

Windows[®] NT 4.0 Security Configuration

Locking Down a Windows NT Host for Intrusion Detection



6600 Peachtree Dunwoody Road
300 Embassy Road Suite 5000
Atlanta, GA 30328
Tel: 678-443-6000
Toll-free: 800.776.2362
Fax: 678-443-6477
E-mail: sales@iss.net

© Copyright Internet Security Systems, Inc . 1998. All rights reserved. The terms “RealSecure”, “Internet Scanner”, “System Security Scanner”, and “SAFEsuite” are trademarks of ISS. The RealSecure logo is a registered trademark of ISS.

Windows NT is a registered trademark of Microsoft Corporation.

Table of Contents

Introduction	1
Step 1. Update Your Operating System.....	2
A. Ensure that you have Version 4.0.....	2
B. Ensure that you have installed Service Pack 3	2
C. Ensure that you have installed the latest Hot Fixes	2
Step 2. Tighten Your Network Configuration	3
A. Use out-of-band communications over a secure network	3
B. Implement Access Controls for System Protocols, Ports, and IP Services.....	5
Step3. Tighten Your System Configuration	7
A. Shut Down Unnecessary Windows NT Services.....	7
B. Tighten Account and Login Configurations.....	8
<i>Remove Unneeded Accounts</i>	<i>8</i>
<i>Choosing the Administrator Password.....</i>	<i>9</i>
<i>Hiding the Last User Name.....</i>	<i>9</i>
<i>Allowing Only Logged-On Users to Shut Down the Computer.....</i>	<i>9</i>
<i>Disabling Caching of Logon Credentials During Interactive Logon.....</i>	<i>10</i>
<i>Restricting Anonymous Network Access to Lookup Account Names and Groups and Network Shares</i>	<i>11</i>
C. Establish Appropriate File and Directory Protection.....	11
<i>Wiping the System Page File During Clean System Shutdown</i>	<i>11</i>
<i>ACL Settings to Protect Files and Directories</i>	<i>11</i>
<i>Removing Shares</i>	<i>13</i>
D. Enable System Auditing.....	14
<i>Recommended Audit Levels.....</i>	<i>14</i>
<i>Enabling Auditing.....</i>	<i>14</i>
<i>Reviewing Audit Logs</i>	<i>15</i>
Further NT Security Information	15

Introduction

RealSecure is the flagship intrusion detection and response tool from Internet Security Systems. The Windows[®] NT version of RealSecure offers powerful intrusion detection and response capability, on a cost-effective and easily managed Windows NT platform.

Especially in distributed/remote configurations (i.e., the engine is geographically separated from the console) that involve the Internet as a transport, the issue of securing the engine and console platforms is important. Because RealSecure is a security product that handles sensitive network data, ISS wants to provide customers with the necessary information to properly “harden” the engine and console platforms.

This document provides a set of guidelines for increasing the security of a Windows NT system that will run the RealSecure engine or console. Note that ISS recommends separate dedicated platforms for engine and console hosting and this approach is assumed throughout this document. Certain Windows NT Services, network protocols, user management, and other Windows NT functions and capabilities are modified or removed to tailor the platform specifically for supporting secure operation of the engine and basic manageability of the platform.

These guidelines are drawn largely from Microsoft technical support documents and have been tested by ISS in a laboratory environment. However, you should consider each recommendation in light of your actual deployment environment. Manageability and operational convenience are almost always a tradeoff with security, so consider your needs and balance them appropriately.

Note: Several of the recommendations in this document involve significant modification of the Windows NT environment, including accounts, file permissions, and registry entries. Take care in implementing these modifications – mistakes can cause problems up to and including rendering the system inoperable.

Step 1. Update Your Operating System

A. Ensure that you have Version 4.0

RealSecure for Windows NT **requires** Microsoft Windows NT 4.0 (Workstation or Server version); ISS recommends Windows NT Workstation for cost and manageability reasons. Note that versions of Windows NT prior to 4.0 are not supported.

B. Ensure that you have installed Service Pack 3

Service Pack 3 is **required** for RealSecure v2.5. Service Pack 3 (SP3) corrects several bugs and security holes, and provides support for encryption, authentication, and enhanced registry security.

Information on downloading and installing SP3 may be found at <http://backoffice.microsoft.com/downtrial/moreinfo/nt4sp3.asp>.

C. Ensure that you have installed the latest Hot Fixes

Microsoft makes available *hot fixes*, or program patches/upgrades, between releases of Windows NT and its Service Packs. These hot fixes are generally released to fix bugs or address security or performance issues.

