

Configuration

1 System: LAB1.COM/MBRSRV5.LAB1.COM

Collection: **MBRSRV5.LAB1.COM (2008-03-04 09:05:32)**

Generated: **Tuesday, March 04, 2008 1:00:03 PM**

For: **Michael Godin Admin@lab1.com**

By: Ecora Auditor Professional 4.5 - Windows Module 4.5.8056.22350

Using: Full Report (Configuration Report)

Description: The Configuration report provides detailed documentation of configuration settings for compliance audits, disaster recovery plans, security assessments, migration plans, troubleshooting, and preserving IT knowledge and decisions.

Full Report

Table of Contents

LAB1.COM **2**
 Server MBRSRV5.LAB1.COM 21

Collected Not-Collected Legend

DEFAULT	The value presented in the report was not directly reported by the target, but implied by the current value or lack of a value for the attribute
UA	Unavailable attribute. The current configuration or version of target platform does not provide a value for this attribute. More detail in logs
FC	Collection of value failed
NS	Value not selected for collection

Organization: LAB1

This documentation of the Microsoft® Windows NT/2000® network for LAB1 has been prepared at the request of administrator on Mar-04-2008_09-05-32.

The report about organization LAB1 contains information from 1 domains or workgroups.

The user selected computers for reports from the following domains/workgroups :

- LAB1.COM

The set of sites participating in all links: ***NULL***

The set of all Simple Links: ***NULL***

Computer Types:

Domain Controllers

Collected Computers: *NULL*

Servers

- LAB1.COM/MBRSRV5.LAB1.COM

Workstations

Collected Computers: *NULL*

LAB1.COM

1 Active Directory	3
1.1 Sites	4
1.2 Organizational Units	5
2 Universal Users and Groups	7
3 Global Users and Groups	7
4 Domain Policies (NT4.0)	10
5 Domain Local Users and Groups	10
6 Domain Security Settings	13
6.1 Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}	13
6.2 Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}	15
7 Domain DFS	20
8 Computers	20

LAB1.COM is Domain.

This section describes domain level information.

- Domain name: **LAB1.COM**
- Domain controller name: **MBRSRV1.LAB1.COM**

Domains trusted by this domain: *FC*

Domains that trust this domain: *FC*

List of computers documented from this domain:

- MBRSRV5.LAB1.COM

1 Active Directory

General

The domain LAB1.COM is a child of **NULL** domain.

There are 1 domain controllers in this domain.

Domain Mode

Domain LAB1.COM is running in Windows 2000 mixed mode.

Trusts

Automatically Generated Parent-Child Trusts

Child Trusts:

Trusts - Child: **NULL**

Explicit Trusts

External Trusts:

Trusts - External: **NULL**

Shortcut Trusts

Trusts - Shortcut: **NULL**

Global Catalog Servers

- MBRSRv1.lab1.com

FSMO (Flexible Single Master Operations) Roles

The Schema Master is **MBRSRv1.lab1.com**.

The Domain Naming Master is **MBRSRv1.lab1.com**.

The RID (Relative Identifier) Master is **MBRSRv1.lab1.com**.

The PDC Emulator is **MBRSRv1.lab1.com**.

The Infrastructure Master is **MBRSRv1.lab1.com**.

1.1 Sites

Inter-Site Replication

IP transport Options: ***NULL***

SMTP transport Options:

All site links are bridged. All Schedules are ignored.

This domain contains servers belonging to the following sites:

- Default-First-Site-Name

1.1.1 Site Default-First-Site-Name

This site location is ***NULL***.

Servers:

- MBRSRv1

Subnets: ***NULL***

Site Link List:

- DEFAULTIPSITELINK

Site Link Bridge List: ***NULL***

Bridgehead List:

MBRSRv1 is a preferred bridgehead server for the following transports: ***NULL***

SiteLink DEFAULTIPSITELINK:

This link uses IP as a transport protocol.

Sites in this site link:

- Default-First-Site-Name

This cost of this link is 100.

This link replicate every 180 minutes.

Table 1. Replication Schedule, Day vs. Hour

Hour	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	X	X	X	X	X	X	X
2	X	X	X	X	X	X	X
3	X	X	X	X	X	X	X
4	X	X	X	X	X	X	X

Hour	Sun	Mon	Tue	Wed	Thu	Fri	Sat
5	X	X	X	X	X	X	X
6	X	X	X	X	X	X	X
7	X	X	X	X	X	X	X
8	X	X	X	X	X	X	X
9	X	X	X	X	X	X	X
10	X	X	X	X	X	X	X
11	X	X	X	X	X	X	X
12	X	X	X	X	X	X	X
13	X	X	X	X	X	X	X
14	X	X	X	X	X	X	X
15	X	X	X	X	X	X	X
16	X	X	X	X	X	X	X
17	X	X	X	X	X	X	X
18	X	X	X	X	X	X	X
19	X	X	X	X	X	X	X
20	X	X	X	X	X	X	X
21	X	X	X	X	X	X	X
22	X	X	X	X	X	X	X
23	X	X	X	X	X	X	X
24	X	X	X	X	X	X	X

(X = Replication available)

1.2 Organizational Units

Organizational Units are a special category of the Active Directory Container class that allow delegation of administrative control and the assignment of Group Policy.

1.2.1 Domain Controllers

- Name: **Domain Controllers**
- Parent: **No parent**

1.2.2 Personal Computers

- Name: **Personal Computers**
- Parent: **No parent**

Workstations

- Name: **Workstations**
- Parent: **Personal Computers**

Laptops

- Name: **Laptops**
- Parent: **Personal Computers**

1.2.3 Servers

- Name: **Servers**
- Parent: **No parent**

1.2.4 US-Infrastructure

- Name: **US-Infrastructure**
- Parent: **No parent**

Users - Boston

- Name: **Users - Boston**
- Parent: **US-Infrastructure**

Users - Chicago

- Name: **Users - Chicago**
- Parent: **US-Infrastructure**

Users - Dallas

- Name: **Users - Dallas**
- Parent: **US-Infrastructure**

Users - New York

- Name: **Users - New York**
- Parent: **US-Infrastructure**

Users - San Francisco

- Name: **Users - San Francisco**
- Parent: **US-Infrastructure**

Users - Seattle

- Name: **Users - Seattle**
- Parent: **US-Infrastructure**

Users - St. Louis

- Name: **Users - St. Louis**
- Parent: **US-Infrastructure**

2 Universal Users and Groups

Information about universal groups is not available in Windows 2000 mixed mode.

3 Global Users and Groups

Information about global groups

Administrator Group and Guest Group

The **guest account Guest** is disabled

There are **2 administrators** in the Domain Admins group.

Table 2. Domain Admins Group

Logon ID	Full Name	Expiration Date	Last Logon Date	Last Logon Age	Locked	Disabled	SID
Administrator	*NULL*	*NULL*	3/4/2008 8:59:59 AM	0	No	No	S-1-5-21-912927245-1944328887-185121809-9-500
Madman	Mister Adman	*NULL*	*NULL*	*NULL*	No	No	S-1-5-21-912927245-1944328887-185121809-9-1122

There are **1 guests** in the Domain Guests group.

Table 3. Domain Guests Group

Logon ID	Full Name	Expiration Date	Last Logon Date	Last Logon Age	Locked	Disabled	SID
Guest	*NULL*	*NULL*	*NULL*	*NULL*	No	Yes	S-1-5-21-912927245-1944328887-1851218099-501

There are **12 users** in the Domain Users group.

Table 4. Domain Users Group

Logon ID	Full Name	Primary Group	Last Logon Date	Last Logon Age	Disabled	SID
DBroom	Dick Broom	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1118
HBroom	Harry Broom	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1115
IUSR_MBR SR v1	Internet Guest Account	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1110
IWAM_MBR SR v1	Launch IIS Process Account	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1111
KFace	Kerry Face	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1120

Logon ID	Full Name	Primary Group	Last Logon Date	Last Logon Age	Disabled	SID
krbtgt	*NULL*	Domain Users	*NULL*	*NULL*	Yes	S-1-5-21-912927245-1944328887-1851218099-502
Madman	Mister Adman	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1122
MBroom	Mary Broom	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1117
PFace	Peter Face	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1119
SFace	Strange Face	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1121
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	Domain Users	*NULL*	*NULL*	Yes	S-1-5-21-912927245-1944328887-1851218099-1001
TBroom	Terry Broom	Domain Users	*NULL*	*NULL*	No	S-1-5-21-912927245-1944328887-1851218099-1116

Other Global Groups

Group membership is available with the FFR reports. The other global groups in the **LAB1.COM** domain are:

- Group Name: **DnsUpdateProxy**

- Group Name: **CO_Finance**
- Group Name: **CO_Technology**
- Group Name: **CO_Sales**
- Group Name: **CO_Services**
- Group Name: **CO_Human Resources**
- Group Name: **Domain Computers**
- Group Name: **Domain Controllers**
- Group Name: **Schema Admins**
- Group Name: **Enterprise Admins**
- Group Name: **Group Policy Creator Owners**

4 Domain Policies (NT4.0)

UA

* Attributes for this topic have been suppressed *

5 Domain Local Users and Groups

The list of local users.: ***NULL***

Group Name: **Local Administrators Group**

Table 5. Local Administrators Group

Logon ID	SID
LAB1\Administrator	S-1-5-21-912927245-1944328887-1851218099-500
LAB1\Domain Admins	S-1-5-21-912927245-1944328887-1851218099-512
LAB1\Enterprise Admins	S-1-5-21-912927245-1944328887-1851218099-519

Group Name: **Local Guests Group**

Table 6. Local Guests Group

Logon ID	SID
LAB1\Domain Guests	S-1-5-21-912927245-1944328887-1851218099-514
LAB1\Guest	S-1-5-21-912927245-1944328887-1851218099-501
LAB1\IUSR_MBRSRv1	S-1-5-21-912927245-1944328887-1851218099-1110

Other Local Groups

Group Name: HelpServicesGroup

There are **1** users in group.

Table 7. HelpServicesGroup (Group Members)

Logon ID	SID
LAB1\SUPPORT_388945a0	S-1-5-21-912927245-1944328887-1851218099-1001

Group Name: TelnetClients

GroupLocal_GroupUsers: ***NULL***

Group Name: DnsAdmins

GroupLocal_GroupUsers: ***NULL***

Group Name: IIS_WPG

There are **1** users in group.

Table 8. IIS_WPG (Group Members)

Logon ID	SID
LAB1\IWAM_MBRSRv1	S-1-5-21-912927245-1944328887-1851218099-1111

Group Name: Cert Publishers

GroupLocal_GroupUsers: ***NULL***

Group Name: RAS and IAS Servers

GroupLocal_GroupUsers: ***NULL***

Group Name: Users

There are **3** users in group.

Table 9. Users (Group Members)

Logon ID	SID
LAB1\Domain Users	S-1-5-21-912927245-1944328887-1851218099-513
NT AUTHORITY\Authenticated Users	S-1-5-11
NT AUTHORITY\INTERACTIVE	S-1-5-4

Group Name: Account Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Server Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Print Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Backup Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Replicator

GroupLocal_GroupUsers: ***NULL***

Group Name: Pre-Windows 2000 Compatible Access

There are **1** users in group.

