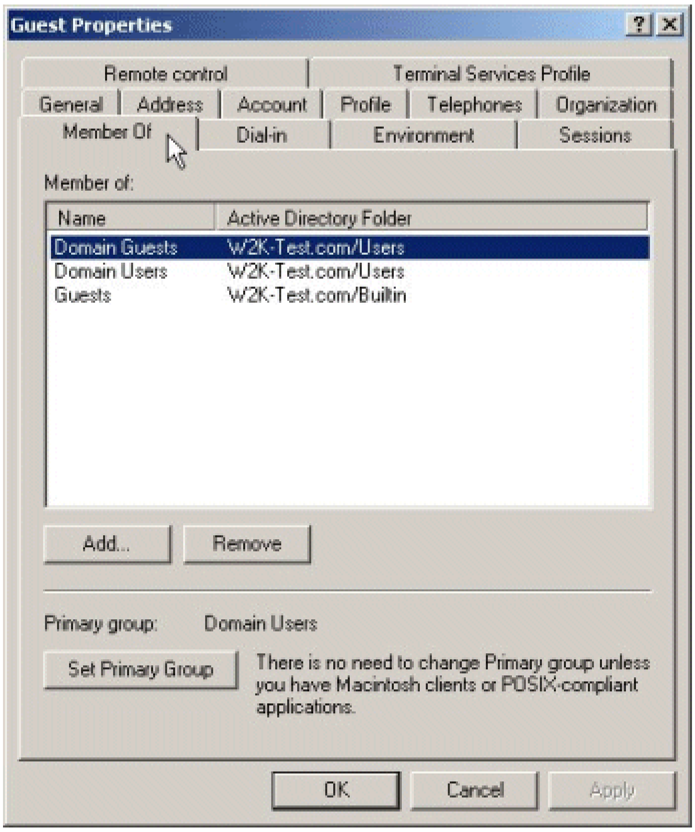


This is the member's primary group, so the member cannot be removed. Go to the Member Of tab of the member's property sheet and set another group as primary. You can then remove the member from this group.

If your browser does not support inline frames, click here to view on a separate page.

Use the following procedures to change an account's primary group:

1. Log in with an administrative account on the Domain Controller.
2. Open Start, point to Administrative Tools, and then click Active Directory Users and Computers.
3. In the console tree, double-click the domain node.
4. User accounts are found in the **Users** container.
5. Right-click on the account name and select **Properties** from the menu. The account **Properties** GUI will appear.
6. Click on the **Member Of** tab to display the list of groups the account belongs to. Observe that when clicking any of the groups in the **Member of:** window, the **Set Primary Group** button will be either active or inactive. The **Set Primary Group** button will be active for groups which can be set as primary groups and will be inactive for groups either cannot be set as primary groups or which are already the primary group.



Member of:

Name	Active Directory Folder
Domain Guests	W2K-Test.com/Users
Domain Users	W2K-Test.com/Users
Guests	W2K-Test.com/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

7. To change the primary group of the account, select the group that will become the new primary group and click on the **Set Primary Group** (must have the **Set Primary Group** button active). Note that the group identified above the **Set Primary Group** button as the **Primary group:** will change to the new selection.
8. Click the **Apply** and click **OK**.

Note The account can also be removed from a group through **Member of** tab interface of the **Properties** GUI by selection the group from which it is to be removed and clicking the **Remove** button.

Table 3.9 up Memberships

Group Account Modifications			**Professional**	**Server**	**DC**	**Required**	**Re**
Global Groups	Default Members	Modification / Verification					
DnsUpdateProxy	None	Do not add accounts to this group.			✓	✓	
Domain Admins	Administrator	Do not add non-administrative accounts to this group.			✓	✓	
Domain Guests	Guest	Do not add accounts to this group.			✓	✓	
Domain Users	Administrator Guest Krbtgt TsInternetUser (All new users are added by default)	Remove the Guest account and ensure the TsInternetUser account is disabled. **Note** Before removing the Guest account, change the primary group for that account to Domain Guests.			✓	✓	
Enterprise Admins	Administrator (Domain Controller Administrator)	Do not add non-administrative accounts to this group.			✓	✓	
Group Policy Creator Owner	Administrator	Do not add non-administrative accounts to this group.			✓	✓	
Schema Admins	Administrator	Do not add non-administrative accounts to this group.			✓	✓	
Domain Local Groups	**Default Members**	**Modification / Verification**					
Account Operators	None	Do not add non-administrative accounts to this group.			✓	✓	
Administrators	Administrator Domain Admins Enterprise Admins	Do not add non-administrative accounts to this group.			✓	✓	
Backup Operators	None	Do not add non-administrative accounts to this group.			✓	✓	
DnsAdmins	None	Do not add non-administrative accounts to this group.			✓	✓	
Guests	Guest (Local) Domain Guests	Do not use this group. Remove all accounts, including			✓	✓	

	TsInternetUser	Guest, from this group.					
Pre-Windows 2000 Compatible Access	None	Provides backward compatibility with pre-Windows 2000 operating systems. Does not meet objectives of the TOE, therefore do not use this group.			✓	✓	
Print Operators	None	Do not add non-administrative accounts to this group.			✓	✓	
Replicator	None	Do not add non-administrative accounts to this group.			✓	✓	
Server Operators	None	Do not add non-administrative accounts to this group.			✓	✓	
Users	Authenticated Users Domain Users INTERACTIVE (All new local users are added by default)	Do not add accounts with a potential for unauthenticated access (such as Guest) to this group.			✓	✓	
Local Groups	**Default Members**	**Modification / Verification**					
Administrators	Stand-Alone: Administrator Domain Member: Administrator Domain Admins	Do not add non-administrative accounts to this group.	✓	✓		✓	
Backup Operators	None	Do not add non-administrative accounts to this group.	✓	✓		✓	
Guests	Stand-Alone Professional: Guest Stand-Alone Server: Guest TsInternetUser Domain Member: Add Domain Guests to the above	Do not use this group. Remove all accounts, including Guest, from this group.	✓	✓		✓	
Power Users	None	Do not add non-administrative accounts to this group.	✓	✓		✓	

Replicator	None	Do not add non-administrative accounts to this group.	✓	✓		✓	
Users	Stand-Alone: Authenticated Users INTERACTIVE (All new local users are added by default) Domain Member: Authenticated Users Domain Users INTERACTIVE (All new local users are added by default)	Do not add accounts with a potential for unauthenticated access (such as Guest) to this group.	✓	✓		✓	
System Groups	**Default Members**	**Modification / Verification**					
Anonymous Logon	All unauthenticated users	Do not use this group. Do not grant resource permissions or user rights to this group.	✓	✓	✓	✓	
Authenticated Users	All authenticated users	Use the Authenticated Users group instead of the Everyone to prevent the potential for anonymous access to a resource.	✓	✓	✓	✓	
DIALUP	All dial-in users	Dial-up service support is not an objective of the TOE. Therefore, do not grant resource permissions or user rights to this account.	✓	✓	✓	✓	
Everyone	All users accessing the computer, either locally, through the network, or through RAS. This includes all authenticated and unauthenticated users.	Do not assign resource permissions or user rights to this account. Use Authenticated Users or specific user accounts and groups where necessary.	✓	✓	✓	✓	
TERMINAL SERVER USER	None	Terminal Service support is not an objective of the TOE. Therefore, do not grant resource	✓	✓	✓	✓	

		permissions or user rights to this account.					

Default User Accounts

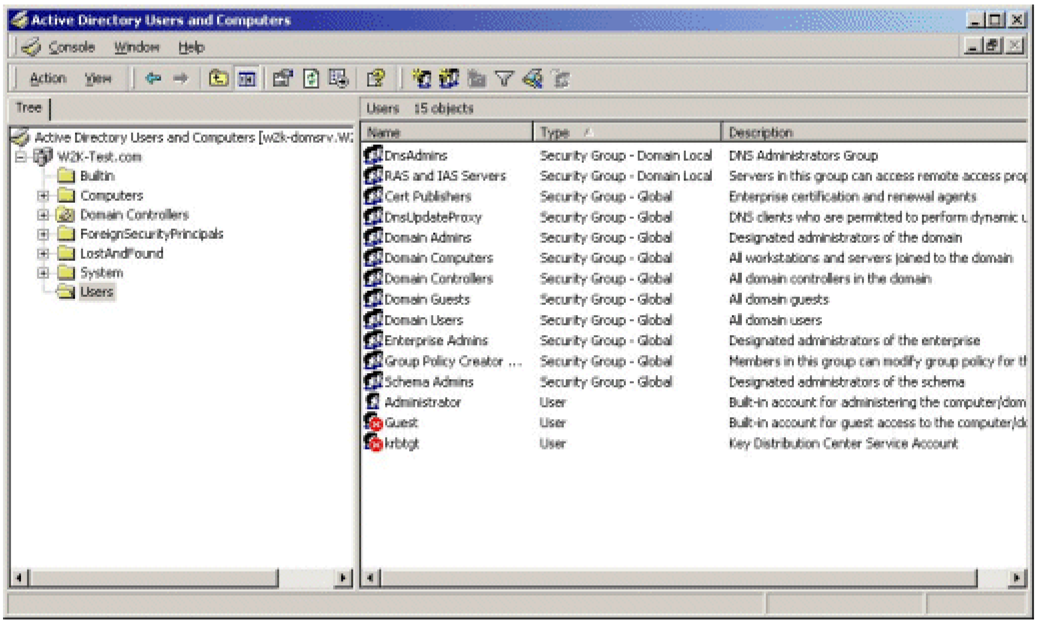
This subsection discusses required and recommended changes to built-in user accounts found in default Windows 2000 operating system installations. The built-in user accounts include Administrator, Guest, and TsInternetUser.

> **Note** Appendix D – User and Group Accounts, provides a complete description of the default group account settings to be maintained in the evaluated configuration, including additional details, applicable ST requirements, and recommended changes.

Review / Modify Default User Accounts for a Domain

Review or modify user accounts to ensure compliance with ST requirements.

1. To access user accounts within a Domain, log in with an administrative account on the Domain Controller.
2. Open Start, point to Administrative Tools, and then select Active Directory Users and Computers.
3. In the console tree, expand the domain node.
4. User accounts are found in the **Users** container.


Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Active Directory Users and Computers [w2k-domsrv.W:
W2K-Test.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
System
Users

Users 15 objects

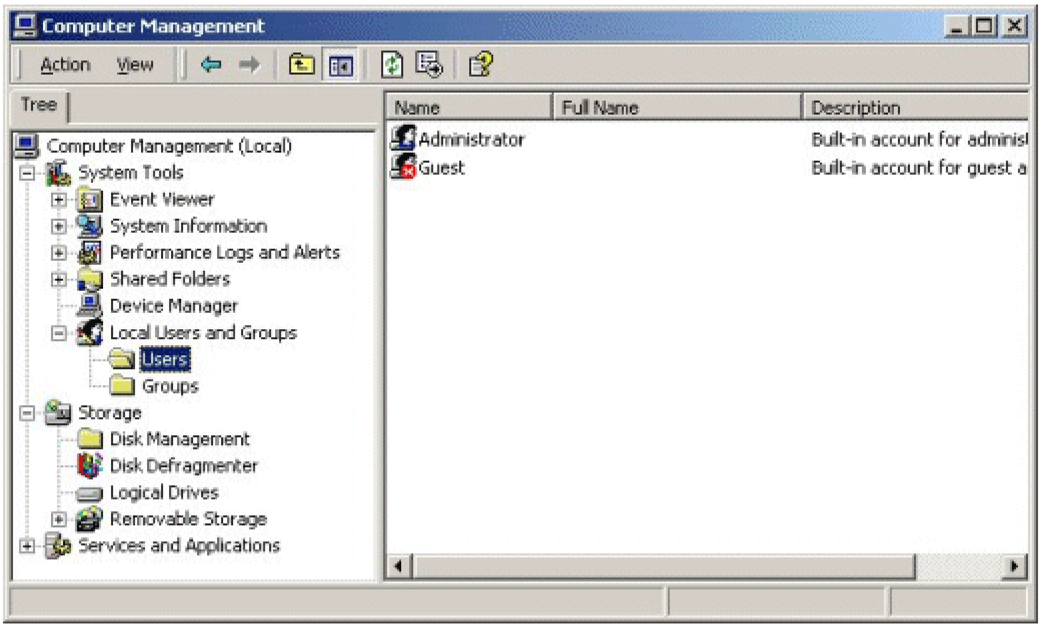
Name	Type	Description
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access prop
Cert Publishers	Security Group - Global	Enterprise certification and renewal agents
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic u
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Global	Designated administrators of the enterprise
Group Policy Creator ...	Security Group - Global	Members in this group can modify group policy for th
Schema Admins	Security Group - Global	Designated administrators of the schema
Administrator	User	Built-in account for administering the computer/dom
Guest	User	Built-in account for guest access to the computer/do
krbtgt	User	Key Distribution Center Service Account

If your browser does not support inline frames, click here to view on a separate page.

Review / Modify Default User Accounts Locally

Review or modify user accounts within a Standalone or individual Domain Member computer to ensure compliance with ST requirements.

1. Open Start, point to Administrative Tools, and then select Computer Management.
2. In the console tree, expand **Local Users and Groups**.
3. User accounts are found in the **Users** container.



Name	Full Name	Description
Administrator		Built-in account for adminis
Guest		Built-in account for guest a

If your browser does not support inline frames, click here to view on a separate page.

Modify User Accounts as required or recommended in Table 3.10.

Table 3.10 Default User Accounts

User Account Modifications			**Professional**	**Server**	**DC**	**Required**	**Recom**
Local User Accounts	Description	Modification / Verification					
Administrator	Built-in account for administering the computer/Domain.	Do not use this account for day-to-day administration. Assign roles to authorized administrators by placing their user accounts in administrative groups appropriate to their level of responsibility. Rename the Administrator account and secure the password for emergency use only.	✓	✓	✓	✓	
Guest	Built-in account for guest access to the computer/Domain.	This account must remain disabled.	✓	✓	✓	✓	
TsInternetUser	User account used by Terminal Services. It is used by the Terminal Services Internet Connector License and is available on Windows 2000	Terminal Services is not an objective of the Evaluated Configuration and accounts that support anonymous access are not		✓	✓	✓	

	Servers. When Internet Connector Licensing is enabled, a Windows 2000-based server accepts 200 anonymous-only connections. Terminal Services clients are not prompted with a logon dialog box; they are logged on automatically with the TsInternetUser account.	to be allowed. Therefore, disable this account.					

System Services

Table 3.11 lists the system services that may be enabled in an Evaluated Configuration. To remain in the Evaluated Configuration, it is acceptable to have all of the listed services, or a subset of them, enabled and running.

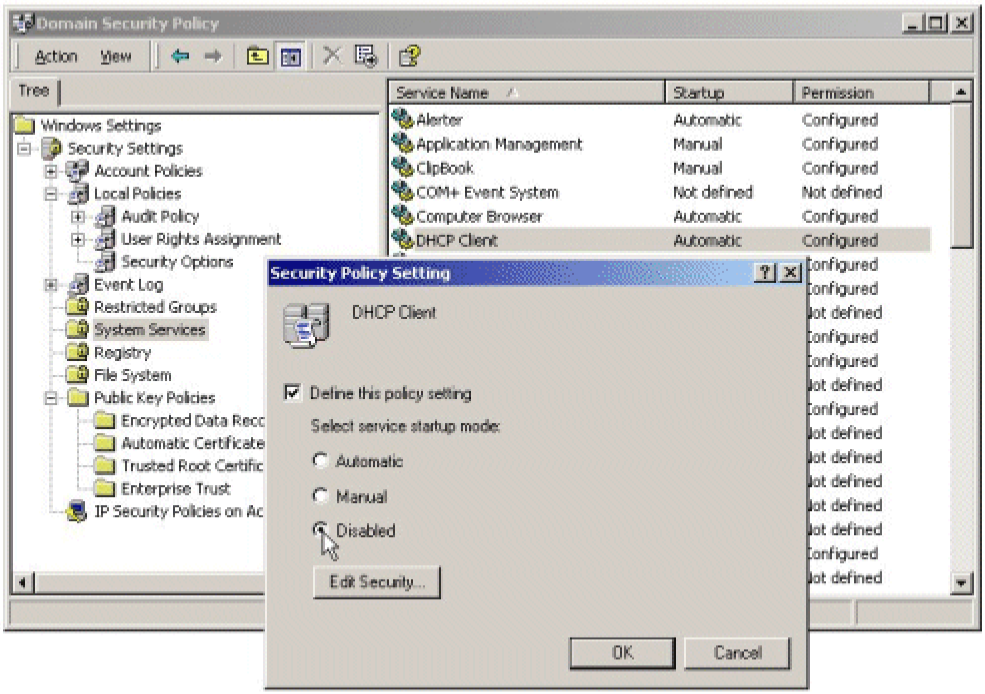
To enable or disable services on all or a group of Windows 2000 platforms in a domain set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local settings on individual Windows 2000 platforms can be set through the Computer Management interface.

> **Note** Enabling or installing new services not identified as enabled in the table below is outside the scope of Common Criteria Evaluated Configuration. The Common Criteria Evaluated Configuration includes no auditing capability for administrators installing, enabling, or disabling services. Hence, management of services can only be accomplished outside the Evaluated Configuration, though the Evaluated Configuration can be reestablished subsequently.

Disable Unnecessary System Services on Domain Computers

Set a policy to disable unnecessary services within a Domain. Set a policy to disable unnecessary services for Domain Controllers.

1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand Security Settings and click on System Services.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Security**.
4. In the **Security Policy Setting** dialog window, check the **Define this policy setting** box and then select the **Disabled** radio button.



Service Name	Startup	Permission
Alerter	Automatic	Configured
Application Management	Manual	Configured
ClipBook	Manual	Configured
COM+ Event System	Not defined	Not defined
Computer Browser	Automatic	Configured
DHCP Client	Automatic	Configured

Security Policy Setting

DHCP Client

☑ Define this policy setting

Select service startup mode:

○ Automatic

○ Manual

● Disabled

Edit Security... OK Cancel

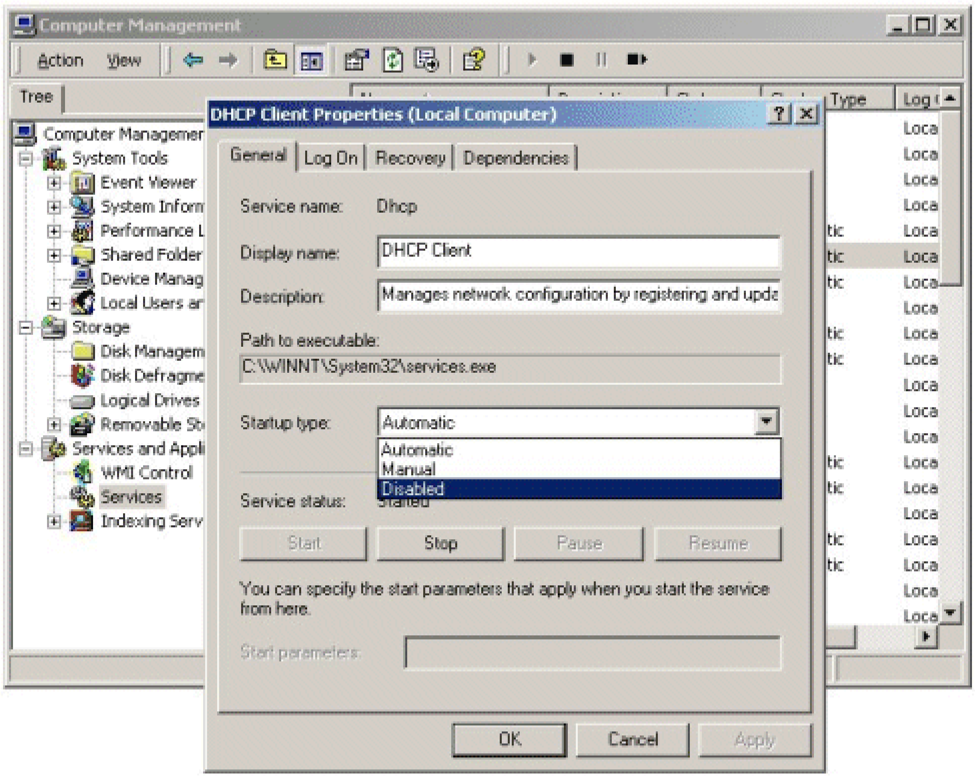
If your browser does not support inline frames, click here to view on a separate page.

5. Click the **OK** button.

Disable Unnecessary System Services Locally

Disable unnecessary services locally on Windows 2000 Server or Professional operating systems.

1. Open the **Computer Management** interface.
2. In the console tree, expand **Services and Applications** and select **Services**.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Properties**.
4. The **Properties** dialog box for the selected services will appear. From the **Startup type:** drop down menu, select **Disabled**.



DHCP Client Properties (Local Computer)

Service name: Dhcp

Display name: DHCP Client

Description: Manages network configuration by registering and upda

Path to executable:
C:\WINNT\System32\services.exe

Startup type: Automatic
Automatic
Manual
Disabled

Service status: Started

Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

If your browser does not support inline frames, click here to view on a separate page.

5. Under **Service status:** click on the **Stop** button.
6. Click the **OK** button.

Evaluated Configuration System Services

Table 3.11 lists the system services that may be enabled in an Evaluated Configuration. To remain in the Evaluated Configuration, it is acceptable to have all of the listed services, or a subset of them, enabled and running, all other services must be disabled.

Table 3.11 Acceptable Services for the Evaluated Configuration

List of Evaluated Services	
Alerter Service	Network Connections
COM+ Event System	NTLM Security Support Provider
Computer Browser	Plug and Play
DHCP Client	Print Spooler
DHCP Server	Protected Storage
Distributed File System (DFS)	Remote Procedure Call (RPC)
DNS Client	Remote Procedure Call (RPC) Locator
DNS Server	Remote Registry Service
Event Log	Security Accounts Manager
File Replication Service	Server
Intersite Messaging	System Event Notification
IPSec Policy Agent	TCP/IP NetBIOS Helper Service
Kerberos Key Distribution Center	Windows Internet Name Service (WINS)
Logical Disk Manager	Windows Management Instrumentation
Logical Disk Manager Administrative Service	Windows Management Instrumentation Driver Extensions
Messenger	Windows Time
Net Logon	Workstation

Securing the File System

Among the files and directories to be protected are those that make up the Windows 2000 operating system itself. The default set of file and directory permissions provides a minimal level of security that allows ease of software installation and customization of the operating environment without impacting usability. Default file and directory permissions that are applied during operating system installation are captured into the “setup security.inf” security template file, which is described as containing the “out of box default security settings.”