Windows NT 4.0 post-Service Pack 3 hot fixes may be downloaded from Microsoft's FTP site at <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3>. The following hot fixes increase the network security of the engine platform and are **highly recommended**:

- Chargen** in the simptcp-fix subdirectory – fixes a chargen-based UDP packet denial of service vulnerability
- Priv-fix** in the Pri-fix subdirectory -fixes the use of Sechole.exe, which allows a non-administrative user to gain debug-level access on a system process. Using this utility, the non-administrative user is able to run some code in the system security context and thereby grant himself or herself local administrative privileges on the system.
- GetAdmin** in the getadmin-fix subdirectory – fixes a weakness in the operating system that allows any user to gain Administrator access rights.
- TearDrop2** in the teardrop2-fix subdirectory – fixes an operating system vulnerability to the TearDrop denial of service attack. Also includes fixes to OOB, ICMP, and LAND associated attacks.

Additional hot fixes are posted by Microsoft on an ongoing basis.

Note: Hot fixes are intended to be installed in a certain order. Please read Microsoft's installation instructions carefully.

Step 2. Tighten Your Network Configuration

There are two ways to reduce the vulnerability of your engine host to attack from the monitored network:

- Using out-of-band communications over a secure network;
- Implementing access controls for system protocols, ports, and IP services.

These techniques are not mutually exclusive. Both may be used for the highest level of security.

A. Use out-of-band communications over a secure network

A RealSecure engine can use out-of-band communications to communicate with the management console. This is called “stealth” mode and is most commonly accomplished by using two separate adapter cards: one to monitor the local network segment and another to communicate with the console. This increases the security of the RealSecure engine by having it use a separate, possibly more secure, communications channel to send information back to the console.

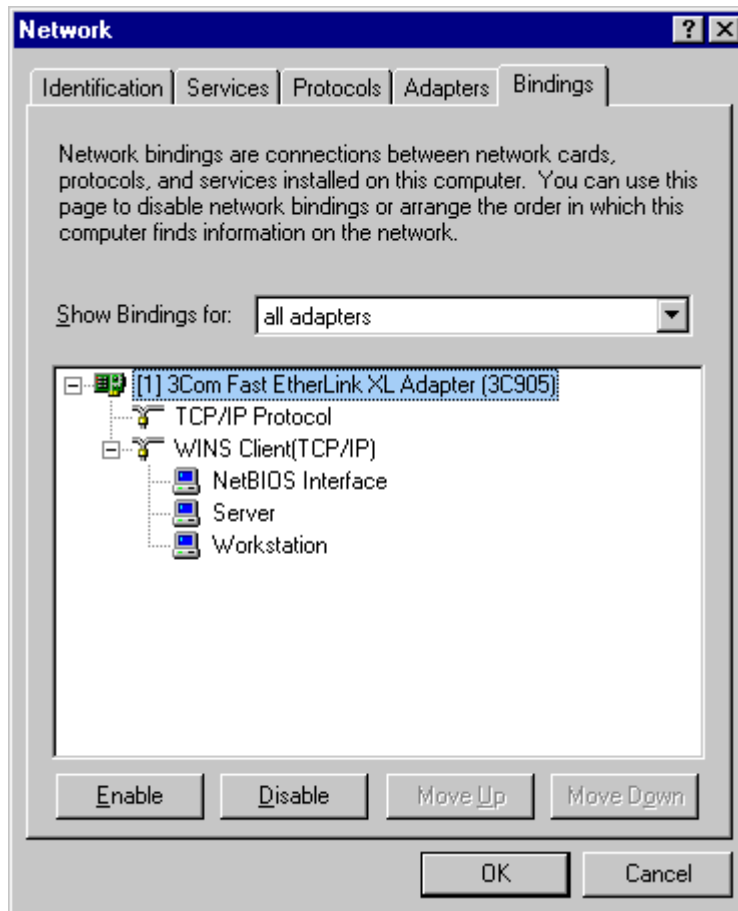


Figure 1. Removing TCP/IP Service from Adapters on Monitored Segment

1. The first step is to ensure that the adapter card connected to the *monitored* network has no protocol stack bound to it.
2. From the Network Control panel, select the “Bindings” tab and show all the bindings for “all adapters”. (See Figure 1.)
3. For the adapter that’s connected to the monitored network segment (be sure you select the right one), highlight each of the entries below the adapter name and select “Disable”. This will disable that particular service through the selected adapter card. By disabling TCP/IP, you are effectively making the adapter invisible from the monitored network segment.
4. The adapter that will be used for communications with the management console, ensure that the TCP/IP service is enabled. Since this is the only service that RealSecure uses, this can be the only service enabled for that adapter, if you wish.