Table 10. Pre-Windows 2000 Compatible Access (Group Members)

Logon ID	SID
NT AUTHORITY\Authenticated Users	S-1-5-11

Group Name: Remote Desktop Users

GroupLocal_GroupUsers: ***NULL***

Group Name: Network Configuration Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Incoming Forest Trust Builders

GroupLocal_GroupUsers: ***NULL***

Group Name: Performance Monitor Users

GroupLocal_GroupUsers: ***NULL***

Group Name: Performance Log Users

There are **1** users in group.

Table 11. Performance Log Users (Group Members)

Logon ID	SID
NT AUTHORITY\NETWORK SERVICE	S-1-5-20

Group Name: Windows Authorization Access Group

There are **1** users in group.

Table 12. Windows Authorization Access Group (Group Members)

Logon ID	SID
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	S-1-5-9

Group Name: Terminal Server License Servers

GroupLocal_GroupUsers: ***NULL***

Group Name: Distributed COM Users

GroupLocal_GroupUsers: ***NULL***

6 Domain Security Settings

6.1 Default Domain Policy

{31B2F340-016D-11D2-945F-00C04FB984F9}

6.1.1 Account Policies

Password Policy (unconfigured options are not shown)

Table 13. Password Policy

Policy	Security Setting	Overridden By
Enforce password history	24 passwords remembered	{31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum password age	42 days	{31B2F340-016D-11D2-945F-00C04FB984F9}
Minimum password age	1 days	{31B2F340-016D-11D2-945F-00C04FB984F9}
Minimum password length	9 characters	{31B2F340-016D-11D2-945F-00C04FB984F9}
Password must meet complexity requirements	Enabled	{31B2F340-016D-11D2-945F-00C04FB984F9}
Store passwords using reversible encryption	Disabled	{31B2F340-016D-11D2-945F-00C04FB984F9}

Account Lockout Policy (unconfigured options are not shown)

Table 14. Account Lockout Policy

Policy	Security Setting	Overridden By
Account lockout threshold	0 invalid logon attempts	{31B2F340-016D-11D2-945F-00C04FB984F9}

Kerberos Policy (unconfigured options are not shown)

Table 15. Kerberos Policy

Policy	Security Setting	Overridden By
Enforce user logon restrictions	Enabled	{31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum lifetime for service ticket	600 minutes	{31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum lifetime for user ticket	10 hours	{31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum lifetime for user ticket renewal	7 days	{31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum tolerance for computer clock synchronization	5 minutes	{31B2F340-016D-11D2-945F-00C04FB984F9}

6.1.2 Local Policies

Audit Policy (unconfigured options are not shown)

NULL

* Attributes for this topic have been suppressed *

User Rights Assignment (unconfigured privilege levels are not shown)

NULL

* Attributes for this topic have been suppressed *

Security Options (unconfigured options are not shown)

NULL

* Attributes for this topic have been suppressed *

6.2 Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}

6.2.1 Account Policies

Password Policy (unconfigured options are not shown)

NULL

* Attributes for this topic have been suppressed *

Account Lockout Policy (unconfigured options are not shown)

NULL

* Attributes for this topic have been suppressed *

Kerberos Policy (unconfigured options are not shown)

NULL

* Attributes for this topic have been suppressed *

6.2.2 Local Policies

Audit Policy (unconfigured options are not shown)

Table 16. Audit Policy

Policy	Security Setting	Overridden By
Audit account logon events	Success	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit account management	Success	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit directory service access	Success	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit logon events	Success	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit object access	No Auditing	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit policy change	Success	{6AC1786C-016F-11D2-945F-00C04fB984F9}

Policy	Security Setting	Overridden By
Audit privilege use	No Auditing	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit process tracking	No Auditing	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Audit system events	Success	{6AC1786C-016F-11D2-945F-00C04fB984F9}

User Rights Assignment (unconfigured privilege levels are not shown)

Table 17. User Rights

Privilege Level	Accounts	Overridden By
Access this computer from the network	Everyone (well-known group) BUILTIN\Administrators (alias) NT AUTHORITY\Authenticated Users (well-known group) NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS (well-known group) BUILTIN\Pre-Windows 2000 Compatible Access (alias) LAB1\IWAM_MBR SRv1 (user)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Add workstations to domain	NT AUTHORITY\Authenticated Users (well-known group)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Adjust memory quotas for a process	LAB1\IWAM_MBR SRv1 (user) NT AUTHORITY\LOCAL SERVICE (well-known group) NT AUTHORITY\NETWORK SERVICE (well-known group) BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Allow log on locally	LAB1\IUSR_MBR SRv1 (user)	{6AC1786C-016F-11D2-945F-00C04fB984F9}

Privilege Level	Accounts	Overridden By
	BUILTIN\Administrators (alias) BUILTIN\Backup Operators (alias) BUILTIN\Account Operators (alias) BUILTIN\Server Operators (alias) BUILTIN\Print Operators (alias)	
Back up files and directories	BUILTIN\Administrators (alias) BUILTIN\Backup Operators (alias) BUILTIN\Server Operators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Bypass traverse checking	Everyone (well-known group) BUILTIN\Administrators (alias) NT AUTHORITY\Authenticated Users (well-known group) BUILTIN\Pre-Windows 2000 Compatible Access (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Change the system time	NT AUTHORITY\LOCAL SERVICE (well-known group) BUILTIN\Administrators (alias) BUILTIN\Server Operators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Create a pagefile	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Debug programs	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Deny access to this computer from the network	LAB1\SUPPORT_388945a0 (user)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Deny to log on locally	LAB1\SUPPORT_388945a0 (user)	{6AC1786C-016F-11D2-945F-00C04fB984F9}

Privilege Level	Accounts	Overridden By
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Force shutdown from a remote system	BUILTIN\Administrators (alias) BUILTIN\Server Operators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Generate security audits	NT AUTHORITY\LOCAL SERVICE (well-known group) NT AUTHORITY\NETWORK SERVICE (well-known group)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Increase scheduling priority	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Load and unload device drivers	BUILTIN\Administrators (alias) BUILTIN\Print Operators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Log on as a batch job	LAB1\Administrator (user) LAB1\IUSR_MBR SRv1 (user) NT AUTHORITY\LOCAL SERVICE (well-known group) LAB1\SUPPORT_388945a0 (user) LAB1\IWAM_MBR SRv1 (user) LAB1\IIS_WPG (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Log on as a service	NT AUTHORITY\NETWORK SERVICE (well-known group)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Manage auditing and security log	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Modify firmware environment values	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Profile single process	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Profile system performance	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}

Privilege Level	Accounts	Overridden By
Remove computer from docking station	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Replace a process level token	LAB1\IWAM_MBRsrV1 (user) NT AUTHORITY\LOCAL SERVICE (well-known group) NT AUTHORITY\NETWORK SERVICE (well-known group)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Restore files and directories	BUILTIN\Administrators (alias) BUILTIN\Backup Operators (alias) BUILTIN\Server Operators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Shut down the system	BUILTIN\Administrators (alias) BUILTIN\Backup Operators (alias) BUILTIN\Server Operators (alias) BUILTIN\Print Operators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Take ownership of files or other objects	BUILTIN\Administrators (alias)	{6AC1786C-016F-11D2-945F-00C04fB984F9}

Security Options (unconfigured options are not shown)

Table 18. Security Options

Policy	Security Setting	Overridden By
Domain controller: LDAP server signing requirements	None	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Microsoft network server: Digitally sign communications (always)	Enabled	{6AC1786C-016F-11D2-945F-00C04fB984F9}

Policy	Security Setting	Overridden By
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Network security: LAN Manager authentication level	Send NTLM response only	{6AC1786C-016F-11D2-945F-00C04fB984F9}

7 Domain DFS

With Distributed File System (DFS), system administrators can make it easy for users to access and manage files that are physically distributed across a network. With DFS, you can make files distributed across multiple servers appear to users as if they reside in one place on the network. Users no longer need to know and specify the actual physical location of files in order to access them.

Domain DFS.: ***NULL***

8 Computers

The following sections contain configuration information for the documented computers.

Computer object.: ***NULL***

Server MBRSRV5.LAB1.COM

- 1 Environment Variables 24**
- 2 Hotfixes 25**
 - 2.1 OS - Installed hotfixes 25
 - 2.2 OS - Required hotfixes 27
 - 2.3 OS - Unconfirmed hotfixes 29
 - 2.4 IIS - Installed hotfixes 29
 - 2.5 IIS - Required hotfixes 29
 - 2.6 IIS - Unconfirmed hotfixes 30
 - 2.7 IE - Installed hotfixes 30
 - 2.8 IE - Required hotfixes 30
 - 2.9 IE - Unconfirmed hotfixes 31
 - 2.10 SQL - Installed hotfixes 31
 - 2.11 SQL - Required hotfixes 31
 - 2.12 SQL - Unconfirmed hotfixes 32
 - 2.13 MDAC - Installed hotfixes 32
 - 2.14 MDAC - Required hotfixes 32
 - 2.15 MDAC - Unconfirmed hotfixes 32
- 3 Applications 32**
- 4 Drivers 33**
- 5 Event Log 47**
- 6 Server DFS roots 47**
- 7 File and Print 47**
 - 7.1 Subfolders Permissions : ADMIN\$ 51
 - 7.2 Subfolders Permissions : C\$ 80
 - 7.3 Subfolders Permissions : IPC\$ 87
- 8 Custom Methods 87**
- 9 Hardware 87**
 - 9.1 Disk Drives 87
 - 9.2 Modems 91
 - 9.3 Network Adapters 91
- 10 Installation 92**
- 11 Local Policies (NT4.0) 92**

- 12 Local Users and Groups 92**
- 13 Networking 96**
 - 13.1 NIC VMware Accelerated AMD PCNet Adapter 96
 - 13.2 Protocol: TCP/IP 97
 - 13.3 SNMP 98
- 14 Processes 98**
- 15 RAS Server 99**
- 16 Replication 100**
- 17 Services 100**
- 18 Scheduled Tasks 104**
- 19 Security Settings 110**
 - 19.1 Account Policies 110
 - 19.2 Local Policies 111
- 20 Terminal server 121**
 - 20.1 Terminal server configuration 121
 - 20.2 Connection RDP-Tcp 121
- 21 WINS Server 123**

Operating system information:

- System Type: **Windows Server**
- Operating System: **Windows 2003 Server, Enterprise Edition**
- Operating System Version: **2003**
- Service Pack: **Service Pack 2**
- System Role: **Member Server**

Internet Explorer information:

- Internet Explorer Version: **6.0.3790.3959**
- Internet Explorer Update Versions: **;SP2;**

Microsoft SQL Server information:

- Microsoft SQL Server Version (registry): **8.00.194**
- Microsoft SQL Server Version (SQLDMO): ***FC***

Internet Information Server information:

- Internet Information Server Version: **6**
- Internet Information Server Minor Version: **0**

This computer's description field contains: ***NULL***

This computer's name and comment cannot be viewed by other computers in the domain: **No**

This machine is providing the following services:

1. Microsoft SQL server
2. Browser Service as backup
3. Root of a DFS tree

To minimize the amount of broadcast traffic on a Microsoft network, Windows NT utilizes a networking browser system. This system consists of a domain Master Browser, Master Browsers, backup browsers, and client computers. When a domain is contained within one subnet, a Master Browser maintains the complete browse list of all registered computers in the domain and the list of other domains on the network. The backup browsers query the Master Browser for the browse list every 15 minutes. The client computers receive browsing information from the Master Browser or a backup browser. When a domain spans more than one subnetwork, the Domain Master Browser (usually the Primary Domain Controller (PDC) of the domain) maintains the complete browse list of all registered computers in the domain and each subnetwork has its own Master Browser and backup browsers.