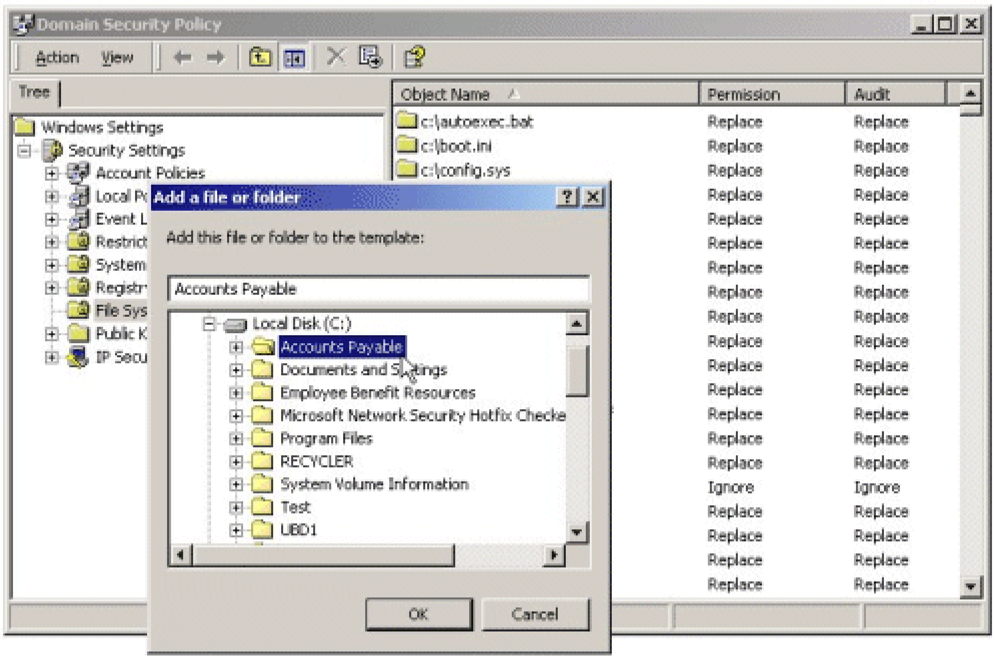
To ensure greater security, consider modifying file, directory, and subdirectory permissions as recommended in the table presented in this subsection, immediately after installing the operating system. Be sure to apply permissions to parent directories before applying them to subdirectories. The permission changes recommended below apply to all Windows 2000 operating systems. To implement permissions on all or a group of Windows 2000 platforms in a domain set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local permissions on individual Windows 2000 platforms can be set through the Windows Explorer interface.

Detailed instructions for setting individual permissions using the Windows Explorer interface are provided in the Data Protection subsection of the Windows 2000 Evaluated Configuration Administrator’s Guide.

Set Permissions through a Domain Policy

Set a file and folder permissions policy for the Domain. Set a file and folder permissions policy for Domain Controllers.

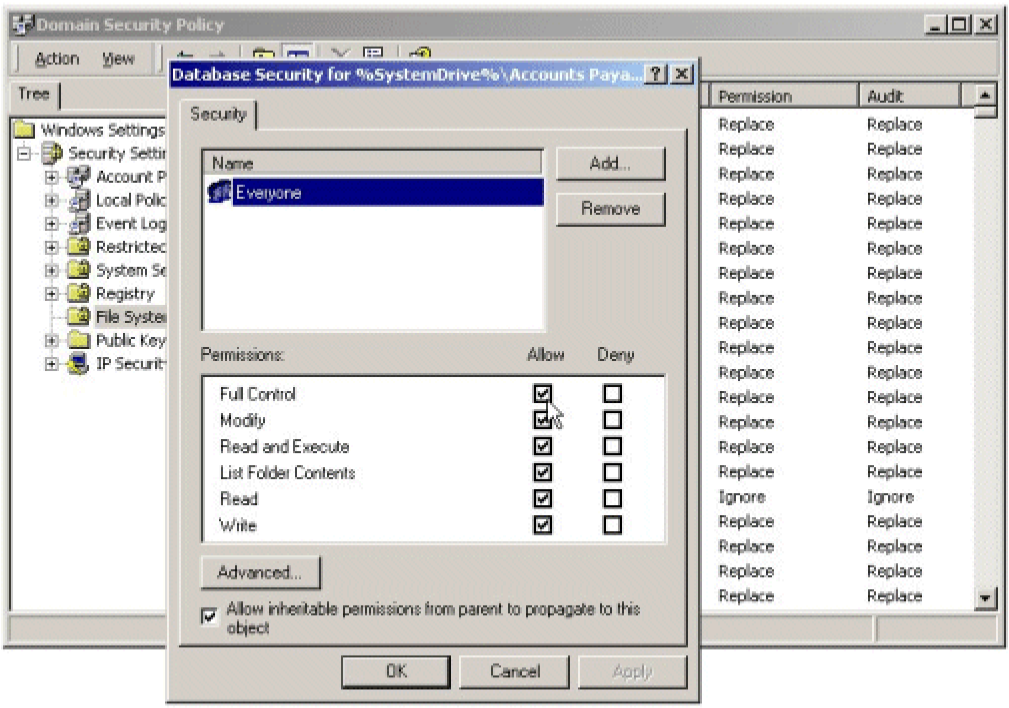
1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand Security Settings.
3. Within Security Settings, right-click on File System.
4. Select **Add File**.
5. From the **Add a file or folder window**, navigate to and select the desired file or folder.



Add this file or folder to the template: Accounts Payable

If your browser does not support inline frames, click here to view on a separate page.

6. Click the OK button. A Database Security for *path\filename* Properties window will appear.



Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read and Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

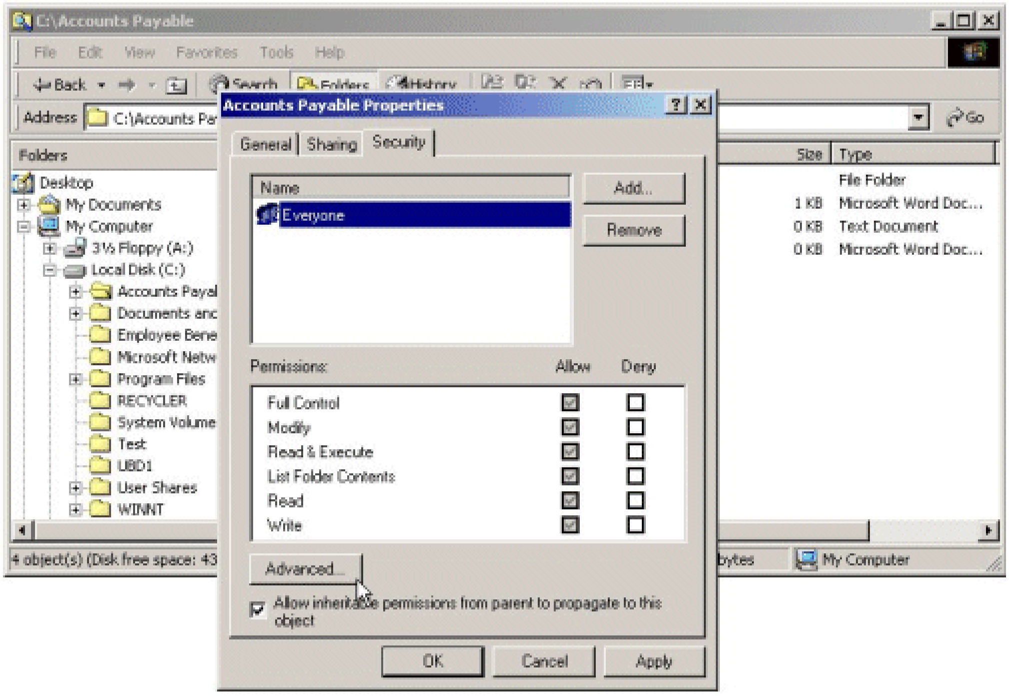
If your browser does not support inline frames, click here to view on a separate page.

7. Set permissions as necessary. Detailed procedures are provided in the Windows 2000 Evaluated Configuration Administrator's Guide. File and Folder permission settings are provided in Table 3.12.

Set Permissions Locally through Windows Explorer

Set file and folder permissions locally on Windows 2000 Server or Professional operating systems.

1. Open Windows Explorer.
2. Navigate to and select the desired file or folder.
3. Right-click on the file or folder and select **Properties**.
4. In the properties window, select the **Security** tab. Click **Advanced** for more detailed permission settings.



Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object

If your browser does not support inline frames, click here to view on a separate page.

5. Set permissions as necessary. Detailed procedures are provided in the Windows 2000 Evaluated Configuration Administrator’s Guide. File and Folder permission settings are provided in Table 3.12.

Note Through the Advanced tab, permissions are propagated by applying them to the current folder, subfolder, and files. Permissions are replaced locally by applying them only to the current folder and files, or the current file object.

Table 3.12 File and Folder Permission Settings

Files and Folders	ACL Settings	Inheritance Method (Used via Security Policy tools)	Required	Recommended
C:\autoexec.bat	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace	✓	
C:\boot.ini	**Administrators:** Full Control **SYSTEM:** Full Control	Replace	✓	
C:\config.sys	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace	✓	
C:\ntbootdd.sys **Note** used when SCSI is available.	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
C:\ntdetect.com	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
C:\ntldr	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓

%ProgramFiles%	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDirectory%	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDirectory%\appmgmt	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\config	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\dllcache	**Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\DTCLog	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\GroupPolicy	**Administrators:** Full Control **Authenticated Users:** Read, Execute **SYSTEM:** Full Control	Propagate		✓
%SystemDirectory%\ias	**Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\Ntbackup.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\NTMSData	**Administrators:** Full Control **SYSTEM:** Full Control	Propagate		✓
%SystemDirectory%\rcp.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%	**Administrators:** Full	Replace		✓

\Regedt32.exe	Control **SYSTEM:** Full Control			
%SystemDirectory%\repl	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\repl\export	**Administrators:** Full Control **CREATOR OWNER:** Full Control **Replicator:** Read, Execute **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\repl\import	**Administrators:** Full Control **Replicator:** Modify **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\rexec.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\rsh.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\secedit.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDirectory%\Setup	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDirectory%\spool\Printers	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (Folder and Subfolders)	Replace		✓
%SystemDrive% **Note** Drive where the Windows 2000 operating system is installed.	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDrive%\Documents and Settings	**Administrators:** Full Control	Propagate		✓

	SYSTEM: Full Control **Users:** Read, Execute			
%SystemDrive%\Documents and Settings\ Administrator	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemDrive%\Documents and Settings\ All Users	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson **Note** Folder containing Dr Watson application error log.	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders)	Replace	✓	
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson\ drwtsn32.log **Note** Dr Watson application error log file.	**Administrators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control **Users:** Modify	Replace	✓	
%SystemDrive%\io.sys	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDrive%\msdos.sys	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemDrive%\Temp	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders)	Replace	✓	
%SystemRoot%	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Replace		✓
%SystemRoot%	**Administrators:** Full	Replace		✓

\$NtServicePackUninstall$	Control **SYSTEM:** Full Control			
%SystemRoot%\debug	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Read, Execute	Propagate		✓
%SystemRoot% \debug\UserMode	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** (Folder only) - Traverse folder, List folder, Create files. (Files only) – Create files, create folders	Propagate		✓
%SystemRoot%\regedit.exe	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemRoot%\Registration	**Administrators:** Full Control **SYSTEM:** Full Control **Users:** Read	Propagate		✓
%SystemRoot%\repair	**Administrators:** Full Control **SYSTEM:** Full Control	Replace		✓
%SystemRoot%\ Temp	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subfolders and Files) **SYSTEM:** Full Control **Users:** Traverse folder, Create files, Create folders (Folder and Subfolders)	Replace	✓	

Share Folder Permissions

The native Windows 2000 file sharing service is provided using the SMB-based server and redirector services. Even though only administrators can create shares, the default security placed on the shares allows the group Everyone to have Full Control access. These permissions allow access to the network-visible shares themselves. Access to the files and subfolders displayed through the share is controlled by the NTFS permissions that are set on the underlying folder a share maps to. It is therefore recommended that proper security be applied via NTFS permissions to any files and folders mapped by a share. Detailed procedures for setting share permissions are provided in the Windows 2000 Evaluated Configuration Administrator's Guide. However, the Evaluated Configuration must not include any shares other than the administrative shares that are set by default during installation. A description of administrative shares is provided in the Windows 2000 Evaluated Configuration Administrator's Guide.