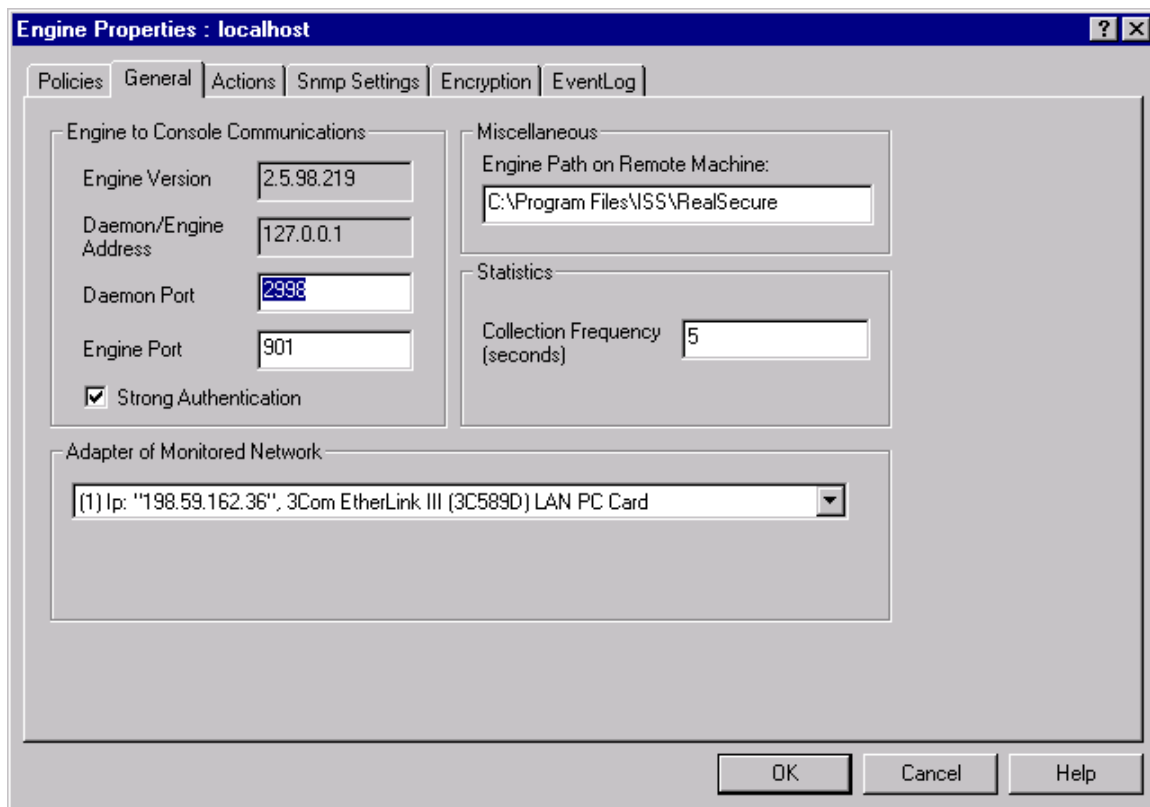


Figure 2. Configuring an Engine to use a second network adapter.

5. From the RealSecure management console, ensure that the “stealth” engine is using the correct IP address to communicate and the correct adapter card for monitoring.
6. In the Engines window, select the engine whose configuration should be stealthy and right-click. Select “Properties”.

7. Select the “General” tab in the window that appears. (Figure 2.)
8. Ensure that the “Engine Address” field contains the IP address that is bound to the adapter that will be used for communications with the management console.
9. Ensure that the “Adapter of Monitored Network” field contains the identifier for the adapter card which is connected to the monitored network and to which no protocol stack is currently attached.

B. Implement Access Controls for System Protocols, Ports, and IP Services

The Windows NT platform should be dedicated for use only as a host for the RealSecure engine or console. (While it is possible to run both the engine and console on the same Windows NT host, it is not recommended, for performance and security reasons.) Therefore, only the network protocols, ports, and services required for RealSecure, plus the minimal set needed for remote configuration and management, should be enabled. All other network access into the host should be disabled.

