

Windows NT Security

The Basics

Wendall Mayson

wendall.mayson@srs.gov

(803) 208-3438

Westinghouse Savannah River Company

Savannah River Site

Aiken, SC 29808

WSRC-MS-97-0338

April 30, 1997



UNITED STATES DEPARTMENT OF DEFENSE



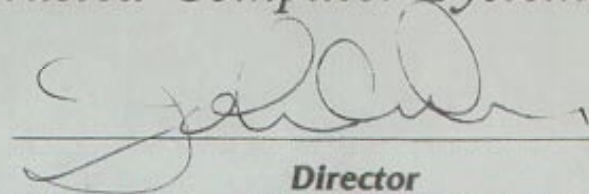
*Certificate of Appreciation
Presented to -*

MICROSOFT Corporation

*This certificate is presented in recognition of the contribution
you have made in the Computer Security Effort
through your success in developing a product,
Microsoft Windows NT Workstation Version & Server Version 3.5 (C2)*

*which meets the criteria for placement on
the Evaluated Products List for Trusted Computer Systems.*





**Director
NATIONAL COMPUTER SECURITY CENTER**

Outline

This Session

Windows NT Overview

Windows NT Security Model Components

Windows NT Domain Model

User Management

Account Policy

User Rights Policy

Groups

Outline (cont)

File Protection

Protection Of Other Objects

Auditing

Alerts

Security Log

Legal Warning Notice

Questions

This Session

This session will introduce you to the basic and the most important security features of Windows NT that all System Administrators should know.

Reference material has been provided.

Windows NT Overview

- A 32-bit, Preemptive, Multitasking OS.
- Security and Networking are Fundamental Components of the OS.
- Includes compatibility with other OS's, File Systems, and Networks.
- Supports TCP/IP, IPX/SPX, NetBEUI, AppleTalk, DLC, SNA, and PPP.

Windows NT Overview

(cont)

- Kernel supports Symmetric Multiprocessors (SMP).
- Familiar Windows 3.x Interface in Version 3.51.
- Windows 95 Interface in version 4.0.
- Will run on both Complex Instruction Set Computing (CISC) and Reduced Instruction Set Computing (RISC) Processors.

Windows NT Overview

(cont)

- Two Flavors:
 - Windows NT Server
 - Includes DHCP, DNS, WINS, FrontPage, and IIS.
 - Provides network services the highest priority.
 - Uses long processor timeslices.
 - Windows NT Workstation
 - Provides current foreground application the highest priority.
 - Uses short processor timeslices.

Windows NT Overview

(cont)

- Designed for C2 Security.
 - Currently only the Base OS (version 3.5 with Service Pack 3) has received C2 rating.
 - The networking component is under evaluation by the NCSC.
- Windows NT:
 - Security, as much as you want to administer.
 - Stability.
 - Reliability.

Windows NT Security Model Components

Logon Processes - Accepts logon request from users.

- Interactive Logons (CTRL+ALT+DEL issued at logon offers defense against a Trojan Horse).
- Remote Logons.

Windows NT Security Model Components (cont)

Local Security Authority - Ensures a user has permission to access the system.

- Also referred to as the Windows NT Security Subsystem.
- Generates Access Tokens.
- Manages the System Security Policy that has been established.
- Provides User Authentication.

Windows NT Security Model Components (cont)

Security Account Manager (SAM) -
Maintains the User Accounts Database.

- Contains data for all users and groups.
- Provides validation request from the Local Security Authority.

Windows NT Security Model Components (cont)

Security Reference Monitor - Enforces object access validation and audit generation rules defined by the Local Security Authority.

- Contains the ONLY copy of the Access Validation Code which ensures that objects are protected uniformly throughout the OS.
- Provides the following services:
 - Validating access to objects,
 - Testing users for privileges,
 - Generating audit messages.

Windows NT Domain Model

- A collection of NT Servers and NT Workstations that share a common Domain Directory Database (a single security policy and user account database (SAM)).
- Provides administrators with an effective way to implement a Security Policy.
- Simplifies administration of a network of NT Servers and NT Workstations.

Windows NT Domain Model (cont)

- Allows users to utilize a single logon to access resources on Servers and Workstations in the Domain.
- Domain Logons and the Domain Security Policy are administered by the Primary Domain Controller (PDC) and one or more Backup Domain Controllers (BDC).

Windows NT Domain Model (cont)

Trust Relationships can be established between Domains.

- One-Way Trust - Only one Domain trusts the other.
- Two-Way Trust - Both Domains trust each other.

Windows NT Domain Model (cont)

- Four Types Of Domain Models
 - Single Domain
 - Master Domain
 - Multiple-Master Domain
 - Complete-Trust Domain

User Management

- Accessed through the User Manager or User Manager for Domains.
- New User Information:
 - Username or ID,
 - Full Name,
 - Description,
 - Initial Password.

User Management (cont)

- New User Properties:
 - User Must Change Password At Next Logon,
 - User Cannot Change Password,
 - Password Never Expires,
 - Account Disabled,
 - Account Locked Out.
- Select Groups the user belongs to.
- Define a Profile.
 - Can be used by administrators to manage a User's Desktop Environment (such as setting a Screen Saver to lock the Workstation after a specified time of inactivity).

