



Ethical Hacking and Countermeasures

Version 6



Module LXI

Threats and Countermeasures

Domain Level Policies

Domain Level Policies are “Group Policy settings”

The built-in Default Domain Controller policy is

- Account policies, Default setting values for these policies are collectively referred as Account policies



Types of Account policies

- Password policies
- Account lockout policies
- Kerberos authentication protocol policies



When these policies are applied to any other level in Active Directory, on the member server the local accounts list will only be affected

Default values are given in the built-in Default Domain Controller policy

Account Policies (cont'd)

The domain Account policy is the default Account policy for a Windows computer which is a member of the domain

Another Account policy for the organizational unit is an exception for this rule

The default computer (local) policies are assigned to nodes that are in a workgroup are a domain and where no organizational unit Account policy or domain policy is associated

Password Policy

A common way to hide user's identity is to use a secret password or a phrase

The assigned password prevents an unauthorized access to the user or administrative account

A regular change of the passwords decreases the threat of password attack

A password policy can be given to put into effect the use of strong passwords



Password Policy (Cont'd)

Password policy settings control the intricacy and existence of passwords

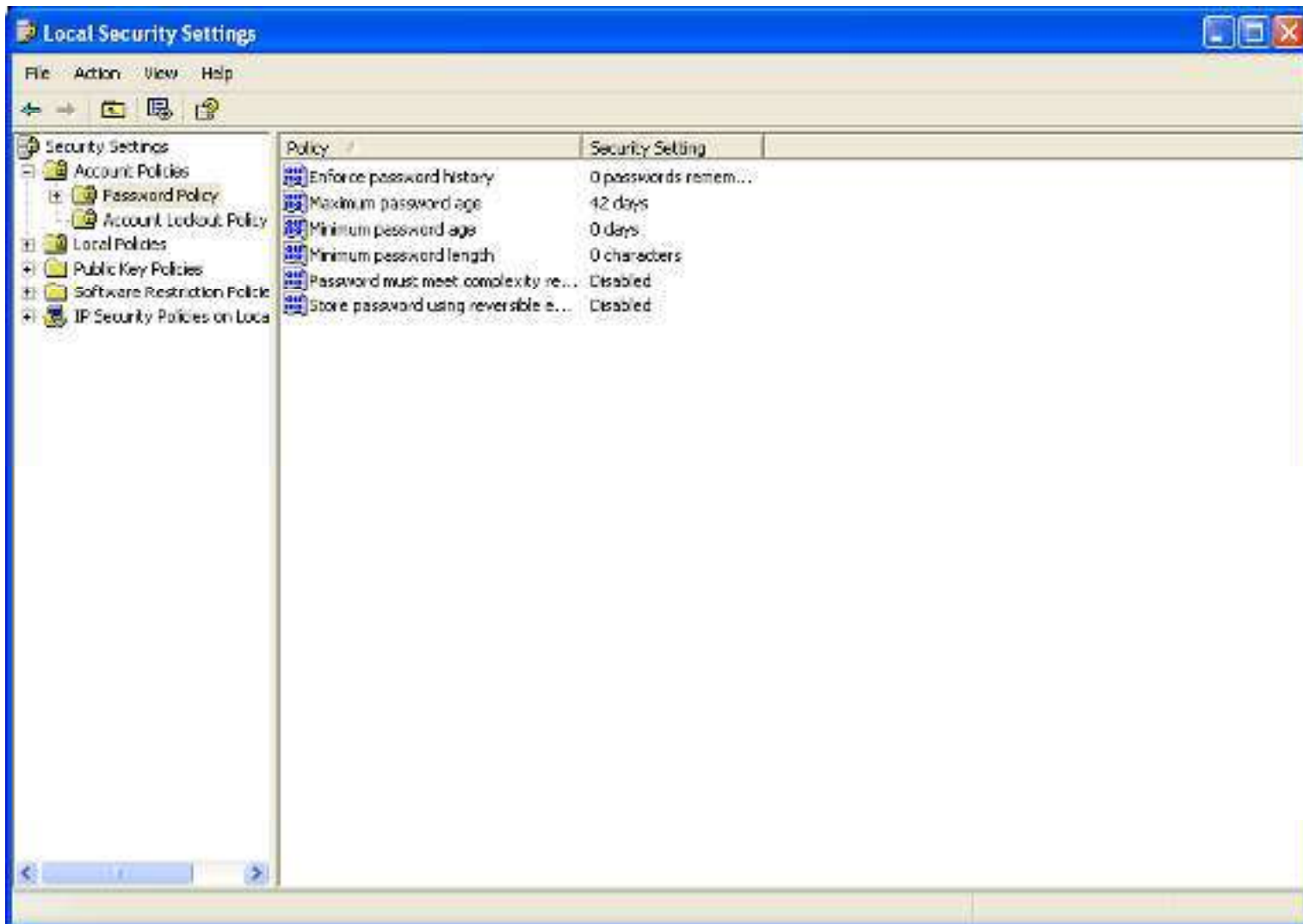
The password policy settings are configured under the Object Editor of Group Policy at the location

- **Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy**

If various groups require different password policies, they must be divided into different sections (domains) depending on the additional requirements



Password Policy



Password Policy - *Policies*

Enforce password history

Maximum password age

Minimum password age

Minimum password length

Passwords must meet complexity requirements

Store password using reversible encryption for all users in the domain



Enforce Password History

This policy determines the various unique passwords that are connected with a user account before reusing the old password

The values for the **Enforce password history** setting are:

- A value between 0 and 24 specified by the user



Enforce Password History - *Vulnerability*

Brute-force attack can be used to determine the password, when the user is reusing the same password for an account for an extended period of time

The efficiency of a high-quality password policy is very much decreased, when a password change is necessary but password reusability is allowed

If **Minimum password age** setting are configured, users will not be able to change there passwords over and over, UN-less they stop reusing there old passwords



Enforce Password History - *Countermeasure*

To decrease the vulnerabilities raised by password reusing, set the **Enforce password history** option to **24** (maximum)

While configuring **Minimum password age** settings, no password should be changed immediately

The **Enforce password history** value should be set at a stage that combines a sensible utmost password age with a sensible password change interval requirement for the users



Enforce Password History - *Potential Impact*

The major impact of this pattern is that users has to generate a new password every time it is necessary to change the old one

Risk Involved

- If the user has to change the password to a new distinct phrase, the risk of writing the pass phrase is increased
- The users might generate passwords that change incrementally (as *password01*, *password02* ...) to ease its remembrance
- By decreasing the value of Minimum password age setting administrative overhead is maximized, as users who forget their pass phrase will be requiring assistance to reset it



Enforce Password History



Maximum Password Age

This policy determines the duration (in days) that a password can be used before it is changed

The values for the Maximum password age setting are:

- The number of days between 0 and 999 as specified by the user.
- Not Defined



Password Age - *Vulnerability*

A password attacker can always guess or crack a difficult password, Some policy settings make it tough to crack them

The risk of breaking a password can be reduced by making the users to change there passwords regularly

Maximum password age setting can be configured to never change the user passwords, but it might lead to a security risk



Maximum Password Age - *Countermeasure*

Maximum password age settings can be configured as per user requirements

Maximum Password Age setting can be assigned to 0 so that passwords will never expire



Maximum Password Age - *Potential Impact*

If the **Maximum password age** setting value is very less, the user has to modify their passwords frequently

This kind of Configuration may decrease security, as the user may write the passwords somewhere by the fear of forgetting them and then they may lose information at some place

If value of the policy setting to set to maximum, the security level will be reduced as the attackers will get a large time span to crack the passwords



Maximum Password Age



Minimum Password Age

This policy setting is used to conclude the number of days in which the user has to change his password

To make **Enforce password history** setting efficient, set the policy value higher than 0

If this value is set to zero the user need not change his password regularly

The values for the Minimum password age setting are:

- The number of days between 0 and 998 as spesified by the user
- Not Defined

Minimum Password Age - *Vulnerability*

It is impractical to modify the password regularly, if the user cycles around to use his regular password

By using this policy setting with **Enforce password history** setting, prevents the use of old passwords

To make **Enforce password history** setting effective, set the policy value to higher than 0



Minimum Password Age - *Countermeasure*

By setting the **Minimum password age** value to **0** days, immediate password changes would be allowed, which is not recommended

To have a limitation over the password change. Set the value to minimum **2** days

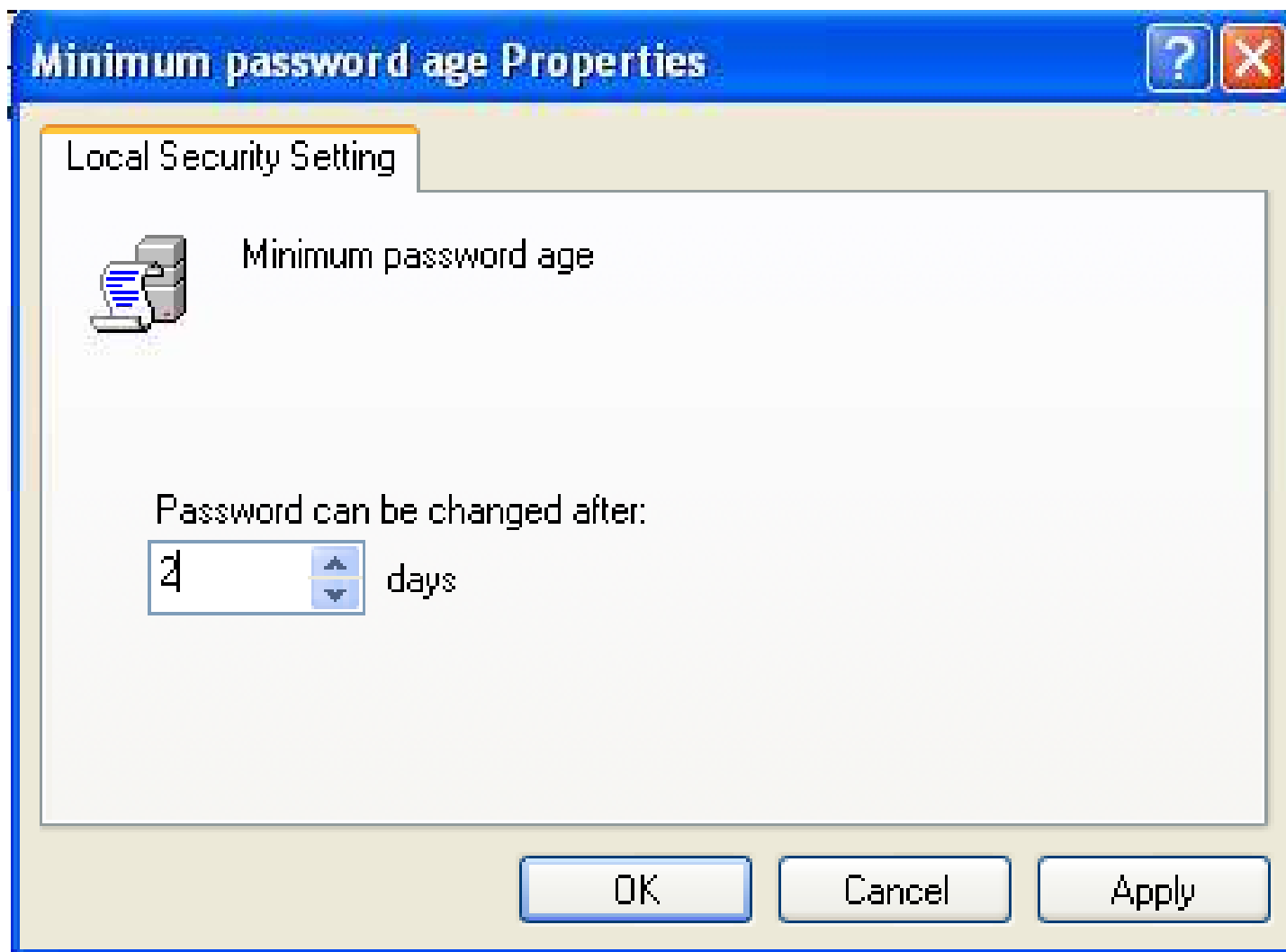


To make a user change his password at his first logon

Administrator has to tick **User must change password at next logon** check box

This will allow the user to change his password on logging his account.
In other case the user has to wait until next day

Minimum Password Age



Minimum Password Length

The policy settings conclude the minimum numeral characters to generate a password for an account

Many theories have been evolved to decide the password length; rather "pass phrase" is a suitable word than "password"

An expression "I am sick!" is an acceptable pass phrase. These expressions are significantly more robust than an 8 or 10 character strings and they are easier to remember

The values for the Minimum password length setting are:

A number between 0 and 14 as user specified

Not Defined

Minimum Password Length - *Vulnerability*

Various kinds of password attacks are implemented to get the password for an account.

- Dictionary attacks (Using general terms and expression)
- Brute force attacks (Possible grouping of characters)

Attackers also try to get hold of the user account database to utilize them to break the accounts and passwords.



Minimum Password Length - *Countermeasure*

If **Minimum password length** is set **0**, password is not necessary

To set a password, assign a value **8** or more. **8** character passwords give enough security from Brute force and Dictionary attacks



Minimum Password Length - *Potential Impact*

Long passwords may cause account lockouts when the passwords are typed wrong by mistake which will maximize the work of help desk

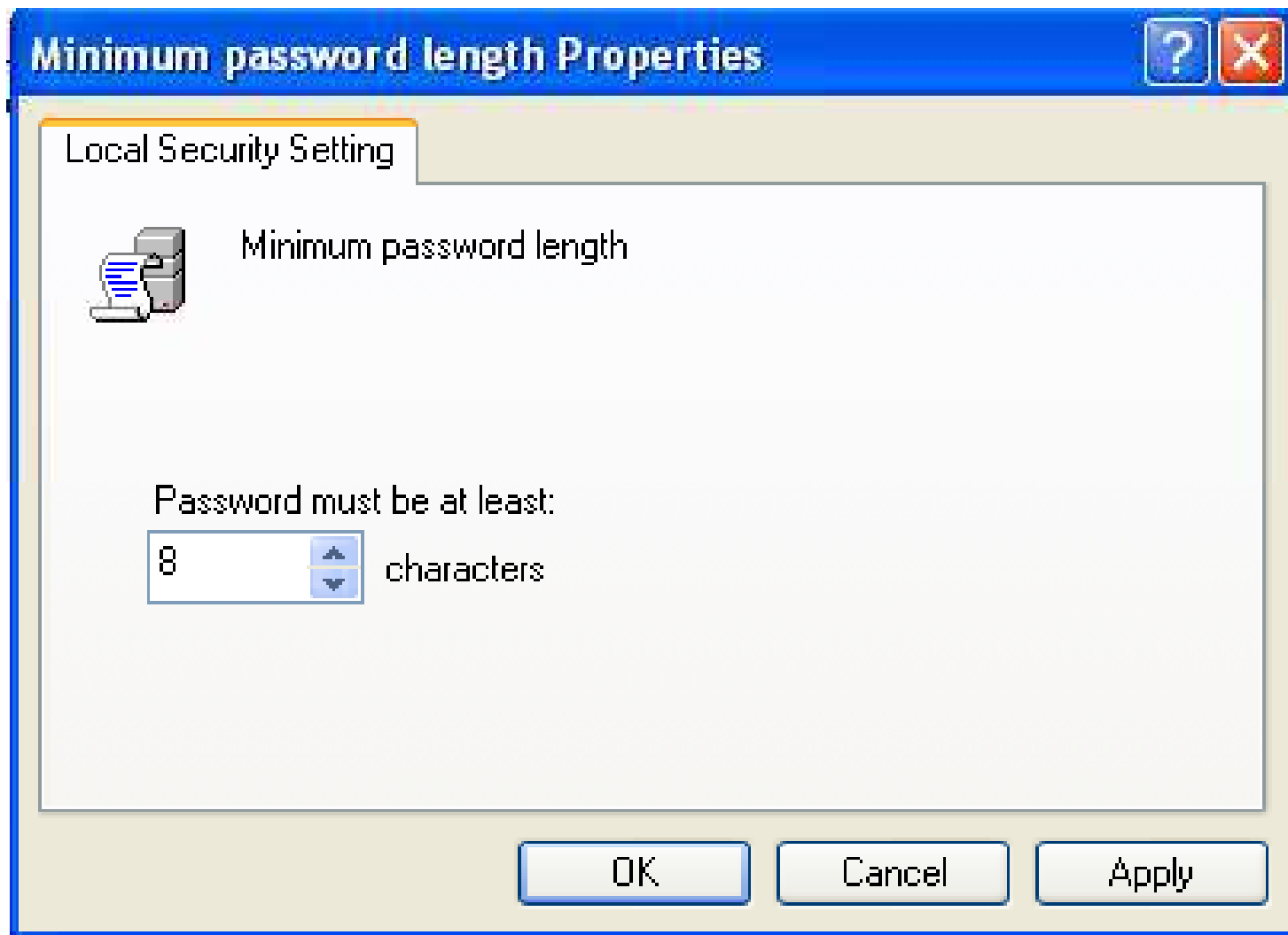
Long Passwords

- Long passwords are hard to remember, so the personnel's might hard to write it down some where which can lead to insecurity of the password

Short Passwords

- Short passwords can be easily broken using any tool which use brute force (or) dictionary attack

Minimum Password Length



Passwords Must Meet Complexity Requirements

If this policy setting is enabled, passwords must fulfill these requirements:

The password length must be minimum 6 characters

The password must contain characters from the below given groups:

Uppercase characters (A, B, C, ...)

Lowercase characters (a, b, c, ...)

Numerals (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)

Non-alphanumeric and Unicode characters (() ` ~ ! @ # \$ % ^ & * - + = | \ { } [] : ; " ' < > , . ? / € Γ f λ and space)

The password shouldn't include three or more successive characters from the user account name or display name

Passwords must Meet Complexity Requirements (cont'd)

These complexity conditions are imposed upon password generation or modification.

The values for the Passwords must meet complexity requirements setting are:

- Enabled
- Disabled
- Not Defined



Passwords must Meet Complexity Requirements - *Vulnerability*

A password generated by the combination of letters and numeric characters is easy to break (crack)

Various character sets should be combined together to generate a passwords which can be prevented from Cracking



Passwords must Meet Complexity Requirements - *Countermeasure*

Configure the **Passwords must meet complexity requirements** setting to **Enabled**.

By Combining **Minimum password length of 8** with the above settings, the various possibilities for a password are so great that it is almost impossible for a brute force attack to be successful.

An attacker capable of processing 1 million passwords per second may crack the password in 7 and 1/2 days or less.

Passwords must Meet Complexity Requirements - *Potential Impact*

If the default password complexity configuration is hold, help desk calls may increase for locked-out accounts as users might not be able to remember the non alphabetic characters

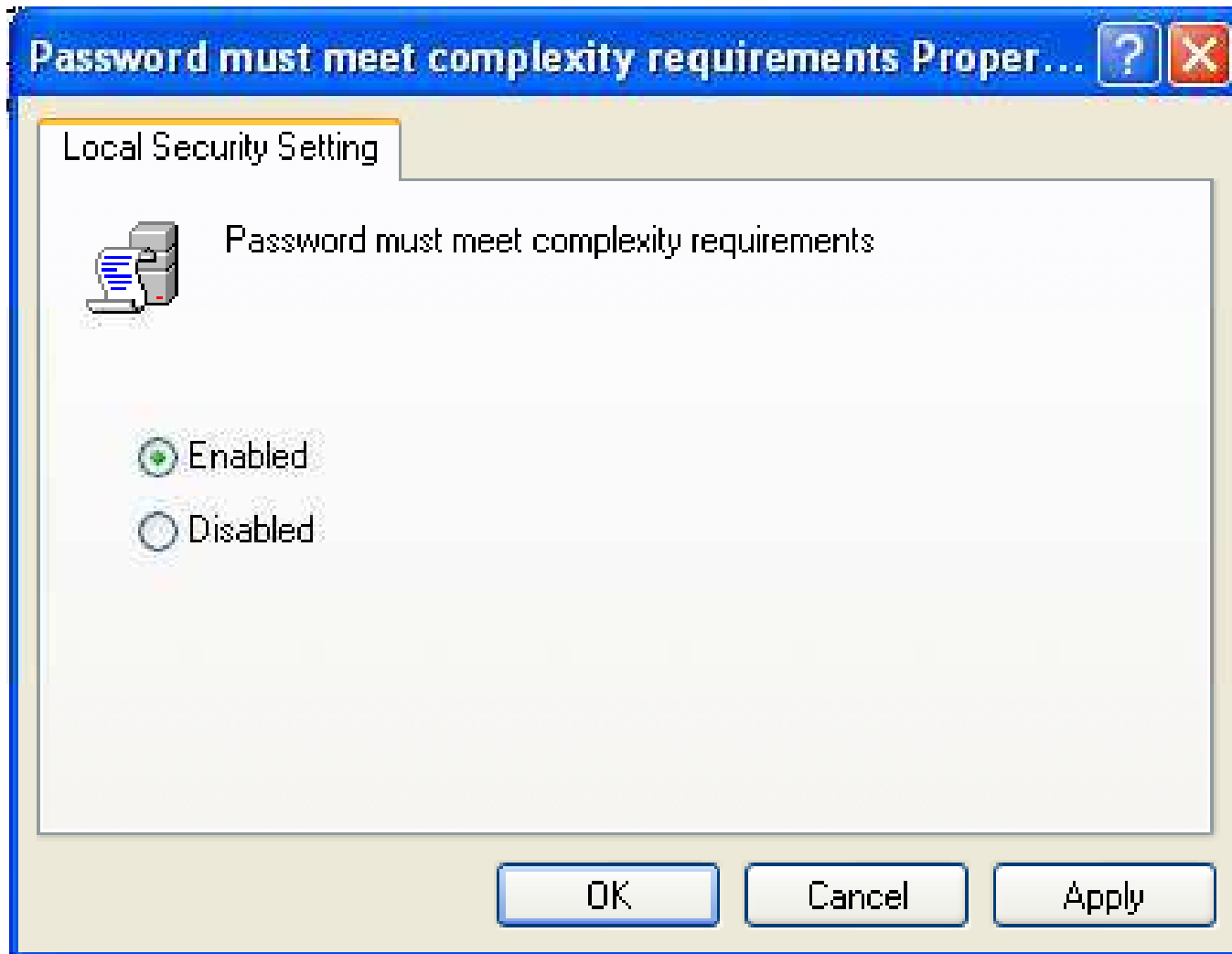


A custom password filter can be created which can perform a dictionary check to make sure the password is free from common words



The use of ALT key character grouping can increase the complexity of a password

Passwords must Meet Complexity Requirements



Store Password using Reversible Encryption for all Users in the Domain

The **Store password using reversible encryption for all users in the domain** setting offers support for application protocols that need information on the user's password for authentication purposes

Encrypted passwords that are stored can be decrypted. An attacker who manages break the encrypted password can logon on a compromised account



Store Password Using Reversible Encryption for all Users in the Domain (Cont'd)

Using the Challenge Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Service (IAS) services need's the policy setting to be enabled.