The following steps will disable all protocols except for TCP/IP and will limit port and service access to the minimum level required for RealSecure. This is done via Microsoft’s access control lists implemented in their protocol stack:

10. Under “Control Panel | Network”, select and delete (one at a time) all protocols except TCP/IP.
11. Select the TCP/IP protocol and click “Properties”.
12. Under Microsoft TCP/IP Properties, click “Advanced”.
13. Under Advanced IP Addressing, click the “Enable Security” box to activate it. Then, click “Configure...”
14. Under TCP/IP Security (Figure 3):

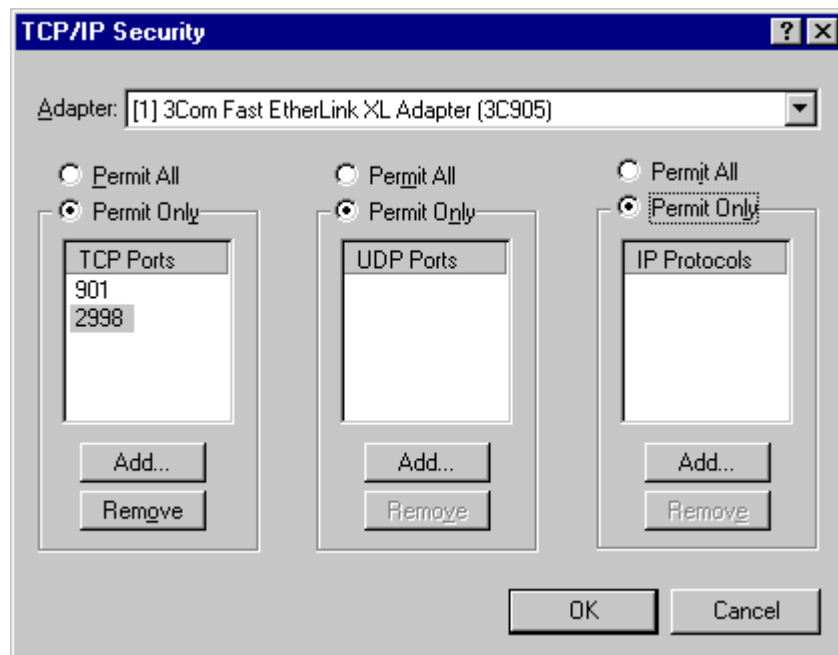


Figure 3. Configuring TCP/IP Access Control List

- a) Over the column "TCP Ports", click "Permit Only"
- b) Under the column "TCP Ports", click "Add"
- c) In the Security Add dialogue box, enter desired TCP Port number(s) for RealSecure engine/console communications then click Add. RealSecure uses one to three TCP ports for engine-console communications. By default, RealSecure will use TCP 2998 for management control data and will dynamically assign an additional TCP port for exchange of event and log data (typically TCP 901). However, you may override these defaults with your own preferences (ports already open through your firewalls, for example). The ports you specify here are the only ones that the engine host will have active, so you need to ensure that they match your preferences for RealSecure engine-console communications.
- d) Over the column "UDP Ports", click "Permit Only" and then leave the list of permitted ports empty. This will prevent any and all UDP traffic to and from the engine host.
- e) Over the column "IP Protocols", click "Permit Only" and then leave the list of permitted protocols empty. This will inhibit any and all IP protocols (other than TCP) to and from the engine host.

Remember that this information is configured on a *per-adapter basis*. So, if you have multiple adapters on the system, you'll need to do this for every adapter with protocol-based network access.

Step3. Tighten Your System Configuration

A. Shut Down Unnecessary Windows NT Services

By default, Windows NT installs with the following services active:

- Alerter
- ClipBook Server
- Computer Browser
- Directory Replicator
- Event Log
- Messenger
- Net Logon
- Network DDE
- Network DDE DSDM
- NT LM Security Support Provider
- Remote Procedure Call (RPC) Locator
- Remote Procedure Call (RPC) Service
- Schedule
- Server
- Spooler
- UPS
- Workstation

In addition to these default services, other services may be listed in the Services dialog box (for example, network transports or other services that have been installed on that computer). RealSecure itself adds the RealSecure Daemon Service.

Services that are not necessary for the operation and management of RealSecure and the platform itself may be disabled as follows:

1. Open the Services control panel. (Figure 4.)
2. In the Services dialogue box, select each of the following services and click “Startup”.
 - Alerter
 - Clipbook Server
 - Computer Browser
 - Directory Replicator
 - Messenger
 - Network DDE
 - Network DDE DSDM
 - Spooler (unless directly-attached printer support is required)
 - UPS (unless the platform will manage its own Uninterruptible Power Supply)
3. In the dialogue box that appears (called “Service”, not *Services*), click the “Disabled” radio button
4. Click OK to confirm