Securing the Registry

In addition to the considerations for standard security described in this document, security administrators may want to increase protections on certain keys within the Windows 2000 Registry. By default, protections are set on various components of the registry that allow work to be done while providing standard-level security. Default Registry key permissions that are applied during operating system installation are captured into the "setup security.inf" security template file, which is described as containing the "out of box default security settings."

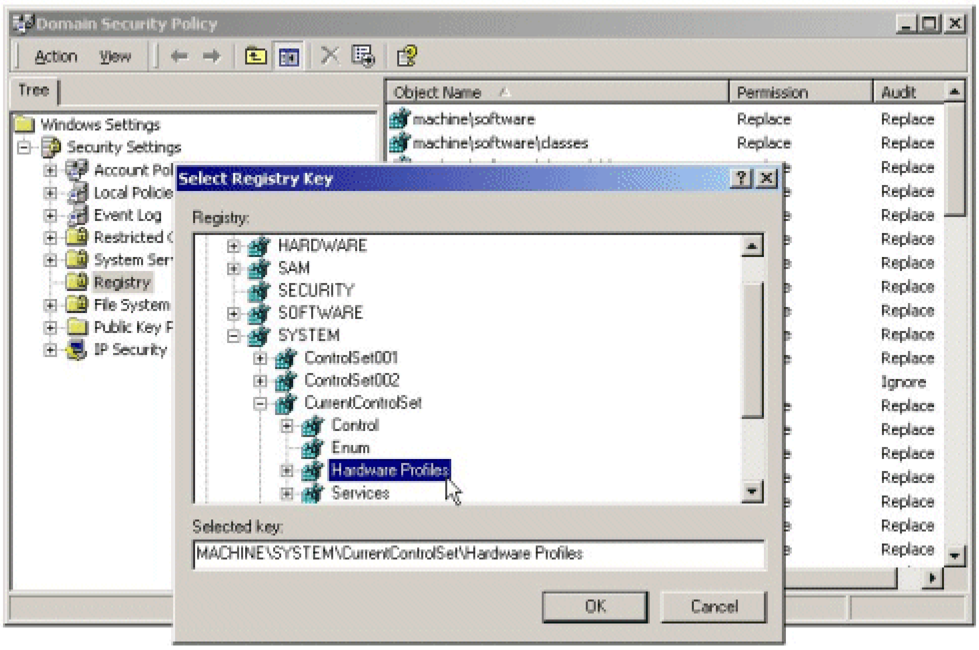
Microsoft has made improvements to the default Registry ACL settings for Windows 2000 to address security issues associated with the default Registry ACL settings identified for Windows NT 4.0. To ensure compliance with Evaluated Configuration requirements for restricting Registry access for non-administrators, it is essential that the default settings not be altered with the exception of the required ACL changes defined in Table 3.13. The changes should be done with caution, because programs that users require in order to access their applications often need access to certain Registry keys on the user's behalf. The required permission changes apply to all Windows 2000 operating systems.

To implement permissions on all or a group of Windows 2000 platforms in a domain set a Domain Security Policy. For settings on domain controllers use the Domain Controller Security Policy interface. Local permissions on individual Windows 2000 platforms can be set through the Regedt32.exe interface. To change a Registry key, a user must have the TakeOwnership privilege or be the owner of the key.

Set Registry Permissions through a Domain Policy

Set Registry permissions policies for the Domain and for Domain Controllers.

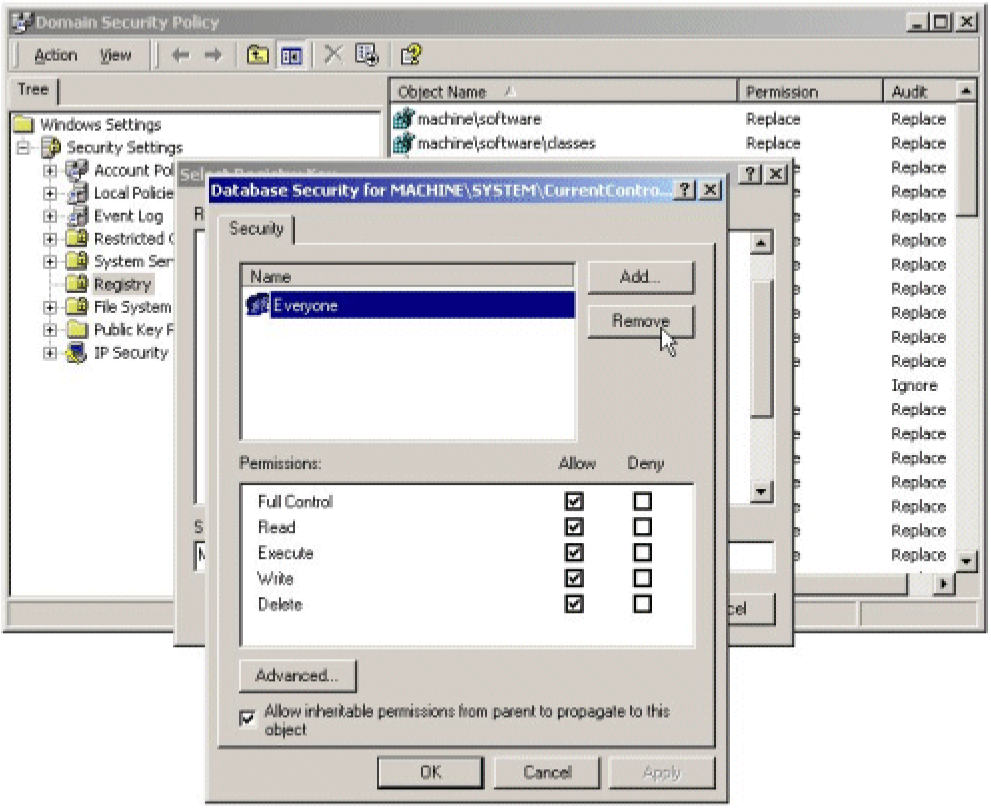
1. Open the **Domain Security Policy** or the **Domain Controller Security Policy** as applicable.
2. Expand **Security Settings**.
3. Within **Security Settings**, right-click on **Registry**.
4. Select **Add key**.
5. From the **Select Registry Key** window, navigate to and select the desired key.



Selected key: MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles

If your browser does not support inline frames, click here to view on a separate page.

6. Click the **OK** button. A **Database Security for *path* Properties** window will appear.



Permissions:	Allow	Deny
Full Control	☑	☐
Read	☑	☐
Execute	☑	☐
Write	☑	☐
Delete	☑	☐

☑ Allow inheritable permissions from parent to propagate to this object

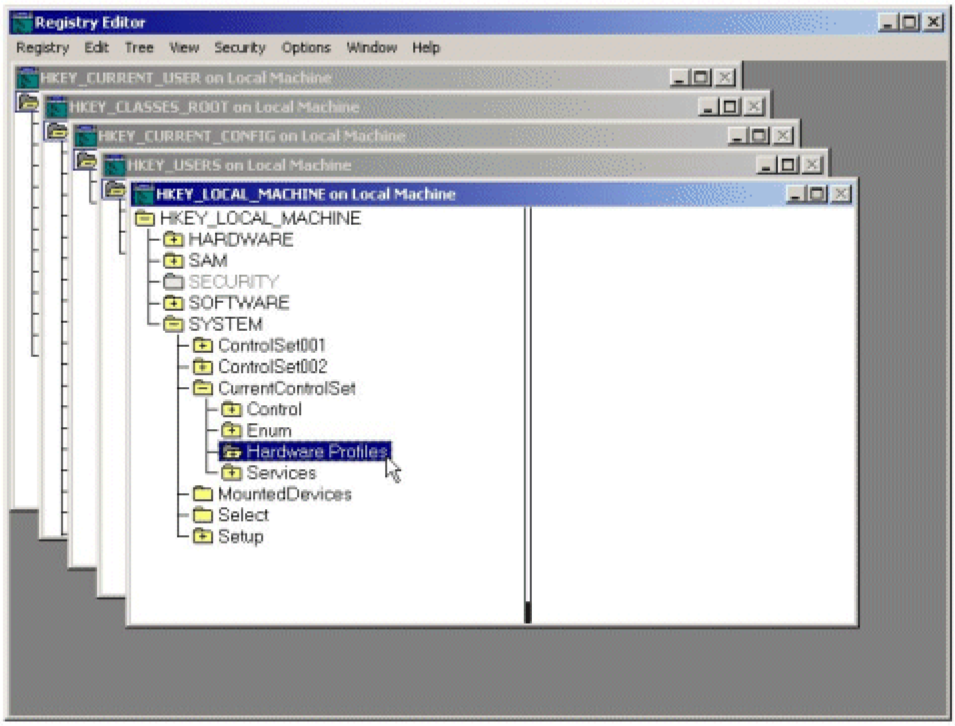
If your browser does not support inline frames, click here to view on a separate page.