The values for the Store password using reversible encryption for all users in the domain setting are:

- Enabled
- Disabled
- Not Defined

Store Password Using Reversible Encryption for all Users in the Domain (Cont'd)

Vulnerability

- This policy setting conclude that whether Windows Server 2003 will store passwords in a weaker format which is more vulnerable to compromise.

Countermeasure

- Configure the **Store password using reversible encryption for all users in the domain** setting to **Disabled**.

Potential Impact

- If an organization uses CHAP authentication protocol through remote access or IAS services (or) Digest Authentication in IIS, the policy settings should be configured **Enabled**.

Store Password Using Reversible Encryption for all Users in the Domain (Cont'd)



Account Lockout Policy

An attacker might try to find out a password by trail and error method

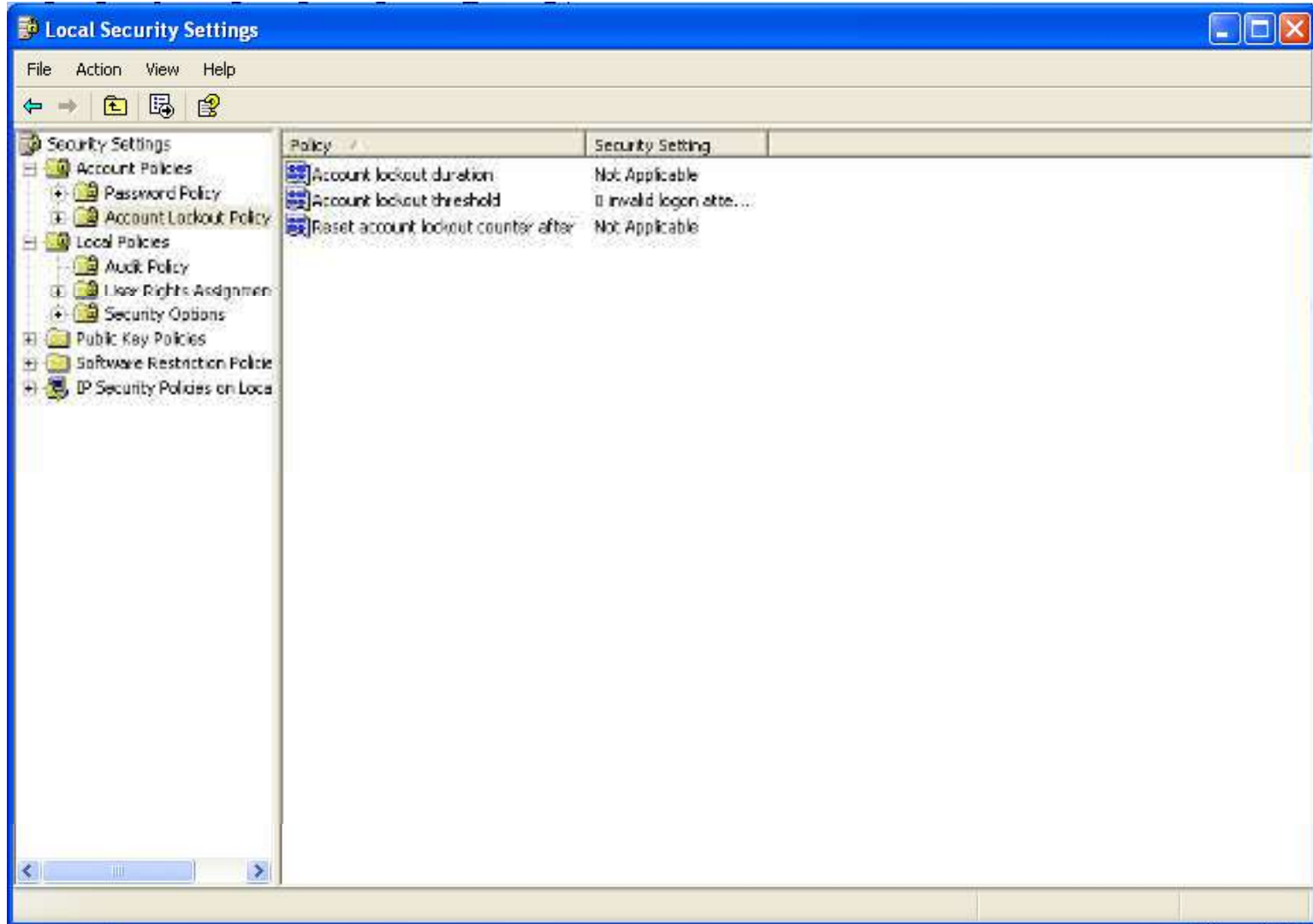
The operating system can be set to disable the account after some number of unsuccessful attempts

Account lockout policy is responsible for taking necessary action for this threshold

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

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

Account Lockout Policy



Account Lockout Policy - *Policies*

1

- **Account lockout duration**

2

- **Account lockout threshold**

3

- **Reset account lockout counter after**



Account Lockout Duration

This policy setting decides the time period of a locked-out account to be unlocked automatically. The time period is within a range of 1 to 99,999 minutes

Configure the value to **0**, if the locked-out account is should be unlocked manually by the administrator

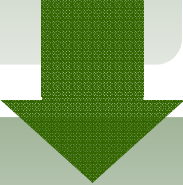
When an account lockout threshold is given, the **Account lockout duration** must be higher or similar to the reset time

The values for the Account lockout duration setting are:

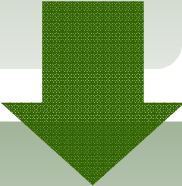
- **A value in minutes between 0 and 99,999**
- **Not Defined**

Account Lockout Duration - *Vulnerability*

When an attacker neglect the **Account lockout threshold** and tries to logon to a specific account, a Denial of service (DoS) situation is created



If **Account lockout threshold** settings can be configured to lock out an account after some number of failed attempts



If the settings are configured to **0**, the administrator has to unlock it manually

Account Lockout Duration - *Countermeasure*

Configure the **Account lockout duration** setting to a suitable value

Configure the value to **0**, to remain the account locked until an administrator manually unlocks it

When the settings are configured to a non-zero value. The automated password guessing attempts should wait for a specific interval

Automated guessing of a password can be made complex or useless, when **Account lockout threshold** settings are used

Account Lockout Duration - *Potential Impact*

The policy settings can be set to 'never automatically unlock an account'. This setting might maximize the help desk calls for unlocking an account



Account Lockout Duration



Account Lockout Threshold

This policy setting concludes the count of failed logon trails which caused an account to be locked out

To use a locked out account, the administrator has to reset the account or lockout duration should expire

- The failed logon attempts can be up to 999
- Setting the value to 0 indicates that the account will never be locked

If **Account lockout threshold** is given, then the **Account lockout duration** should be greater than or equal to the reset time

Account Lockout Threshold

Unsuccessful password attempts which are locked through either CTRL+ALT+DELETE or password-protected screen savers do not count as failed logon attempts

Unless the policy setting **Interactive logon: Require Domain Controller authentication to unlock workstation** is enabled

The values for the Account lockout threshold setting are:

- A value between 0 and 999
- Not Defined

Account Lockout Threshold - *Vulnerability*

If a limit is set on the number of failed logon's performed, the password attackers will not perform any automated method on the account

Attacks



If an account lockout threshold is configured a DoS attack would be carried out.

Programmatically attempt a series of password attacks.

Account Lockout Threshold - *Countermeasure*

Vulnerabilities can occur in two situations

- When this value is configured
- When this value is not configured

The two countermeasure options are:

- Configuring the **Account Lockout Threshold** setting to **0**. With these configuration the accounts will not be locked out, and will prevent a DoS attack.
- As this configuration will not stop brute force attack, it should be chosen only if the below criteria's are met:
 - All users must have critical passwords of 8 or more characters
 - A mechanism should be assigned to alert the administrator when a failed logon occurs

Account Lockout Threshold – *Countermeasure* (Cont'd)

If the earlier criteria cannot be met, configure **Account Lockout Threshold** settings to a greater value, by which the user can wrongly type the value various times

This value will be such that brute force password attack will still lock the account, but DoS attack cannot be prevented



Account Lockout Threshold - *Potential Impact*

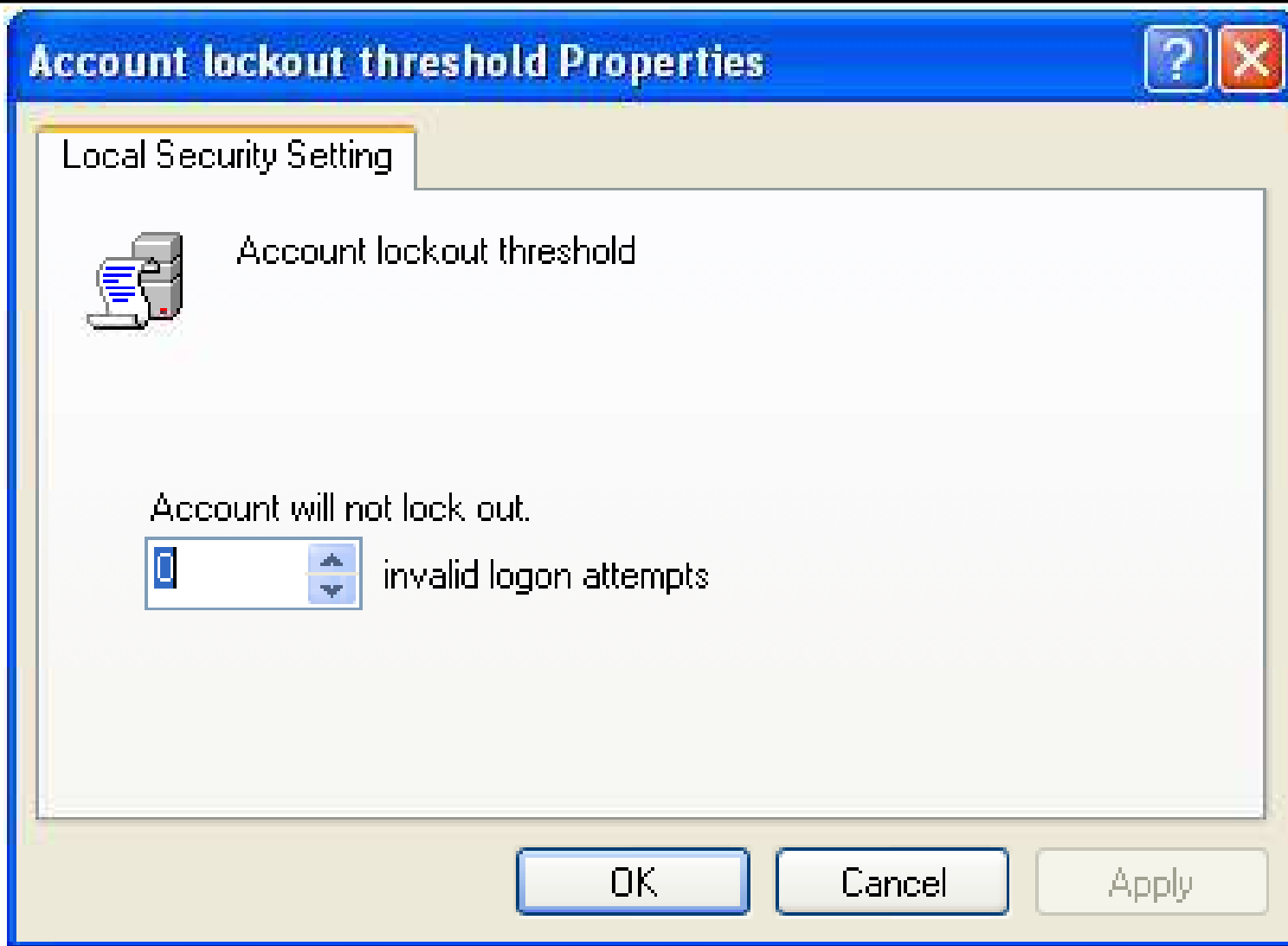
To use a locked out account, the administrator has to reset the account or lockout duration should expire

Long passwords may cause account lockouts when the passwords are typed wrong by mistake which will maximize the help desk calls

Configure the **Account Lockout Threshold to 0**. A mechanism should be assigned to alert the administrator when a failed logon occurs



Account Lockout Threshold



Reset Account Lockout Counter After

This policy is set to keep track on the number of minutes that should pass before resetting the counters which hold the information on number of failed logon to **0**

The **Account lockout threshold** reset time should be less than or equal to the **Account lockout duration** setting configuration

The values for the Reset account lockout counter after setting are:

- **A number of minutes between 1 and 99,999**
- **Not Defined**

Reset Account Lockout Counter After

Vulnerability

- By typing a password multiple times the user can lock their account unintentionally.
- To minimize the possibility of unintended lockouts, the **Reset account lockout counter after** setting find out the number of minutes that should pass before resetting the counters which hold the information on number of failed logon to **0**

Countermeasure

- Configure the **Reset account lockout counter after** setting to **30 minutes**

Potential Impact

- A DoS attack take place, if the policy is not configured (or) if the configured value has a long interval
- If **Reset account lockout counter after** is not set administrator has to unlock the account manually
- The value set for this policy, will keep the Locked user's account blocked for that amount of time
- Incase an account is locked. The user's must be informed about this value such that they can wait for that period of time, before accessing the account

Reset Account Lockout Counter After



Kerberos Policy

If the lifetime of Kerberos tickets is decreased, the risk of a valid user's credentials being stolen and lucratively used by an attacker decreases. However, authorization overhead increases

Modification of Kerberos policy settings are not done in most environments

These are domain level policy settings; the configuration of the default values is done at Default Domain Policy GPO in a default installation of a Windows 2000 or Windows Server 2003 Active Directory domain.

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

- **Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy**

Kerberos Policy - *Policies*

Enforce user logon restrictions

Maximum lifetime for service ticket

Maximum lifetime for user ticket

Maximum lifetime for user ticket renewal

Maximum tolerance for computer clock synchronization

Enforce User Logon Restrictions

This policy concludes that the Key Distribution Center (KDC) legalizes all requests for a session ticket with the user privileges policy

Validation of the requests for the session ticket kept optional, as the process may degrade the network access

The values for the Enforce user logon restrictions setting are:

- Enabled
- Disabled
- Not Defined

Enforce User Logon Restrictions

Vulnerability

- Even if this policy is disabled, the users might get the session tickets for the services that they are unauthorized for, as the authorization is removed after they login

Countermeasure

- Configure the **Enforce user logon restrictions** setting to **Enabled**

Potential Impact

- None

Maximum Lifetime for Service Ticket

The maximum amount of time (minutes) granted for a session ticket is verified by this policy settings. The value can be set to 10 min's or greater and it should be less than or equal to the **Maximum lifetime for user ticket** setting

If a session ticket is expired a new ticket has to be requested for KDC

Once the connection is set, the ticket is not valid. Session tickets are necessary for a new connection. If the ticket expires during the session there will be no interruption in the process

The values for the Maximum lifetime for service ticket setting are:

- A user-defined value in minutes between 10 and 99,999. If you configure this policy setting to 0, service tickets do not expire.
- Not Defined.

Maximum Lifetime for Service Ticket

Vulnerability

- A user can access network resources outside of their logon hours, if a greater value is set to **Maximum lifetime for service ticket** setting
- Users who are deactivated can also access the network with a valid service tickets issued before deactivating there accounts

Countermeasure

- Configure the **Maximum lifetime for service ticket** setting to **600 minutes**

Potential Impact

- None

Maximum Lifetime for User Ticket

The maximum time (in hours) of a user's ticket-granting ticket (TGT) is concluded by this policy

If a users TGT expires a new one should be requested (or) old one must be renewed

The values for the Maximum lifetime for user ticket setting are:

- **A user-defined value in hours between 0 and 99,999. The default value is 10 hours**
- **Not Defined**

Vulnerability

- A user can access network resources outside of their logon hours, if a greater value is set to Maximum lifetime for service ticket setting
- Users who are deactivated can also access the network with a valid service tickets issued before deactivating there accounts

Countermeasure

- Configure the **Maximum lifetime for user ticket** setting to 10 hours

Potential Impact

- None

Maximum Lifetime for User Ticket Renewal

This policy is used to set the time period (days), of renewing user's ticket-granting ticket (TGT)

The values for the Maximum lifetime for user ticket renewal are:

- A value in minutes between 0 and 99,999
- Not Defined



Maximum Lifetime for User Ticket Renewal

Vulnerability

- If this value is too high, it is possible to renew a old user ticket

Countermeasure

- Configure the **Maximum lifetime for user ticket renewal** setting to **10080 minutes (7 days)**

Potential Impact

- None

Maximum Tolerance for Computer Clock Synchronization

The maximum time (minutes) difference between client and server computers which is allowed by Kerberos protocol is determined by this policy

The values for Maximum tolerance for computer clock synchronization are:

- A value in minutes between 1 and 99,999
- Not Defined



Maximum Tolerance for Computer Clock Synchronization

Vulnerability

- Kerberos authentication protocol uses time stamps, for synchronizing the clocks of client and server computers
- This policy is used to set up the maximum elapsed time to complete the Kerberos negotiation
- Time stamp is necessary to calculate the elapsed time

Countermeasure

- Configure the **Maximum tolerance for computer clock synchronization** setting to **5 minutes**

Potential Impact

- None

Audit log is used to record the user actions, these actions are recorded as an entry

Both successful and failed entries are recorded

If there are any changes made in a network, the security system will also change, as the state of the operating system and applications on a computer are dynamic. If the made changes are not reset the security system will no longer be effective

Regular re-view of the security settings, helps the admin to follow security measures

Audit Policy (Cont'd)

The information acquired by this, is used to concentrate on security measures. The information helps to find out security flaws in the computer

The security audits are necessary to know a security breach

Failure log details are considerably important than successful as they allow to errors in the settings

Separate event logs are maintained for applications and system events

Audit Policy (Cont'd)

A Group policies event log contain information on application, security and security event log, as maximum log size, access rights for each log, and retention settings and methods

Before any audit processes are implemented, an organization should determine how they will collect, organize, and analyze the data

There is little value in large volumes of audit data if there is no underlying plan to exploit it. Also, audit settings can affect computer performance

Audit Policy (Cont'd)

The effect of a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server

Therefore, you should perform some performance tests before you deploy new audit settings in your production environment

A detailed plan should be set on how to collect, organize, and analyze the data before an audit process

As the audit settings shouldn't affect the server performance

Audit Policy (Cont'd)

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

- **Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy**

In all the audit settings vulnerabilities, countermeasures, and potential impacts are similar

The options for each of the audit settings are:

- **Success.** An audit entry is generated when the requested action succeeds
- **Failure.** An audit entry is generated when the requested action fails
- **No Auditing.** No audit entry is generated for the associated action

Vulnerability

- If audit setting is not configured it is difficult to find information on security process
- If the setting are configured the security event log be full of useless stuff
- Large number of objects in the audit settings may minimize the computer performance

Countermeasure

- To sense an unauthorized action audit policy settings are must

Potential Impact

- A legal obligation may be held with some industries, to log certain events and activities

Audit Account Logon Events

This policy setting is configured to state an audit success, audit failure or no audit

A success audit indicates that an attempt to login has succeeded

A Failure audits indicate a failed or false login attempt, this help in detecting intrusion detection

These setting create the possibility for a denial of service (DoS) attack. If **Audit: Shut down system immediately if unable to log security audits** setting is enabled, an attacker can force the computer to shut down by generating millions of logon failures

Audit Account Logon Events



Audit Account Management

This policy setting finds out either to audit each computer on logon or not.