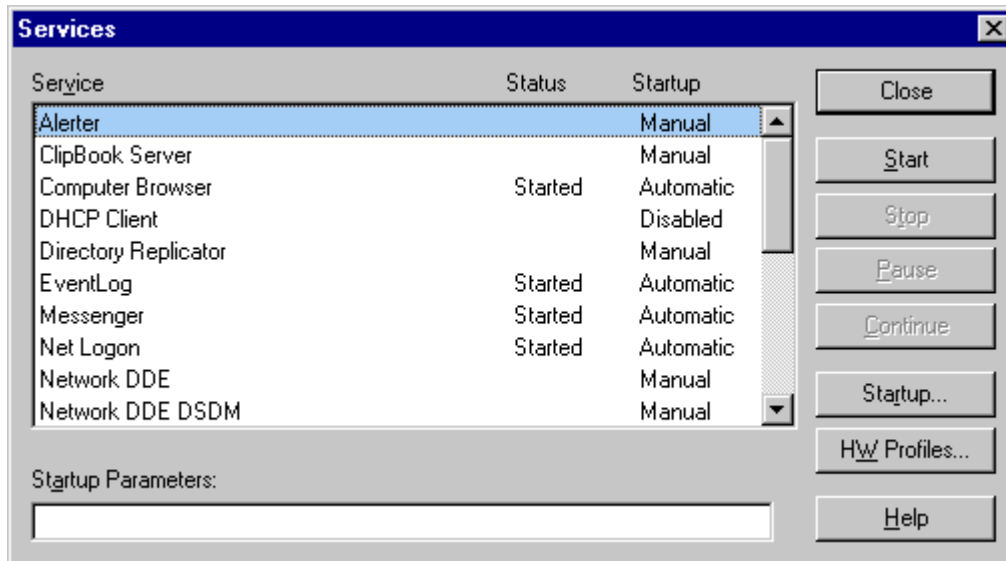


Figure 4. Disabling unnecessary Windows NT services.

These services can generally be disabled, although the need for specific Services depends to a high degree on how the platform is to be remotely managed.

Some Services that *are* required for proper security and operations include:

- EventLog
- RealSecure Daemon

These should never be disabled.

B. Tighten Account and Login Configurations

NT security may be greatly increased by the removal of unnecessary accounts and the proper management of the Administrator account. In addition, registry changes can be made that increase the security of the logon and shutdown procedures, as well as help control network access to information about the platform.

Remove Unneeded Accounts

The only account required for RealSecure engine operation is the Administrator account (technically, any account with Administrator rights), which is provided as a default account in NT. No other accounts should be created, and if they have been, they may be deleted, as follows:

1. Start | Programs | Administrative Tools | User Manager
2. Select the user, then press the Delete key, then OK to confirm, *or*
3. Select the user, then User | Delete from the menu, then OK to confirm
4. Note that default accounts such as Guest cannot be deleted, but should instead be disabled, as follows:
5. Start | Programs | Administrative Tools | User Manager

6. Double click the Guest user, or select Guest and then User | Properties from the menu
7. Under User Properties, click the Account Disabled box to put a checkmark in it
8. Click OK to confirm

Choosing the Administrator Password

The password for the Administrator account (which should be renamed, as described above) should be chosen carefully. It should:

- be a minimum of eight characters
- contain numbers and other symbols (i.e., “+”, “&”, “.”, etc.) as well as letters
- not be a common word, name, or phrase
- be not found in a dictionary in any major language
- not be identified with a person (birthdate, nickname, school mascot) or corporation

Hiding the Last User Name

By default, Windows NT displays the name of the last logged in user in the User name text box of the Logon dialogue box. This potentially allows an attacker to see this name, and then only have to guess the associated password. Hiding the name makes it more difficult for an attacker to obtain both the user name and password.

The Registry Editor can be used to create or assign the following key value to stop the display of the last logged on user name. Figure 5 shows a sample of editing the registry.

Note: Editing the registry involves directly accessing the system’s most sensitive configuration setting. Use extreme care when making these changes. Failure to do so can cause serious operational problems for the host upon reboot.

1. Start | Run | type in REGEDT32 or REGEDIT <enter>

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	DontDisplayLastUserName (under ADD KEY VALUE)
Type:	REG_SZ
Value:	1

Allowing Only Logged-On Users to Shut Down the Computer

Normally, a user can shut down a computer running Windows NT Workstation without logging on by choosing Shutdown in the **Logon** dialog box. This is appropriate where users can access the computer’s operational switches; otherwise, they might tend to turn off the computer’s power or reset it without properly shutting down Windows NT Workstation. However, this feature can be removed if the CPU is locked away. (This step is not required for Windows NT Server, because it is configured this way by default.)