This server is configured to use **Eastern Standard Time** zone.

Windows will always keep its operating system code in memory even if that memory is needed for something else: **No**

The system **writes** an event to the system log when Windows terminates abnormally.

An existing debug file is overwritten if the system terminates abnormally: **Yes**

Windows reacts to a critical error in the following way:

- This server is set up to reboot automatically after a crash (blue screen): **Yes**
- This server **creates complete memory dump** when it crashes.
- System debugging information is written to file: **%SystemRoot%\MEMORY.DMP**
- This server sends an administrative alert when a crash occurs: **Yes**

Administrative alert names: ***NULL***

This computer is a browse server: **Yes**

This computer is included in the global LMHOSTS file for TCP/IP: **FALSE**

Filename Settings

A short filename is an 8.3 filename; at most eight characters for the name, a period, then at most three characters for the extension.

On this server a mode to create a short filename when it saves to an NTFS partition is disabled: **No**

By default, short filenames are created on an NTFS partition. Disabling this feature increases file performance, but applications that cannot process long filenames cannot find these files.

Long and short filenames are supported on partitions with the FAT file system. By default, Windows supports long filenames on the FAT file system. This allows files that are stored on FAT

volumes in Windows to remain compatible with MS-DOS-based applications and applications designed for previous versions of Windows.

Windows accepts only 8.3 format filenames: **false**

Windows shortens filename extensions to three characters: **true**

By default, Windows truncates all extensions to three characters. This does not change any filename extensions, nor does it change the way filename extensions are displayed or managed by Find, File Manager, or Windows Explorer. This only affects file management commands that are entered in a Command Prompt window (e.g. copy, dir, del).

File Share Settings

This computer is configured to **maximize throughput for file sharing**.

The computer performs SMB signing : **false**

The computer requires SMB signing : **false**

This computer uses the following paging file:

C:\pagefile.sys

- Initial size: **DEFAULT: 768 MB**
- Maximum size: **DEFAULT: 1536 MB**

The system **does not fill** inactive pages in the paging file with zeros when the system stops.

The system **updates** the last-access time stamp on each directory in an NTFS volume as they are listed.

1 Environment Variables

Environment Variables

The %SystemRoot% variable value is: C:\WINDOWS

Table 1. Environment Variables

Variable	Value
ComSpec	%SystemRoot%\system32\cmd.exe
Path	%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;C:\Program Files\Microsoft SQL Server\80\Tools\Binn\
windir	%SystemRoot%
FP_NO_HOST_CHECK	NO
OS	Windows_NT

Variable	Value
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_LEVEL	6
PROCESSOR_IDENTIFIER	x86 Family 6 Model 15 Stepping 8, GenuineIntel
PROCESSOR_REVISION	0f08
NUMBER_OF_PROCESSORS	1
ClusterLog	C:\WINDOWS\Cluster\cluster.log
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
TEMP	%SystemRoot%\TEMP
TMP	%SystemRoot%\TEMP

2 Hotfixes

The information about hotfixes was last updated: Wednesday, February 20, 2008 7:00:00 PM

2.1 OS - Installed hotfixes

The following OS Hotfixes are installed on this computer:

Table 2. Hotfixes

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS07-012	924667	WindowsServer2003-KB924667-v2-x86-ENU.exe	Yes	Yes	Important	The file C:\WINDOWS\system32\mfc42u.dll has a file version that is greater than what is expected.
MS07-029	935966	WindowsServer2003-KB935966-x86-ENU.exe	No	Yes	Critical	Patch Found
MS07-040	931212	NDP20-KB928365-X86.exe	No	Yes	Critical	Patch Found
MS07-040	931212	NDP1.0sp3-KB928367-X86-ENU.exe	Yes	Yes	Critical	The file C:\WINDOWS\microsoft.net\Framework\v1.1.4322\

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
						microsoft.dll has a file version that is greater than what is expected.
MS07-042	936227	msxml6-KB933579-enu-x86.exe	No	Yes	Important	Patch Found
MS07-042	936227	msxml4-KB936181-ENU.exe	No	Yes	Important	Patch Found
MS07-055	923810	WindowsServer2003-KB923810-x86-ENU.exe	No	Yes	Critical	Patch Found
MS07-058	933729	WindowsServer2003-KB933729-x86-ENU.exe	Yes	Yes	Important	The file C:\WINDOWS\system32\rpcrt4.dll has a file version that is greater than what is expected.
MS07-061	943460	WindowsServer2003-KB943460-x86-ENU.exe	Yes	Yes	Critical	The file C:\WINDOWS\system32\shell32.dll has a file version that is greater than what is expected.
MS07-062	941672	WindowsServer2003-KB941672-x86-ENU.exe	No	Yes	Important	Patch Found
MS08-001	941644	WindowsServer2003-KB941644-x86-ENU.exe	Yes	Yes	Critical	The file C:\WINDOWS\system32\drivers\tcpip.sys has a file version that is greater than what is expected.
MS08-002	943485	WindowsServer2003-KB943485-x86-ENU.exe	Yes	Yes	Important	The file C:\WINDOWS\system32\lsasrv.dll has a file version that is greater

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
						than what is expected.

2.2 OS - Required hotfixes

The following OS Hotfixes are not installed and are required on this computer:

Table 3. Hotfixes

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS06-078	923689	WindowsMedia6-KB925398-v2-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\dxmasf.dll has an invalid version.
MS07-017	925902	WindowsServer2003-KB925902-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\user32.dll has an invalid version.
MS07-020	932168	WindowsServer2003-KB932168-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\msagent\agentdpv.dll has an invalid version.
MS07-021	930178	WindowsServer2003-KB930178-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\winsrv.dll has an invalid version.
MS07-022	931784	WindowsServer2003-KB931784-x86-ENU.exe	Yes	No	Important	The file C:\WINDOWS\system32\ntoskrnl.exe has an invalid version.
MS07-031	935840	WindowsServer2003-KB935840-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\schannel.dll has an invalid version.

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS07-035	935839	WindowsServer2003-KB935839-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\kernel32.dll has an invalid version.
MS07-039	926122	WindowsServer2003-KB926122-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\ntdsa.dll has an invalid version.
MS07-040	931212	WindowsServer2003-KB933854-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\microsoft.net\Framework\v1.1.4322\mscorlib.dll has an invalid version.
MS07-042	936227	WindowsServer2003-KB936021-x86-ENU.exe	Yes	No	Important	The file C:\WINDOWS\system32\msxml3.dll has an invalid version.
MS07-043	921503	WindowsServer2003-KB921503-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\oleaut32.dll has an invalid version.
MS07-064	941568	WindowsServer2003-KB941568-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\quartz.dll has an invalid version.
MS07-067	944653	WindowsServer2003-KB944653-x86-ENU.exe	Yes	No	Important	The file C:\WINDOWS\system32\drivers\secdrv.sys has an invalid version.
MS08-003	946538	WindowsServer2003-KB943484-x86-ENU.exe	Yes	No	Important	The file C:\WINDOWS\system32\ntdsa.dll

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
						has an invalid version.
MS08-007	946026	WindowsServer2003-KB946026-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\drivers\mrxdav.sys has an invalid version.
MS08-008	947890	WindowsServer2003-KB943055-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\oleaut32.dll has an invalid version.

2.3 OS - Unconfirmed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.4 IIS - Installed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.5 IIS - Required hotfixes

The following IIS Hotfixes are not installed and are required on this computer:

Table 4. Hotfixes

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS08-005	942831	WindowsServer2003-KB942831-x86-ENU.exe	Yes	No	Important	The file C:\WINDOWS\system32\inetsrv\in focomm.dll has an invalid version.
MS08-006	942830	WindowsServer2003-KB942830-x86-ENU.exe	Yes	No	Important	The file C:\WINDOWS\system32\inetsrv\...

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
						sp.dll has an invalid version.

2.6 IIS - Unconfirmed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.7 IE - Installed hotfixes

The following IE Hotfixes are installed on this computer:

Table 5. Hotfixes

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS07-057	939653	WindowsServer2003-KB939653-x86-ENU.exe	Yes	Yes	Critical	The file C:\WINDOWS\system32\browseui.dll has a file version that is greater than what is expected.
MS07-069	942615	WindowsServer2003-KB942615-x86-ENU.exe	Yes	Yes	Critical	The file C:\WINDOWS\system32\urlmon.dll has a file version that is greater than what is expected.

2.8 IE - Required hotfixes

The following IE Hotfixes are not installed and are required on this computer:

Table 6. Hotfixes

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS07-033	933566	WindowsServer2003-KB933566-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\mshtml.d

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
						ll has an invalid version.
MS07-045	937143	WindowsServer2003-KB937143-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\mshtml.dll has an invalid version.
MS07-050	938127	WindowsServer2003-KB938127-x86-ENU.exe	Yes	No	Critical	The file C:\Program Files\Common Files\microsoft shared\vgx\vgx.dll has an invalid version.
MS08-010	944533	WindowsServer2003-KB944533-x86-ENU.exe	Yes	No	Critical	The file C:\WINDOWS\system32\browseui.dll has an invalid version.

2.9 IE - Unconfirmed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.10 SQL - Installed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.11 SQL - Required hotfixes

The following SQL Hotfixes are not installed and are required on this computer:

Table 7. Hotfixes

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
MS03-031	815495	SQL2000-KB815495-8.00.0818-ENU.exe	Yes	No	Important	The file C:\Program Files\Microsoft

Bulletin	Hotfix name	Service Pack	Required	Installed	Severity	Comment
						SQL Server\MSSQL\bin\sqlrepss.dll has an invalid version.

2.12 SQL - Unconfirmed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.13 MDAC - Installed hotfixes

NULL

* Attributes for this topic have been suppressed *

2.14 MDAC - Required hotfixes

NULL

* Attributes for this topic have been suppressed *

2.15 MDAC - Unconfirmed hotfixes

NULL

* Attributes for this topic have been suppressed *

3 Applications

The following programs are run whenever the system starts up:

1. SunJavaUpdateSched("C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe")
2. VMware Tools(C:\Program Files\VMware\VMware Tools\VMwareTray.exe)
3. VMware User Process(C:\Program Files\VMware\VMware Tools\VMwareUser.exe)
4. WinAutoconfig(wscript /nologo "C:\Program Files\VMware\LM Tools\win_autoconfig.vbs")

Start up applications:

- sqlmangr.exe(C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe)

The following applications are installed:

1. Ecora Auditor 4.1 for Active Directory
2. Ecora Auditor 4.1 for Exchange

3. Ecora Auditor 4.1 for IIS
4. Ecora Auditor 4.1 for MSSQL
5. Ecora Auditor 4.1 for Unix
6. Ecora Auditor 4.1 for Windows
7. Ecora Auditor Professional Executive Dashboard
8. Ecora Reporting Center 2.0
9. Java(TM) 6 Update 3
10. LM Tools
11. Microsoft SQL Server Desktop Engine
12. Microsoft SQL Server Desktop Engine (AUDITOR41)
13. VMware Tools
14. Windows Server 2003 Service Pack 2