Account management events

- A user account or group is created, changed, or deleted
- A user account is renamed, disabled, or enabled
- A password is set or changed

Configuring **Audit account management** setting:

- Enable to set an audit for success and failure events

When an account management event fails failure event is generated

Audit Account Management



Audit Directory Service Access

Whether to audit user access an active directory service object associated with system access control list (SACL) or not, is conclude by this policy. SACL is list of users and groups to perform audit on the network

By configuring **Audit directory service access** setting to enable, you actually mean to use the information that is generated

Audit Directory Service Access



Audit Logon Events

This policy finds out whether to audit each occasion of user login, logoff (or) only on the computer that records the audit event

If a successful logon event on a domain is recorded, workstation logon do not produce logon audits

Account logon events are created wherever the account lives

Logon events are created wherever the logon attempt occurs

Configure **Audit logon events** setting, to indicate audit successes, audit failures, or not audit event

- The configuration also creates a DoS condition

Audit Logon Events



Audit Object Access

This policy concludes whether or not to access an object by a user

Configure **Audit object access** setting, audit successes, audit failures, or not audit

If failure auditing is enabled and SACL on the file, the event will be recorded, when ever it happens

Enabling metabase object auditing:

- Enable **Audit object access** on the target computer
- Set SACLs on metabase objects to audit

On configuring **Audit object access** policy setting and SACLs on objects. Large volume of entries can be created in the Security logs

Audit Object Access



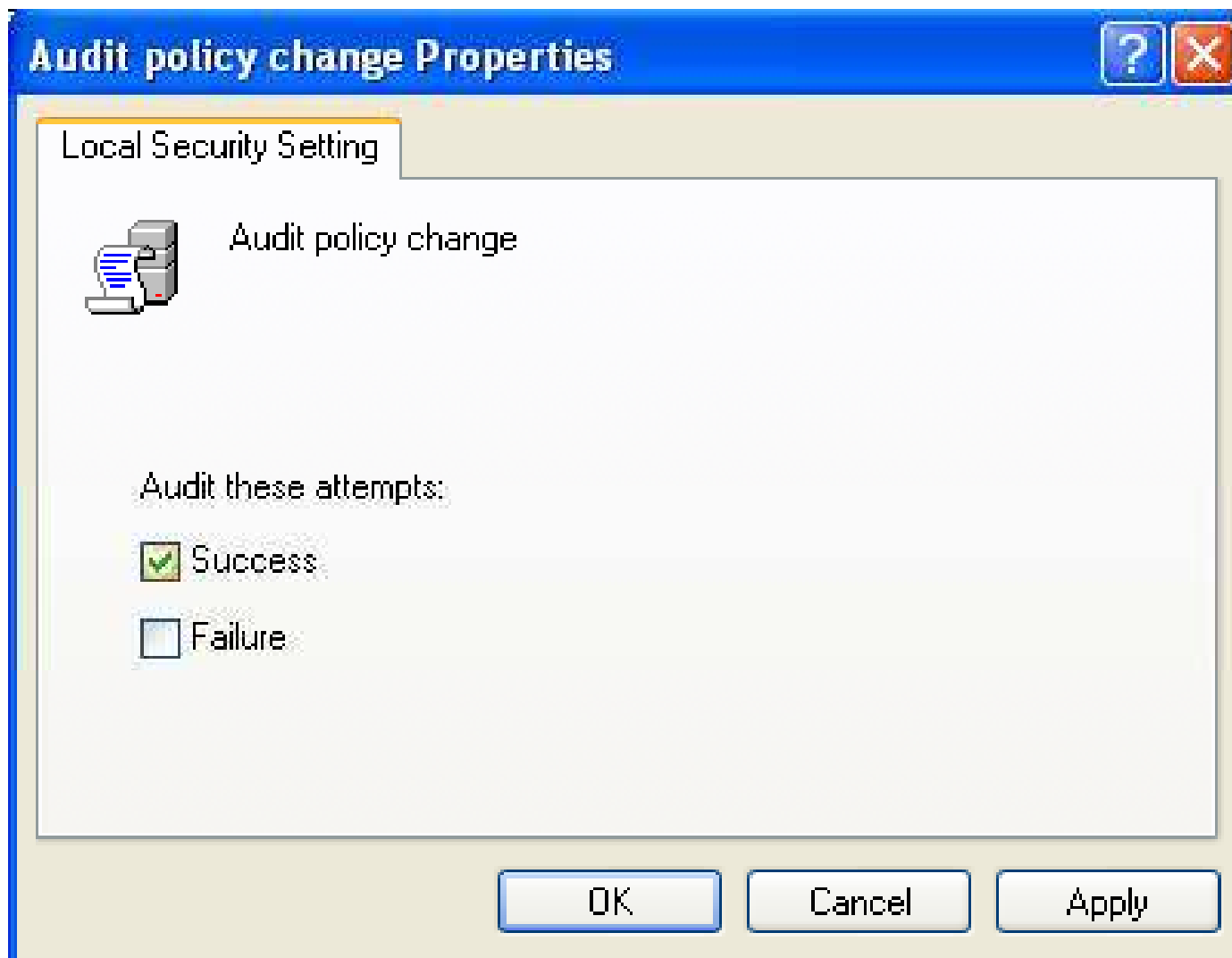
Audit Policy Change

To conclude every modification to user rights assignment policies, Windows Firewall policies, Audit policies, or trust policies configure this setting

This policy specifies to audit successes, failures, or not audit. This helps in finding out the successful modifications done in a domain or computer

Configuration changes in Windows Firewall component are enabled when this policy setting are enabled for Windows XP with SP2 and Windows Server 2003 with SP1

Audit Policy Change



Audit Privilege Use

This policy is used to conclude an audit a user for his each instance, when he put into effect his rights

On configuring **Audit privilege use** setting, audits successes, failures, or no audit

This policy can generate large events, which might be complex to sort out

This policy should be enabled, with a plan to use the evolved output

User rights which are not generated for audit event (Success or failure audit)

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate security audits
- Backup files and directories
- Restore files and directories

Audit Privilege Use



Audit Process Tracking

Detailed tracking information such as program activation, process exit, handle duplication, and indirect object access can be audited by configuring this policy

On configuring **Audit process tracking** setting, audits successes, failures, or no audit

In Windows XP with SP2 and Windows Server 2003 with SP1, when this policy is enabled, it will log information on the operating mode and status of the Windows Firewall component

This policy generates large volume of events. General value of this policy is **No Auditing**

Audit Process Tracking



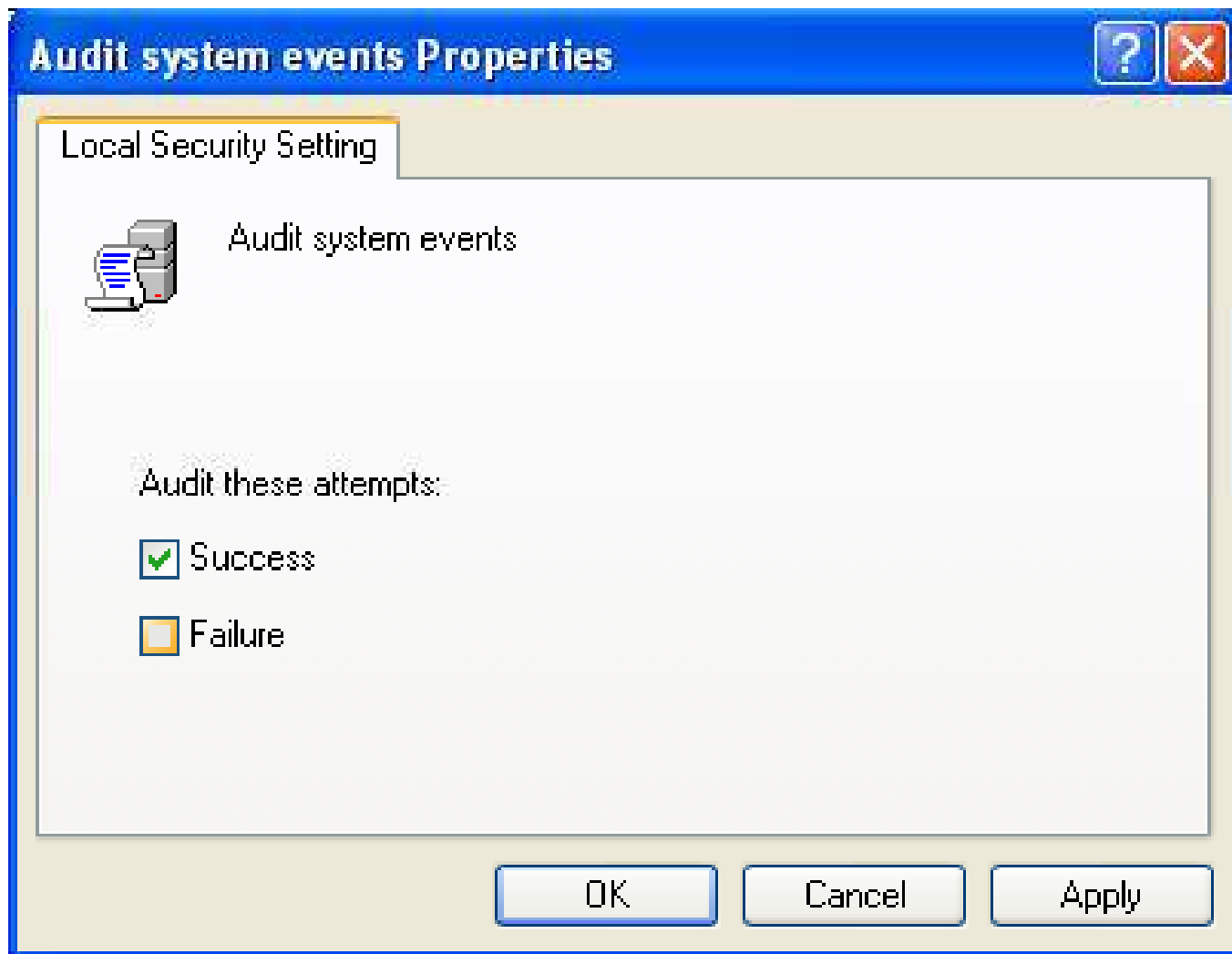
Audit System Events

This policy concludes on auditing when user restarts or shutdown the computer, (Or) When an event affecting system security or security log

Audit system event generate audits successes, failures, or no audit

This policy should be set **Enabled** on all computers in the network

Audit System Events



User Rights

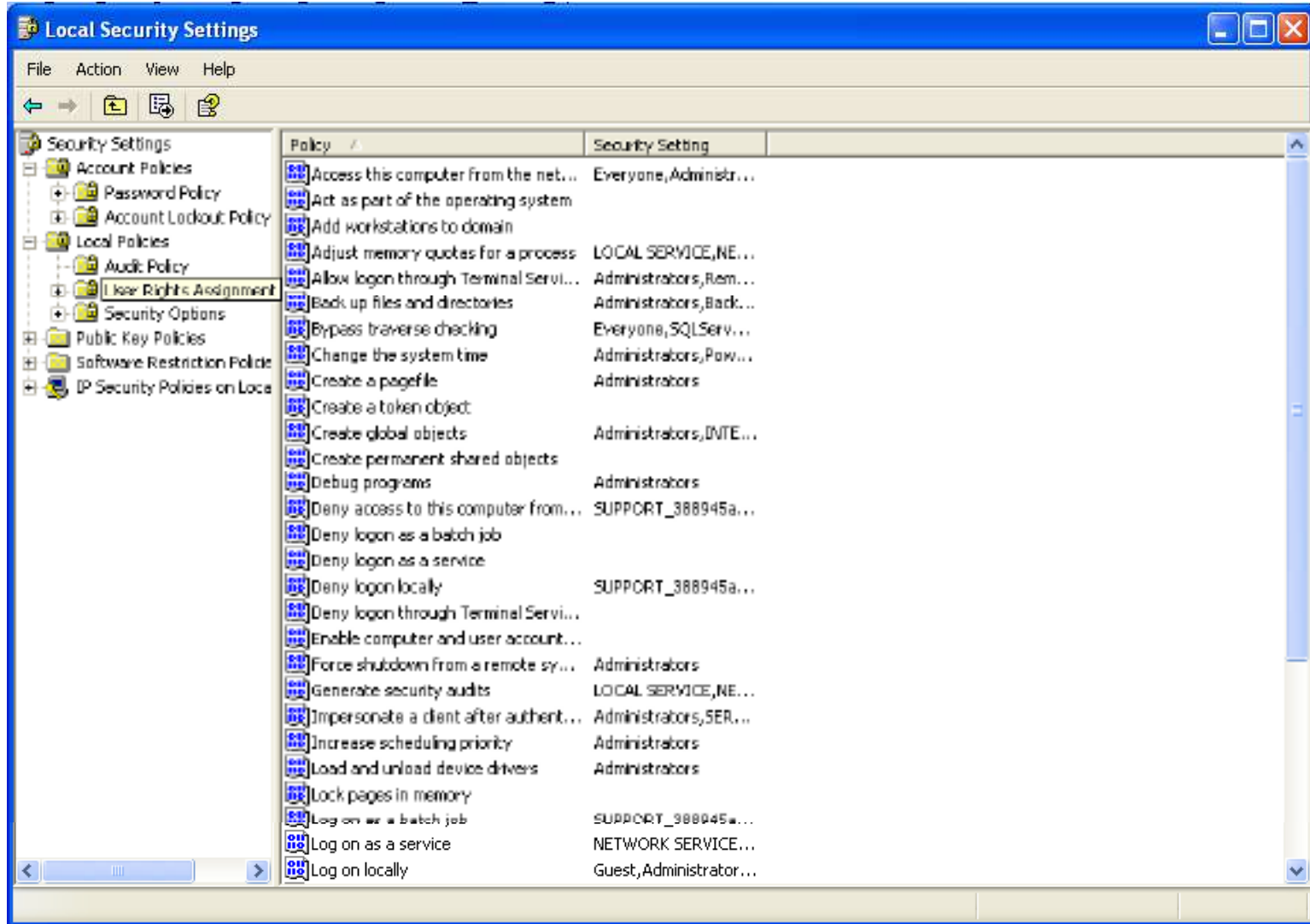
User rights are to permit the user to perform a specific task on the domain; they include

- Logon rights – Only authorized personnel have to log on to the domain. (Example: Logging on to local computer)
- Privileges – Used to control user access. (Example: Shutting down the PC)

Individual and group user rights are set by the administrator.

In a Group Policy Object Editor configure the **User Rights Assignment Settings** at:

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



Access this Computer from the Network

This policy concludes that a user can connect to a computer from the network

Various network protocols as Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+) require this ability

The values for the Access this computer from the network setting are:

- A user-defined list of accounts
- Not Defined

Access this Computer from the Network

Vulnerability

- User's having privileges to resources on the other computers can access them through the network
- A user must have **Access this computer from the network** user right is necessary to share printers and shared folders

Countermeasure

- This right should be limited to only those users who should necessarily access the server

Access this Computer from the Network

Potential Impact

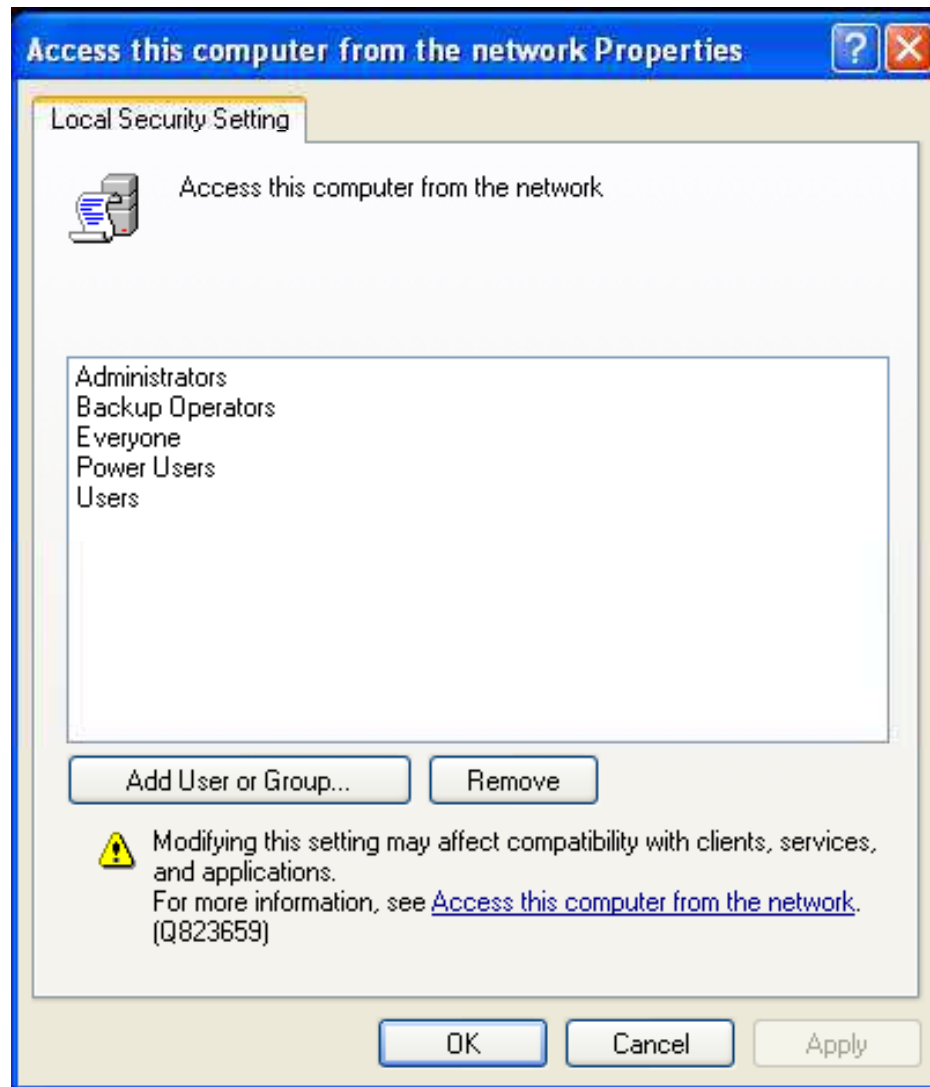
If this right is blocked on domain controller, the users will not be allowed to logon to the domain or use network resources

If the right is removed on the member server, user will be restricted to connect to the server

If any additional (optional) components are installed, the users needing these components should be given the rights to access them



Access this Computer from the Network



Act as Part of the Operating System

This policy setting is used to decide that a process can use the identity of any user and access the resources authorized to the user

These user rights are given to low level users

The values for the **Act as part of the operating system** setting are:

- A user-defined list of accounts
- Not Defined



Act as Part of the Operating System

Vulnerability

- This user right is very authoritative; it provides complete control over the computer

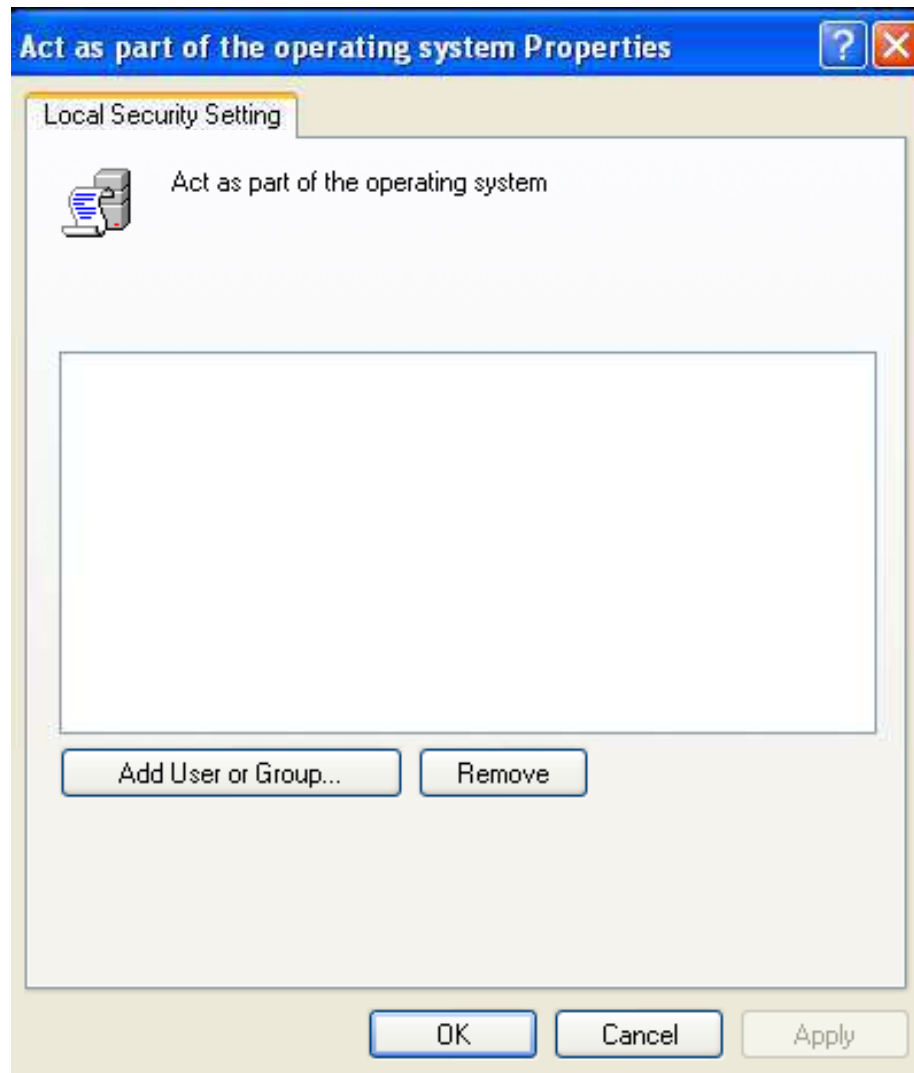
Countermeasure

- This user right should be assigned to only few accounts. Even administrators are not given these rights
- To assign this user right
- Configure the service to logon with the local system account (It has an inherent privilege)
- Don't create a separate account for assigning the user right

Potential Impact

- The impact provided should be very low as this user right is needed infrequently by accounts other than local system account

Act as Part of the Operating System



Add Workstations to Domain

This policy finds out that a user can add a computer to a specific domain or not. It must be assigned to one domain controller to make the policy condition affective. The limit on the number of workstations to add is up to 10

To add a computer to a domain the user must have permissions for **Create Computer Object**

The users with permission can add unlimited computers to the domain

The values for the Add workstations to domain setting are:

- A user-defined list of accounts
- Not Defined

Add Workstations to Domain

Vulnerability

- This right has a moderate vulnerability, which provides the right to add a computer to the domain configured to violate organizational security policy
- If a user with this right does not have an administrator privileges he can install windows and add to a domain, and can logon with that account and add them selves to the administrator group (local)

Countermeasure

- By configuring this setting only authorized members are allowed to add computers to the domain

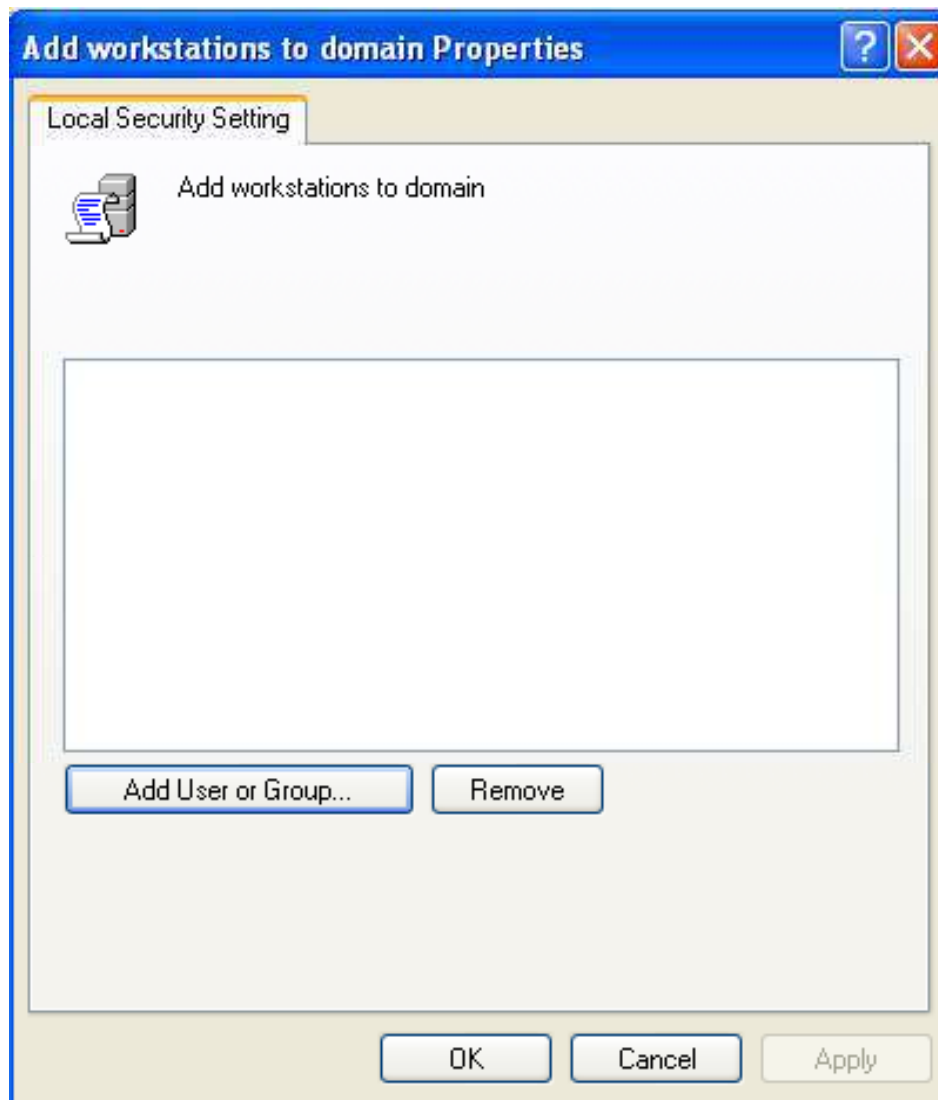
Add Workstations to Domain

Potential Impact

- This countermeasure won't be having any impact on the security policy, if the users are not allowed to configure there own computers and added them to the domain.
- In an organization if a user is allowed to configure there own computer, the organization has to set a process as a countermeasure.