User Management (cont)

- Hours (permitted logon times).
- Logon From/To.
 - Workstations user can logon from.
 - Servers user can logon to.
- Account
 - Account Expiration Date.
 - Global (Users in local Domain) or Local Account (Users in another Domain) .

User Management (cont)

Dialin

- Grant dialin permission to user.
- Call Back options.
 - No Call Back
 - Set By Caller
 - Preset To (a given number)

User Management (cont)

Built-In Accounts

- Guest Account.
 - Disabled by default on NT Server.
 - Enabled by default on NT Workstation.
 - No Password.
 - Can be used for both local and network logons.
 - Account cannot be deleted but can and should be renamed.

User Management (cont)

Built-In Accounts

- Administrator Account.
 - Account has complete control over the entire system.
 - Password is set during NT installation.
 - Account cannot be deleted but can and should be renamed.
 - Account cannot be locked out.

User Properties



Username: Mayson

Full Name: Wendall Mayson

Description:

Password:

XXXXXXXXXX

Confirm

Password:

XXXXXXXXXX

User Must Change Password at Next Logon

User Cannot Change Password

Password Never Expires

Account Disabled

Account Locked Out

OK

Cancel

Help



Groups



Profile



Djalin

Account Policy

- Maximum Password Age
 - Password Never Expires
 - Expires In # Days
- Minimum Password Length
 - Permit Blank Password
 - At Least # Characters
- Minimum Password Age
 - Allow Changes Immediately
 - Allow Changes In # Days

Account Policy (cont)

- Password Uniqueness
 - Do Not Keep Password History
 - Remember # Passwords
- No Account Lockout
- Account Lockout
 - Lockout After # Bad Logon Attempts
 - Reset Count After # Minutes
 - Lockout Duration
 - Forever (until admin unlocks)
 - Duration # Minutes

Account Policy (cont)

- Users must logon in order to change password.
Note: Do not use this in conjunction with “User Must Change Password at Next Logon” in User Manager.
- Forcibly disconnect remote users from server when logon hours expire.

Account Policy [X]

Computer: TRIT_INGR11

Password Restrictions

Maximum Password Age

Password Never Expires

Expires In Days

Minimum Password Age

Allow Changes Immediately

Allow Changes In Days

Minimum Password Length

Permit Blank Password

At Least Characters

Password Uniqueness

Do Not Keep Password History

Remember Passwords

No account lockout

Account lockout

Lockout after bad logon attempts

Reset count after minutes

Lockout Duration

Forever (until admin unlocks)

Duration minutes

Users must log on in order to change password

OK
Cancel
Help

User Rights Policy

- Right - Privilege for a user to perform certain actions on the system.
- A Right applies to the entire system.
- Rights override Permissions on an object.
- Rights should be utilized for users who require additional access to perform their jobs, but do not need all of the Privileges of an administrator.

User Rights Policy (cont)

- Administrators should be selective in granting Rights to users.
- If practical, utilize permissions instead of Rights because Rights are system wide and permissions are object specific.

User Rights Policy (cont)

Some common Rights are:

- Access This Computer From Network.
- Back Up Files And Directories.
- Change The System Time.
- Force Shutdown From A Remote System.
- Log On Locally.
- Manage Auditing And Security Log.
- Restore Files And Directories.
- Shut Down The System.
- Take Ownership Of Files Or Other Objects.
- Load And Unload Device Drivers.
- Add Workstations To Domain (NT Server).

User Rights Policy



Computer: TRIT_INGR11

Right: Access this computer from network

Grant To:

Administrators

Everyone

Power Users

OK

Cancel

Help

Add...

Remove

Show Advanced User Rights

Groups

- Essentially, an account containing other accounts.
- An account in a Group is a Member of the Group.
- Permissions and Rights granted to a Group are granted to each of the Group Members.

Groups (cont)

- Groups are an administrative tool used to provide a collection of users with common needs, Rights and Permissions to perform their job.
- Groups are managed with the User Manager or User Manager for Domains.
- NT Server and NT Workstation provide a number of built-in Groups.

Groups (cont)

- Create new Groups using the User Manager or User Manager for Domains
- Three types of Groups:
 - Global Groups
 - Local Groups
 - Special Groups

Groups (cont)

Global Groups

- Defined at the Domain level.
- Have Domain user accounts only as members.
- Are used to effectively administer Domain users.

Note: A Global Group can be a Member of a Local Group.

Groups (cont)

Local Groups

- Maintained on a local system or Domain.
- Used on a local Workstation or Domain to grant Permissions and Rights needed only on the local Workstation or Domain Servers.

Groups (cont)

Special Groups

- Created by Windows NT for unique or specific purposes.
- Can not be viewed, changed, or have members added like Global and Local groups.
- Membership is determined by how a user access resources on a system (i.e., network, interactive)

Groups (cont)

Special Groups:

- Network - any user connected to a system via the network.
- Interactive - any user logged on interactively at a local system
- Everyone - any user logged on to the system (both the Network and Interactive groups).