4 Drivers

Table 8. Driver Status Table

Name	Type	Start Mode	State	Error Control	Status
Abiosdsk	Kernel	Disabled	not running	Ignore	OK
ACPIEC	Kernel	Disabled	not running	Normal	OK
adpu160m	Kernel	Disabled	not running	Normal	OK
adpu320	Kernel	Disabled	not running	Normal	OK
afcnt	Kernel	Disabled	not running	Normal	OK
AFD	Kernel	System	running	Normal	OK
aic78u2	Kernel	Disabled	not running	Normal	OK
aic78xx	Kernel	Disabled	not running	Normal	OK
AliIde	Kernel	Disabled	not running	Normal	OK
AMD PCNET Compatable Adapter Driver	Kernel	Manual	not running	Normal	OK
AmdIde	Kernel	Disabled	not running	Normal	OK
arc	Kernel	Disabled	not running	Normal	OK
Atdisk	Kernel	Disabled	not running	Ignore	OK
ATM ARP Client Protocol	Kernel	Manual	not running	Normal	OK
Audio Stub Driver	Kernel	Manual	running	Normal	OK
Beep	Kernel	System	running	Normal	OK
cbidf2k	Kernel	Disabled	not running	Normal	OK
cd20xrnt	Kernel	Disabled	not running	Normal	OK

Name	Type	Start Mode	State	Error Control	Status
CD-Burning Filter Driver	Kernel	System	not running	Normal	OK
Cdfs	File System	Disabled	not running	Normal	OK
CD-ROM Driver	Kernel	System	running	Normal	OK
Changer	Kernel	System	not running	Ignore	OK
Cluster Disk Driver	Kernel	Disabled	not running	Normal	OK
CmdIde	Kernel	Disabled	not running	Normal	OK
Cpqarray	Kernel	Disabled	not running	Normal	OK
cpqarray2	Kernel	Disabled	not running	Normal	OK
cpqcissm	Kernel	Disabled	not running	Normal	OK
cpqfcalm	Kernel	Disabled	not running	Normal	OK
CRC Disk Filter Driver	Kernel	Boot	running	Normal	OK
dac2w2k	Kernel	Disabled		Unknown	
dac960nt	Kernel	Disabled	not running	Normal	OK
dellcerc	Kernel	Disabled	not running	Normal	OK
DfsDriver	File System	Boot	running	Normal	OK
Digital CD Audio Playback Filter Driver	Kernel	System	running	Normal	OK
Direct Parallel	Kernel	Manual	running	Normal	OK
Direct Parallel Link Driver	Kernel	Manual	running	Normal	OK
Disk Driver	Kernel	Boot	running	Normal	OK
dmboot	Kernel	Disabled	not running	Normal	OK
dmload	Kernel	Boot	running	Normal	OK
dpti2o	Kernel	Disabled	not running	Normal	OK
elxstor	Kernel	Disabled	not running	Normal	OK
Fastfat	File System	Disabled	running	Normal	OK
Fips	Kernel	System	running	Normal	OK
Floppy Disk Controller Driver	Kernel	Manual	running	Normal	OK
Floppy Disk Driver	Kernel	Manual	running	Normal	OK
FltMgr	File System	Boot	running	Normal	OK

Name	Type	Start Mode	State	Error Control	Status
Fs_Rec	File System Driver Service	System		Ignore	
Generic Packet Classifier	Kernel	Manual	running	Normal	OK
hpcisss	Kernel	Disabled	not running	Normal	OK
hpn	Kernel	Disabled	not running	Normal	OK
hpt3xx	Kernel	Disabled	not running	Normal	OK
HTTP	Kernel	Manual	running	Normal	OK
i2omgmt	Kernel	System	not running	Normal	OK
i2omp	Kernel	Disabled	not running	Normal	OK
i8042 Keyboard and PS/2 Mouse Port Driver	Kernel	System	running	Normal	OK
iirsp	Kernel	Disabled	not running	Normal	OK
Intel AGP Bus Filter	Kernel	Boot	running	Normal	OK
Intel Processor Driver	Kernel	Manual	running	Normal	OK
IntelIde	Kernel	Boot	running	Normal	OK
IP in IP Tunnel Driver	Kernel	Manual	not running	Normal	OK
IP Network Address Translator	Kernel	Manual	not running	Normal	OK
IP Traffic Filter Driver	Kernel	Manual	not running	Normal	OK
IPSEC driver	Kernel	System	running	Normal	OK
ipsraidn	Kernel	Disabled	not running	Normal	OK
IPv6 Windows Firewall Driver	Kernel	Manual	not running	Normal	OK
Keyboard Class Driver	Kernel	System	running	Normal	OK
KSecDD	Kernel	Boot	running	Normal	OK
LicenseInfo	Adapter Arguments	Manual		Normal	
Logical Disk Manager Driver	Kernel	Boot	running	Normal	OK

Name	Type	Start Mode	State	Error Control	Status
Ip6nds35	Kernel	Disabled	not running	Normal	OK
Microcode Update Driver	Kernel	Manual	running	Normal	OK
Microsoft AC Adapter Driver	Kernel	Manual	running	Normal	OK
Microsoft ACPI Driver	Kernel	Boot	running	Normal	OK
Microsoft Composite Battery Driver	Kernel	Boot	running	Normal	OK
Microsoft System Management BIOS Driver	Kernel	Manual	running	Normal	OK
mnmdd	Kernel	System	running	Ignore	OK
Modem	Kernel	Manual	not running	Ignore	OK
Mount Point Manager	Kernel	Boot	running	Normal	OK
Mouse Class Driver	Kernel	System	running	Normal	OK
mraid35x	Kernel	Disabled	not running	Normal	OK
MRXSMB	File System	System	running	Normal	OK
Msfs	File System	System	running	Normal	OK
Mup	File System	Boot	running	Normal	OK
NDIS System Driver	Kernel	Boot	running	Normal	OK
NDIS Usermode I/O Protocol	Kernel	Manual	running	Normal	OK
NDProxy	Kernel	Manual	running	Normal	OK
NetBIOS Interface	File System	System	running	Normal	OK
NetBios over Tcpip	Kernel	System	running	Normal	OK
Network Load Balancing	Kernel	Manual	not running	Normal	OK
nfrd960	Kernel	Disabled	not running	Normal	OK
Npfs	File System	System	running	Normal	OK
Ntfs	File System	Disabled	running	Normal	OK

Name	Type	Start Mode	State	Error Control	Status
Null	Kernel	System	running	Normal	OK
Parallel port driver	Kernel	Manual	running	Normal	OK
Partition Manager	Kernel	Boot	running	Normal	OK
Parvdm	Kernel	Automatic	running	Ignore	OK
PCI Bus Driver	Kernel	Boot	running	Critical	OK
PCIIde	Kernel	Disabled	not running	Normal	OK
Pcmcia	Kernel	Disabled	not running	Normal	OK
PDCOMP	Kernel	Manual	not running	Ignore	OK
PDFRAME	Kernel	Manual	not running	Ignore	OK
PDRELI	Kernel	Manual	not running	Ignore	OK
PDRFRAME	Kernel	Manual	not running	Ignore	OK
perc2	Kernel	Disabled	not running	Normal	OK
perc2hib	Kernel	Disabled	not running	Normal	OK
PnP ISA/EISA Bus Driver	Kernel	Boot	running	Critical	OK
ql1080	Kernel	Disabled	not running	Normal	OK
Ql10wnt	Kernel	Disabled	not running	Normal	OK
ql12160	Kernel	Disabled	not running	Normal	OK
ql1240	Kernel	Disabled	not running	Normal	OK
ql1280	Kernel	Disabled	not running	Normal	OK
ql2100	Kernel	Disabled	not running	Normal	OK
ql2200	Kernel	Disabled	not running	Normal	OK
ql2300	Kernel	Disabled	not running	Normal	OK
RAS Asynchronous Media Driver	Kernel	Manual	not running	Normal	OK
Rdbss	File System	System	running	Normal	OK
RDPCDD	Kernel	System	running	Ignore	OK
RDPWD	Kernel	Manual	running	Ignore	OK
Remote Access Auto Connection Driver	Kernel	System	running	Normal	OK
Remote Access IP ARP Driver	Kernel	Manual	running	Normal	OK

Name	Type	Start Mode	State	Error Control	Status
Remote Access NDIS TAPI Driver	Kernel	Manual	running	Normal	OK
Remote Access NDIS WAN Driver	Kernel	Manual	running	Normal	OK
Remote Access PPPOE Driver	Kernel	Manual	running	Normal	OK
sacdrv	Kernel	Unknown		Unknown	
Secdrv	Kernel	Manual	not running	Normal	OK
Serenum Filter Driver	Kernel	Manual	running	Normal	OK
Serial port driver	Kernel	System	running	Ignore	OK
Sfloppy	Kernel	System	not running	Ignore	OK
Simbad	Kernel	Disabled	not running	Normal	OK
Software Bus Driver	Kernel	Manual	running	Normal	OK
Srv	File System	Manual	running	Normal	OK
Standard IDE/ESDI Hard Disk Controller	Kernel	Boot	running	Normal	OK
Storage volumes	Kernel	Boot	running	Normal	OK
sym_hi	Kernel	Disabled	not running	Normal	OK
sym_u3	Kernel	Disabled	not running	Normal	OK
symc810	Kernel	Disabled	not running	Normal	OK
symc8xx	Kernel	Disabled	not running	Normal	OK
symmpi	Kernel	Disabled	not running	Normal	OK
Sync Driver	Kernel	Automatic	running	Ignore	OK
TCP/IP Protocol Driver	Kernel	System	running	Normal	OK
TDPIPE	Kernel	Manual	not running	Ignore	OK
TDTCP	Kernel	Manual	running	Ignore	OK
Terminal Device Driver	Kernel	System	running	Normal	OK
Terminal Server Device Redirector Driver	Kernel	Manual	running	Normal	OK
TosIde	Kernel	Disabled	not running	Normal	OK

Name	Type	Start Mode	State	Error Control	Status
Udfs	File System	Disabled	running	Normal	OK
ultra	Kernel	Disabled	not running	Normal	OK
vga	Kernel	Manual	not running	Ignore	OK
VGA Display Controller.	Kernel	System	running	Ignore	OK
ViaIde	Kernel	Disabled	not running	Normal	OK
vmdesched Descheduled Time Accounting Service [Driver]	Kernel	Automatic	running	Normal	OK
vm SCSI	Kernel	Boot	running	Normal	OK
VMware Ethernet Adapter Driver	Kernel	Manual	running	Normal	OK
VMware Pointing Device	Kernel	Manual	running	Ignore	OK
VMware server memory controller	Kernel	Automatic	running	Normal	OK
vmx_svga	Kernel	Manual	running	Ignore	OK
Volume Manager Driver	Kernel	Boot	running	Normal	OK
WAN Miniport (L2TP)	Kernel	Manual	running	Normal	OK
WAN Miniport (PPTP)	Kernel	Manual	running	Normal	OK
WDICA	Kernel	Manual	not running	Ignore	OK
WebDav Client Redirector	File System	Manual	not running	Normal	OK
Winsock	Adapter Arguments	Manual		Normal	

Table 9. Driver Information Table

Name	File	Checksum	Version
Abiosdsk	*NULL*	*NULL*	*NULL*
ACPIEC	*NULL*	*NULL*	*NULL*
adpu160m	*NULL*	*NULL*	*NULL*
adpu320	*NULL*	*NULL*	*NULL*