7. Set permissions as necessary. Required ACL changes are provided in Table 3.13.

Set Registry Permissions through Regedt32.exe

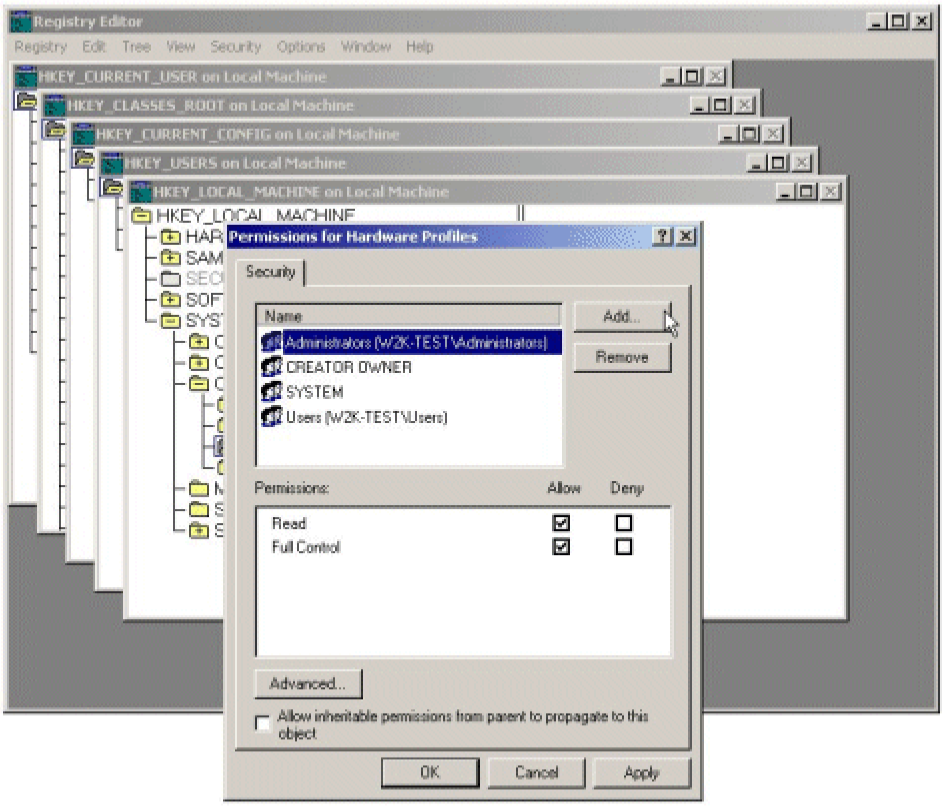
Set file and folder permissions locally on Windows 2000 Server or Professional operating systems.

1. Click the **Start** button and select **Run...**
2. Within the **Run** dialog window's text box, type **regedt32** and click the **OK** button to open the **Registry Editor** (Regedt32.exe).
3. Navigate to and select the desired Registry key.


Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_CURRENT_USER on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_USERS on Local Machine
HKEY_LOCAL_MACHINE on Local Machine
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet001
ControlSet002
CurrentControlSet
Control
Enum
Hardware Profiles
Services
MountedDevices
Select
Setup

If your browser does not support inline frames, click here to view on a separate page.

4. From the **Security** menu, select **Permissions**. The **Permissions for…** dialog window will appear. Click **Advanced** for more detailed permission settings.


Registry Editor
Registry Edit Tree View Security Options Window Help
HKEY_CURRENT_USER on Local Machine
HKEY_CLASSES_ROOT on Local Machine
HKEY_CURRENT_CONFIG on Local Machine
HKEY_USERS on Local Machine
HKEY_LOCAL_MACHINE on Local Machine
HKEY_LOCAL_MACHINE
HAR
SAM
SEC
SOF
SYS
Permissions for Hardware Profiles
Security
Name
Add...
Remove
Administrators (W2K-TEST\Administrators)
CREATOR OWNER
SYSTEM
Users (W2K-TEST\Users)
Permissions:
Allow
Deny
Read ☑ □
Full Control ☑ □
Advanced...
□ Allow inheritable permissions from parent to propagate to this object
OK
Cancel
Apply

If your browser does not support inline frames, click here to view on a separate page.

5. Set permissions as necessary. Required ACL changes are provided in Table 3.13.

Notes

- Through the Advanced tab, permissions are propagated by applying them to the current key, and subkeys. Permissions are replaced by applying them to the current key only.
- The "Read Control" ACL in Regedt32.exe is called "Read Permissions" in the Security Policy tools.
- The Power Users group shown in the table below is not available on a Domain Controller and cannot be manually set from a Domain Controller.

Table 3.13 Required Registry Permission Changes

Registry Key	**Subkey ACL Settings** **Special (Read, Write, Delete) = Query value, set value, create subkey, enumerate subkey, notify, delete, read control** **Read = Query value, enumerate subkey, notify, read control** **Apply to "This subkey and subkeys" unless otherwise noted.**	**Inheritance Method** **(Used via Security Policy tools)**
HKEY_LOCAL_MACHINE		
\SOFTWARE	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subkeys only) **Power Users**: Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate
\SOFTWARE\classes	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only)	Propagate

	Power Users: Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	
\SOFTWARE\classes\.hlp	**Administrators**: Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate
\SOFTWARE\classes\helpfile	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate
\SOFTWARE\Microsoft\OS/2 Subsystem for NT	**Administrators:** Full Control **CREATOR OWNER:** Full Control (Subkeys only) **SYSTEM:** Full Control **Note** It may be necessary to remove the inheritance and replace the ACLs.	Propagate
\SOFTWARE\Microsoft\Windows NT\CurrentVersion	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\ComputerName	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\currentcontrolset\control\ContentIndex	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\Keyboard Layout	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\Keyboard Layouts	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Control\Print\Printers	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read **Note** Remove inheritance and replace all ACLs. Inherited ACLs may be copied to the current key.	Replace
\SYSTEM\CurrentControlSet\Control\ProductOptions	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
\SYSTEM\CurrentControlSet\Services\Eventlog	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate

\SYSTEM\CurrentControlSet\ Services\Tcpip	**Authenticated Users:** Read **Note** Replace Eveyone with Authenticated Users. All inherited ACLs remain.	Propagate
HKEY_CLASSES_ROOT		
\HKEY_CLASSES_ROOT **Note** This key is an alias to HKEY_LOCAL_MACHINE \SOFTWARE\Classes	**Administrators:** Full Control **Authenticated Users:** Read **CREATOR OWNER:** Full Control (Subkeys only) **Power Users:** Special (Read, Write, Delete) **SYSTEM:** Full Control **Users:** Read	Propagate

IPSec Policy

IPSec policies, rather than application programming interfaces (APIs), are used to configure IPSec security services. The policies provide variable levels of protection for most traffic types in most existing networks. IPSec policies can be configured to meet the security requirements of a user, group, application, domain, site, or global enterprise. Microsoft Windows 2000 provides an administrative interface called IPSec Policy Management to define IPSec policies for computers at the Active Directory level for any domain members, or on the local computer for non–domain members.

IPSec policies can be applied to computers, sites, domains, or any organizational units created in Active Directory. IPSec policies should be based on an organization’s guidelines for secure operations. Through the use of security actions, called ***rules***, one policy can be applied to heterogeneous security groups of computers or to organizational units.

There are two storage locations for IPSec policies:

- Active Directory
- The local registry for stand-alone computers and computers which are not joined to the domain. When the computer is temporarily not joined to a trusted Microsoft Windows 2000 domain, the policy information is cached in the local registry.

Each policy should apply to a scenario considered in an organization’s established security plan. Special configuration settings might apply if policies are assigned to a DHCP server, Domain Name System (DNS), Windows Internet Name Service (WINS), Simple Network Management Protocol (SNMP), or remote access server.

Detailed procedures for creating IPSec policies are provided in the Windows 2000 Evaluated Configuration Administrator’s Guide. There are no specific IPSec setting requirements for the Evaluated Configuration.

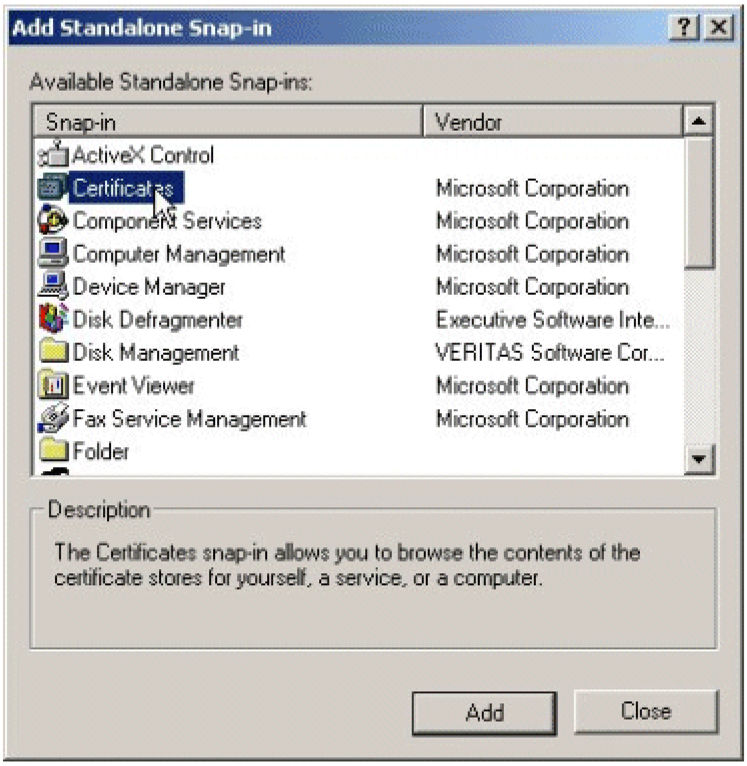
Encrypting File System

Windows 2000 operating systems provide a native ability to encrypt files and folders on an NTFS volume through the use of its Encrypting File System (EFS). EFS uses a private key encryption mechanism for storing data in encrypted form on the network. EFS runs as a service and uses both private key encryption and public key encryption.

The ST requires the ability to enable, disable, and control EFS on NTFS volumes, however, there are no specific EFS configuration requirements for the Evaluated Configuration. Detailed procedures for enabling, using, and managing EFS, as well as for the storage and retrieval of encryption keys are provided in the Windows 2000 Evaluated Configuration Administrator’s Guide.

After the initial installation of the operating system, it is recommended that a backup of the Administrator’s encryption certificate and private key be made. The backup procedures are as follows:

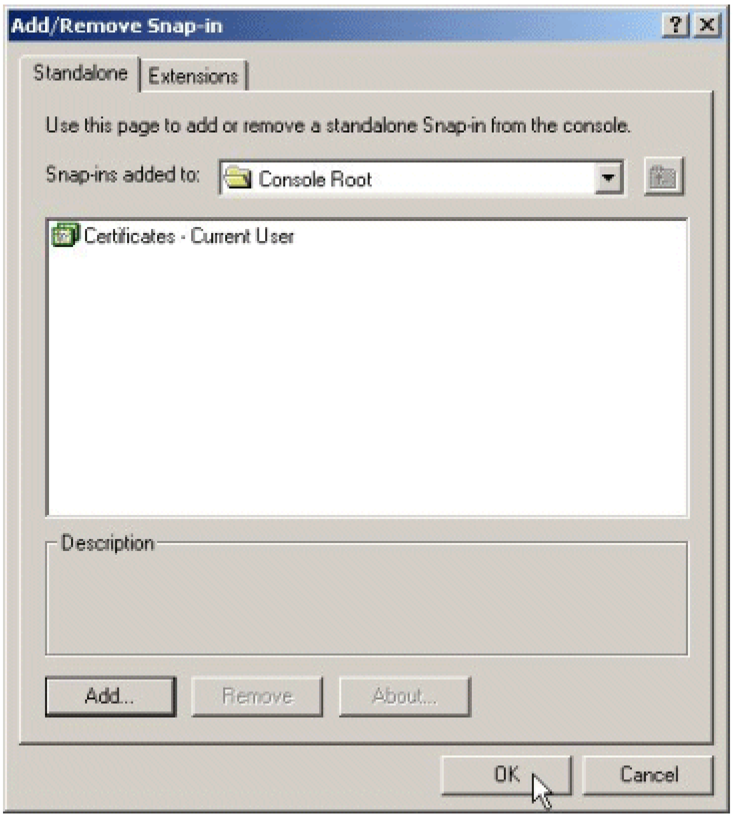
1. Click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.
2. On the **Console** menu, click **Add/Remove snap-ins**, and click **Add**.
3. Locate the **Certificates** snap-in, and click **Add**.