Add Workstations to Domain



Adjust Memory Quotas for a Process

User concludes on allocating the maximum amount of memory available to a process. This is needed to tune computers.

This could even be used to start a launch denial of service (DoS) attack.

The values for the **Adjust memory quotas for a process** setting are:

- A user-defined list of accounts
- Not Defined



Adjust Memory Quotas for a Process

Vulnerability

- A user with this privilege can minimize the amount of memory available a process, which can lead to slowing down or failing an business network application

Countermeasure

- This privilege must be given only to limited personnel's as application administrator or domain administrators

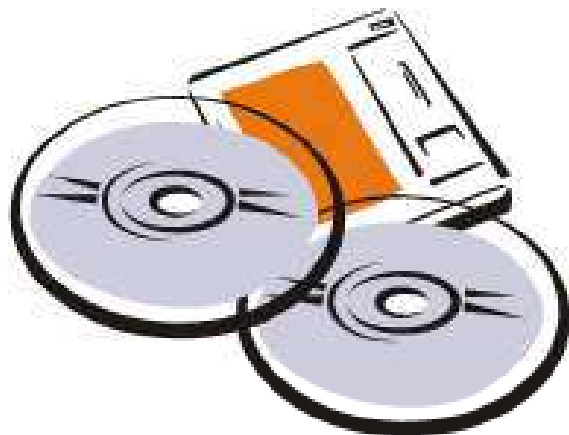
Potential Impact

- Organizations which are not following rule of limited privileges to the user, will find it difficult to follow this measure

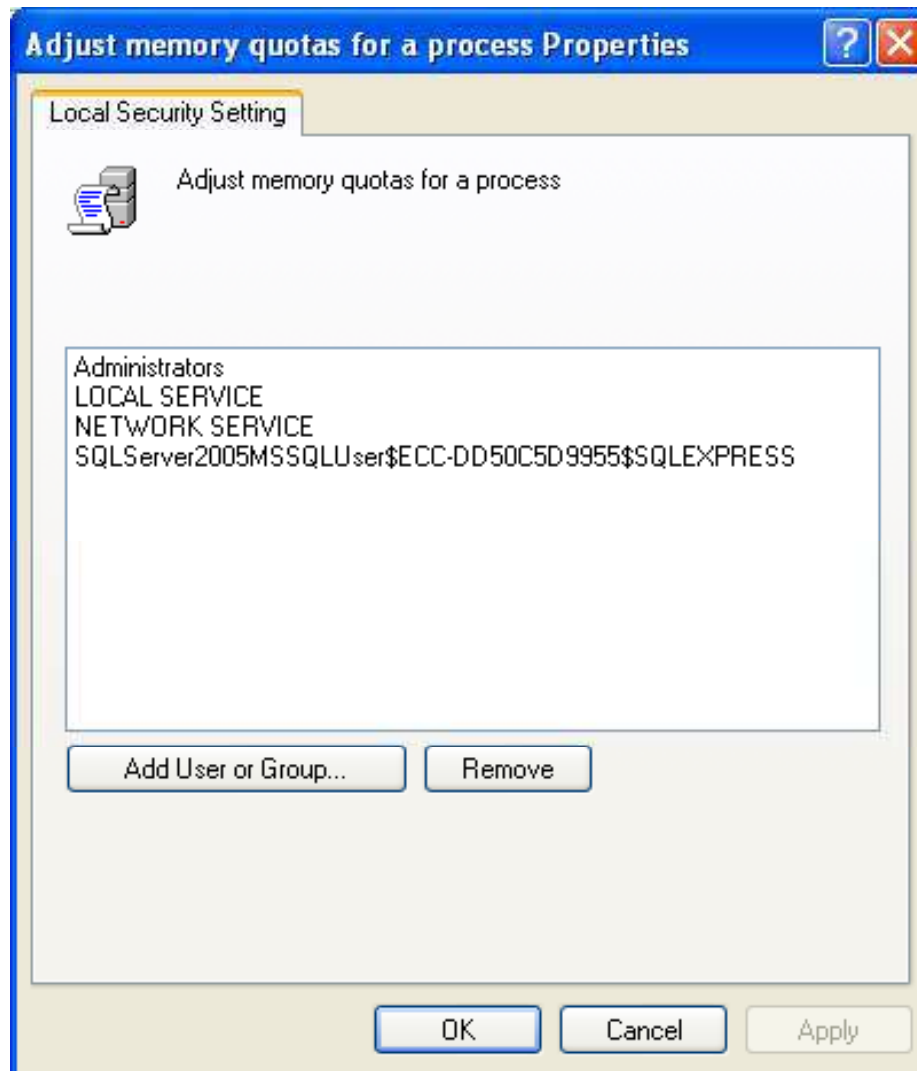
Adjust Memory Quotas for a Process

This privilege has to be assigned if the user is using optional components ASP.NET or IIS

In IIS this privilege has to be given to IWAM_<ComputerName>, Network Service, and Service accounts



Adjust Memory Quotas for a Process



Allow Log On Locally

This policy is used to start a interactive session on the computer

If **Allow logon through Terminal Services** right is given a remote interactive session can be started on the computer

The values for the **Allow log on locally** setting are:

- A user-defined list of accounts
- Not Defined



Allow Log On Locally

Vulnerability

- This policy provides the right to logon to the console computer. AN unauthorized user with this right can logon and execute some malicious code

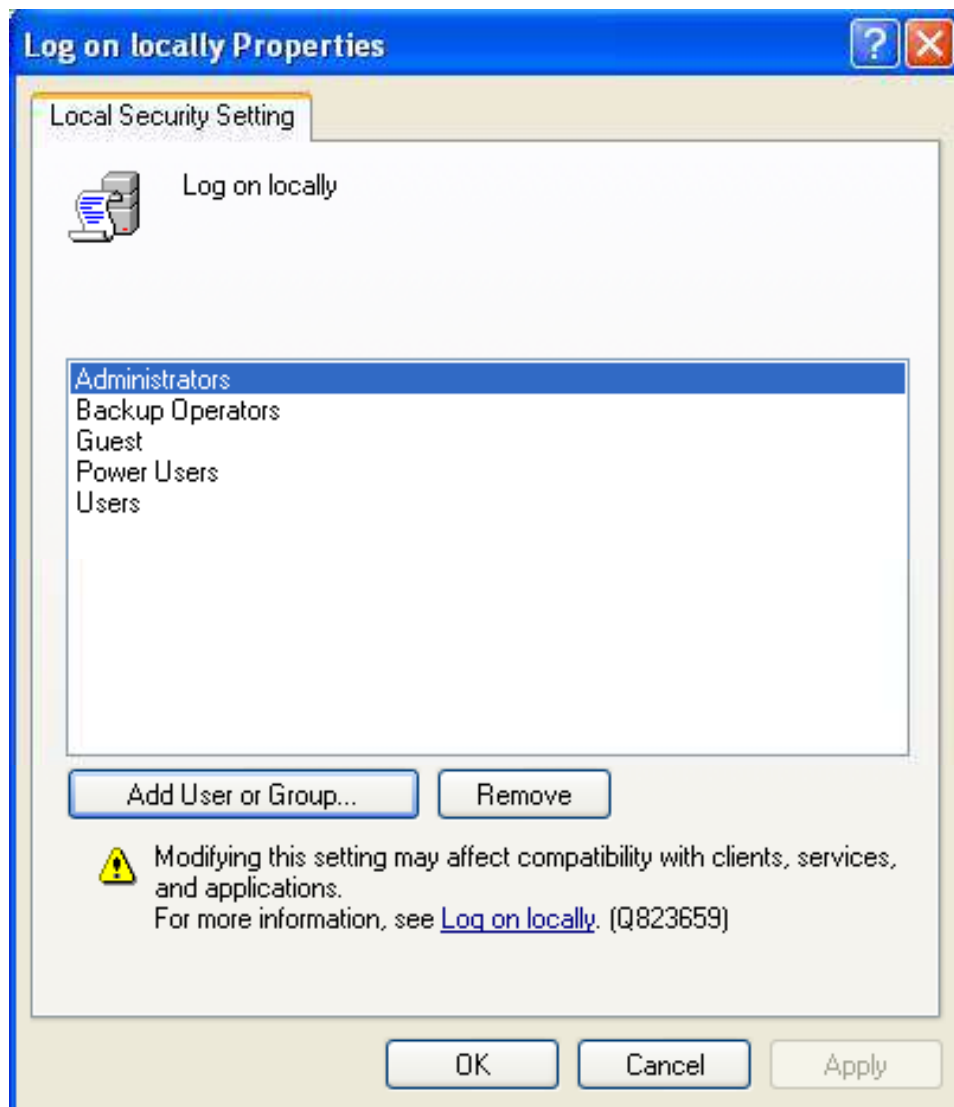
Countermeasure

- Give the right **Allow log on locally** to the **Administrators** group over domain controllers. On end-user computers allow this right to user groups

Potential Impact

- With a limitation on the default groups, it is possible to keep an eye on the allotted administrative privileges
- User with additional components as ASP.NET and IIS need this policy to be set

Allow Log On Locally



Allow Log On through Terminal Services

Allow log on through Terminal Services is used to figure out, whether a user can logon to another computer through a remote desktop connection

To keep a control on the personnel's opening a remote desktop connection is to add/remove them from **Remote Desktop Users** group

The values for the Allow log on through Terminal Services setting are:

- A user-defined list of accounts
- Not Defined



Allow Log On through Terminal Services

Vulnerability

- If this right is not limited to legitimate personnel's, unauthorized personnel's can logon to the computer console and execute malicious code.

Countermeasure

- Assign the **Allow log on through Terminal Services** user right to the **Administrators** group on domain controllers.
- For server roles and end-user computers, also add the **Remote Desktop Users** group.

Allow Log On through Terminal Services

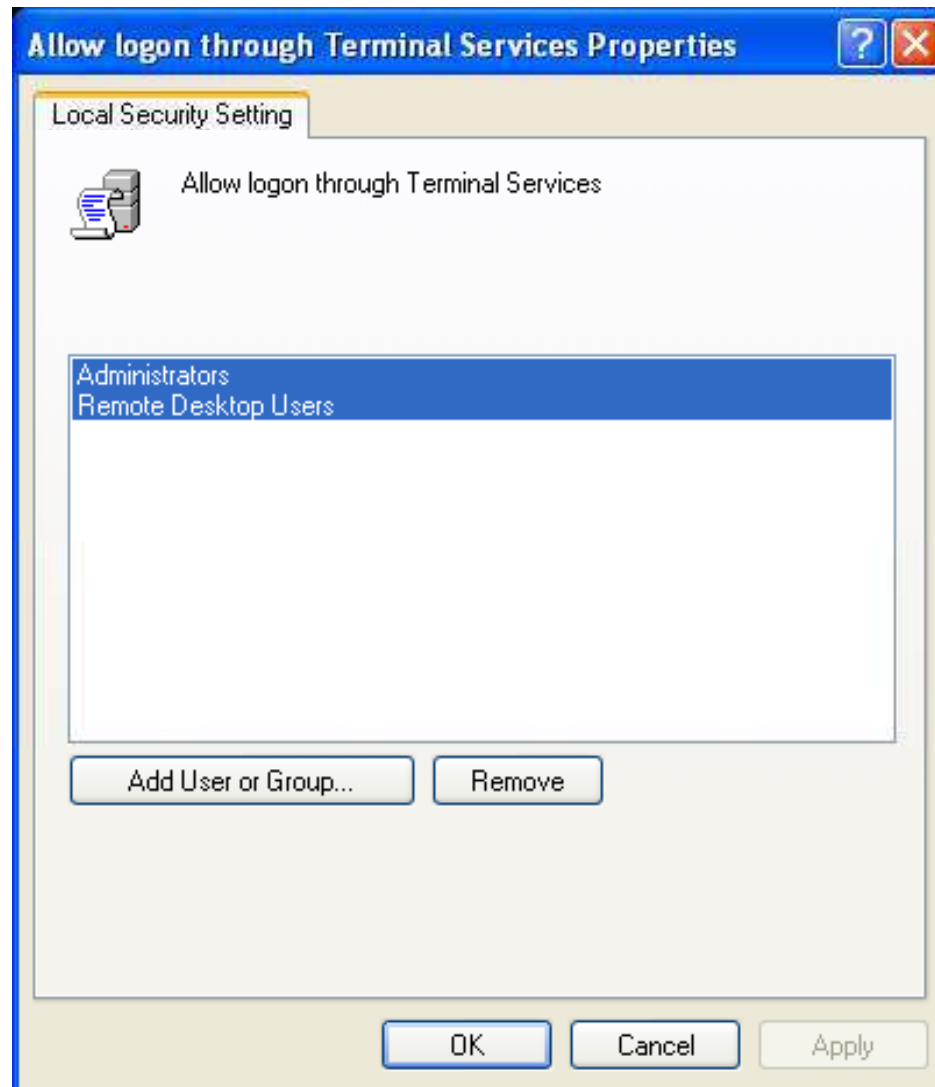
Give **Deny Logon Through Terminal Services** right to groups as **Account Operators, Server Operators, and Guests**

As administrators may also be in **Deny Logon Through Terminal Services** group do not block there right

Potential Impact

- Confirm that hand over activities will not be adversely affected

Allow Log On through Terminal Services



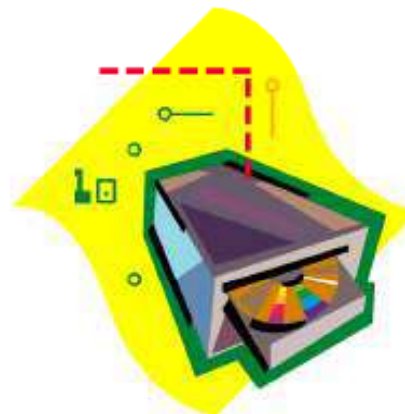
Back Up Files and Directories

This policy is used to conclude on avoiding file and directory permissions to take a back up of the computer

This right exists, when the application makes an NTFS backup, through a backup utility such as NTBACKUP.EXE

The values for the Back up files and directories setting are:

- A user-defined list of accounts
- Not Defined



Back Up Files and Directories

Vulnerability

- Once the backup is taken the data can be moved to a non-domain computer, with administrative privileges.
- After restoring the data they can view any unencrypted data in the backup

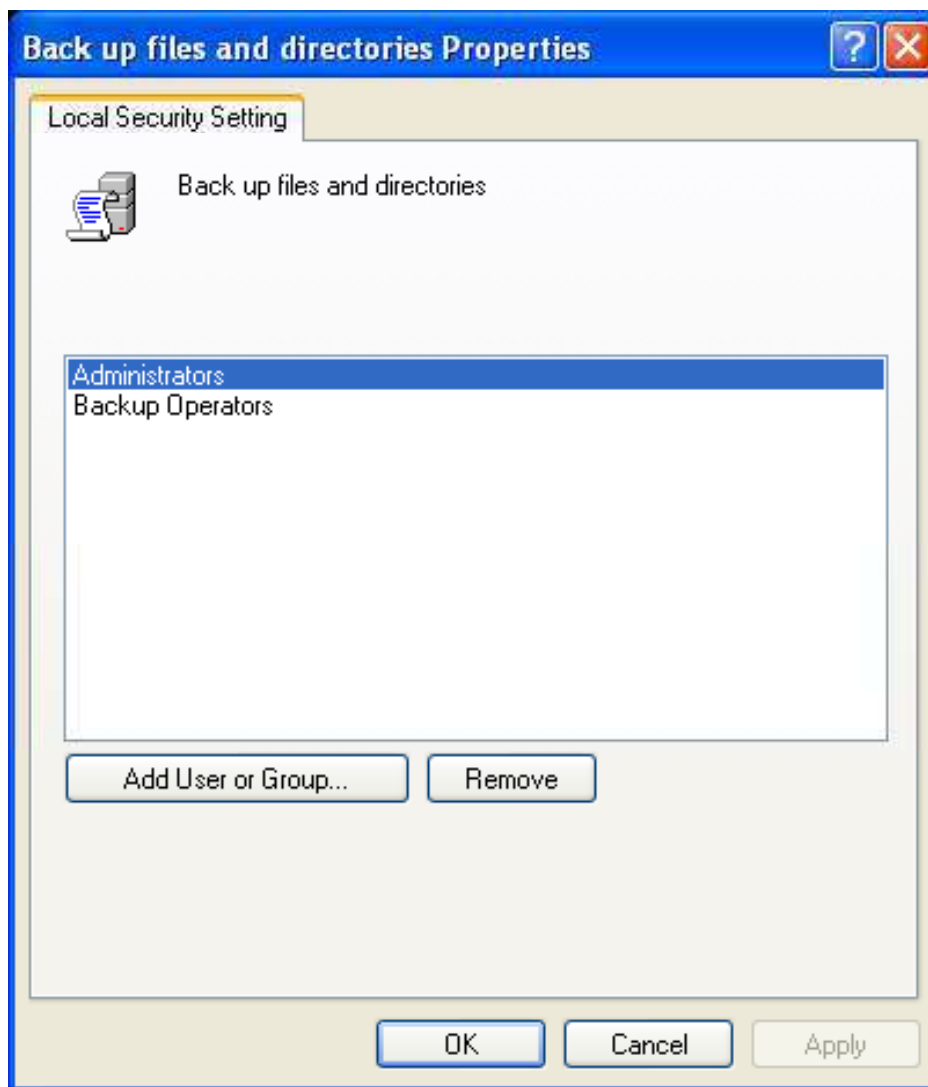
Countermeasure

- This right has to be given to people who need to perform this operation in a day-to-day job
- If any software is used for taking backup using some service account then these account require the right

Potential Impact

- If any changes in the membership of the group are made, it has to make sure that the authorized personnel's are able to perform the backup task properly

Back Up Files and Directories



Bypass Traverse Checking

This policy concludes checking for permissions on the folders that are passed through “Traverse Folder”. As per the right user cannot list the folder contents but can traverse it

The values for the Bypass traverse checking setting are:

- A user-defined list of accounts
- Not Defined



Bypass Traverse Checking

Vulnerability

- By default this right is set to bypass traverse checking
- The administrator should have a keen understanding about the rights while assigning to the user

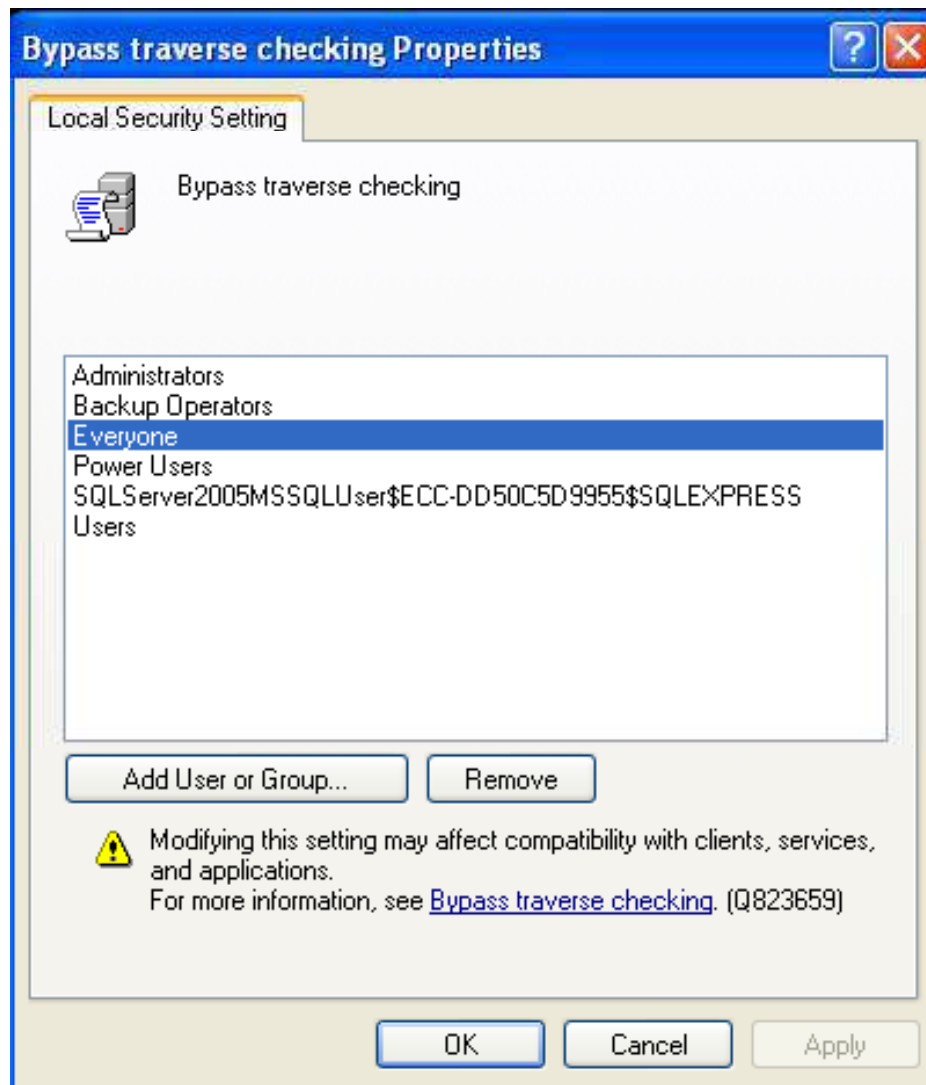
Countermeasure

- Organizations remove the **Everyone** group (or) **Users** group from the **Bypass traverse checking** user right
- A control should be made on traversal assignments to protect the sensitive information

Potential Impact

- In Windows and many other applications **Bypass traverse checking** user right are assigned by default. So, the administrator must check the operations before making the changes
- The IIS and ASP.NET component users may need this user right

Bypass Traverse Checking



Change the System Time

This policy allows the user to change the system clock (internal). Changing Time zone and display settings of the system time doesn't require this policy setting

The values for the Change the system time setting are:

- A user-defined list of accounts
- Not Defined



Change the System Time

Vulnerability

Kerberos need requestor's and authenticator's clocks synchronized

Several problems caused when system time is changed by the users.

An attacker may unable a Kerberos ticket by changing the system time.



Time stamps on the event log could be inaccurate.

Time stamps on files and folders could be incorrect.

Computers on the domain could not authenticate themselves.