Name	File	Checksum	Version
afcnt	*NULL*	*NULL*	*NULL*
AFD	\C:\WINDOWS\System32\drivers\afd.sys	E55AD49AD3DF929D9858DB4274784DC0	5.2.3790.3959
aic78u2	*NULL*	*NULL*	*NULL*
aic78xx	*NULL*	*NULL*	*NULL*
AliIde	*NULL*	*NULL*	*NULL*
AMD PCNET Compatable Adapter Driver	C:\WINDOWS\system32\DRIVERS\pcntpci5.sys	80655C894B333909EEA0DE92A837F8DD	4.38.0.0
AmdIde	*NULL*	*NULL*	*NULL*
arc	*NULL*	*NULL*	*NULL*
Atdisk	*NULL*	*NULL*	*NULL*
ATM ARP Client Protocol	C:\WINDOWS\system32\DRIVERS\atmarpc.sys	D12DAD5032285343CE3AA4906F661181	5.2.3790.3959
Audio Stub Driver	C:\WINDOWS\system32\DRIVERS\audstub.sys	5BFD980C2107D88101D1DC14055526FC	5.2.3790.0
Beep	*NULL*	*NULL*	*NULL*
cbidf2k	*NULL*	*NULL*	*NULL*
cd20xrnt	*NULL*	*NULL*	*NULL*
CD-Burning Filter Driver	C:\WINDOWS\system32\DRIVERS\imapi.sys	44C132B35921B54B4A9AC64369D86D83	5.2.3790.3959
Cdfs	*NULL*	*NULL*	*NULL*
CD-ROM Driver	C:\WINDOWS\system32\DRIVERS\cdrom.sys	825AA877A852ECC731FA0C39C8C37744	5.2.3790.3959
Changer	*NULL*	*NULL*	*NULL*
Cluster Disk Driver	C:\WINDOWS\system32\DRIVERS\ClusDisk.sys	54308CDF97622FAE1620BB1EC39EF014	5.2.3790.3959
CmdIde	*NULL*	*NULL*	*NULL*
Cpqarray	*NULL*	*NULL*	*NULL*
cpqarry2	*NULL*	*NULL*	*NULL*
cpqcissm	*NULL*	*NULL*	*NULL*
cpqfcalm	*NULL*	*NULL*	*NULL*
CRC Disk Filter Driver	C:\WINDOWS\system32\DRIVERS\crcdisk.sys	0EE27D9DBB208C13314F3C60F66AED26	5.2.3790.3959
dac2w2k	*NULL*	*NULL*	*NULL*
dac960nt	*NULL*	*NULL*	*NULL*
dellcerc	*NULL*	*NULL*	*NULL*

Name	File	Checksum	Version
DfsDriver	C:\WINDOWS\system32\drivers\Dfs.sys	444726B01C31D29C70E60F7C35DE43E5	5.2.3790.3959
Digital CD Audio Playback Filter Driver	C:\WINDOWS\system32\DRIVERS\rebook.sys	C6F8751F3263603935866E71629CFAE4	5.2.3790.3959
Direct Parallel	C:\WINDOWS\system32\DRIVERS\raspti.sys	5B11871DE804D3ED28BBDCC65FE14EDE	5.2.3790.3959
Direct Parallel Link Driver	C:\WINDOWS\system32\DRIVERS\ptilink.sys	0320FD91FB5ED4298355977CECFC0EB4	1.1.0.0
Disk Driver	C:\WINDOWS\system32\DRIVERS\disk.sys	98433302C02F1168EFB7364F8111A179	5.2.3790.3959
dmboot	C:\WINDOWS\System32\drivers\dmboot.sys	89FA376D83042F6F1AED505106A5719D	5.2.3790.3959
dmload	C:\WINDOWS\System32\drivers\dmload.sys	3D9BFA13B6F1CD2D91C50C52B32E91A2	5.2.3790.0
dpti2o	*NULL*	*NULL*	*NULL*
elxstor	*NULL*	*NULL*	*NULL*
Fastfat	*NULL*	*NULL*	*NULL*
Fips	*NULL*	*NULL*	*NULL*
Floppy Disk Controller Driver	C:\WINDOWS\system32\DRIVERS\fdc.sys	5090CD3F6AB1D71AD507953CFF556EA9	5.2.3790.3959
Floppy Disk Driver	C:\WINDOWS\system32\DRIVERS\flpydisk.sys	C621A51F415419A3145A5939ABDE39FA	5.2.3790.0
FltMgr	C:\WINDOWS\system32\drivers\fltmgr.sys	F978277EF786532195CDD9F88E908632	5.2.3790.3959
Fs_Rec	*NULL*	*NULL*	*NULL*
Generic Packet Classifier	C:\WINDOWS\system32\DRIVERS\msgpc.sys	30B1653A955F548352024A5FEE203CC3	5.2.3790.3959
hpcisss	*NULL*	*NULL*	*NULL*
hpn	*NULL*	*NULL*	*NULL*
hpt3xx	*NULL*	*NULL*	*NULL*
HTTP	C:\WINDOWS\System32\Drivers\HTTP.sys	5B2B71A50CCCA34C453D415D2ECE7426	5.2.3790.3959
i2omgmt	*NULL*	*NULL*	*NULL*
i2omp	*NULL*	*NULL*	*NULL*
i8042 Keyboard and	C:\WINDOWS\system32\DRIVERS\i8042prt.sys	68E8FF9EEAF8B37A66CAC2C57835FFBD	5.2.3790.3959

Name	File	Checksum	Version
PS/2 Mouse Port Driver			
iirsp	*NULL*	*NULL*	*NULL*
Intel AGP Bus Filter	C:\WINDOWS\system32\DRIVERS\agp440.sys	B9985042687A43685 FC64B282B627653	5.2.3790.3959
Intel Processor Driver	C:\WINDOWS\system32\DRIVERS\intelppm.sys	7D7575B971B3A0FE2 6FAC6F5D58F5180	5.2.3790.3959
IntelIde	C:\WINDOWS\system32\DRIVERS\intelide.sys	1690A4BE249BA6195 BA7258943CADA58	5.2.3790.3959
IP in IP Tunnel Driver	C:\WINDOWS\system32\DRIVERS\ipinip.sys	*NULL*	
IP Network Address Translator	C:\WINDOWS\system32\DRIVERS\ipnat.sys	890E7A14A63AEC2EA 9257A79A88BE784	5.2.3790.3959
IP Traffic Filter Driver	C:\WINDOWS\system32\DRIVERS\ipfltdrv.sys	5A41F207B7C39EE49 18F7496A4F19B14	5.2.3790.3959
IPSEC driver	C:\WINDOWS\system32\DRIVERS\ipsecc.sys	1A9AEAC49683B32D F55B7FB1516F3028	5.2.3790.3959
ipsraidn	*NULL*	*NULL*	*NULL*
IPv6 Windows Firewall Driver	C:\WINDOWS\system32\drivers\ip6fw.sys	D7E7E7898A05C53D D862B49828747C1E	5.2.3790.3959
Keyboard Class Driver	C:\WINDOWS\system32\DRIVERS\kbdclass.sys	E5097A07E14F36ABC 21FA18D88F93655	5.2.3790.3959
KSecDD	*NULL*	*NULL*	*NULL*
LicenseInfo	*NULL*	*NULL*	*NULL*
Logical Disk Manager Driver	C:\WINDOWS\System32\drivers\dmio.sys	15081421EE62DC1C9 5ABB387D9081571	5.2.3790.3959
Ip6nds35	*NULL*	*NULL*	*NULL*
Microcode Update Driver	C:\WINDOWS\system32\DRIVERS\update.sys	424421053064846A8 5D32B048EA27E7E	5.2.3790.3959
Microsoft AC Adapter Driver	C:\WINDOWS\system32\DRIVERS\CmBatt.sys	F9D6ABD426E51ED3 F688D42D8467C62D	5.2.3790.3959
Microsoft ACPI Driver	C:\WINDOWS\system32\DRIVERS\ACPI.sys	A0A850BAC6F8A88A D0FC964C6BEA170D	5.2.3790.3959
Microsoft Composite Battery Driver	C:\WINDOWS\system32\DRIVERS\compbatt.sys	1DCBF98F0FA712E38 4A1A2926F774673	5.2.3790.3959

Name	File	Checksum	Version
Microsoft System Management BIOS Driver	C:\WINDOWS\system32\DRIVERS\msmbios.sys	92AFAB2F216CE8FFB AD3BC510FCF4A33	5.2.3790.3959
mnmdd	*NULL*	*NULL*	*NULL*
Modem	*NULL*	*NULL*	*NULL*
Mount Point Manager	*NULL*	*NULL*	*NULL*
Mouse Class Driver	C:\WINDOWS\system32\DRIVERS\mouseclass.sys	AA50DA5AB638CE0B AB5F7D5D633110C2	5.2.3790.0
mraid35x	*NULL*	*NULL*	*NULL*
MRXSMB	C:\WINDOWS\system32\DRIVERS\mrxsm.sys	C6C81D1B96F6090C 10D517BDCD504D6A	5.2.3790.3959
Msfs	*NULL*	*NULL*	*NULL*
Mup	*NULL*	*NULL*	*NULL*
NDIS System Driver	*NULL*	*NULL*	*NULL*
NDIS Usermode I/O Protocol	C:\WINDOWS\system32\DRIVERS\ndisuio.sys	8B8E682B03483092E 17AB9DFE70FEDFF	5.2.3790.3959
NDProxy	*NULL*	*NULL*	*NULL*
NetBIOS Interface	C:\WINDOWS\system32\DRIVERS\netbios.sys	A0D5D6AE530CA78A 062FC0471F1E6F78	5.2.3790.3959
NetBios over Tcpip	C:\WINDOWS\system32\DRIVERS\netbt.sys	5CD7CCA08498EC87 53B22E92D367CA11	5.2.3790.3959
Network Load Balancing	C:\WINDOWS\system32\DRIVERS\wlbs.sys	D346E2F289F23E557 DDFB9132D1DAB35	5.2.3790.3959
nfrd960	*NULL*	*NULL*	*NULL*
Npfs	*NULL*	*NULL*	*NULL*
Ntfs	*NULL*	*NULL*	*NULL*
Null	*NULL*	*NULL*	*NULL*
Parallel port driver	C:\WINDOWS\system32\DRIVERS\parport.sys	EE3333B36DEB86A0 D472F037172DA10A	5.2.3790.3959
Partition Manager	*NULL*	*NULL*	*NULL*
Parvdm	C:\WINDOWS\system32\DRIVERS\parvdm.sys	A9D29F3D7AE71B7E A721B53A0C436C66	5.2.3790.0