Groups (cont)

Special Groups

- Creator Owner - the user that created or took ownership of an object. Note: if the user was the system administrator or other user that is a member of the Administrators group, the Administrator group would be a member of the Creator Owner group.
- System - the Windows NT operating system.

New Local Group



Group Name:

OK

Description:

Cancel

Members:

Show Full Names

Help

Add...

Remove

File Protection

Windows NT supports Discretionary Access Controls for Files or Directories of Files.

- Must use the Windows NT File System (NTFS).
- File Owners access a files properties or use File Manager to setup access control using Access Control Lists (ACLs).
- File Owners can grant Full Control, Read, Write, Execute, Delete, Change Permission, Take Ownership, or No Access.

File Protection (cont)

- ACLs allow File Owners to assign specific Access Permissions to individual users or Groups.
- ACLs are made-up of Access Control Entries (ACEs).
 - Each ACE will grant or deny access to the file.
 - A Deny Access ACE always overrides a Grant Access ACE.

File Protection (cont)

- By default, files inherit permissions from their parent directory.
- If a file has an ACL with no ACEs, no access has been granted and any access requested will be denied. Therefore, by not granting users or groups permissions to a particular object, you deny them any access by default.

File Protection (cont)

- Each ACE will either grant or deny some access to an object. A deny ACE is always placed in the ACL higher than a grant ACE (Note: This can be altered by third-party products or locally-developed software which may place certain grant ACEs ahead of deny ACEs, so BEWARE).
- Grant ACEs are cumulative

File Protection (cont)

- When a file is copied it inherits permissions from the directory into which it is copied.
- When a file is moved it retains its existing permissions.
- Establishing permissions for groups of users instead of each individual user is a more effective way to implement file and directory controls.

Readme Properties



General

Security



Readme

Type: Text Document
Location: C:\Program Files\Netscape\Navigator
Size: 15.5KB (15,954 bytes)
Compressed Size: File is not compressed

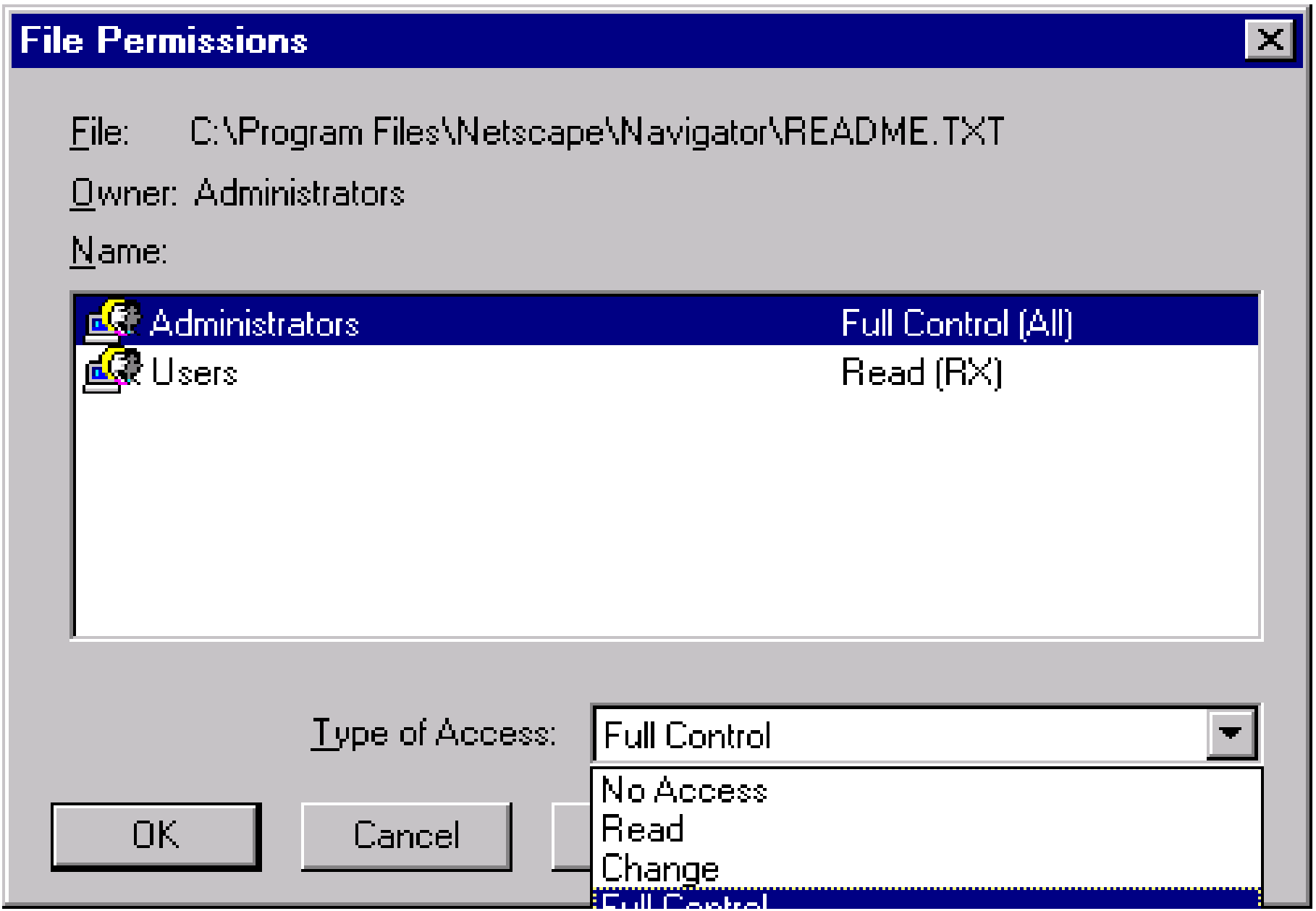
MS-DOS name: README.TXT
Created: Thursday, March 20, 1997 3:31:26 PM
Modified: Thursday, March 20, 1997 3:31:14 PM
Accessed: Wednesday, April 02, 1997 1:16:26 PM