Change the System Time

The Windows Time service synchronizes time with domain controllers by design in the following ways:

- A domain controller acts as a inbound time partner between client desktop computers and member servers
- The Primary Domain Controller (PDC) is the inbound time partner for all domain controllers
- PDC emulates follow a hierarchy of domains for selecting an inbound time partner.
- PDC emulator (route) must be configured from an external time server



If an attacker changes the system time and reconfigure it with an inaccurate time server, this vulnerability is more severe.

Change the System Time



Countermeasure

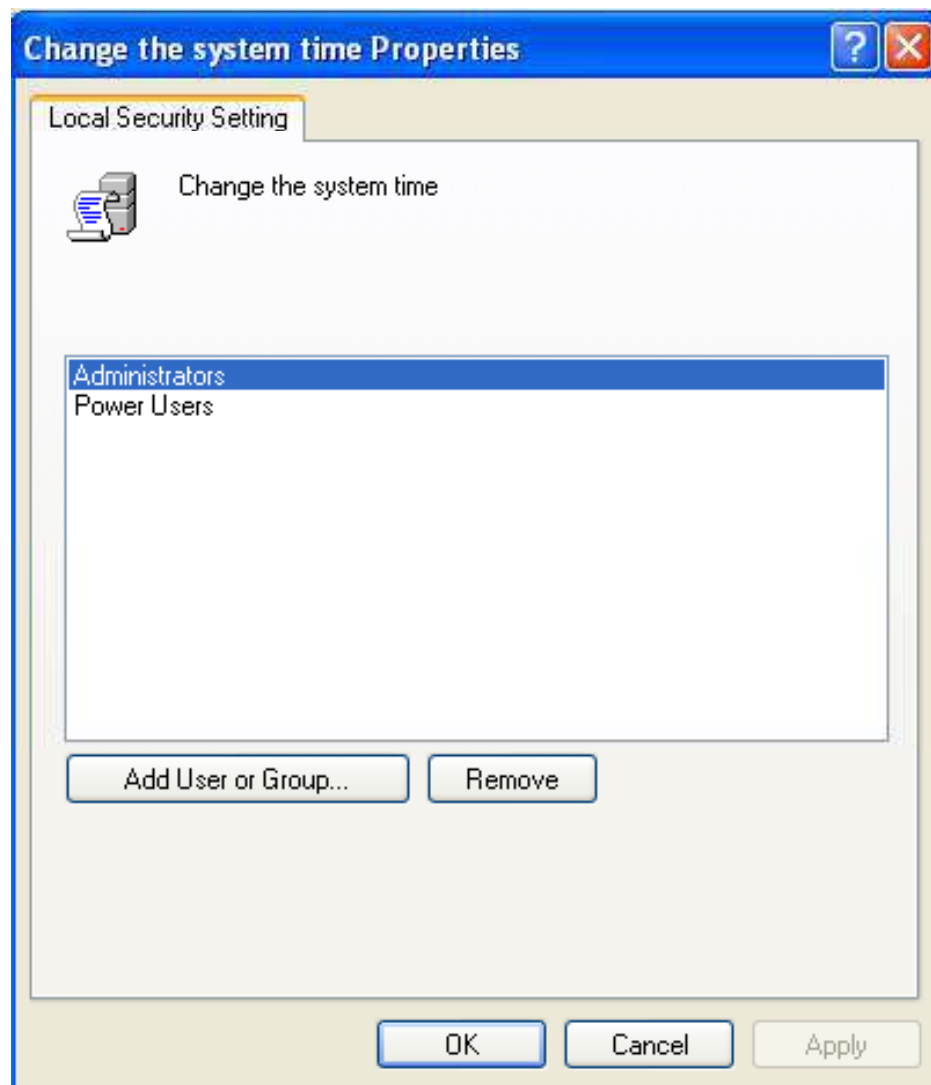
- This right should be given only to the members of the IT team who are legitimate to change the system time



Potential Impact

- Time synchronization should be automated for all computers in domain
- Individual systems should be synchronized by the help of external resources

Change the System Time



Create a Page File

This policy setting concludes that user can create and change the size of a page file

It is concluded by the policy that the page file size on a specific drive in the **Performance option** box placed under **Advanced** tab of the **System Property** dialog box can be created or changed

The values for the Create a page file setting are:

- A user-defined list of accounts
- Not Defined



Create a Page File

Vulnerability

- On changing the page file size to tremendously small (or) moving it to an extremely partitioned storage volume the user can reduce the system performance

Countermeasure

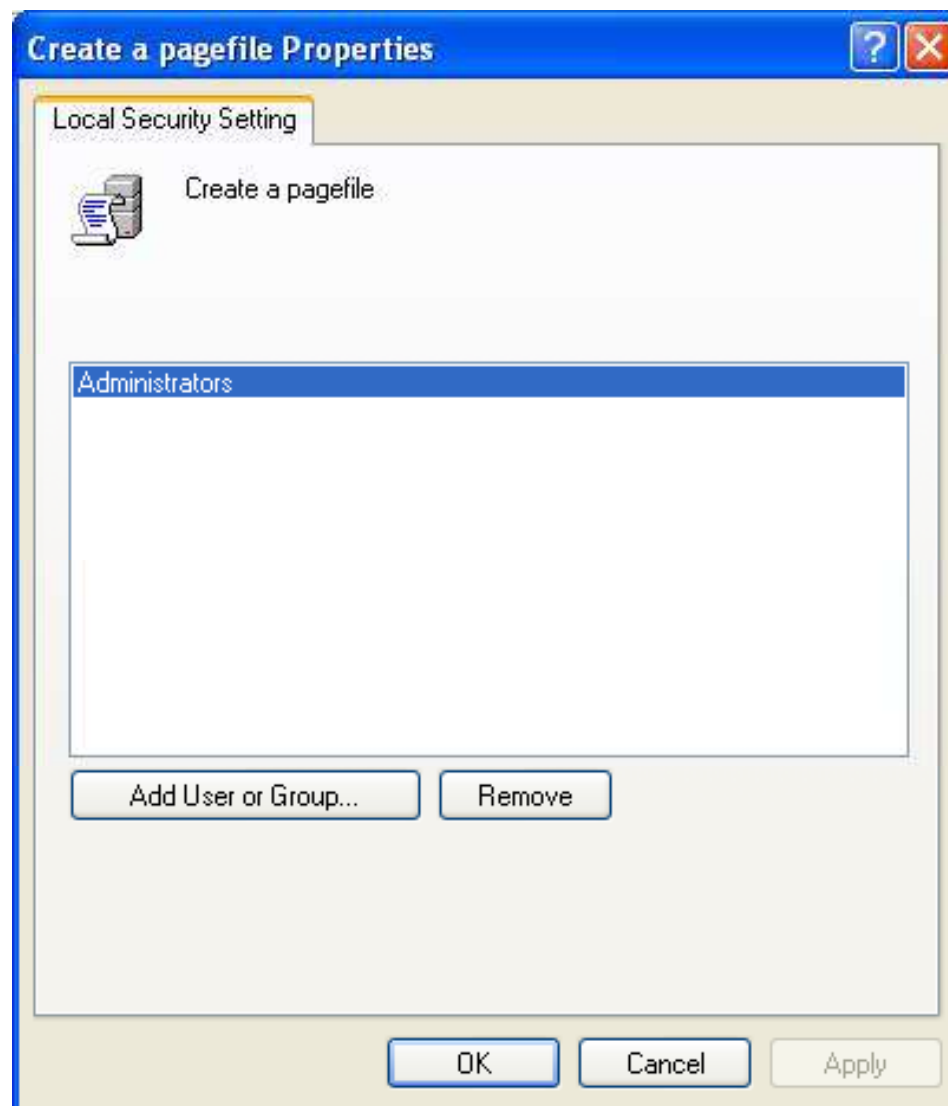
- This right should be given to the **Administrators** group only

Potential Impact

- None



Create a Page File



Create a Token Object

This policy decides a application can create a token or not. Used to gain access to local resources while using NtCreateToken() or a token creation object

The values for the Create a token object setting are:

- A user-defined list of accounts
- Not Defined



Create a Token Object

Vulnerability

- If a user connects to a local computer or remote computer on the network a token is created
- Access tokens specify the user privileges and his level
- A change in the privileges is at once recorded to the token but they are not effective until the user logon again
- A user with the ability to modify tokens can change his privileges or create a DoS condition



Create a Token Object

Countermeasure

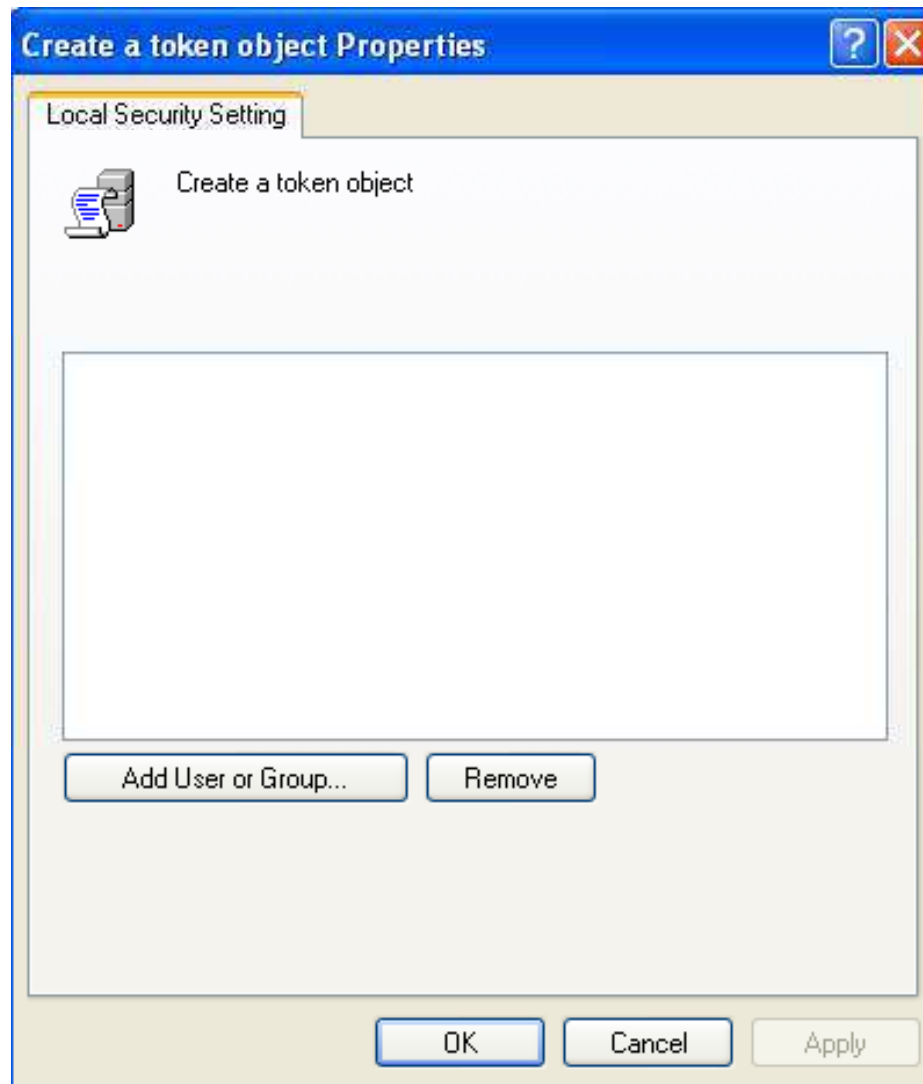
- Any process in necessity of a right should use a system account, which holds the right
- This right should not be assigned to a specific user

Potential Impact

- None



Create a Token Object



Create Global Objects

This policy checks that the user can create a global object which will be accessible by all sessions

The values for the Create global objects setting are:

- A user-defined list of accounts
- Not Defined



Create Global Objects

Vulnerability

- The created global object could have an effect on processes of other users. This could lead to application failure or data corruption.

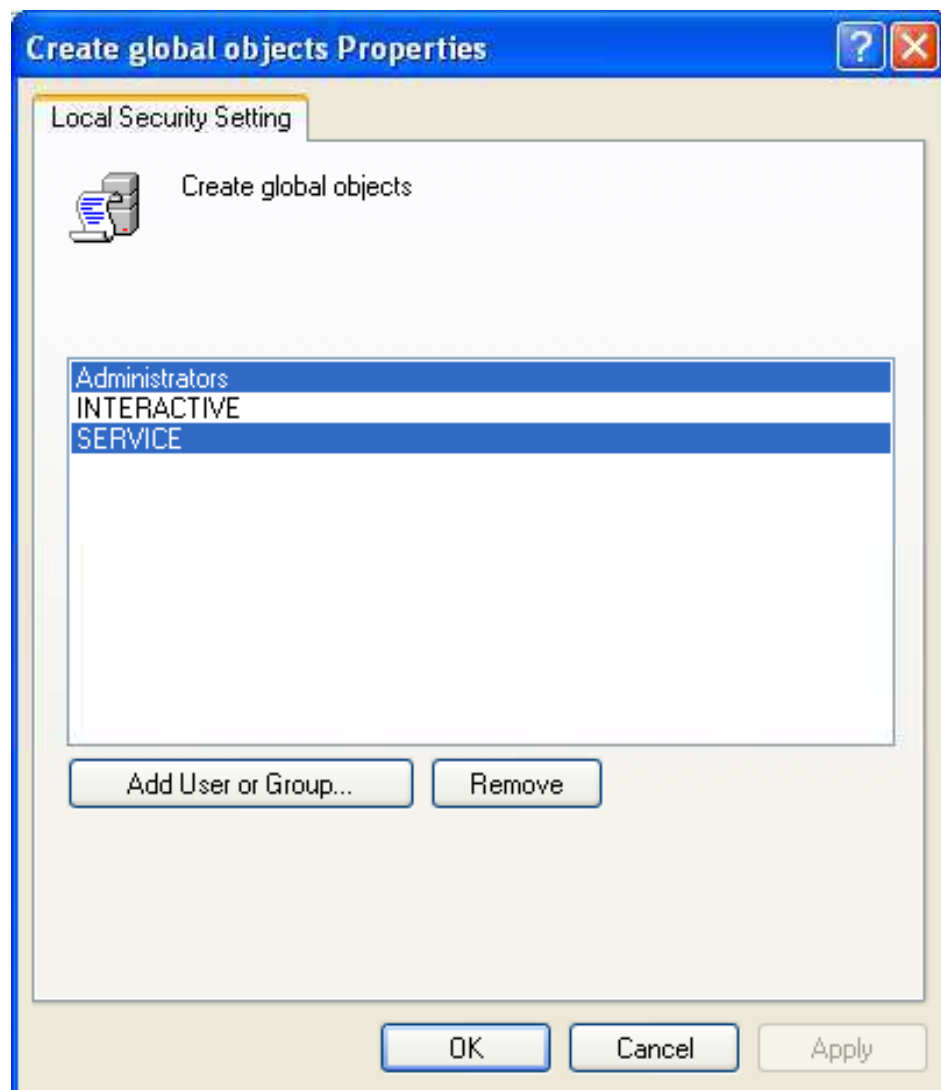
Countermeasure

- This right should be given to local **Administrators** and **Service** groups.

Potential Impact

- None

Create Global Objects



Create Permanent Shared Objects

This policy concludes on creating a directory objects in the object manager, with which users can create permanent shared objects, including devices, semaphores, and mutexes. Kernel mode components can use this right to extend object namespace

The values for the Create permanent shared objects setting are:

- A user-defined list of accounts
- Not Defined

Create Permanent Shared Objects

Vulnerability

- Users with this right can create new shared objects and reveal sensitive data to the network

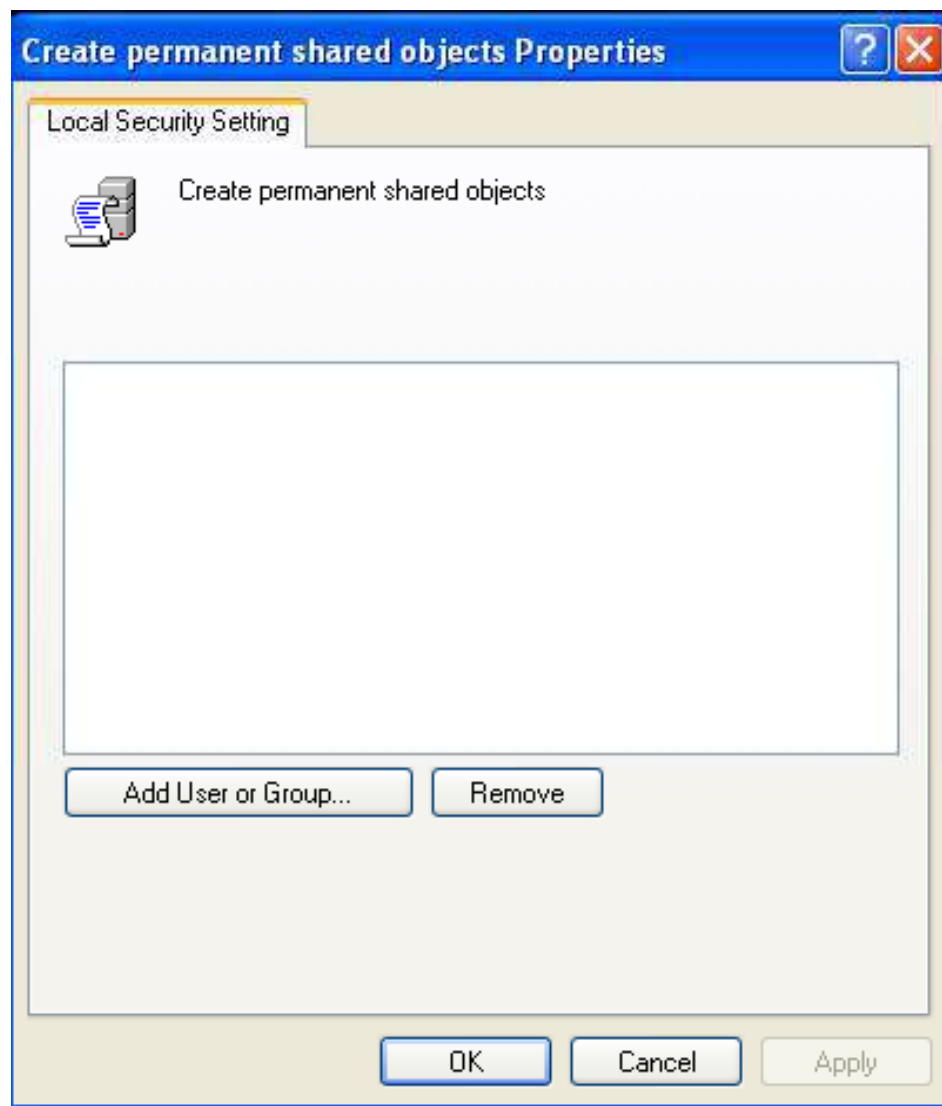
Countermeasure

- Processes which need this right must work with the system account (which already includes this user right)

Potential Impact

- None

Create Permanent Shared Objects



Debug Programs

This policy checks that users can open or attach to any process, even if they don't own it.

This right gives access to sensitive and critical operating system components.

The values for the Debug programs setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

- It congregates sensitive information from system memory (or) gain entry to kernel or application structure and changes it.
- Attacks are made through this right to get passwords from hashed tables and gain access to other security information.
- This right is only assigned to an administrator.

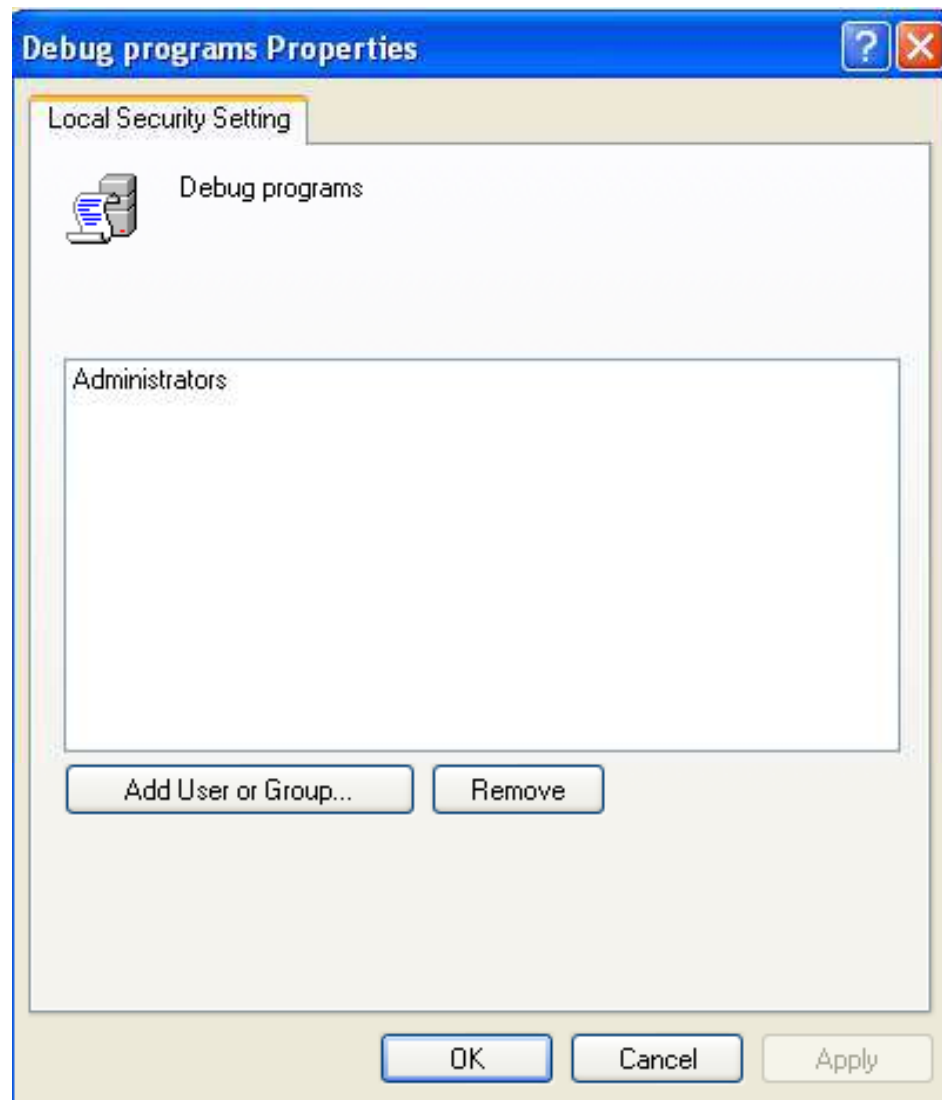
Countermeasure

- Timely change this right from users who do not require it.

Potential Impact

- If this right is revoked no program can be debugged.
- This right is necessary for service accounts, which acts as a cluster service.