Name	File	Checksum	Version
PCI Bus Driver	C:\WINDOWS\system32\DRIVERS\pci.sys	8217000E5C53CE823 B3111F339E47C41	5.2.3790.3959
PCIIde	*NULL*	*NULL*	*NULL*
Pcmcia	*NULL*	*NULL*	*NULL*
PDCOMP	*NULL*	*NULL*	*NULL*
PDFRAME	*NULL*	*NULL*	*NULL*
PDRELI	*NULL*	*NULL*	*NULL*
PDRFRAME	*NULL*	*NULL*	*NULL*
perc2	*NULL*	*NULL*	*NULL*
perc2hib	*NULL*	*NULL*	*NULL*
PnP ISA/EISA Bus Driver	C:\WINDOWS\system32\DRIVERS\isapnp.sys	B71BA04A3B5D4404 225CCDBF1969078F	5.2.3790.3959
ql1080	*NULL*	*NULL*	*NULL*
Ql10wnt	*NULL*	*NULL*	*NULL*
ql12160	*NULL*	*NULL*	*NULL*
ql1240	*NULL*	*NULL*	*NULL*
ql1280	*NULL*	*NULL*	*NULL*
ql2100	*NULL*	*NULL*	*NULL*
ql2200	*NULL*	*NULL*	*NULL*
ql2300	*NULL*	*NULL*	*NULL*
RAS Asynchronous Media Driver	C:\WINDOWS\system32\DRIVERS\asynmac.sys	A35B971F631D4DFD EB68D71E770D2CE9	5.2.3790.0
Rdbss	C:\WINDOWS\system32\DRIVERS\rd bss.sys	54EA9B760EC1BEBFF 9E1DE5FA97F029D	5.2.3790.3959
RDPCDD	C:\WINDOWS\System32\DRIVERS\R DPCDD.sys	AC5BB528ECD2BEA4 FF4BFF9DF9BAF749	5.2.3790.0
RDPWD	*NULL*	*NULL*	*NULL*
Remote Access Auto Connection Driver	C:\WINDOWS\system32\DRIVERS\ras acd.sys	48EE7B6802C0306F9 A66F34DB7E9EF75	5.2.3790.0
Remote Access IP ARP Driver	C:\WINDOWS\system32\DRIVERS\wa narp.sys	CE030B1D05A01FA01 2D32F2D25676B1C	5.2.3790.3959
Remote Access NDIS TAPI Driver	C:\WINDOWS\system32\DRIVERS\ndi stapi.sys	BBAB8CE7A8D2B130 2DA0B03825D9CAE4	5.2.3790.3959

Name	File	Checksum	Version
Remote Access NDIS WAN Driver	C:\WINDOWS\system32\DRIVERS\ndiswan.sys	1B397EEF4614419BE5679E0209F7848B	5.2.3790.3959
Remote Access PPPOE Driver	C:\WINDOWS\system32\DRIVERS\rasppoe.sys	59842F0A22216A71CADE6F89FE84C973	5.2.3790.3959
sacdrv	*NULL*	*NULL*	*NULL*
Secdrv	C:\WINDOWS\system32\DRIVERS\secdrv.sys	07F7F501AD50DE2BA2D5842D9B6D6155	4.0.60.0
Serenum Filter Driver	C:\WINDOWS\system32\DRIVERS\serenum.sys	B261D4597BF9A2723B7020207260C72A	5.2.3790.3959
Serial port driver	C:\WINDOWS\system32\DRIVERS\serial.sys	95768FDE08DD34089AA90DCCB5537704	5.2.3790.3959
Sfloppy	*NULL*	*NULL*	*NULL*
Simbad	*NULL*	*NULL*	*NULL*
Software Bus Driver	C:\WINDOWS\system32\DRIVERS\swenum.sys	93965919785102BA847545AB460CE2DF	5.3.3790.3959
Srv	C:\WINDOWS\system32\DRIVERS\srvsrv.sys	7B50365292862D4825AB014E0719C524	5.2.3790.3959
Standard IDE/ESDI Hard Disk Controller	C:\WINDOWS\system32\DRIVERS\atapi.sys	FF953A8F08CA3F822127654375786BBE	5.2.3790.3959
Storage volumes	C:\WINDOWS\system32\DRIVERS\volmgr.sys	45AE67C387A640EC6E228F30D421F088	5.2.3790.3959
sym_hi	*NULL*	*NULL*	*NULL*
sym_u3	*NULL*	*NULL*	*NULL*
symc810	*NULL*	*NULL*	*NULL*
symc8xx	*NULL*	*NULL*	*NULL*
symmpi	*NULL*	*NULL*	*NULL*
Sync Driver	\\?\C:\WINDOWS\system32\Drivers\lgtosync.sys	*NULL*	
TCP/IP Protocol Driver	C:\WINDOWS\system32\DRIVERS\tcpip.sys	76788FA017C0FD42E32D21555AB4FD89	5.2.3790.3959
TDPIPE	*NULL*	*NULL*	*NULL*
TDTCP	*NULL*	*NULL*	*NULL*
Terminal Device Driver	C:\WINDOWS\system32\DRIVERS\termdd.sys	A01E46FFF445A38D35DB188C5458582C	5.2.3790.3959

Name	File	Checksum	Version
Terminal Server Device Redirector Driver	C:\WINDOWS\system32\DRIVERS\rdpdr.sys	FF678596B761E1CCB A79F49981EF51BC	5.2.3790.3959
TosIde	*NULL*	*NULL*	*NULL*
Udfs	*NULL*	*NULL*	*NULL*
ultra	*NULL*	*NULL*	*NULL*
vga	C:\WINDOWS\system32\DRIVERS\vgaapnp.sys	2EB062B434792BB6B B614F107DD3A5CF	5.2.3790.3959
VGA Display Controller.	\C:\WINDOWS\System32\drivers\vga.sys	062FBC10147FD837D 819F94AA394E661	5.2.3790.3959
ViaIde	*NULL*	*NULL*	*NULL*
vmdesched Descheduled Time Accounting Service [Driver]	\??\C:\WINDOWS\system32\Drivers\vmdesched.sys	*NULL*	
vm SCSI	C:\WINDOWS\system32\drivers\vm SCSI.sys	55A928C40C11870DF 5B90300BA329878	1.2.0.4
VMware Ethernet Adapter Driver	C:\WINDOWS\system32\DRIVERS\vmxnet.sys	86E4207553B1179E1 163D570FF7E67BC	2.0.0.8
VMware Pointing Device	C:\WINDOWS\system32\DRIVERS\vmmouse.sys	84E67BAA77A8C508 A05B9FEBB1ED2EAE	12.2.0.0
VMware server memory controller	\??\C:\Program Files\VMware\VMware Tools\Drivers\memctl\vmemctl.sys	*NULL*	
vmx_svga	C:\WINDOWS\system32\DRIVERS\vmx_svga.sys	6E237C0A8E248DDB 6811C05834C8A15F	11.2.0.0
Volume Manager Driver	C:\WINDOWS\system32\DRIVERS\ftdisk.sys	4C533B70AFA917416 AEC57FCBEECB57D	5.2.3790.3959
WAN Miniport (L2TP)	C:\WINDOWS\system32\DRIVERS\rasl2tp.sys	3633175613E052ECB 41776DEE2777A89	5.2.3790.3959
WAN Miniport (PPTP)	C:\WINDOWS\system32\DRIVERS\raspptp.sys	4454F2639BCCA93BE 86A45137E427277	5.2.3790.3959
WDICA	*NULL*	*NULL*	*NULL*

Name	File	Checksum	Version
WebDav Client Redirector	C:\WINDOWS\system32\DRIVERS\mrxdav.sys	8CEEAC40903CE5DD 1B82F813BAF0A4AB	5.2.3790.3959
Winsock	*NULL*	*NULL*	*NULL*

5 Event Log

The following lists the **Application** log settings for this computer:

- The maximum size of the log file is **16384** KB
- **The log will overwrite events as needed once the maximum size of the log file has been reached.**
- The Application Event Log is located at **%SystemRoot%\system32\config\AppEvent.Evt**
- Guest access to this log **is restricted.**

The following lists the **Security** log settings for this computer:

- The maximum size of the log file is **16384** KB
- **The log will overwrite events as needed once the maximum size of the log file has been reached.**
- The Security Event Log is located at **%SystemRoot%\System32\config\SecEvent.Evt**
- Guest access to this log **is restricted.**

The following lists the **System** log settings for this computer:

- The maximum size of the log file is **16384** KB
- **The log will overwrite events as needed once the maximum size of the log file has been reached.**
- The System Event Log is located at **%SystemRoot%\system32\config\SysEvent.Evt**
- Guest access to this log **is restricted.**

6 Server DFS roots

Server DFS roots.: ***NULL***

7 File and Print

Amount of idle time required before suspending session: **15** minutes

This computer broadcasts its presence to LAN Manager servers: **No**

Restrict anonymous access to Named Pipes and Shares: **Yes**

The following shares are listed for access through a null session:

1. COMCFG
2. DFS\$

The following pipes are listed for access through a null session:

1. COMNAP
2. COMNODE
3. SQL\QUERY
4. SPOOLSS
5. NETLOGON
6. LSARPC
7. SAMR
8. BROWSER

File Shares

There are **3 shared directories** on this machine

File Share **ADMIN\$** :

- Share Name: **ADMIN\$**
- Remark: **Remote Admin**
- Path: **C:\WINDOWS**
- User Limit: **unlimited**
- NTFS Owner: **BUILTIN\Administrators (alias)**
- Share Protection: **UNPROTECTED**
- NTFS Protection: **PROTECTED**
- Share Encryption: **UNENCRYPTED**
- Share Compression: **UNCOMPRESSED**

Table 10. Share Permissions for ADMIN\$

Share	Account	Share Permissions
ADMIN\$	BUILTIN\Administrators (alias)	Allow - Main(Full).

Table 11. Share NTFS Permissions for ADMIN\$

Share	Account	NTFS Permissions	Applies To	Inherited	Inherited From
ADMIN\$	BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only	No	
ADMIN\$	BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only	No	
ADMIN\$	BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only	No	
ADMIN\$	BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only	No	

Share	Account	NTFS Permissions	Applies To	Inherited	Inherited From
ADMIN\$	BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only	No	
ADMIN\$	BUILTIN\Users (alias)	Allow - Main(Read).	This folder only	No	
ADMIN\$	CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only	No	
ADMIN\$	NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only	No	
ADMIN\$	NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only	No	

File Share **C\$** :

- Share Name: **C\$**
- Remark: **Default share**
- Path: **C:**
- User Limit: **unlimited**
- NTFS Owner: **BUILTIN\Administrators (alias)**
- Share Protection: **UNPROTECTED**
- NTFS Protection: **PROTECTED**
- Share Encryption: **UNENCRYPTED**
- Share Compression: **UNCOMPRESSED**

Table 12. Share Permissions for C\$

Share	Account	Share Permissions
C\$	BUILTIN\Administrators (alias)	Allow - Main(Full).

Table 13. Share NTFS Permissions for C\$

Share	Account	NTFS Permissions	Applies To	Inherited	Inherited From
C\$	BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files	No	
C\$	BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files	No	
C\$	BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	Subfolders only	No	
C\$	BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders	No	
C\$	CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only	No	
C\$	Everyone (well-known group)	Allow - Main(Read).	This folder only	No	
C\$	NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files	No	

File Share **IPC\$** :

- Share Name: **IPC\$**
- Remark: **Remote IPC**
- Path:
- User Limit: **unlimited**
- NTFS Owner:
- Share Protection: **UNPROTECTED**
- NTFS Protection: **ACCESSERROR**
- Share Encryption: **ENCRYPTED**
- Share Compression: **COMPRESSED**

Table 14. Share Permissions for IPC\$

Share	Account	Share Permissions
IPC\$	BUILTIN\Administrators (alias)	Allow - Main(Full).