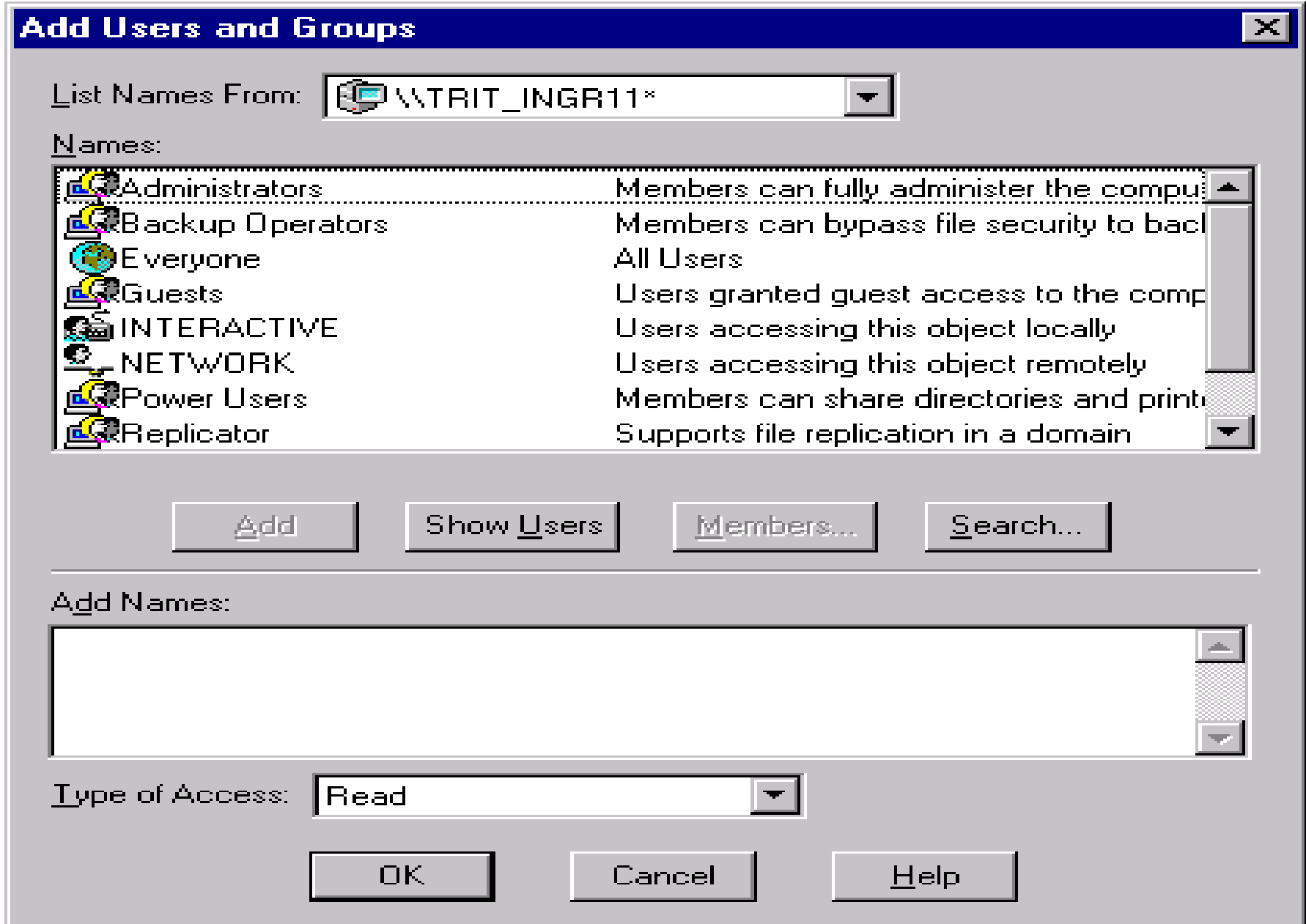
Attributes: Read-only Hidden
 Archive System
 Compressed

OK

Cancel

Apply





Directory Permissions



Directory: C:\Program Files

Owner: Administrators

Replace Permissions on Subdirectories

Replace Permissions on Existing Files

Name:

Administrators	Full Control (All) (All)
Users	Add & Read (RWX) (RX)

Type of Access:

Full Control

OK

Cancel

- No Access
- List
- Read
- ...