Debug Programs



Deny Access to this Computer from the Network

This policy ascertains that user can connect to the computer from the network.

The values for the **Deny access to this computer from the network** setting are:

- A user-defined list of accounts
- Not Defined



Deny Access to this Computer from the Network

Vulnerability

- By setting this policy a user can be restricted from accessing some particular resources, as shared folders and files
- Without this right the user can access, view and modify the data over the network
- This right gives a limitation over some accounts as a guest account who don't need to access the shared files

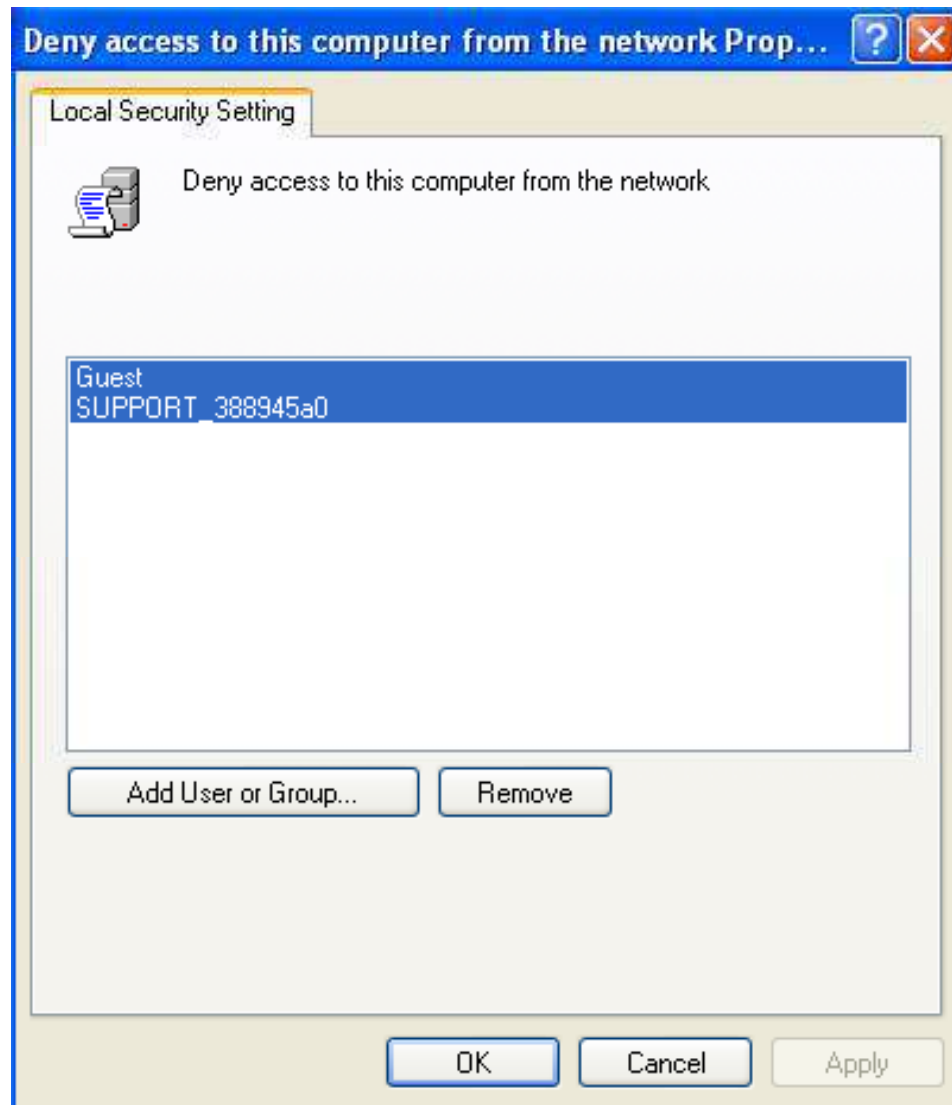
Countermeasure

- This right should be allocated to:
 - ANONYMOUS LOGON
 - The built-in local Administrator account
 - The local Guest account
 - The built-in Support account
 - All service accounts
- This right is useful while configuring servers and workstations with sensitive information

Potential Impact

- The user abilities can be affected by assigning this user right

Deny Access to this Computer from the Network



Deny Log On as a Batch Job

This protocol determines if you can log on through a batch-queue facility or not. Its characteristics in Windows Server 2003 are used to schedule and launch a task automatically one or more times.

This right is used to start a scheduled task.

The possible values for the **Deny log on as a batch job** setting are:

- A user-defined list of accounts
- Not Defined

Deny Log On as a Batch Job

Vulnerability

- This protocol schedules a task that consumes huge computer resources and causes a DoS state.

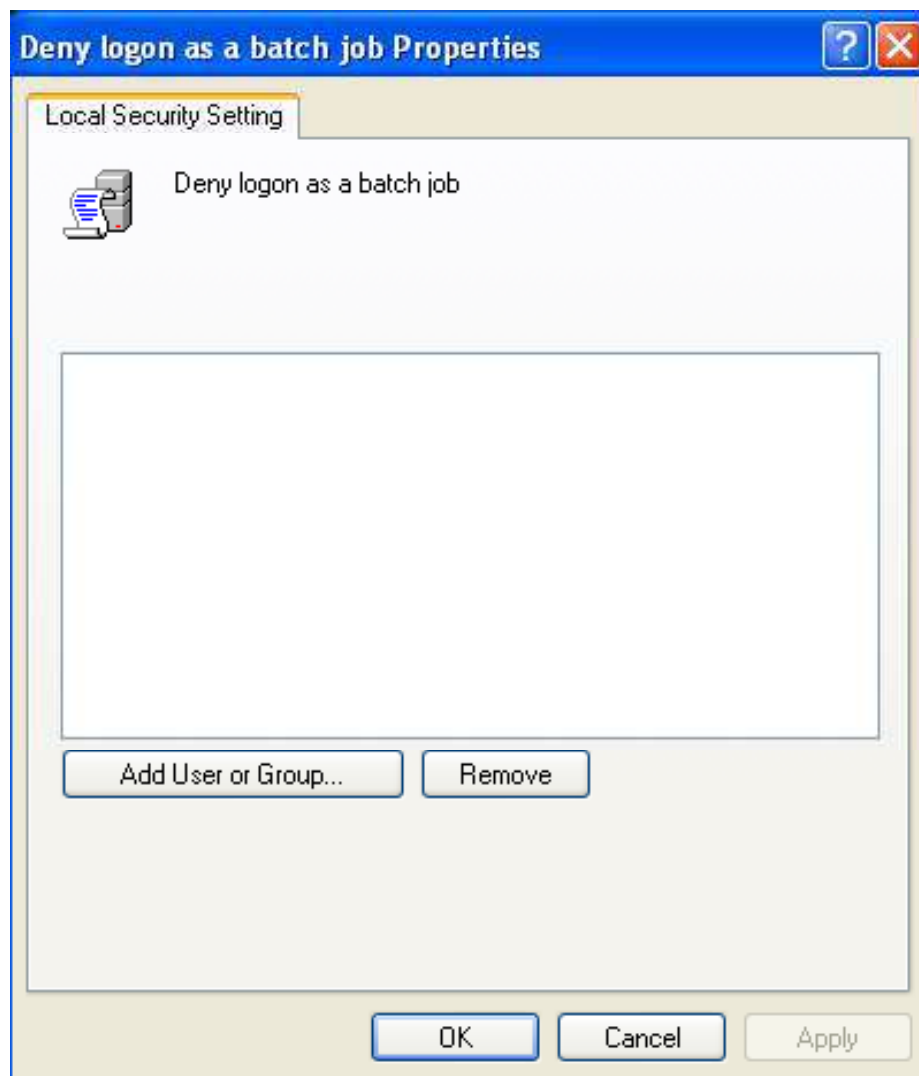
Countermeasure

- This right is given to the built-in Support account and the local Guest account.

Potential Impact

- By allotting this right you can deny users assigned to administrative roles (the ability to perform their required job activities).
- On a computer that runs Windows Server 2003 the account do not fit in to the **Guests** group, but on a computer which is upgraded from Windows 2000 this account is associated to a **Guests** group.

Deny Log On as a Batch Job



Deny Log On as a Service

Check whether a user can logon to a service or not

The values for the **Deny log on as a service** setting are:

- A user-defined list of accounts
- Not Defined

Deny Log On as a Service

Vulnerability

- Users with accounts capable of logging on as a service can start new unauthorized services as keylogger or any malware
- As per the countermeasures only accounts with administrative privileges can install and configure the services

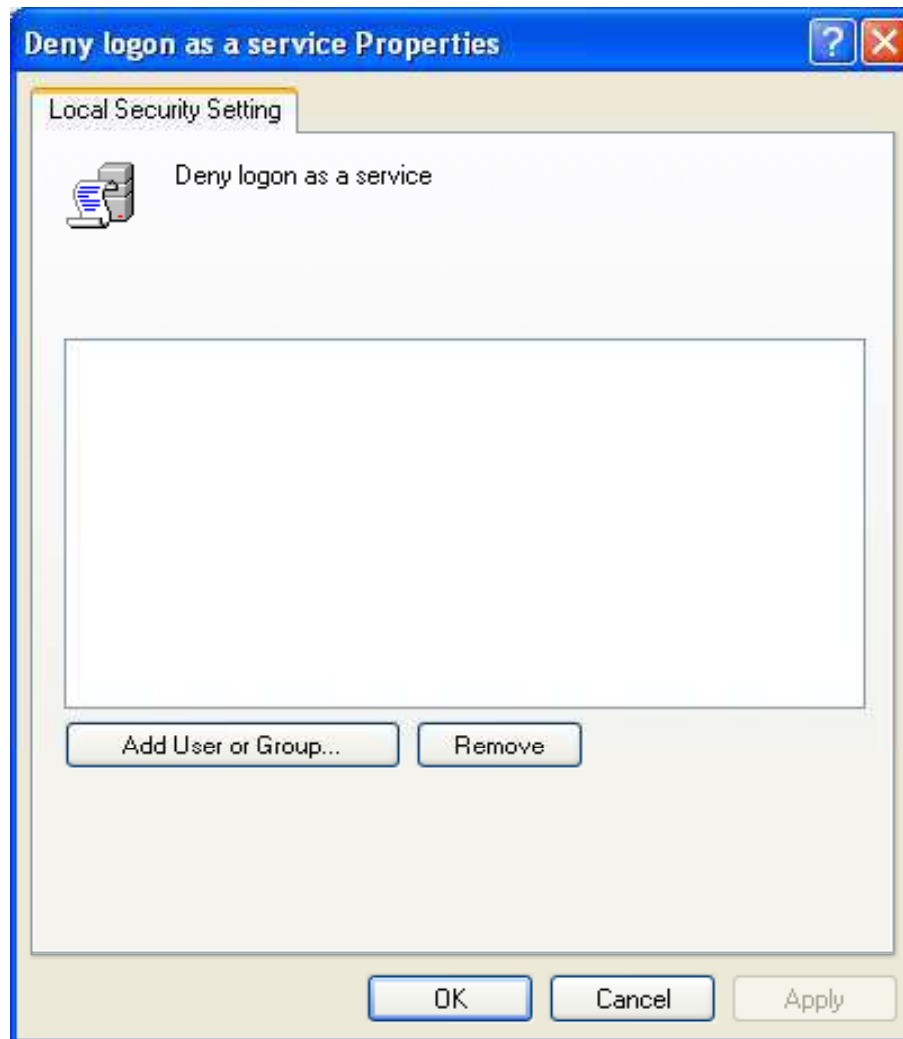
Countermeasure

- It is suggested not to avail this right to the accounts with default configuration

Potential Impact

- If this right is assigned to specific accounts, services may not start and could raise DoS condition

Deny Log On as a Service



Deny Log On Locally

These settings conclude whether you can logon directly on a computers keyboard.

The values for the **Deny log on locally** setting are:

- A user-defined list of accounts
- Not Defined

Deny Log On Locally

Vulnerability

- If this right is not limited to justifiable users, unauthorized users can download and execute malicious code
- An account with the ability to log on locally could be used to log on at the console

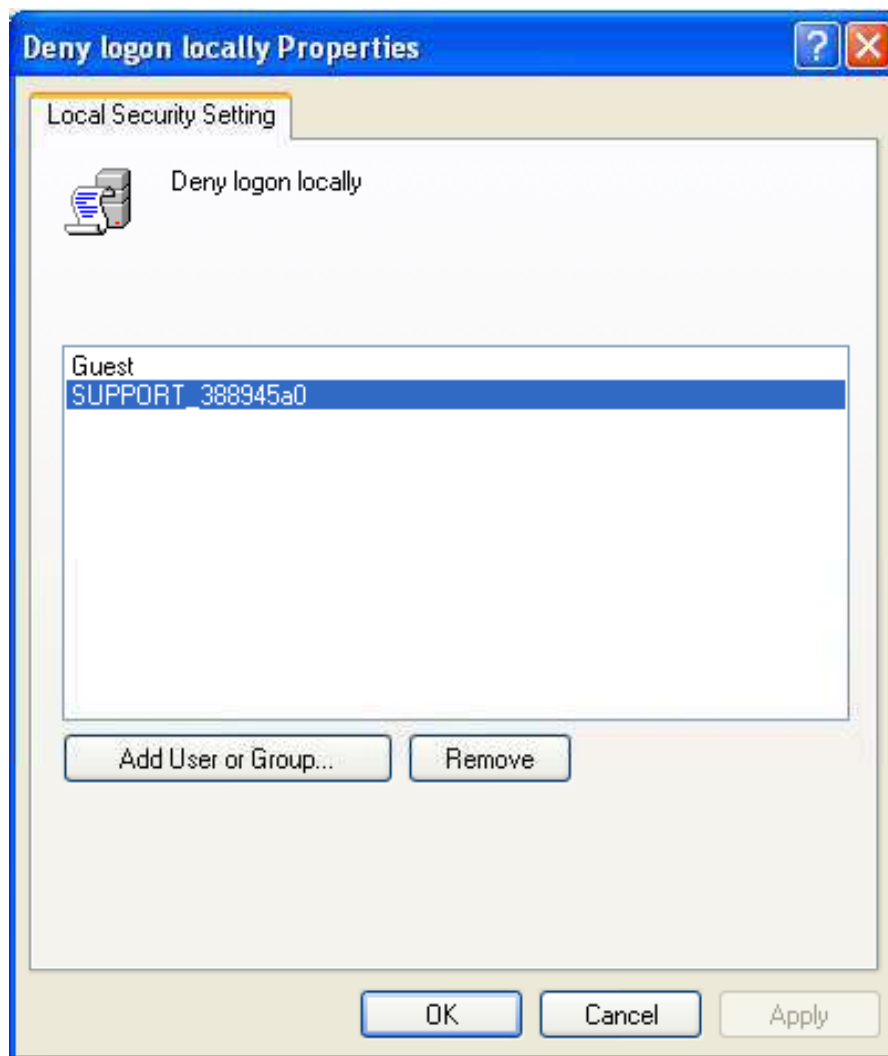
Countermeasure

- This right can be given to built-in Support account
- This user right might have to be given to additional accounts that use ASP.NET Components

Potential Impact

- This right should be allotted to user having ASP.NET and IIS 6.0
- It should be confirmed that assigned activities will not be adversely affected

Deny Log On Locally



Deny Log On through Terminal Services

This determines on the user right to logon to the computer through a remote desktop connection.

The values for the **Deny log on through Terminal Services** setting are:

- A user-defined list of accounts
- Not Defined

Deny Log On through Terminal Services

Vulnerability

- If users are not restricted for logging on from a distinct console, then unauthorized users may download and install malicious code

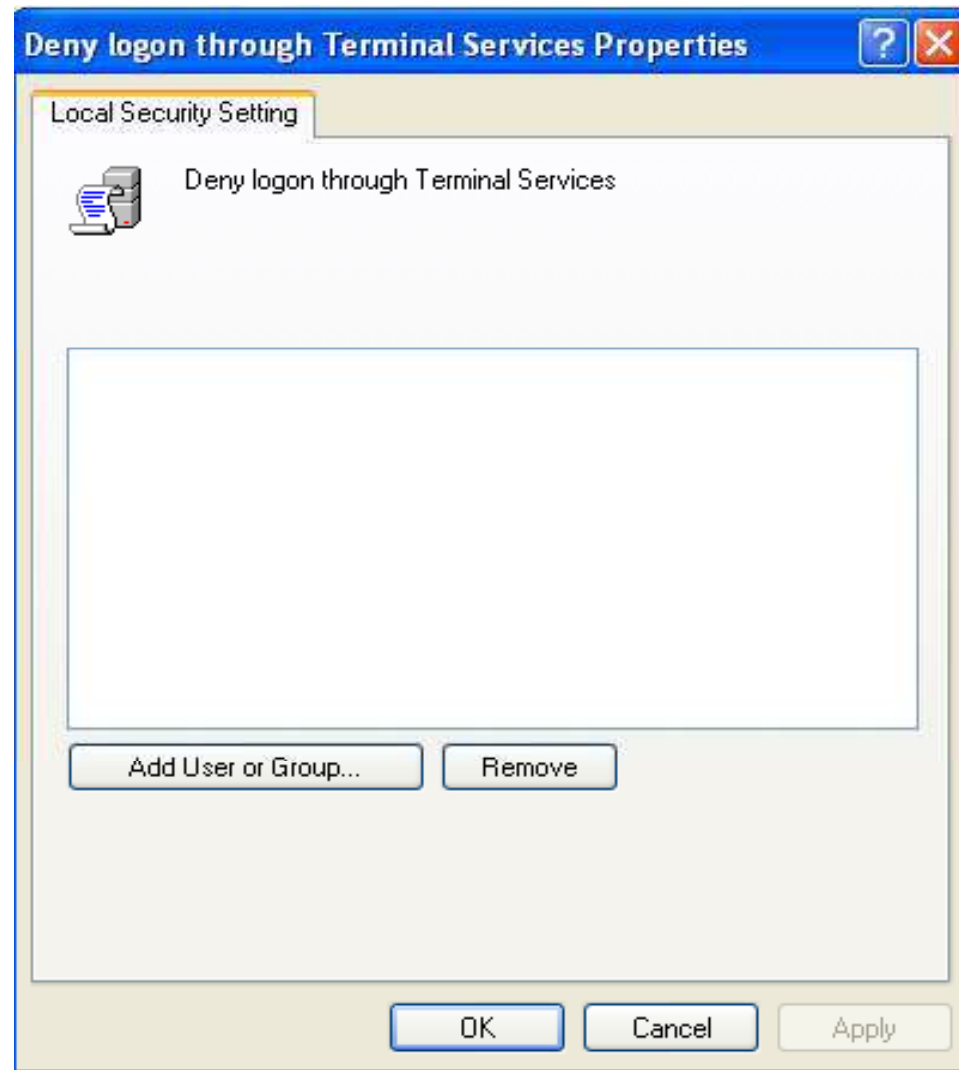
Countermeasure

- This right has to be assigned to local Administrator account and all service accounts
- Users with ASP.NET components might need this right

Potential Impact

- Assigning this right to other group could restrict the abilities of users with specific administrative roles in your environment
- Accounts with this user right are unable to connect to a computer through either Terminal Services or Remote Assistance

Deny Log On through Terminal Services



Enable Computer and User Accounts to be Trusted for Delegation

This right checks that a user can modify the **Trusted for Delegation** settings on a user or computer object in Active Directory

Users with this right must have write access to the account control flags on the object

Delegation of authentication is an ability that is used by multi-tier client/server applications, through which a front-end service uses client identification to authenticate to a back-end service

Both client and server accounts must be trusted for delegation

The values for the **Enable computer and user accounts to be trusted for delegation** setting are:

- A user-defined list of accounts
- Not Defined

Enable Computer and User Accounts to be Trusted for Delegation

Vulnerability

- By unauthorized use of the right, users on the network might be impersonated
- An attacker can gain access to network resources

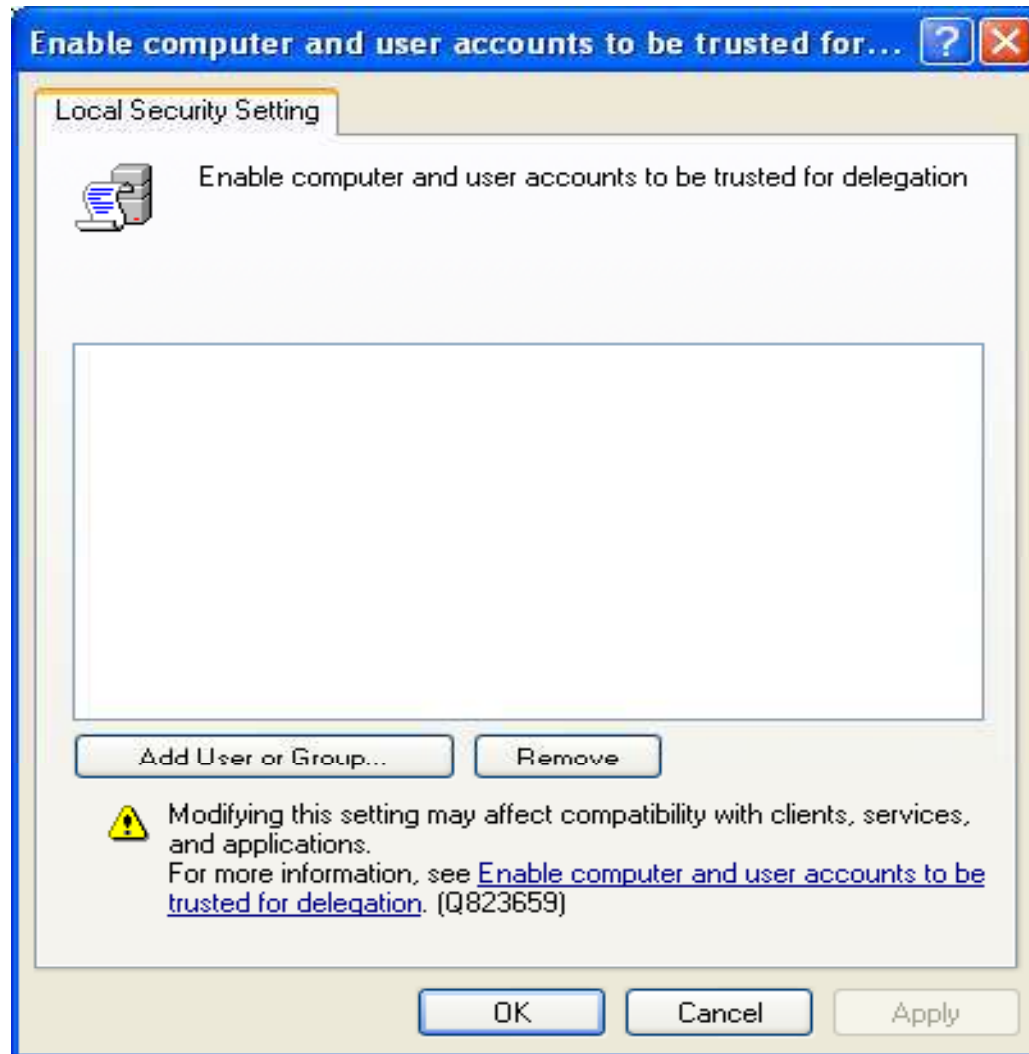
Countermeasure

- This right should be assigned with a clear need for its functionality
- While assigning this right, you should investigate on the use of constrained delegation to control the activities of a delegated account

Potential Impact

- None

Enable Computer and User Accounts to be Trusted for Delegation



Force Shutdown from a Remote System

This right gives the ability to shut down a computer from a remote location on the network.