The share NTFS permission.: ***NULL***

Printer Settings: ***NULL***

Default Spool Directory: **C:\WINDOWS\system32\spool\PRINTERS**

7.1 Subfolders Permissions : ADMIN\$.

Subfolders search was limited as following:

- Depth Limit : **1**

Permissions for ADMIN\$\\$NtServicePackUninstall\$:

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

Permissions for ADMIN\$\adam :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\addins :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\adfs :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Application Compatibility Scripts :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\AppPatch :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\assembly :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Cluster :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Config :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Connection Wizard :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Cursors :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Debug :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Special(Traverse Directory/Execute File,Read Attributes,Read Permissions).	This folder only
BUILTIN\Users (alias)	Allow - Special(Traverse Directory/Execute File,Read Attributes,Read Permissions).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Downloaded Program Files :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Driver Cache :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\ehome :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Fonts :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Help :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\TERMINAL SERVER USER (well-known group)	Allow - Main(Read); Special(Create Files/Write Data,Create Folders/Append Data,Write Extended Attributes,Write Attributes).	This folder only
NT AUTHORITY\TERMINAL SERVER USER (well-known group)	Allow - Main(Read, Write & Execute).	Subfolders and files only

Permissions for ADMIN\$\IIS Temporary Compressed Files :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
MBSRVS5\IIS_WPG (alias)	Allow - Main(Full).	This folder, subfolders and files
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\ime :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\inf :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Installer :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
Everyone (well-known group)	Allow - Main(Read & Execute).	Subfolders and files only
Everyone (well-known group)	Allow - Main(Read).	This folder only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\java :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Media :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Microsoft.NET :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\msagent :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\msapps :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\mui :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\OemDir :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Offline Web Pages :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\pchealth :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\PeerNet :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\PolicyBackup :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Prefetch :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Provisioning :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Registration :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
Everyone (well-known group)	Allow - Main(Read).	Files only

Account	NTFS Permissions	AppliesTo
Everyone (well-known group)	Allow - Main(Read).	This folder only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\repair :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(List).	Subfolders only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Resources :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\SchCache :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\security :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Special(.	Subfolders only
BUILTIN\Power Users (alias)	Allow - Special(Traverse Directory/Execute File,Read Attributes,Read Permissions).	This folder only
BUILTIN\Users (alias)	Allow - Special(.	Subfolders only
BUILTIN\Users (alias)	Allow - Special(Traverse Directory/Execute File,Read Attributes,Read Permissions).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\ServicePackFiles :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\SoftwareDistribution :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\srchasst :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Sun :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\system :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read); Special(Traverse Directory/Execute File).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\system32 :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\TAPI :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Write); Special(Delete).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read & Write); Special(Delete).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\LOCAL SERVICE (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\LOCAL SERVICE (well-known group)	Allow - Main(Full).	This folder only
NT AUTHORITY\NETWORK SERVICE (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\NETWORK SERVICE (well-known group)	Allow - Main(Full).	This folder only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Tasks :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Backup Operators (alias)	Allow - Main(Read); Special(Create Files/Write Data).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files
S-1-5-32-549	Allow - Main(Read); Special(Create Files/Write Data).	This folder only

Permissions for ADMIN\$\Temp :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data,Create Folders/Append Data,Traverse Directory/Execute File).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\NETWORK SERVICE (well-known group)	Allow - Special(List Folder/Read Data,Delete).	This folder, subfolders and files
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\twain_32 :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\Web :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only

Account	NTFS Permissions	AppliesTo
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for ADMIN\$\WinSxS :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

7.2 Subfolders Permissions : C\$.

Subfolders search was limited as following:

- Depth Limit : **1**

Permissions for C\$\41 installers :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

Permissions for C\$\Add-Ins :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files
S-1-5-21-30278392-942497004-1890470277-500	Allow - Main(Full).	This folder only

Permissions for C\$\Builds :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files
S-1-5-21-30278392-942497004-1890470277-500	Allow - Main(Full).	This folder only

Permissions for C\$\Documents and Settings :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Power Users (alias)	Allow - Main(Read).	This folder only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
Everyone (well-known group)	Allow - Main(Read & Execute).	Subfolders and files only
Everyone (well-known group)	Allow - Main(Read).	This folder only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for C\$\Inetpub :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

Permissions for C\$\MSDERelA :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

Permissions for C\$\MSSQL :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

Permissions for C\$\Program Files :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\TERMINAL SERVER USER (well-known group)	Allow - Main(Change).	This folder only
NT AUTHORITY\TERMINAL SERVER USER (well-known group)	Allow - Main(Modify).	Subfolders and files only

Permissions for C\$\RECYCLER :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

Permissions for C\$\System Volume Information :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only

Account	NTFS Permissions	AppliesTo
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for C\$\WINDOWS :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	Subfolders and files only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Change).	This folder only
BUILTIN\Power Users (alias)	Allow - Main(Modify).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	Subfolders and files only
BUILTIN\Users (alias)	Allow - Main(Read).	This folder only
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder only

Permissions for C\$\wmpub :

Account	NTFS Permissions	AppliesTo
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder only
BUILTIN\Administrators (alias)	Allow - Main(Full).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Main(Read & Execute).	This folder, subfolders and files
BUILTIN\Users (alias)	Allow - Special(Create Files/Write Data).	This folder and subfolders
BUILTIN\Users (alias)	Allow - Special(Create Folders/Append Data).	This folder and subfolders

Account	NTFS Permissions	AppliesTo
CREATOR OWNER (well-known group)	Allow - Main(Full).	Subfolders and files only
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).	This folder, subfolders and files

7.3 Subfolders Permissions : IPC\$.

Subfolders search was limited as following:

- Depth Limit : **1**

The share subfolder item.: **NULL**

8 Custom Methods

Custom Method object.: **NULL**

9 Hardware

The hardware information for this computer is presented in the table.

- # of CPUs: **1**
- # of physical CPUs: **1**
- Processors:
 - Processor #0
 - Name: Intel(R) Xeon(R) CPU 5130 @ 2.00GHz
 - Type: x86 Family 6 Model 15 Stepping 8
 - Speed: 1995 MHz
- Model: **AT/AT COMPATIBLE**
- Physical memory: **511 MB**
- System BIOS version:
 - A. PTLTD - 6040000
 - B. PhoenixBIOS 4.0 Release 6.0
- Video BIOS version: **NULL**
- Video BIOS date:

9.1 Disk Drives

Disk Overview:

- Total number of logical disks on this system: **1**
- Total disk space on this system: **20466 MB**
- Total free disk space on this system: **15060 MB**

9.1.1 Physical Drives

The following sections contain configuration information for the physical devices on this computer.

Physical Drive 0

The information about physical disk 0 is presented in the list.

Table 15. Disk Drive 0

Short Description:	VMware Virtual disk SCSI Disk Device
Manufacturer:	(Standard disk drives)
Description:	Disk drive
Capabilities:	Random Access Supports Writing
Error Code:	0
Device ID:	\\.\PHYSICALDRIVE0
Name:	\\.\PHYSICALDRIVE0
Index:	0
Interface Type:	SCSI
Media Loaded:	Yes
Media Type:	Fixed hard disk media
No. of partitions:	1
PnP Device ID:	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK&REV_1.0\4&5FCAAFC&0&000
Attached to SCSI Bus:	0
SCSI LUN:	0
SCSI Port:	1
SCSI ID:	0
System Name:	MBRSRV5
Device status:	OK
Bytes per sector:	512
Sectors per track:	63
Tracks per cylinder:	255
Total sectors:	41929650
Total cylinders:	2610
Total heads:	255
Total disk size:	20 GB

The information about partitions for physical disk 0 is presented in the table.

Disk #0, Partition #0

- Short Description: **Disk #0, Partition #0**
- Description: **Installable File System**
- Total size: **20 GB**
- DeviceID: **Disk #0, Partition #0**
- Name: **Disk #0, Partition #0**
- Bootable: **Yes**
- Active (boot) partition: **Yes**
- Is primary partition: **Yes**
- Partition type: **Installable File System**
- Physical disk containing this partition: **0**
- Number of this partition: **0**
- Starting offset(bytes) of this partition: **32256**
- Block size: **512**
- Number of blocks: **41913522**
- System Name: **MBRSRV5**

9.1.2 Logical Drives

The information about logical drives is presented in list.

Drive C:

- Letter: **C:**
- Size: **20**
- Free Space: **15**
- Caption: **C:**
- Description: **Local Fixed Disk**
- Volume Name: ***NULL***
- Volume Serial Number: **9C511562**
- File System: **NTFS**
- Drive Type: **Local Disk**
- Access: ***NULL***
- Install Date: ***NULL***
- Block Size: ***NULL***
- Number of Blocks: ***NULL***
- Max Component Length: **255**
- Provider Name: ***NULL***
- File Based Compression: **1**
- Compressed: **0**
- Configuration Manager Error Code: ***NULL***
- Media Type: **12**
- Device ID: **C:**
- PNP Device ID: ***NULL***
- Power Management Supported: ***NULL***

- System Name: **MBRSRV5**
- Availability: ***NULL***
- Status: ***NULL***
- Partition:
 - Disk #0, Partition #0

Drive D:

- Letter: **D:**
- Size: **2**
- Free Space: **0**
- Caption: **D:**
- Description: **CD-ROM Disc**
- Volume Name: **Windows 2003**
- Volume Serial Number: **C6E3F017**
- File System: **UDF**
- Drive Type: **Compact Disc**
- Access: ***NULL***
- Install Date: ***NULL***
- Block Size: ***NULL***
- Number of Blocks: ***NULL***
- Max Component Length: **255**
- Provider Name: ***NULL***
- File Based Compression: **0**
- Compressed: **0**
- Configuration Manager Error Code: ***NULL***
- Media Type: **11**
- Device ID: **D:**
- PNP Device ID: ***NULL***
- Power Management Supported: ***NULL***
- System Name: **MBRSRV5**
- Availability: ***NULL***
- Status: ***NULL***
- Partition: ***NULL***

Drive A:

- Letter: **A:**
- Size: ***NULL***
- Free Space: ***NULL***
- Caption: **A:**
- Description: **3 1/2 Inch Floppy Drive**
- Volume Name: ***NULL***
- Volume Serial Number: ***NULL***
- File System: ***NULL***
- Drive Type: **Removable Disk**
- Access: ***NULL***
- Install Date: ***NULL***
- Block Size: ***NULL***

- Number of Blocks: **NULL**
- Max Component Length: **NULL**
- Provider Name: **NULL**
- File Based Compression: **NULL**
- Compressed: **NULL**
- Configuration Manager Error Code: **NULL**
- Media Type: **5**
- Device ID: **A:**
- PNP Device ID: **NULL**
- Power Management Supported: **NULL**
- System Name: **MBRSRV5**
- Availability: **NULL**
- Status: **NULL**
- Partition: **NULL**

9.2 Modems

The following sections contain configuration information for the modems on this computer.

The modems information (registry-based).: **NULL**

9.3 Network Adapters

The network adapter information for this computer is presented in list.

9.3.1 NIC VMware Accelerated AMD PCNet Adapter

Description: VMware Accelerated AMD PCNet Adapter

Device Service Name: vmxnet

Device Driver Description: VMware Ethernet Adapter Driver

Device Driver: C:\WINDOWS\system32\DRIVERS\vmxnet.sys

Manufacturer: VMware, Inc.

MAC Address: 00:50:56:1A:00:3B

DMA Channel: **NULL**

I/O Port Resources: 0x00001080-0x000010FF

NetCfgInstanceIdList: **NULL**

TCP/IP Adapter Configuration

- IP Address:
10.1.3.149

- Default Gateway:
10.1.0.7
- Subnet Mask:
255.255.0.0
- DHCP Enabled: **false**
- DHCP Server: ***NULL***
- Name Server: **10.1.3.141,192.168.3.2,192.168.0.10**
- WINS Primary: ***NULL***
- WINS Secondary: ***NULL***
- DNS Service Search Order:
10.1.3.141
192.168.3.2
192.168.0.10

10 Installation

OS version: Windows 2003 Server, Enterprise Edition, Service Pack 2

This instance of Windows is registered to user: **Ecora**

This instance of Windows is registered to organization: **Ecora Software**

The type of the Windows installed on this machine: **Uniprocessor Free**

The Windows operating system was installed on: **Thursday, June 28, 2007 12:46:08 PM**

Windows was installed on the partition: **\Device\HarddiskVolume1**

Windows was installed in: **C:\WINDOWS**

Windows was installed from: **D:\ENGLISH\WIN2003\32BIT\ENT_WITH_SP1**

The computer was installed with the Microsoft Product ID: **69713-357-6515425-42700**

The computer is installed with the CD key: **357-6515425**

11 Local Policies (NT4.0)

UA

* Attributes for this topic have been suppressed *

12 Local Users and Groups

The admin account is **Administrator**. The account 'Administrator' (Administrator) has not been renamed.