Protection Of Other Objects

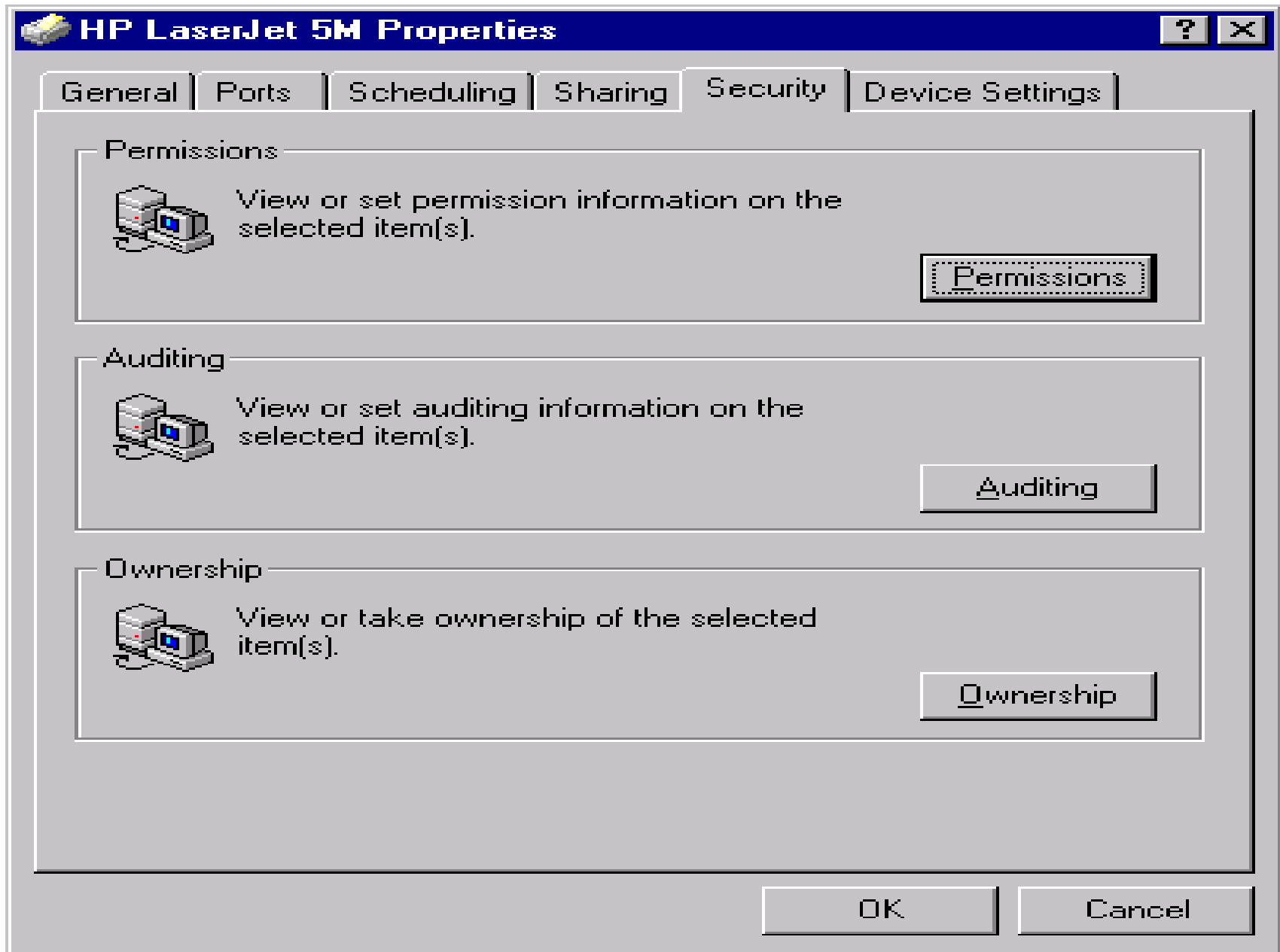
- Access Controls can be established for printers.
 - Access a printers properties (Security Tab) to grant or deny access to an individual user or a Group.
- Access Controls can be established for the registry.
 - The Registry is a database containing all of the system's configuration information. Access to this database must be controlled.
 - Use the Registry Editor to grant or deny access to Registry Keys or Subkeys for an individual user or a group.

Protection Of Other Objects (cont)

The presence of this key disables remote registry access (except for Administrators)

```
HKEY_LOCAL_MACHINE\SYSTEM\  
CurrentControlSet\Control\SecurePipeServers\  
winreg
```

Note: Present by default in NT Server (versions after 3.51) and can be added to NT Workstation.