The values for the **Force shutdown from a remote system** setting are:

- A user-defined list of accounts
- Not Defined



Force Shutdown from a Remote System

Vulnerability

- This right should be restricted as if a computer not shutdown properly a DoS condition may occur.

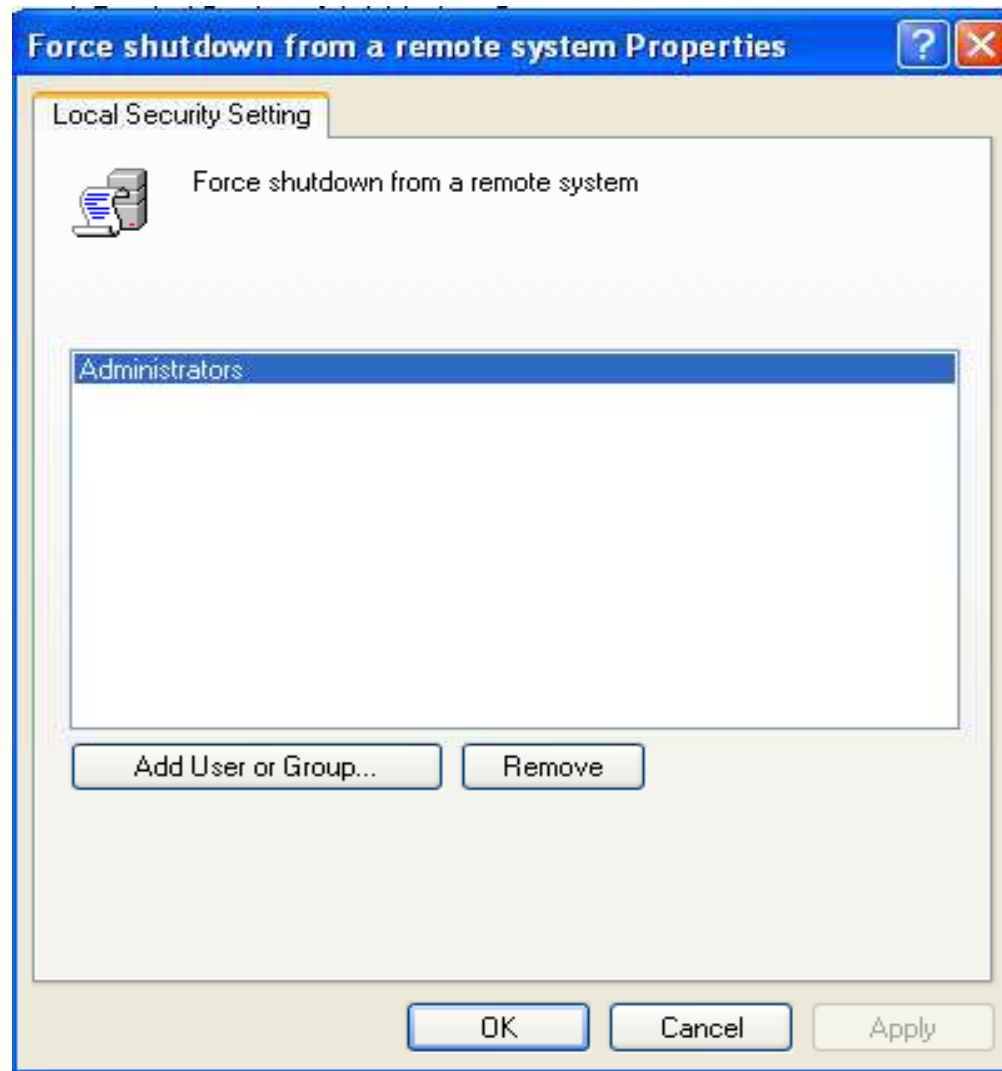
Countermeasure

- This right should only be given to Administrators or other personnel are who needed to perform some administrative operations.

Potential Impact

- By restricting this right to the server operator group, you may limit specific administrative roles.

Force Shutdown from a Remote System



Generate Security Audits

This policy can determine that a process can generate audit records in the Security log

The information in the Security log can trace unauthorized computer access

The values for the **Generate security audits** setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

- If an attacker gets access to a computer capable of writing security logs could fill that log with meaningless data. An attacker can clear the evidence of an unauthorized activity if the computer is configured to overwrite events
- If the computer is configured to shut down on unable of writing to Security log and it is not set to take a backup, this method could be used to create a denial of service

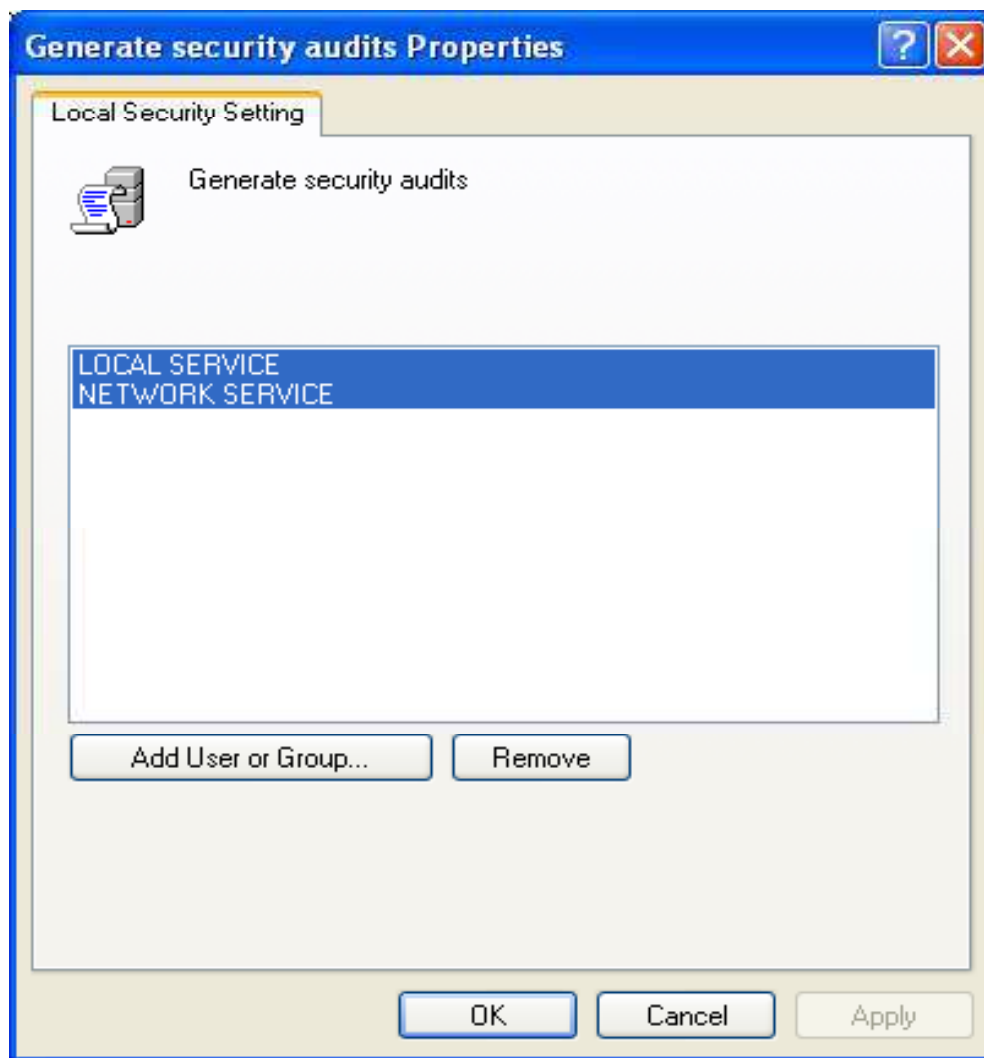
Countermeasure

- This right should be given to the Service and Network Service accounts

Potential Impact

- None

Generate Security Audits



Impersonate a Client after Authentication

This right allows programs that run on behalf of a user to impersonate that user or account

By this kind of impersonation, an unauthorized user can not convince a client to connect

Services started by the Service Control Manager and COM servers started by the COM infrastructure and configured to run under a specific account, have a built-in **Service** group added to their access tokens

These processes are assigned this user right when they are started

Impersonate a Client after Authentication

A user can impersonate an access token if any of the following conditions exist:

- The access token that is being impersonated is for this user
- The user, in this logon session, logged on to the network with explicit credentials to create the access token
- The requested level is less than Impersonate, such as Anonymous or Identify.

Users do not usually need to have this user right assigned

The values for the **Impersonate a client after authentication** setting are:

- A user-defined list of accounts
- Not Defined

Impersonate a Client after Authentication

Vulnerability

- An attacker with this right can create a service to trick a client and make them connect to the service to impersonate that client and elevate his level of access to the clients

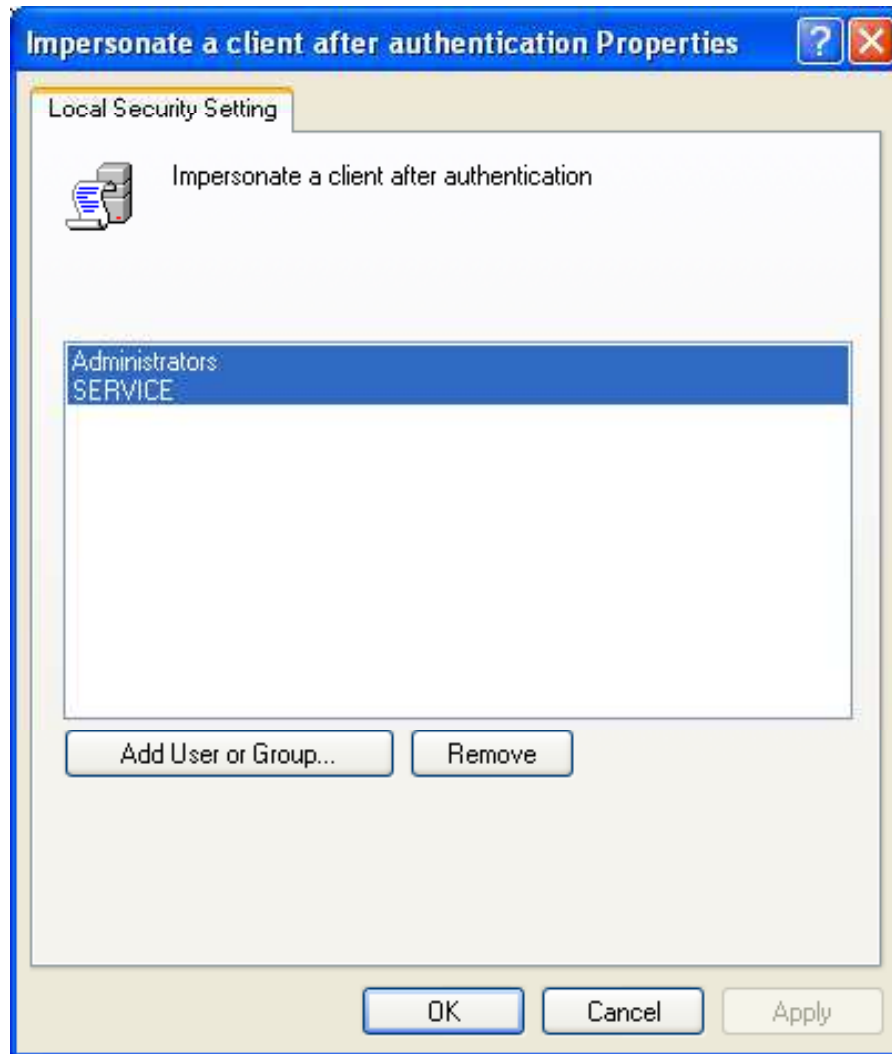
Countermeasure

- This right has to be with **Administrators** and **Service** groups
- Computers that run IIS 6.0 must have this user right assigned to the IIS_WPG group

Potential Impact

- If there are any optional components as ASP.NET or IIS, this right has to be given to those accounts

Impersonate a Client after Authentication



Increase Scheduling Priority

The Base priority class of a process can be increased by this policy.

This right might be required by software development tools.

The values for the **Increase scheduling priority** setting are:

- A user-defined list of accounts
- Not Defined

Increase Scheduling Priority

Vulnerability

- With this right the user can increase the scheduling priority of a process, which might lead to a DoS condition as very less amount of processing time will be left for other processes

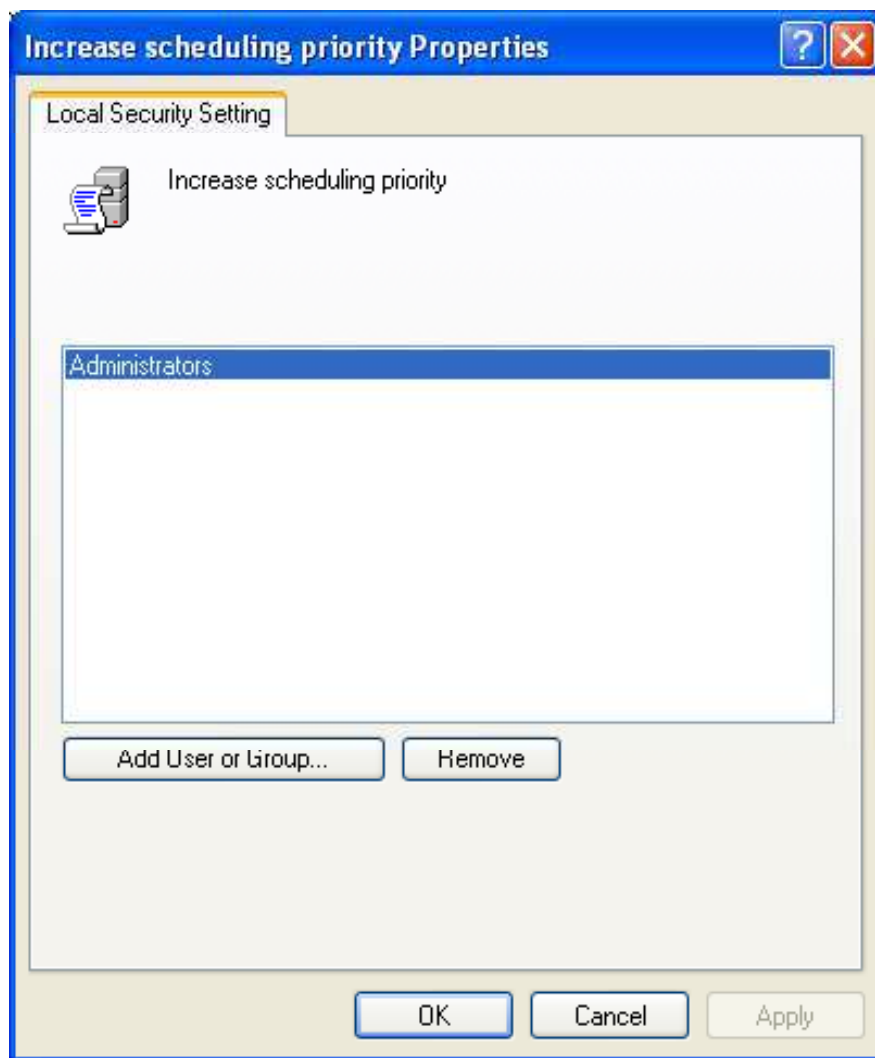
Countermeasure

- *This right should be only with Administrators*

Potential Impact

- None

Increase Scheduling Priority



Load and Unload Device Drivers

This policy checks on dynamically loading and unloading device drivers. If a signed driver for the hardware already exists in the Driver.cab file, setting this right is not necessary

The values for the **Load and unload device drivers** setting are:

- A user-defined list of accounts
- Not Defined



Load and Unload Device Drivers

Vulnerability

- Device drivers are highly privileged codes. Administrators should take extra care and install only drivers with verified digital signatures

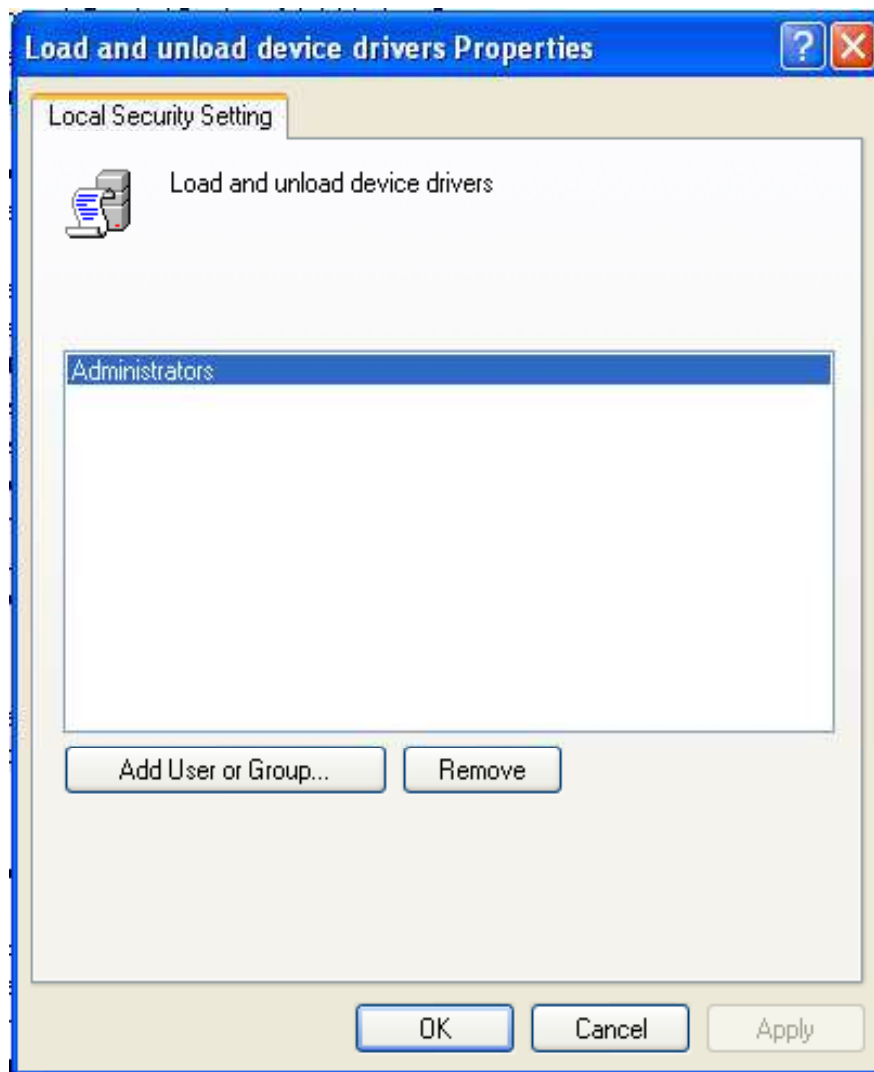
Countermeasure

- Only **Administrators** on member servers should have this right. On domain controllers this right has to be given only to **Domain Administrators**

Potential Impact

- By restricting this right to **Print Operators** group or other accounts, the abilities of users with administrative roles are limited

Load and Unload Device Drivers



Lock Pages in Memory

This right permits a process to store data in physical memory and prevents the data from paging to virtual memory

With this right the computer performance can be decreased

The values for the **Lock pages in memory** setting are:

- A user-defined list of accounts
- Not Defined



Lock Pages in Memory

Vulnerability

- This right can assign physical memory to several processes, which could lead to no RAM for other processes and create a DoS condition

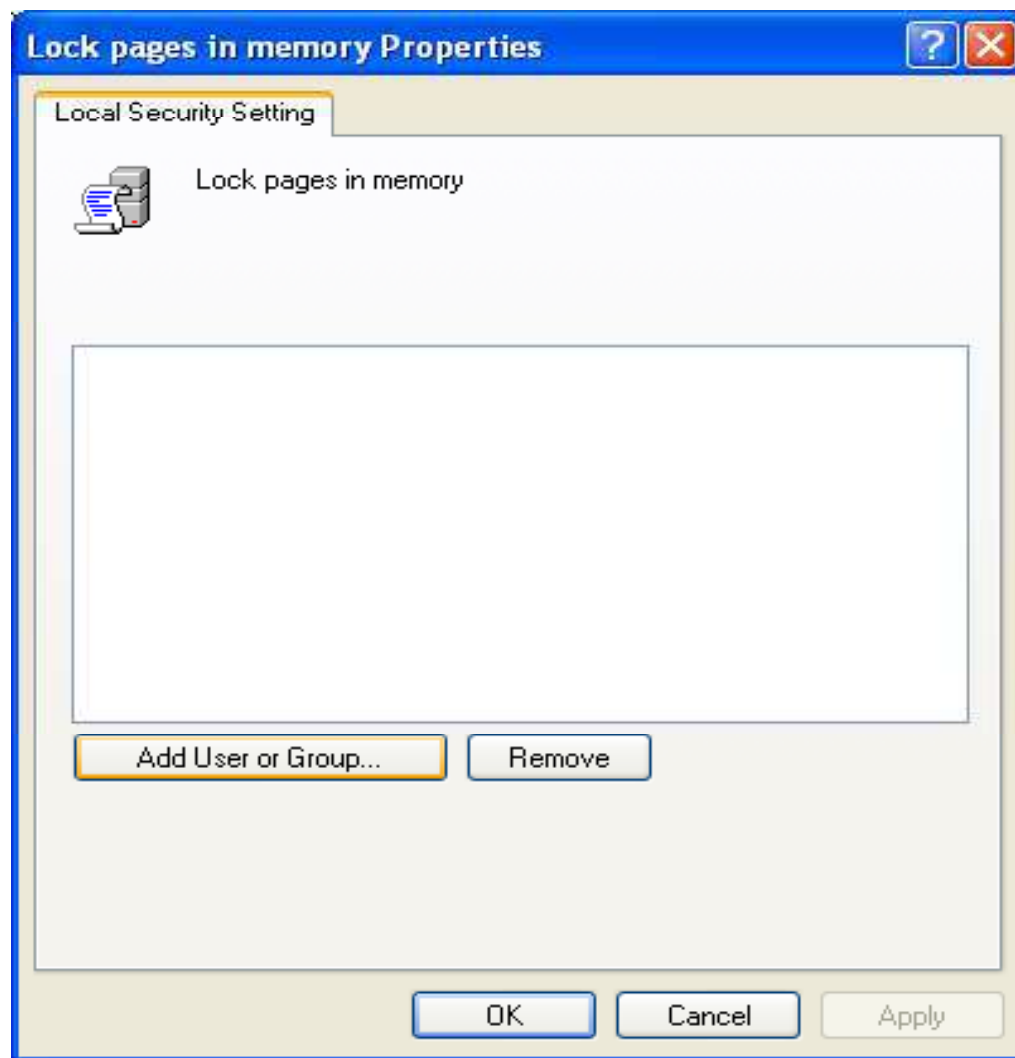
Countermeasure

- This right should not be assigned to any account

Potential Impact

- None

Lock Pages in Memory



Log On as a Batch Job

By this policy a user logs on a batch-queue facility such as the Task Scheduler service