To require users to log on before shutting down the computer, use the Registry Editor to create or assign the following Registry key value. (**Note:** If key exists change value to “0”).):

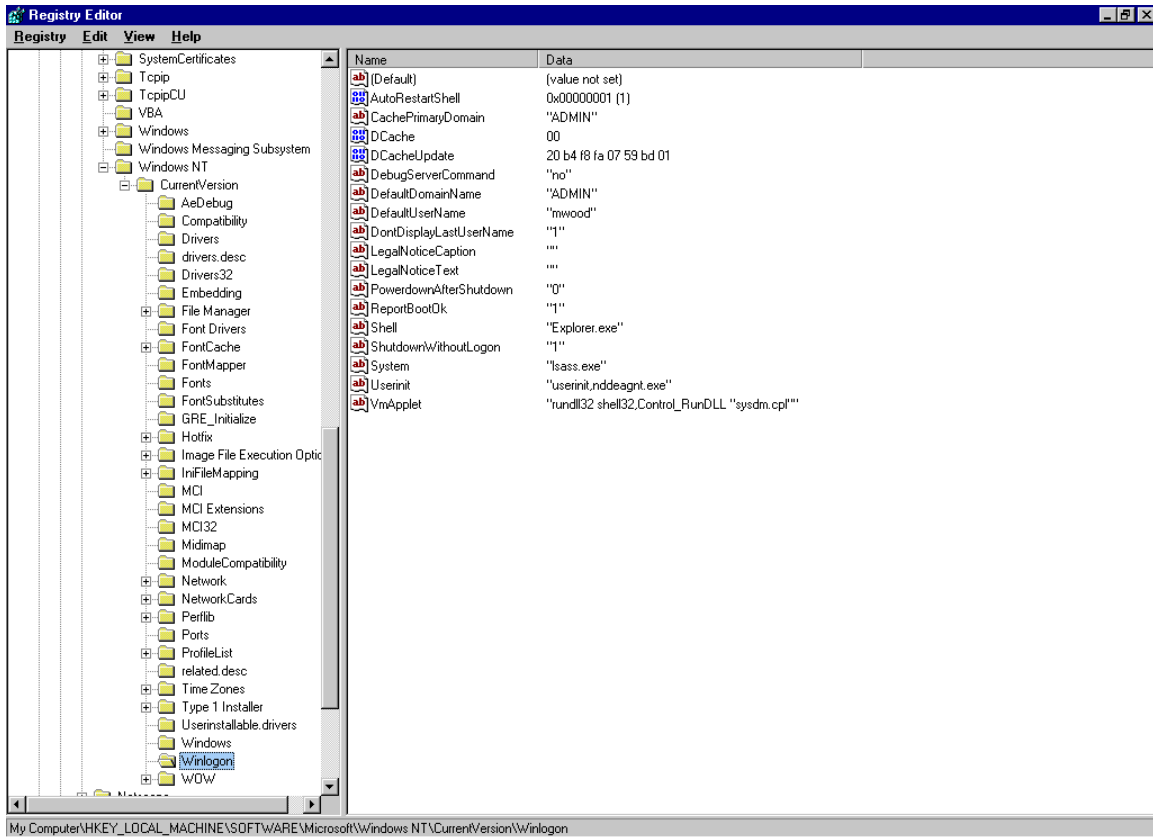


Figure 5. Adding registry entries.

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	ShutdownWithoutLogon
Type:	REG_SZ
Value:	0

Disabling Caching of Logon Credentials During Interactive Logon.

The default configuration of Windows NT caches the last logon credentials for a user who logged on interactively to a system. This feature is provided for system availability reasons such as the user’s machine is disconnected or none of the domain controllers are online.

Even though the credential cache is well protected, in a highly secure environments, customers may want to disable this feature. This can be done by setting the following registry key:

Hive:	HKEY_LOCAL_MACHINE
Key:	Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name:	CachedLogonsCount
Type:	REG_DWORD
Value:	0

Restricting Anonymous Network Access to Lookup Account Names and Groups and Network Shares

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Windows NT 4.0 Service Pack 3 provides a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. Listing account names from Domain Controllers is required by the Windows NT ACL editor, for example, to obtain the list of users and groups to select who a user wants to grant access rights. Listing account names is also used by Windows NT Explorer to select from list of users and groups to grant access to a share.

The registry key value to set for enabling this feature is:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Control\LSA
Name:	RestrictAnonymous
Type:	REG_DWORD
Value:	1.

Please refer to Microsoft Knowledge Base article Q143474 for more details on this.

C. Establish Appropriate File and Directory Protection

Wiping the System Page File During Clean System Shutdown

Virtual Memory support of Windows NT uses a system page file to swap pages from memory of different processes onto disk when they are not being actively used. On a running system, this page file is opened exclusively by the operating system and hence is well-protected. However, systems that are configured to allow booting to other operating systems, may want to ensure that system page file is wiped clean when Windows NT shuts down. This ensures that sensitive information from process memory that may have made into the page file is not available to a snooping user. This can be achieved by setting up the following key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Control\SessionManager\Memory Management
Name:	ClearPageFileAtShutdown
Type:	REG_DWORD
Value:	1

Note that this protection works only during a clean shutdown; therefore it is important that untrusted users do not have ability to power off or reset the system manually.