Snap-in	Vendor
ActiveX Control	
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...
Disk Management	VERITAS Software Cor...
Event Viewer	Microsoft Corporation
Fax Service Management	Microsoft Corporation
Folder	

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.

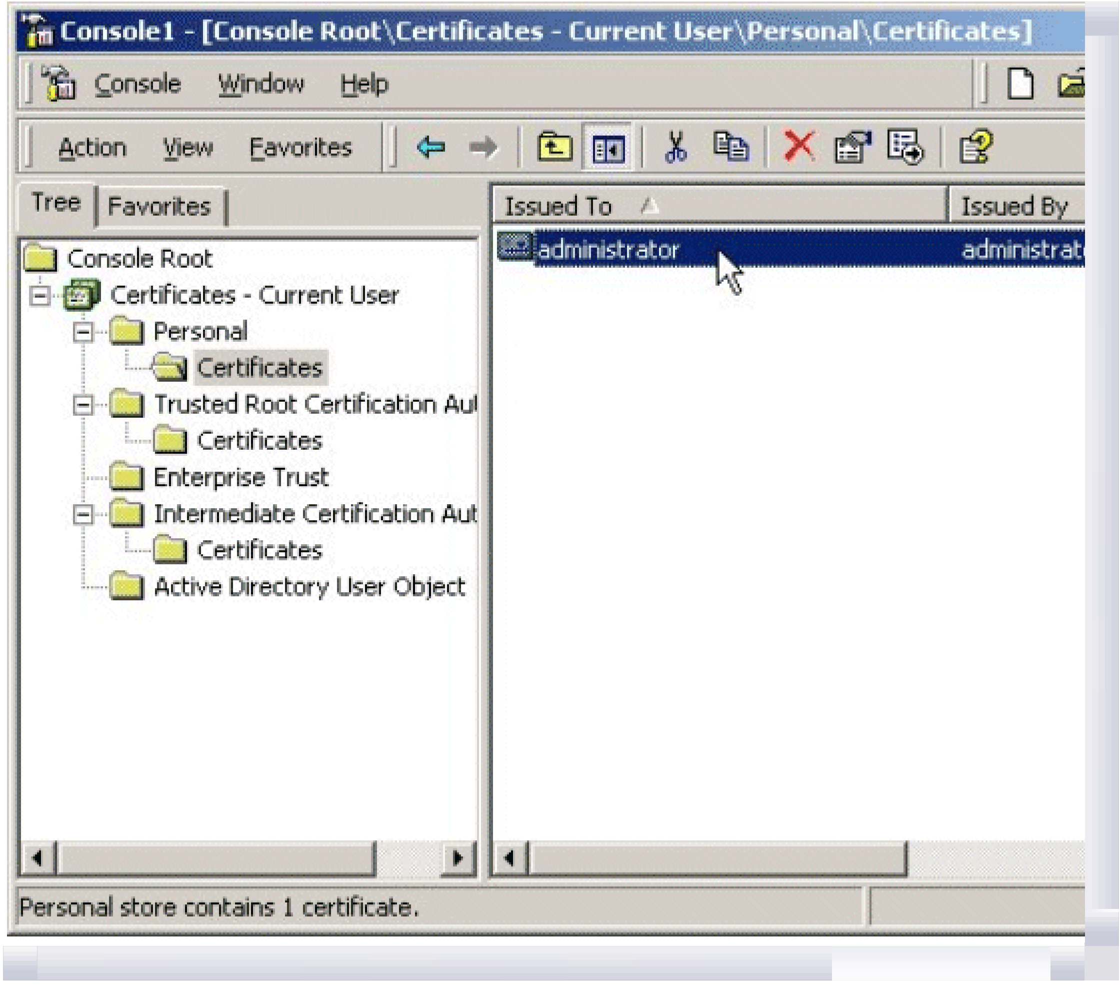


Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Certificates - Current User

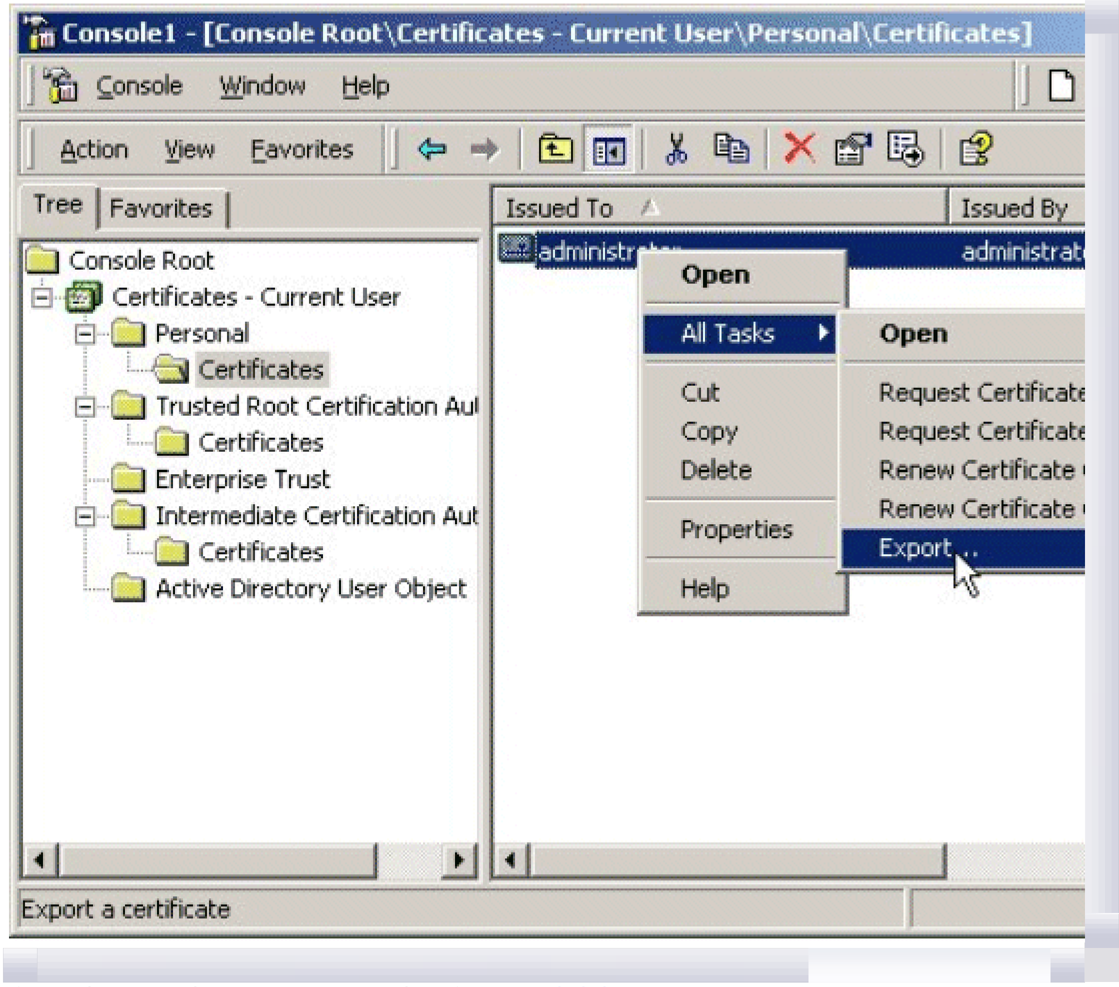
5. Locate the **Encrypting File System** certificates in the Personal certificate store. Click the **+** next to **Certificates–Current User**. Expand the **Personal** folder. Select **Certificates**.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Aut
Certificates
Enterprise Trust
Intermediate Certification Aut
Certificates
Active Directory User Object
Issued To
Issued By
administrator
administrat

Personal store contains 1 certificate.

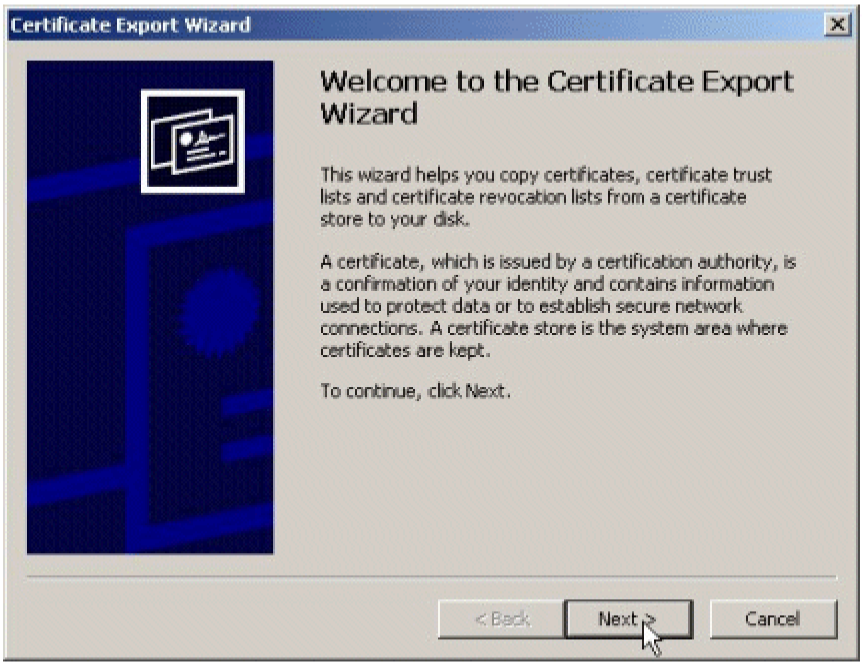
If your browser does not support inline frames, click here to view on a separate page.

6. Right-click on the Administrator certificate, from the menu, select **All Tasks**, and click **Export**.



If your browser does not support inline frames, click here to view on a separate page.