When Add Scheduled Task wizard is used to run under a particular user name and password, that user automatically gets this right assigned to him

The values for the **Log on as a batch job** setting are:

- A user-defined list of accounts
- Not Defined

Log On as a Batch Job

Vulnerability

- This right has low-risk vulnerability

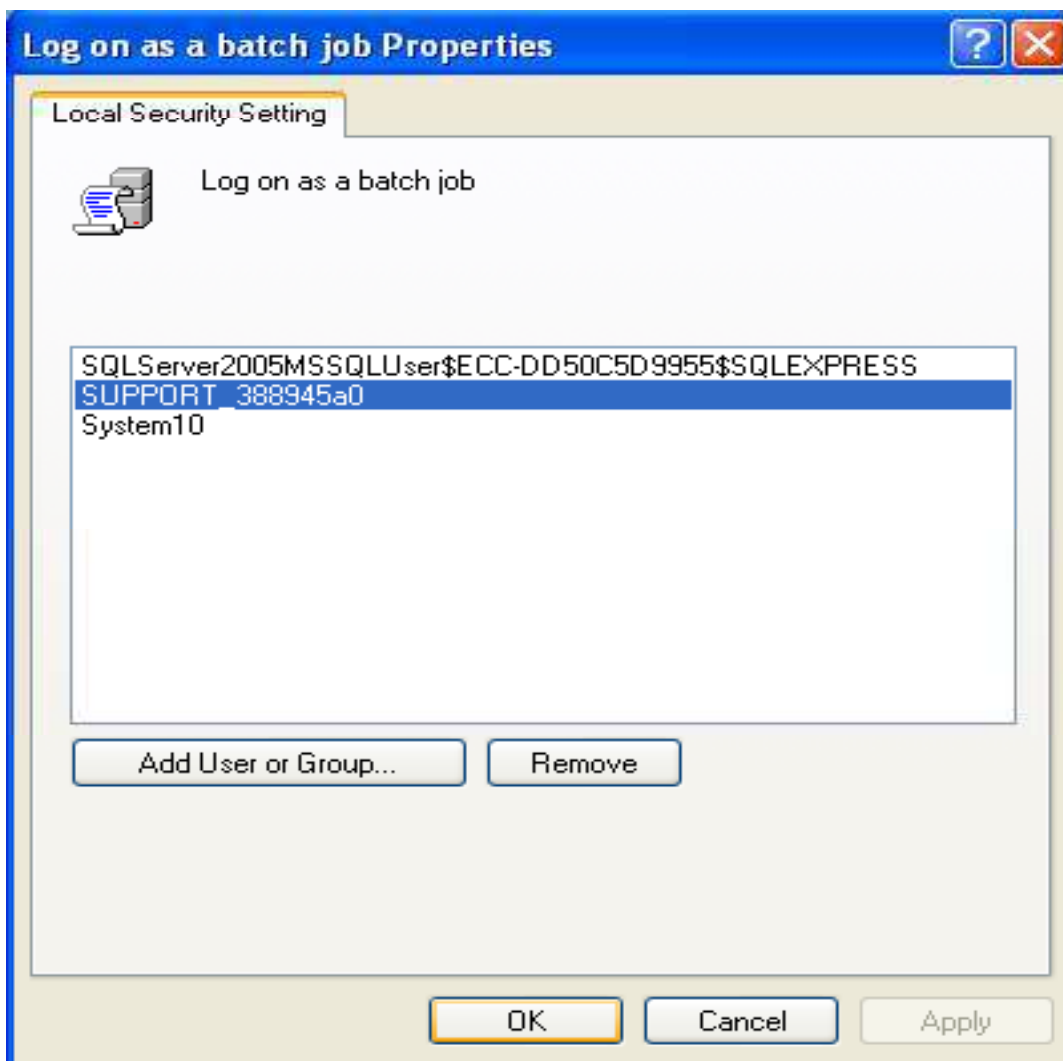
Countermeasure

- This right has to be managed automatically, if scheduled tasks have to run for specific user accounts. If Task Scheduler is not to be used in this manner, configure the right for only the Local Service account and the local support account

Potential Impact

- Configure settings for domain-based Group Policies; the computer will not be able to assign the user right to accounts that are used for scheduled jobs in the Task Scheduler
- If optional components as ASP.NET or IIS or used, you might need to assign this user right to additional accounts that are required by those components

Log On as a Batch Job



Log On as a Service

This policy decides whether a security principal can log on as a service, these services can be configured to run under the Local System, Local Service, or Network Service accounts

A service running under a different user account should have this right

The values for the **Log on as a service** setting are:

- A user-defined list of accounts
- Not Defined

Log On as a Service

Vulnerability

- This right allows users to network services or services which run without any assistance.
- The installation and configuring of the services can only be performed by an administrator

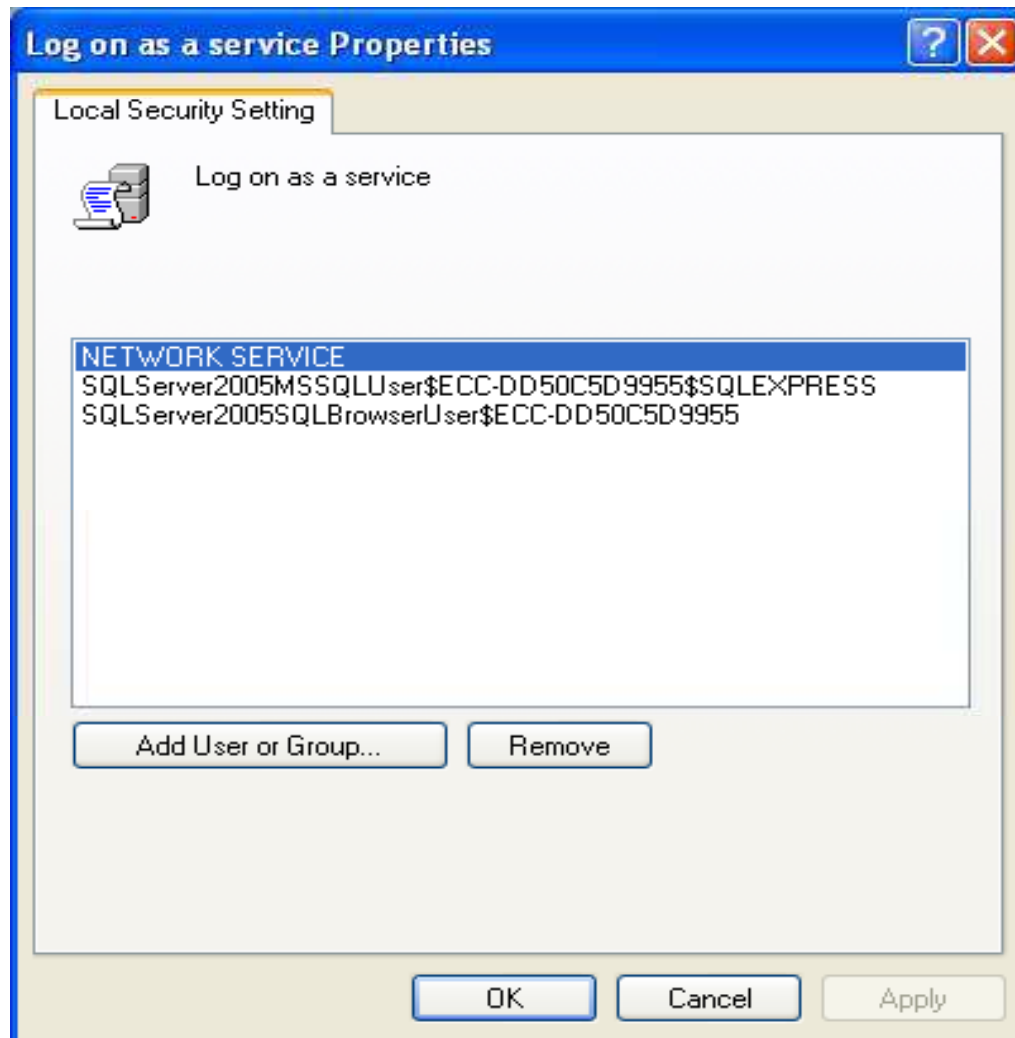
Countermeasure

- This right is restricted to local accounts as Local System, Local Service, and Network Service
- There should be a limit in assigning this user right

Potential Impact

- This right is a default configuration on most of the computers
- Computers having optional components as ASP.NET and IIS should have this user right

Log On as a Service



Manage Auditing and Security Log

This policy checks whether you can specify object access audit option for individual resources such as files, Active Directory objects, and registry keys.

Object access audits have to be enabled through **Audit Policy**, which is located under **Security Settings, Local Policies**

A user with this right can view and clear the Security event log from Event Viewer

The values for the **Manage auditing and security log** setting are:

- A user-defined list of accounts
- Not Defined

Vulnerability

- Managing security event log is a powerful right. A user with this right can clear the security log and erase the necessary log information

Countermeasure

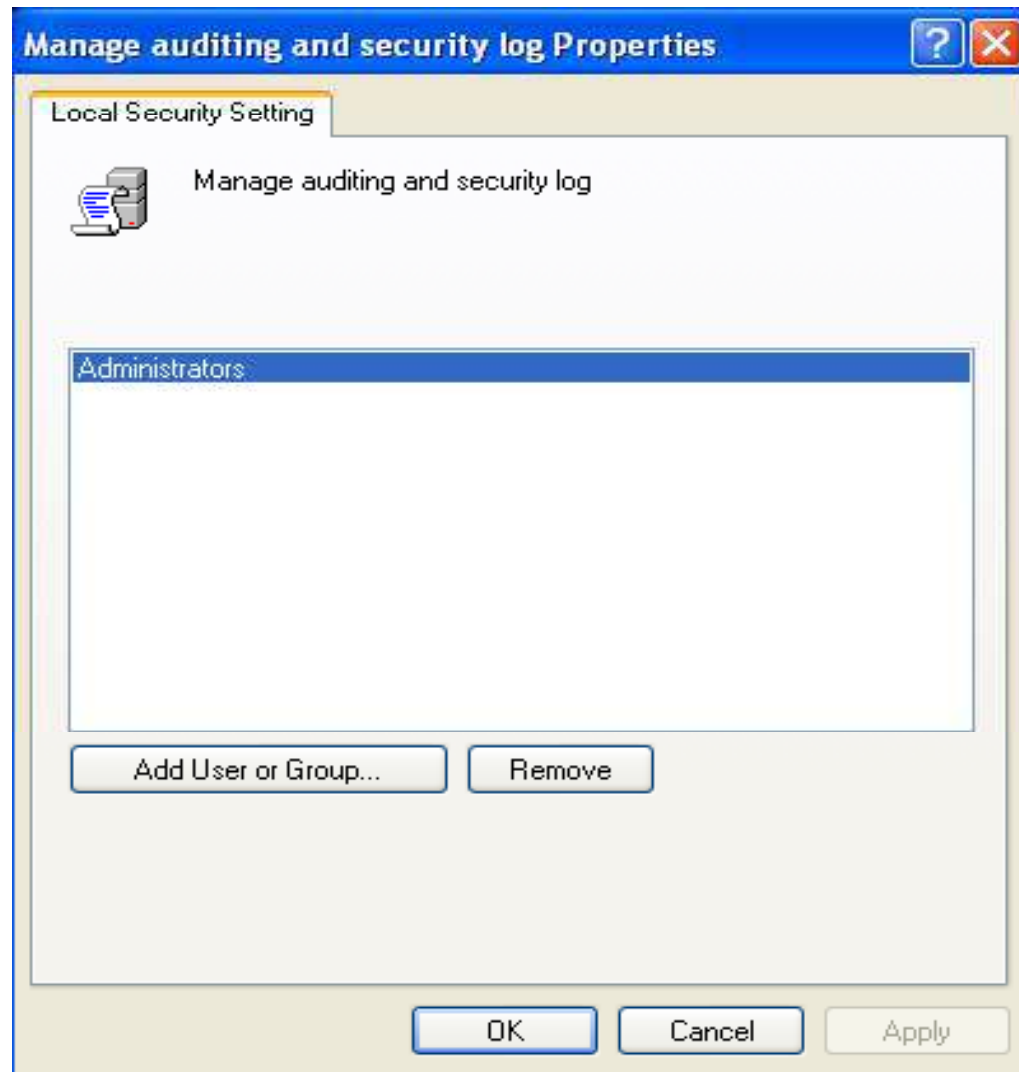
- This user right should be assigned only to local Administrators group

Potential Impact

- None



Manage Auditing and Security Log



Modify Firmware Environment Values

By this right the user can modify system environment variables either by a process (API) or by a user through System Properties

The values for the **Modify firmware environment values** setting are:

- A user-defined list of accounts
- Not Defined

Modify Firmware Environment Values

Vulnerability

- Any one with this right can configure a hardware and cause it to fail

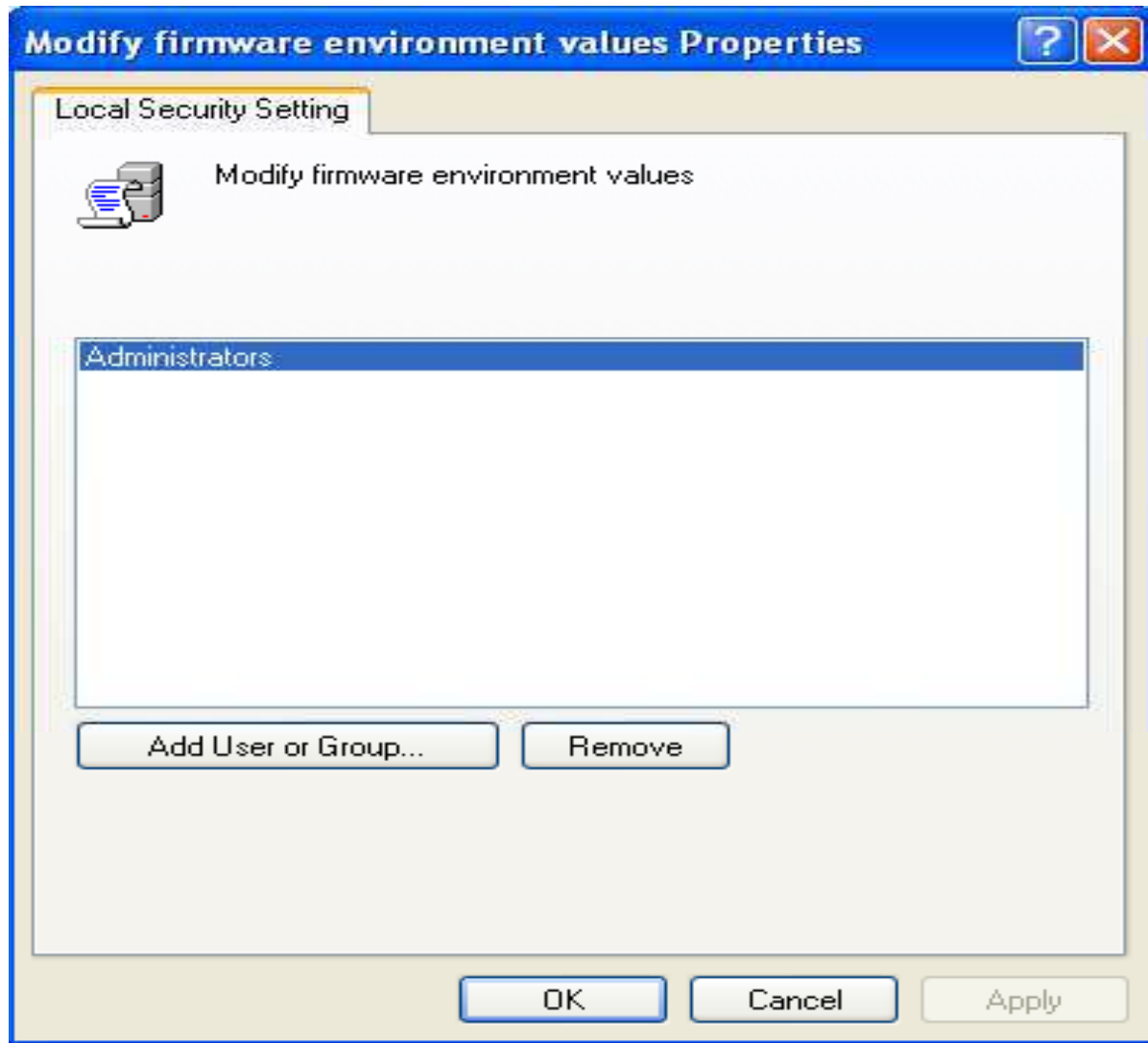
Countermeasure

- This right should be assigned only to local **Administrators** group

Potential Impact

- None

Modify Firmware Environment Values



Perform Volume Maintenance Tasks

This policy concludes on performing volume and disk management tasks by non-administrative or remote users as defragmenting an existing volume, create or remove volume and running the Disk Cleanup tool

Windows Server 2003 checks this right in user's access token when process runs in security context calls SetFileValidData()

The values for the **Perform volume maintenance tasks** setting are:

- A user-defined list of accounts
- Not Defined

Perform Volume Maintenance Tasks

Vulnerability

- With this right the user can delete a volume, which leads to loss of data or a DoS condition

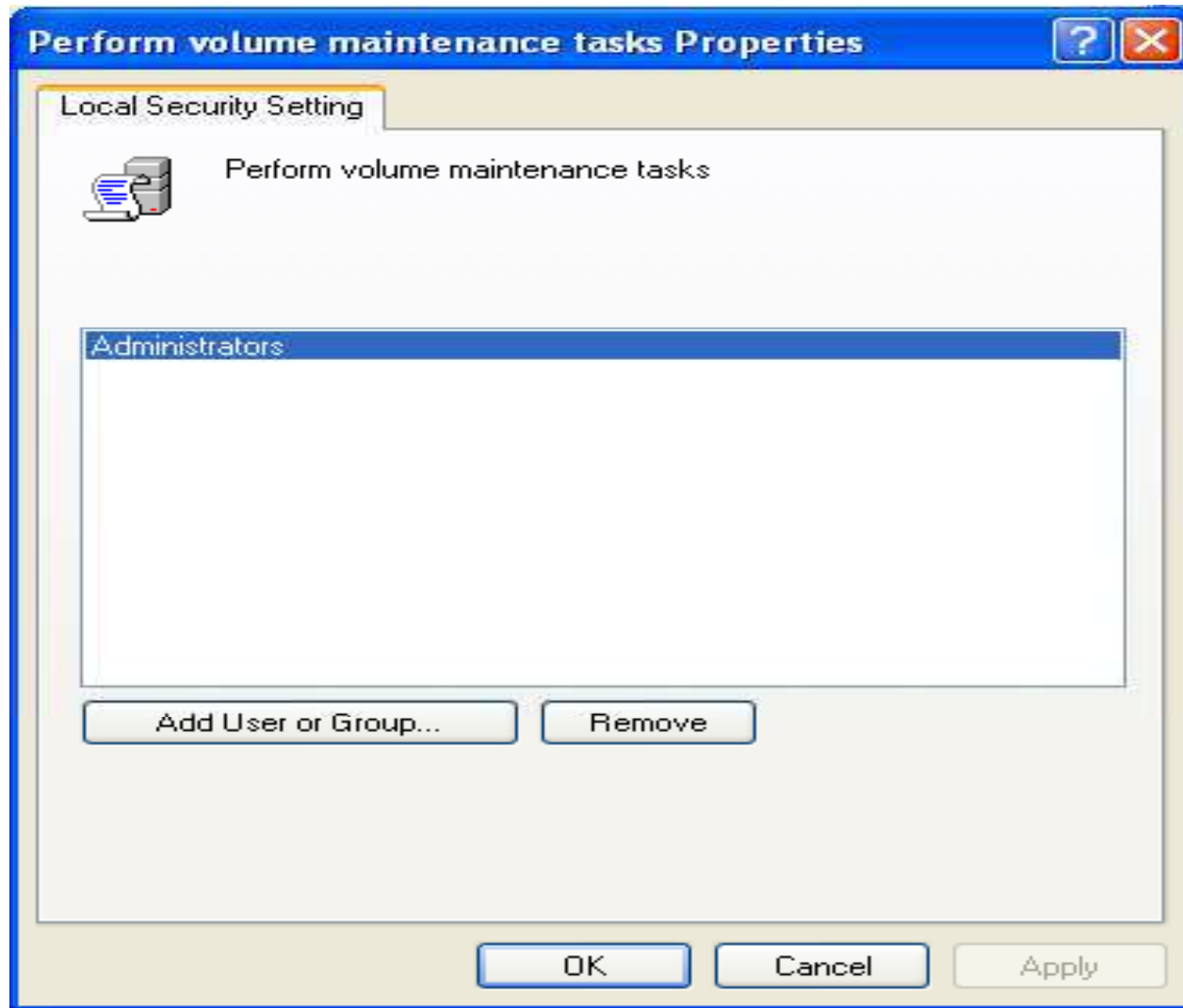
Countermeasure

- Only local **Administrators** group should have this right

Potential Impact

- None

Perform Volume Maintenance Tasks



Profile Single Process

By this right you can examine the performance of an application process

You don't need this right for using Microsoft Management Console (MMC) Performance snap-in

You do need this right to collect data through Windows Management Instrumentation (WMI) while System Monitor is configured

The values for the **Profile single process** setting are:

- A user-defined list of accounts
- Not Defined

Profile Single Process

Vulnerability

- Attacker with this user right can
 - Monitor computer's performance to help identify critical processes that they might wish to attack directly
 - Check what processes run on the computer to identify countermeasures to avoid, as antivirus software, an intrusion-detection system

Countermeasure

- Only Local Administrators group should have this right

Potential Impact

- By restricting this right to **Power Users** group or other accounts, the abilities of this group are limited