ACL Settings to Protect Files and Directories

Note: The content of this section is drawn from the Microsoft Corporation white paper, “Microsoft Windows NT – Securing Windows NT Installation”, dated October 23, 1997.

See this white paper, *guidesecnt.doc*, at <http://www.microsoft.com>, for additional information on Windows NT security.

For highly secure platforms, Microsoft recommends the following file protections, applied *immediately after Windows NT is installed*. Be sure to apply permissions to parent directories before applying permissions to subdirectories.

2. First apply the following using the ACL editor:

C: | single click file name | Properties | Security | Permission Tab

Figure 6 shows the resulting screen.

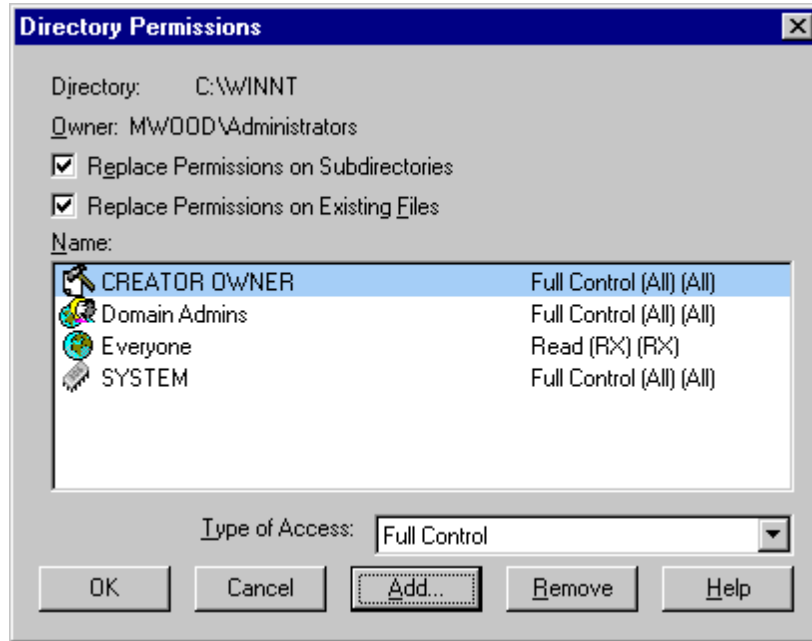


Figure 6. Changing file access permissions.

Directory	Permissions
\WINNT and <i>all subdirectories</i> under it.	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control

3. Now, within the \WINNT tree, apply the following exceptions to the general security:

Directory	Permissions
\WINNT\REPAIR	Administrators: Full Control
\WINNT\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control

\\WINNT\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control
\\WINNT\COOKIES \\WINNT\FORMS \\WINNT\HISTORY \\WINNT\OCCACHE \\WINNT\PROFILES \\WINNT\SENDTO \\WINNT\Temporary Internet Files	Administrators: Full Control CREATOR OWNER: Full Control Everyone: (a)Special Directory Access - Read, Write and Execute (b) Special File Access – None System : Full Control

4. Several critical operating system files exist in the root directory of the system partition on Intel 80486 and Pentium-based systems. In high-security installations, the following permissions are recommended:(under C:\)

File	C2-Level Permissions
\\Boot.ini, \\Ntdetect.com, \\Ntldr	Administrators: Full Control SYSTEM: Full Control
\\Autoexec.bat, \\Config.sys	Everyone: Read Administrators: Full Control SYSTEM: Full Control
\\TEMP directory	Administrators: Full Control SYSTEM: Full Control CREATOR OWNER: Full Control Everyone: (a)Special Directory Access – Read, Write and Execute (b)Special File Access – None

To view these files in File Manager(NT Explorer), choose the **By File Type** command from the **View** menu, then select the **Show Hidden/System Files** check box in the **By File Type** dialog box.(on viewing make sure you can see all under “Options”). Figure 7 shows the dialogue box for the C:\boot.ini file.

Removing Shares

File sharing (i.e., via Microsoft’s SMB, or Server Message Block architecture) is not required for RealSecure, and should be disabled.

Administrative shares may be deleted from the command prompt:

1. Start | Programs | Command Prompt
2. In the DOS Command Prompt window (at the C:\ prompt), enter:

```
C:\> net share admin$ /d
```

(Note: You will need to type in the new name of Administrator, if you have changed it as suggested in the previous section.)