7. This starts the **Certificate Manager Export** wizard. Click **Next**.


Certificate Export Wizard

Welcome to the Certificate Export Wizard

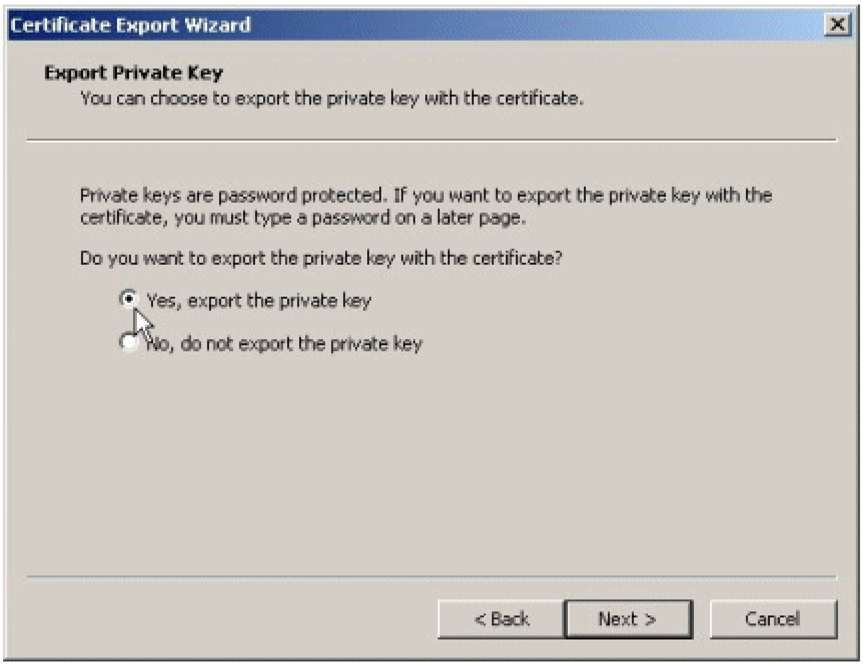
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

If your browser does not support inline frames, click here to view on a separate page.

8. Select the **Yes, export the private key** radio button. Click **Next**.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

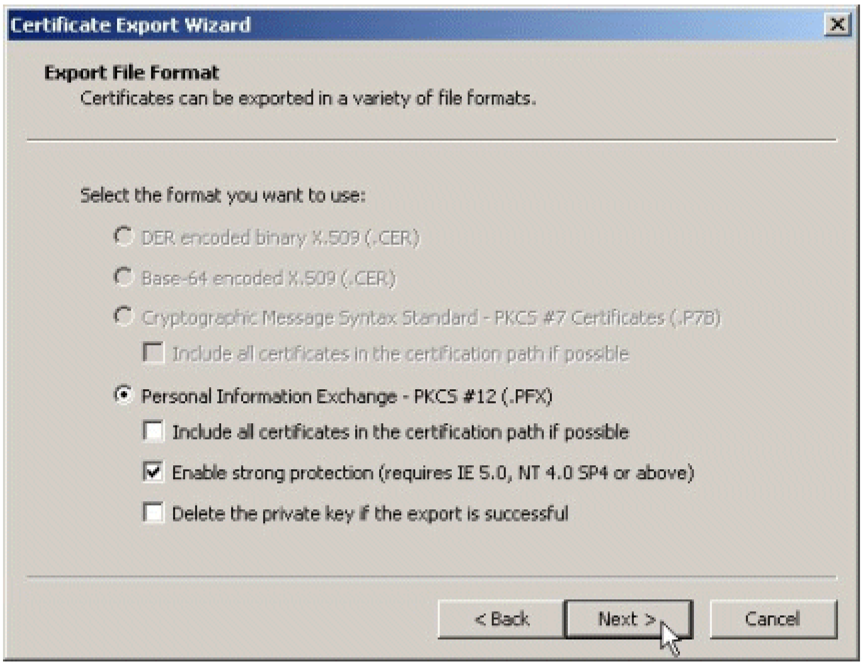
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

If your browser does not support inline frames, click here to view on a separate page.

9. The export format available is **Personal Information Exchange-PKCS#12**, or .pfx - personal exchange format. Click **Next**.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

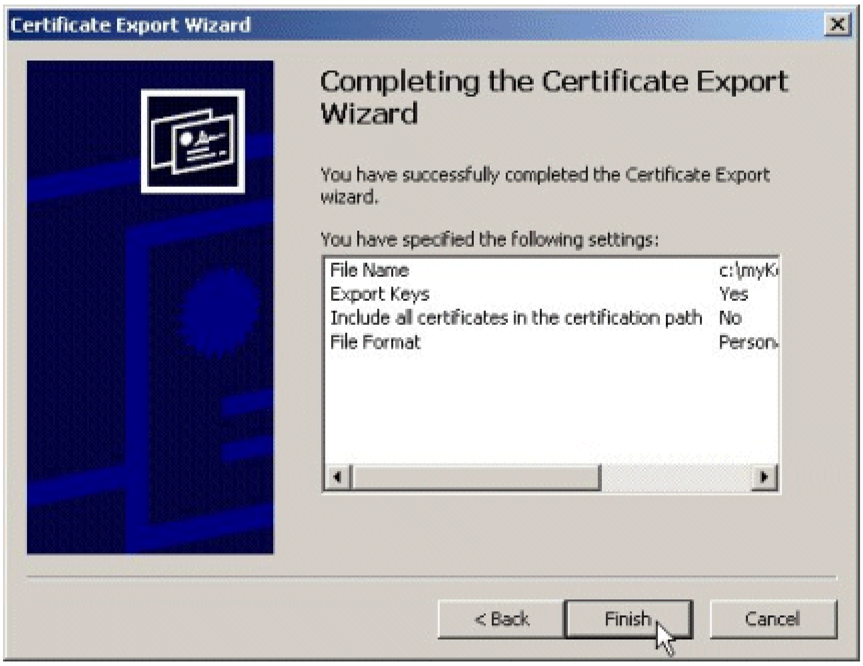
☑ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

If your browser does not support inline frames, click here to view on a separate page.

10. Provide the password to protect the .pfx data. Click **Next**.

11. Provide the path and file name where the .pfx data is to be stored. For example, **c:\mykey**. Click **Next**.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	c:\myK
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

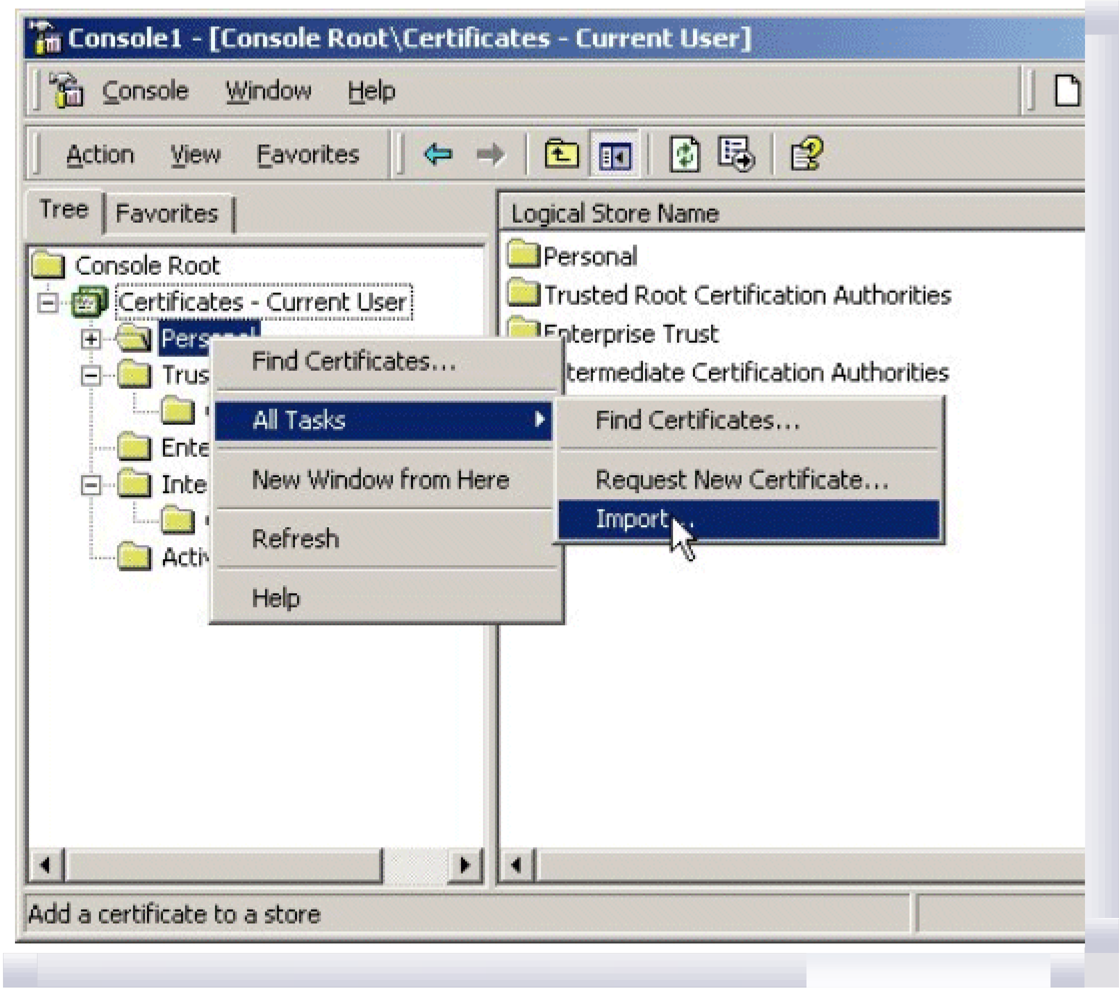
If your browser does not support inline frames, click here to view on a separate page.

12. A list of certificates and keys to be exported is displayed. Click **Finish** to confirm.
13. Click **OK** to close the wizard, and close the snap-in.

This exports the encryption certificate and private key to a .pfx file that must be backed up securely.

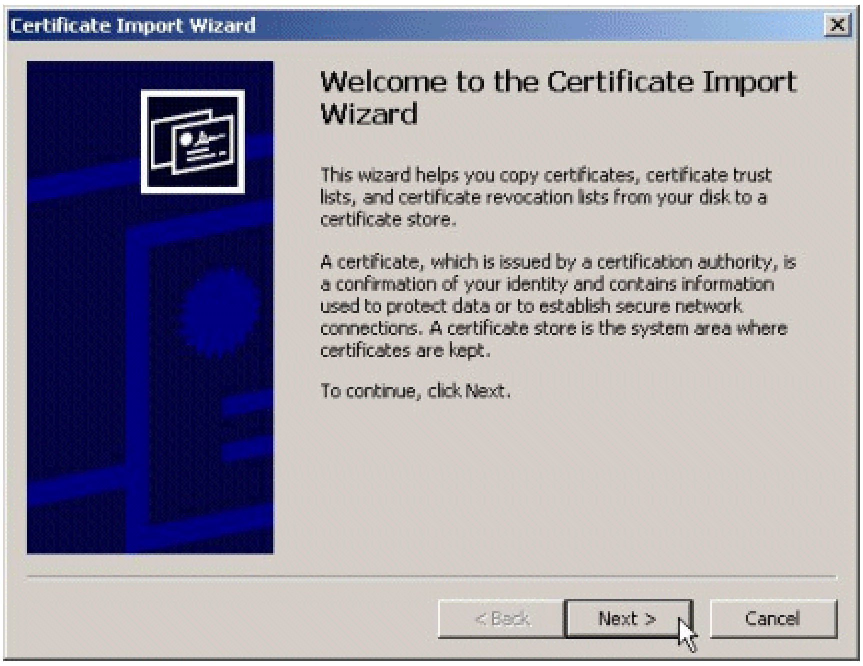
To restore the encryption certificate and private key on a different system do the following:

1. Copy the .pfx file to a floppy disk, and take it to the computer where the encryption certificate and private key will be imported to.
2. Start the **Certificates** snap-in by clicking **Start**, clicking **Run**, and then typing **mmc**.
3. On the **Console** menu, click **Add/Remove snap-ins**, and click **Add**.
4. Click **Certificates**, and click **Add**. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.
5. Right-click **Personal store**, click **All Tasks**, and click **Import** to import the .pfx file.