Printer Permissions

Printer: HP LaserJet 5M

Owner: Administrators

Name:

 Administrators	Full Control
 CREATOR OWNER	Manage Documents
 Power Users	Full Control
 Users	Print

Type of Access:

Full Control

OK

Cancel

No Access

Print

Manage Documents




Registry Key Permissions

Registry Key: HKEY_LOCAL_MACHINE

Owner: Administrators

Replace Permission on Existing Subkeys

Name:

 Administrators	Full Control
 Everyone	Read
 SYSTEM	Full Control

Type of Access:

Full Control

OK

Cancel

Read

Full Control

Special Access...

Auditing

- Turned OFF by default.
 - Administrator must enable auditing and turn on each category explicitly.
 - System Auditing is set in the User Manager or User Manager for Domains under Policies.
- Each User Action, Event, and Process can be audited, but it is not recommended.

Auditing (cont)

- For each category, both “successes” and “failures” can be audited, but it is not recommended.
- Audit Records can be reviewed using the Event Viewer.

Auditing (cont)

Categories:

- Logon and Logoff
- File And Object Access
 - Note: Objects must explicitly be set for auditing (Next Slide).
- Use Of User Rights
- User And Group Management
- Security Policy Changes
- Restart, Shutdown, And System
- Process Tracking

Auditing (cont)

- Objects must be explicitly set for auditing.
 - Would include Files, Directories, Printers, and Registry Keys and Subkeys.
 - The File and Object Access category must be selected in the System Audit Policy in order to audit objects.
- When enabling auditing for objects, administrators can select individuals users and/or Groups to be audited.

Auditing (cont)

- Files and Directories are set in the file properties (Security Tab) or File Manager.
- Printers are set in the printers properties (Security Tab) .
- Registry Keys and Subkeys are set in the Registry Editor.

Auditing (cont)

To ensure the use of Rights to access objects is audited, add the following Registry value.

```
HKEY_LOCAL_MACHINE\SYSTEM\  
CurrentControlSet\Control\Lsa
```

```
FullPrivilegeAuditing  
Type is REG_BINARY  
Value is 1
```

Audit Policy



Computer: TRIT_INGR11

Do Not Audit

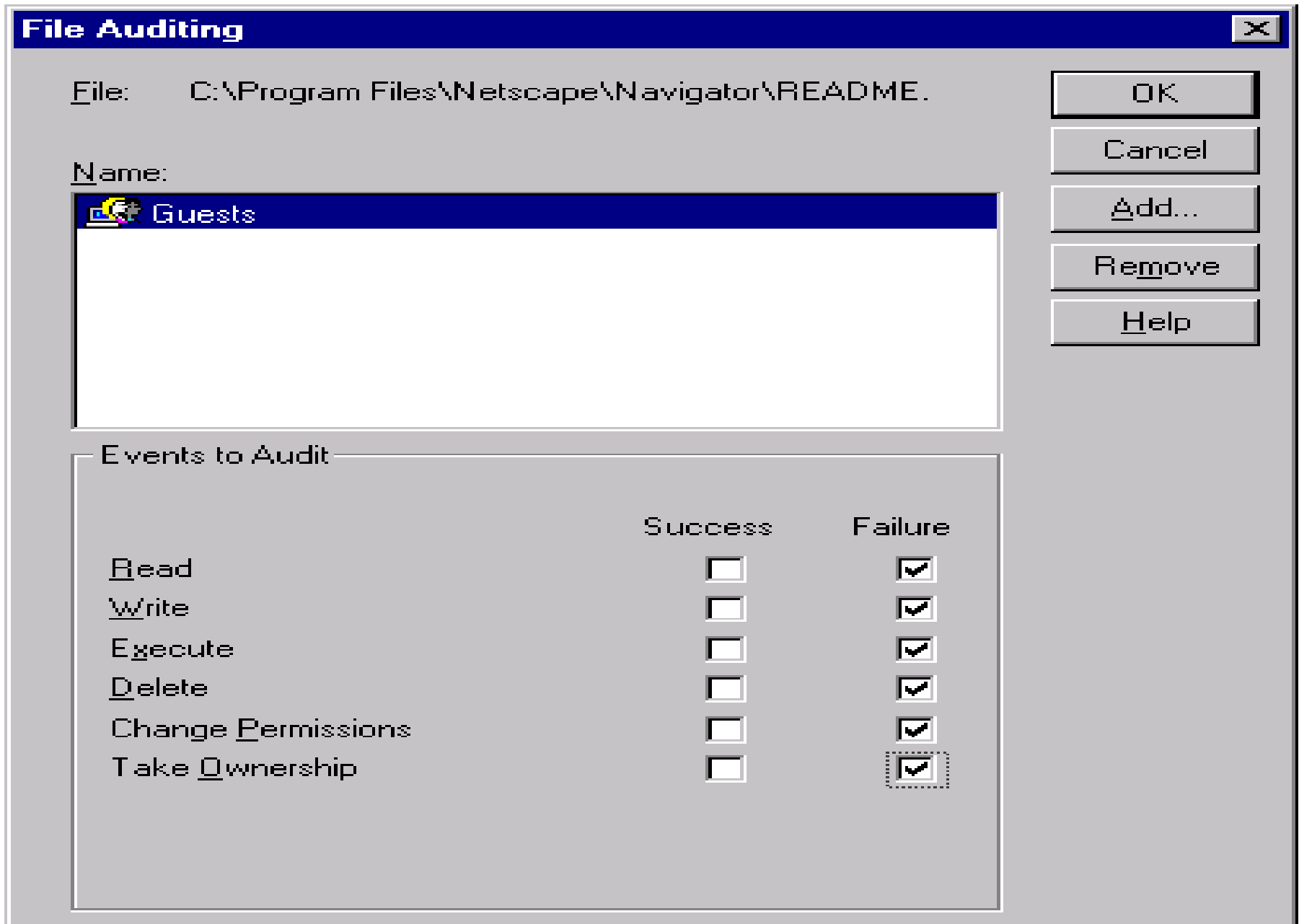
Audit These Events:

	Success	Failure
Logon and Logoff	<input type="checkbox"/>	<input checked="" type="checkbox"/>
File and Object Access	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use of User Rights	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User and Group Management	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Security Policy Changes	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Restart, Shutdown, and System	<input type="checkbox"/>	<input type="checkbox"/>
Process Tracking	<input type="checkbox"/>	<input type="checkbox"/>

OK

Cancel

Help



Directory Auditing



Directory: C:\Program Files

Replace Auditing on Subdirectories

Replace Auditing on Existing Files

Name:

- Users

OK

Cancel

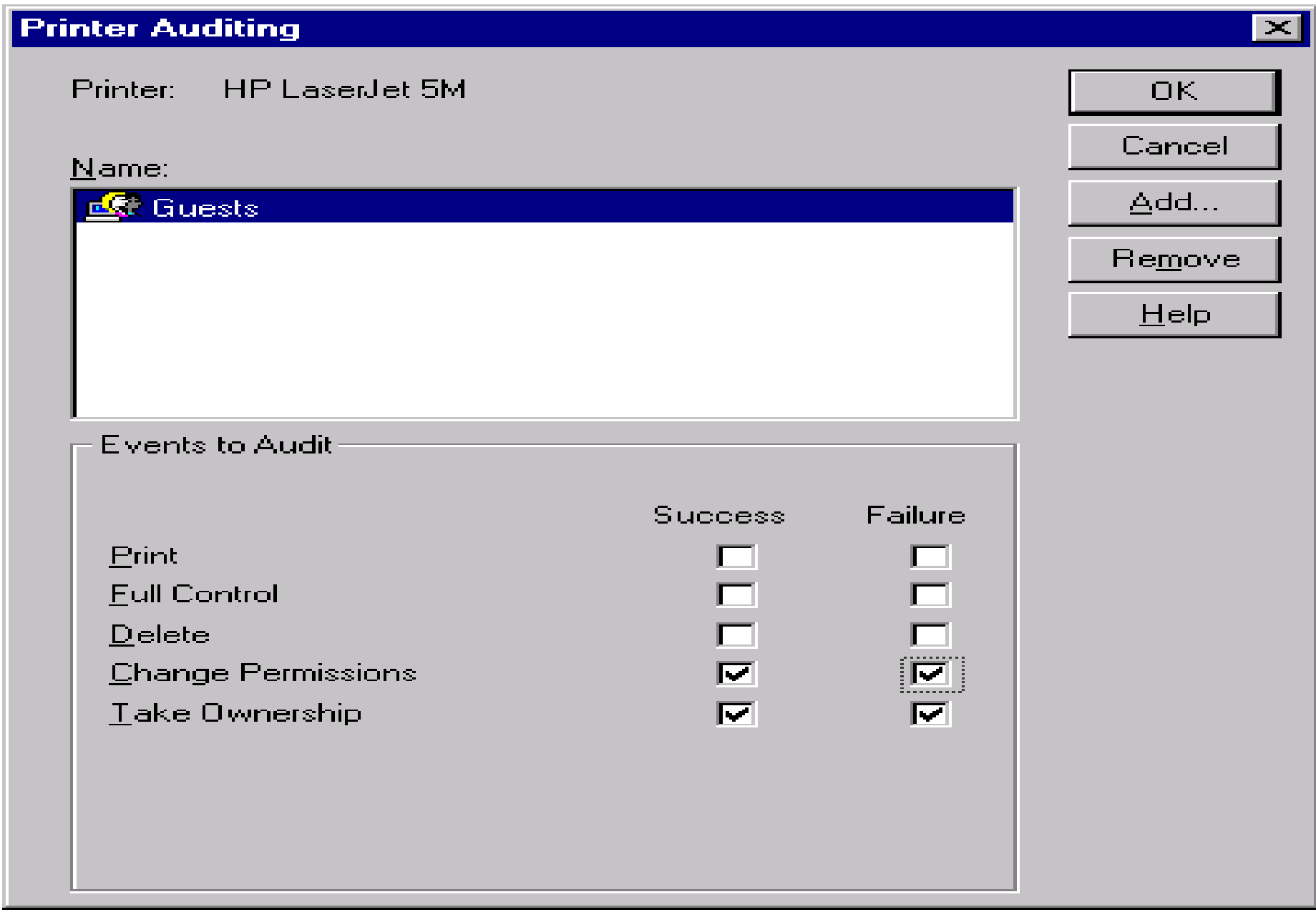
Add...