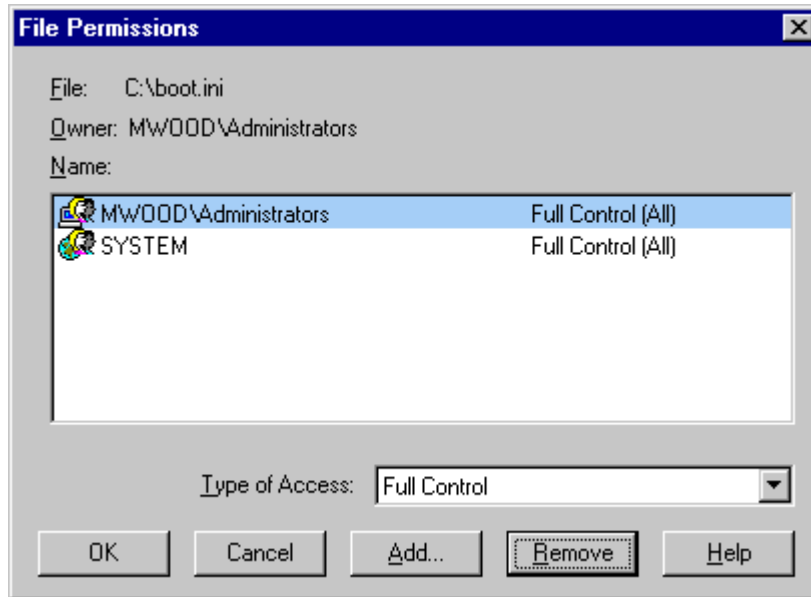


Figure 7. Setting access permissions for critical system files.

3. The response should be “admin\$” was deleted successfully”.

D. Enable System Auditing

An appropriate audit policy balances security against performance and resource usage generated by the logging events.

Recommended Audit Levels

For a dedicated RealSecure engine host, the recommended auditing level is:

- Success and failure auditing for logons and logoffs
- Success auditing for user and group management
- Success auditing for restart, shutdown, and system events
- Success and failure write access auditing for files with .exe and .dll extensions

Enabling Auditing

The above audit levels are enabled as follows:

1. Start | Programs | Administrative Tools | User Manager
2. From User Manager | Policies | Audit. Figure 8 shows the resulting dialogue box.
3. Under Audit Policy, click the Audit These Events radio button
4. Click the following radio buttons:

Logon and Logoff:	Success, Failure
User and Group Management:	Success
Security Policy Changes:	Success, Failure
Restart, Shutdown, and System:	Success, Failure
5. Click OK to confirm

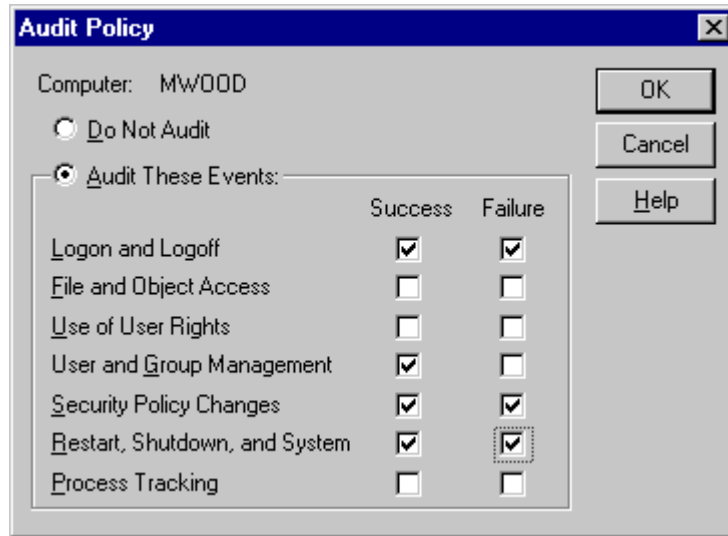


Figure 8. Activating system auditing.

Reviewing Audit Logs

The audit log should be reviewed from time to time by via the Event View utility, to look for unexpected or suspicious events.

1. Start | Programs | Admin Tools | Event View

The RealSecure engine itself writes to the Windows NT Application log.

Further NT Security Security

“In April 1998, Trusted Systems completed a 1-year project for the National Security Agency (NSA) Research Organization to produce guidelines for securely configuring the Windows NT operating system. These guidelines target best commercial and military practice, and are based on extensive research into previous and concurrent efforts. The completed 110-page guidelines are available free from the Trusted Systems website.”
<http://www.trustedsystems.com/NSAGuide.htm>