If your browser does not support inline frames, click here to view on a separate page.

6. This starts the **Certificate Manager Import** wizard. Follow the wizard steps to successfully import the certificate and private key.


Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

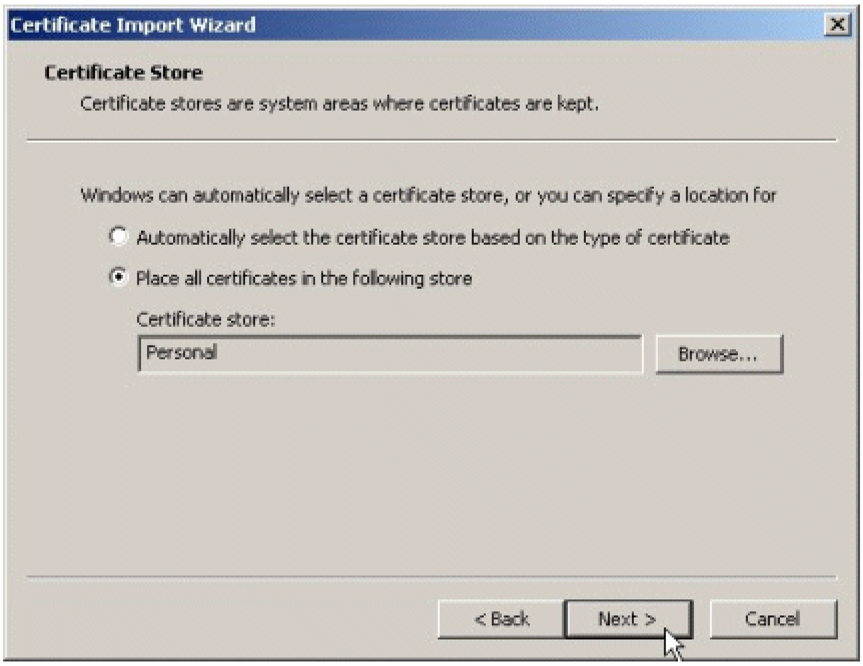
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

If your browser does not support inline frames, click here to view on a separate page.

7. Provide the path to the .pfx file.
8. Type the password to unwrap the .pfx data.
9. Click **Place all certificates in the following store**, and accept the Personal certificate store. Click

Next.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

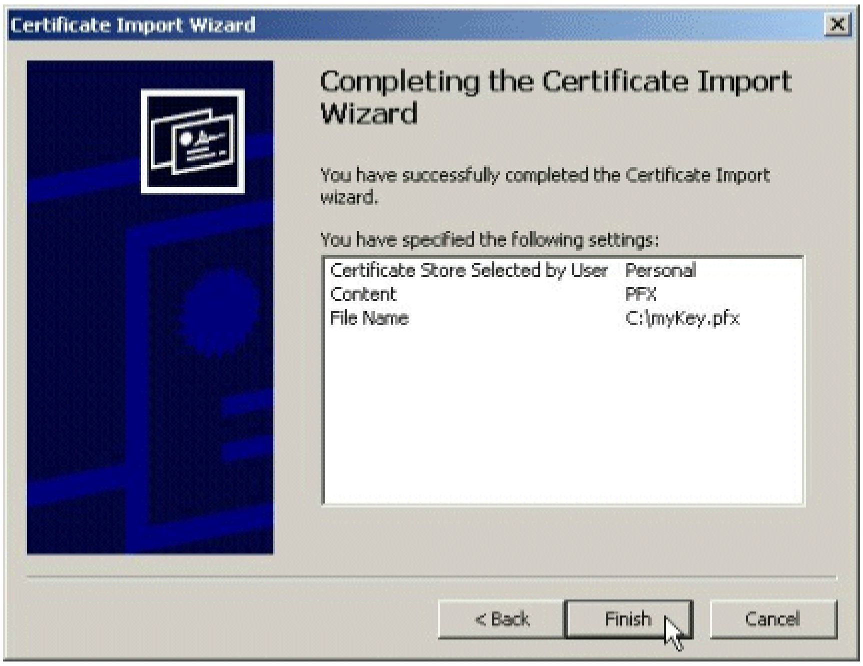
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal

If your browser does not support inline frames, click here to view on a separate page.

10. Click **Finish**, and then click **OK** to start the import operation. When the import is complete, click **OK** to close the wizard.



Certificate Import Wizard

Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\myKey.pfx

If your browser does not support inline frames, click here to view on a separate page.

Once the same keys are available, encrypted files that may have been backed up on different computer can be transparently used.

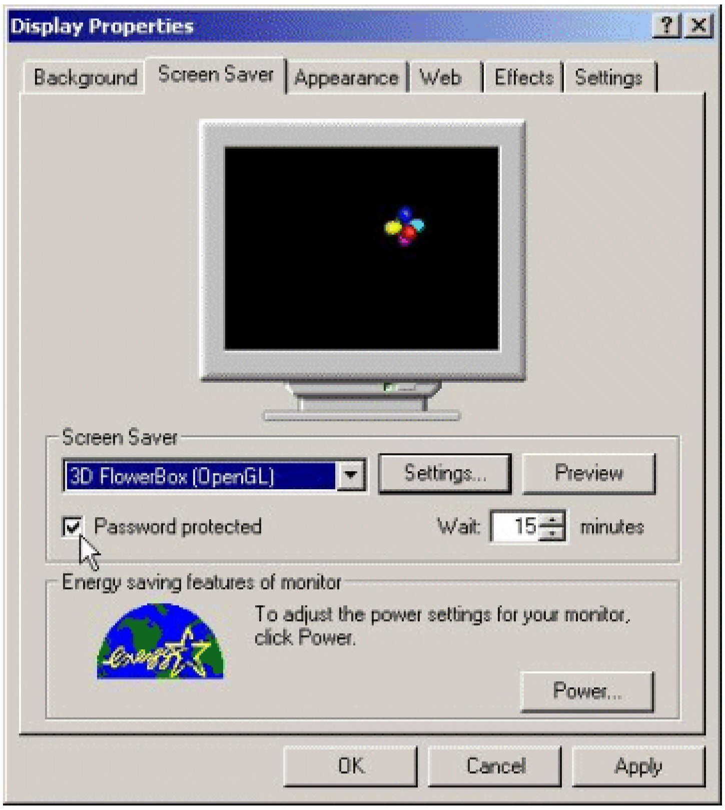
Enable Automatic Screen Lock Protection

Enable a password-protected screensaver for the Evaluated Configuration. Doing so will enable a user desktop to be locked for security reasons by setting an automatic screen lock that is initiated with the screensaver after a set period of inactivity. Once the computer screen lock is invoked, access to the computer will only be allowed to the user whose account is currently logged on to the computer or by an authorized administrator.

Set an automatic screen lock by setting screensaver based screen lock as follows:

1. Right click on the user desktop and select **Properties**. The **Display Properties** window will appear.

2. Click on the **Screen Saver** tab.
3. Select a screen saver from the **Screen Saver** drop down menu.
4. Enter the number of minutes of inactivity that the system must wait before initiating the screen saver in the **Wait**: dialog box (the default of 15 minutes is recommended).
5. Select the Password Protected box.



Screen Saver: 3D FlowerBox (OpenGL)

☑ Password protected

Wait: 15 minutes

To adjust the power settings for your monitor, click Power.

6. Click **OK** to set the password protected screen saver.

Update the system Emergency Repair Disk

Update the system's ERD to reflect all the changes made. For instructions, see "Recommended Actions Prior to Installing Service Pack and Hotfix Updates."

Application Installation Procedures on a Secure Configuration

Installation of applications conforming to Windows Installer-based package requirements will have difficulty installing from a CD-ROM on a computer running a Windows 2000 operating system in the Evaluated Configuration. The reason is that the Windows Installer service is not a service that was evaluated and is therefore disabled in the Evaluated Configuration of Windows 2000. Additionally, the AllocateCDRoms Registry value that is set in the Evaluated Configuration will not allow Windows Installer to open a .Cap file directly from a CD-ROM. Therefore, to install an application conforming to Windows Installer-based package requirements, the Windows Installer service must be temporarily enabled and the "MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms" Registry value must be temporarily set to 0 (this can be accomplished through the Local Security Policy interface).

> **Note** To un-install applications conforming to Windows Installer-based package requirements, the Windows Installer service must be again temporarily enabled. After un-installing the application, the Windows Installer service should then be disabled to return to the evaluated configuration. To un-install an application, the "AllocateCDRoms" Registry value need not be modified; it should remain enabled, as set in the evaluated configuration.

The procedures are as follows:

1. Start the Windows Installer service:
   a. Log on to the computer with administrative rights.
   b. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Services**. This opens the local system **Services** interface.
   c. In the right-hand pane, right-click on **Windows Installer** and select **Properties**. The **Windows Installer Properties** interface will appear.
   d. In the **General** tab view, change the **Startup type** from **Disabled** to **Manual** by using the drop down menu.
   e. Click the **Apply** button. The **Start** button under **Service status** will become active.

- f. Click the **Start** button to start the **Windows Installer** service.
- g. Click the **OK** button to close the **Windows Installer Properties** interface.
- h. Close the **Services** interface.

2. Change the Restrict CD-ROM access to locally logged-on user only setting in the Local Security Policy’s Security Options:
   - a. Logged on as an administrator, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the local system **Local Security Policy** interface.
   - b. Expand Security Settings.
   - c. Within Security Settings, expand **Local Policies** to reveal the Audit, User Rights Assignment, and Security Options policies.
   - d. Click on the **Security Options** object. The right-hand details pane will reveal the configurable security options.
   - e. Double click on **Restrict CD-ROM access to locally logged-on user** only in the right-hand details pane.
   - f. Select the **Disabled** radio button and click the OK button.
   - g. Close the **Local Security Policy** interface and reboot the computer.
3. Install the software application from CD-ROM:
   - a. Once the computer reboots, log on with administrative rights.
   - b. Insert the application installation CD-ROM in the CD-ROM drive and follow the installation procedures.

After completing the application installation, it will be necessary to reset the Evaluated Configuration settings on the computer by disabling the **Windows Installer** service and resetting the **Restrict CD-ROM access to locally logged-on user only** policy setting to **Enabled**.

1. Reset the Evaluated Configuration settings as follows:
   - a. Follow the procedures in **Step 1** above to open the **Service** interface and access the **Windows Installer** service.
   - b. Change the **Startup type** from **Manual** to **Disabled** by using the drop down menu.
   - c. Click the **Stop** button to stop the **Windows Installer** service.
   - d. Click the **OK** button to close the **Windows Installer Properties** interface.
   - e. Close the **Services** interface.
   - f. Next, open the **Security Options** policy in the **Local Security Policy** by following the procedures in **Step 2** above.
   - g. Double click on Restrict CD-ROM access to locally logged-on user only in the right-hand details pane.
   - h. Select the **Enabled** radio button and click the **OK** button.
   - i. Close the **Local Security Policy** interface and reboot the computer.

Send feedback to Microsoft