Remove

Help

Events to Audit

	Success	Failure
Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Execute	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Change Permissions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Take Ownership	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>




Registry Key Auditing

Registry Key: HKEY_LOCAL_MACHINE

Audit Permission on Existing Subkeys

Name:

 Everyone

Events to Audit

	Success	Failure
Query Value	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Set Value	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Create Subkey	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Enumerate Subkeys	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Notify	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Create Link	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Delete	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Write DAC	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Read Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>

OK
Cancel
Add...
Remove
Help

Alerts

- System Administrators can use the NT Performance Monitor to log and/or send Alert Messages to warn of security related events.
- The Performance Monitor will log/send Alerts when the established limit of a particular counter is set.
- A program can be defined to run also.

Alerts (cont)

Some Good Counters:

- Errors Access Permissions
- Errors Granted Access
- Errors Logon
- Errors System
- Logon Total
- Logon/sec
- Sessions Forced Off
- Sessions Timed Out

Add to Alert [X]

Computer: \TRIT_INGR11 [...]

Object: Server [v]

Instance: []

Counter:

- Errors Logon [▲]
- Errors System []
- File Directory Searches []
- Files Open []
- Files Opened Total []
- Logon Total [▼]

Color: [Red] [v]

Alert If:

- Over [7]
- Under

Run Program on Alert:

- c:\winnt\logfail.bat
- First Time
- Every Time

Counter Definition:

The number of failed logon attempts to the server. Can indicate whether password guessing programs are being used to crack the security on the server.

[Add] [Cancel] [Explain>>] [Help]

Alert Options [X]

Switch to Alert View

Log Event in Application Log

Network Alert

Send network message

Net Names:

Update Time

Interval (seconds):

Periodic Update

Manual Update

5.000

OK

Cancel

Help

Security Log

- The Security Log contains the Audit Records.
- The records in the Security Log can be reviewed using the Event Viewer.

Note: The Event Viewer is also used to review records in the System Log and Application Log. System Administrators can find other useful information in these two logs.

Security Log (cont)

- Only administrators or users with the 'Manage Auditing and Security Log' Right can review the Security Log.
- The Path for the Security Log is:
`<SYSTEMROOT>\SYSTEM32\CONFIG\SECEVENT.EVT`

Security Log (cont)

- System administrators can and should increase the size of the Log File using Log Settings under the Log Menu in Event Viewer.

Note: The default size is 512K.

- System administrators must select one of the following Event Log wrapping options:
 - Overwrite Events As Needed
 - Overwrite Events Older Than # Days
 - Do Not Overwrite Events (Clear Log Manually)

Security Log (cont)

- To bring the system down in the event an Audit Record cannot be recorded (for any reason), create the CrashOnAuditFail value (REG_DWORD) and set to 1 in the following Registry path:

HKEY_LOCAL_MACHINE\SYSTEM\

CurrentControlSet\Control\Lsa\CrashOnAuditFail

- The value is set to 2 by Windows NT just before a crash. Must be reset to 1 when the system is restored.

Event Viewer - Security Log on \\TRIT_INGR11 (Filtered)						
Log View Options Help						
Date	Time	Source	Category	Event	User	Computer
4/1/97	1:38:07 PM	Security	Privilege Use	578	o8392	TRIT_INGR11
4/1/97	1:37:45 PM	Security	Object Access	560	o8392	TRIT_INGR11
4/1/97	1:37:45 PM	Security	Object Access	560	o8392	TRIT_INGR11
4/1/97	1:36:12 PM	Security	Logon/Logoff	529	SYSTEM	TRIT_INGR11
4/1/97	1:35:43 PM	Security	Privilege Use	578	s9605	TRIT_INGR11
4/1/97	1:30:59 PM	Security	Logon/Logoff	529	SYSTEM	TRIT_INGR11
4/1/97	1:30:50 PM	Security	Logon/Logoff	529	SYSTEM	TRIT_INGR11
4/1/97	1:30:45 PM	Security	Logon/Logoff	529	SYSTEM	TRIT_INGR11
4/1/97	1:29:59 PM	Security	Privilege Use	578	s9605	TRIT_INGR11

Event Log Settings



Change Settings for Log

OK

Cancel

Maximum Log Size: Kilobytes (64K Increments)

Default

Event Log Wrapping

- Overwrite Events as Needed
- Overwrite Events Older than Days
- Do Not Overwrite Events (Clear Log Manually)

Help

Legal Warning Notice

System administrators can set the system to display a Legal Warning Notice.

- The Notice is displayed between the two logon dialog boxes.
- Users are required to acknowledge the notice by clicking the “OK” button in the message box holding the notice.

Legal Warning Notice (cont)

Two Registry entries need to be made:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeCaption
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\LegalNoticeText

Note: Use regini.exe from the Resource Kit if you need to put a long notice on multiple systems.

QUESTIONS?

ANSWERS?

SUGGESTIONS?