The guest account is **Guest**. Disabled (not renamed)

Local Users

There are **7 users**.

Table 16. Local Users

Logon ID	Full Name	Last Logon Date	Last Logon Age	Locked	Disabled	SID
Administrator	*NULL*	2/25/2008 5:59:35 PM	8	No	No	S-1-5-21-1869771424-154553404-372537654-500
ASPNET	ASP.NET Machine Account	*NULL*	*NULL*	No	No	S-1-5-21-1869771424-154553404-372537654-1006
Guest	*NULL*	*NULL*	*NULL*	No	Yes	S-1-5-21-1869771424-154553404-372537654-501
IUSR_MBR SR V5	Internet Guest Account	2/13/2008 10:30:41 AM	20	No	No	S-1-5-21-1869771424-154553404-372537654-1003
IWAM_MBR SR V5	Launch IIS Process Account	2/7/2008 4:00:40 PM	26	No	No	S-1-5-21-1869771424-154553404-372537654-1004
MBuser	Mister Bad User	*NULL*	*NULL*	No	No	S-1-5-21-1869771424-154553404-372537654-1010
SUPPORT_38 8945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	*NULL*	*NULL*	No	Yes	S-1-5-21-1869771424-154553404-372537654-1001

Group Name: **Local Administrators Group**

Table 17. Local Administrators Group

Logon ID	SID
LAB1\Domain Admins	S-1-5-21-912927245-1944328887-1851218099-512
MBRSRV5\Administrator	S-1-5-21-1869771424-154553404-372537654-500

Group Name: **Local Guests Group**

Table 18. Local Guests Group

Logon ID	SID
MBRSRV5\Guest	S-1-5-21-1869771424-154553404-372537654-501
MBRSRV5\IUSR_MBRSRV5	S-1-5-21-1869771424-154553404-372537654-1003

Other Local Groups

Group Name: HelpServicesGroup

There are **1** users in group.

Table 19. HelpServicesGroup (Group Members)

Logon ID	SID
MBRSRV5\SUPPORT_388945a0	S-1-5-21-1869771424-154553404-372537654-1001

Group Name: TelnetClients

GroupLocal_GroupUsers: ***NULL***

Group Name: IIS_WPG

There are **4** users in group.

Table 20. IIS_WPG (Group Members)

Logon ID	SID
MBRSRV5\IWAM_MBRSRV5	S-1-5-21-1869771424-154553404-372537654-1004
NT AUTHORITY\NETWORK SERVICE	S-1-5-20
NT AUTHORITY\SERVICE	S-1-5-6
NT AUTHORITY\SYSTEM	S-1-5-18

Group Name: EcoraRCA_Viewers

GroupLocal_GroupUsers: ***NULL***

Group Name: EcoraRCA_Runners

GroupLocal_GroupUsers: ***NULL***

Group Name: EcoraRCA_Admins

There are **1** users in group.

Table 21. EcoraRCA_Admins (Group Members)

Logon ID	SID
LAB1\Administrator	S-1-5-21-912927245-1944328887-1851218099-500

Group Name: Users

There are **5** users in group.

Table 22. Users (Group Members)

Logon ID	SID
LAB1\Domain Users	S-1-5-21-912927245-1944328887-1851218099-513
MBRSRV5\ASPNET	S-1-5-21-1869771424-154553404-372537654-1006
MBRSRV5\MBuser	S-1-5-21-1869771424-154553404-372537654-1010
NT AUTHORITY\Authenticated Users	S-1-5-11
NT AUTHORITY\INTERACTIVE	S-1-5-4

Group Name: Power Users

GroupLocal_GroupUsers: ***NULL***

Group Name: Print Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Backup Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Replicator

GroupLocal_GroupUsers: ***NULL***

Group Name: Remote Desktop Users

GroupLocal_GroupUsers: ***NULL***

Group Name: Network Configuration Operators

GroupLocal_GroupUsers: ***NULL***

Group Name: Performance Monitor Users

GroupLocal_GroupUsers: ***NULL***

Group Name: Performance Log Users

There are **1** users in group.

Table 23. Performance Log Users (Group Members)

Logon ID	SID
NT AUTHORITY\NETWORK SERVICE	S-1-5-20

Group Name: Distributed COM Users

GroupLocal_GroupUsers: **NULL**

13 Networking

The following sections list the detected network adapters, the protocol information for each adapter, and the TCP/IP protocol as configured for this machine. Additional adapter hardware information is located in the Hardware section.

13.1 NIC VMware Accelerated AMD PCNet Adapter

This NIC is a VMware Accelerated AMD PCNet Adapter. It has type Ethernet 802.3 adapter.

The status of the device is **NULL**.

The availability of the device is Running/Full Power.

The NIC was last reset on 2/13/2008 4:07:48 PM. This adapter does not support power management.

The name of the device driver for this NIC is vmxnet.sys.

The MAC Address is 00:50:56:1A:00:3B.

The IRQ number is 18.

13.1.1 TCP/IP Adapter Configuration

- IP Address:
10.1.3.149
- Default Gateway:
10.1.0.7
- Subnet Mask:
255.255.0.0
- DHCP Enabled: **false**
- DHCP Server: **NULL**
- DHCP Lease Obtained: **NULL**
- DHCP Lease Expires: **NULL**
- DHCP Domain: **NULL**
- Domain: **NULL**
- DHCP Name Server: **NULL**
- Name Server: **10.1.3.141,192.168.3.2,192.168.0.10**
- WINS Primary: **NULL**
- WINS Secondary: **NULL**
- WINS EnableLMHostsLookup: **1**
- WINS ScopeID: **NULL**
- DNS Service Search Order:
10.1.3.141

192.168.3.2
192.168.0.10

13.1.2 Internet Protocol Security (IPSec)

- IP Security Policy: **NULL**
- IP Security Name: **NULL**
- Description: **NULL**

Port and Protocol Filtering

Port and Protocol filtering is **not enabled** on this computer.

Filtered TCP Ports:

- 0

Filtered UDP Ports:

- 0

Filtered IP Protocols:

- 0

A value of **[0]** indicates that all ports/protocols are permitted.

13.1.3 IPX

The IPX protocol is not present on this computer.

13.1.4 Other Protocols

This section does not include NetBEUI and DLC protocols.

- Caption: **Tcpip**
- Description: **TCP/IP Protocol Driver**
- Name: **MSAFD Tcpip [UDP/IP]**
- Status: **OK**

13.2 Protocol: TCP/IP

This section describes TCP/IP information for this computer.

The hostname for this computer is MBRSRV5.

Windows NT **does not route** IP packets between networks to which it is connected.

The Domain Name Server (DNS) Domain Name for this computer is lab1.com.

TCP/IP **does do** Address Resolution Protocol (ARP) queries with source routing enabled on Token Ring networks.

TCP/IP **does** attempt to detect if a gateway has become inactive.

TCP/IP **allows** **DEFAULT: 128** seconds for an IP packet to reach its destination.

This computer sends and receives IP Multicast (full IGMP).

Keep alive retransmissions are spaced **DEFAULT: 1000** milliseconds apart until a response has been received.

TCP/IP keep alive requests are spaced **DEFAULT: 7200000** milliseconds

TCP/IP will retransmit an IP packet **DEFAULT: 5** before aborting the connection.

The number of bytes that may be transmitted before an acknowledgment is required from the receiving server is **DEFAULT: 8760** bytes

13.3 SNMP

NULL

* Attributes for this topic have been suppressed *

14 Processes

The processes running on this server are presented in the following table:

Table 24. The processes running on this server at the time it was queried by Ecora Enterprise Auditor for Windows

Process Name	Process ID	Parent Process	Memory Usage	Virtual Memory Used
auditor.exe	2884	548	20951040	114592
csrss.exe	332	280	1277952	1608
csrss.exe	2288	280	3600384	1004
dllhost.exe	2268	404	1507328	2448
EcoraLogSvc.exe	1100	404	1667072	740
EcoraMonitor.exe	1764	404	1892352	1904
EcoraSchedulerService.exe	1808	404	2306048	1400
explorer.exe	548	2988	4608000	10396
icmdCController.exe	4088	404	8736768	5836
inetinfo.exe	1224	404	1392640	3260
jusched.exe	3256	548	1482752	1136
lsass.exe	416	356	5464064	8136
msdtc.exe	988	404	364544	1688
RCAWinService.exe	1564	404	10665984	15448
rdpclip.exe	3496	408	1273856	912

Process Name	Process ID	Parent Process	Memory Usage	Virtual Memory Used
scrnsave.scr	3924	408	1204224	248
services.exe	404	356	3842048	3928
smss.exe	280	4	249856	128
spoolsv.exe	960	404	1974272	3076
sqlmangr.exe	2984	548	1044480	1092
sqlservr.exe	1276	404	1802240	14184
sqlservr.exe	1320	404	44142592	42576
svchost.exe	604	404	1564672	840
svchost.exe	668	404	2379776	1516
svchost.exe	740	404	2215936	3996
svchost.exe	756	404	1220608	1228
svchost.exe	792	404	13443072	13716
svchost.exe	1168	404	212992	500
svchost.exe	1652	404	1351680	628
svchost.exe	3200	404	1101824	2872
svchost.exe	1980	404	2101248	2348
System	4	0	65536	0
System Idle Process	0	0	28672	0
VMwareService.exe	1704	404	51363840	49964
VMwareTray.exe	1800	548	581632	844
VMwareUser.exe	2764	548	815104	1064
winlogon.exe	408	280	4399104	4844
winlogon.exe	356	280	8273920	7648
WmcServerService.exe	1120	404	507904	2364
wmiprvse.exe	2312	604	1138688	2064
wmiprvse.exe	3168	604	7999488	6476
wuaucflt.exe	3836	408	4816896	5336

15 RAS Server

This server **has RAS installed.**

RAS connections **are not logged.**

RAS **automatically disconnects** idle connections after **NULL** minutes.

RAS connections are disconnected when user who initiate them logs off.

16 Replication

NULL

* Attributes for this topic have been suppressed *

17 Services

The service start settings for this computer are presented in the following table:

Table 25. Service Start Settings and Current State

Service Name	Start Method	Startup Account	State
Alerter	Disabled	NT AUTHORITY\Local Service	not running
Application Experience Lookup Service	Automatic	LocalSystem	running
Application Layer Gateway Service	Manual	NT AUTHORITY\Local Service	not running
Application Management	Manual	LocalSystem	running
ASP.NET State Service	Manual	NT AUTHORITY\NetworkService	not running
Automatic Updates	Automatic	LocalSystem	running
Background Intelligent Transfer Service	Manual	LocalSystem	not running
ClipBook	Disabled	LocalSystem	not running
COM+ Event System	Automatic	LocalSystem	running
COM+ System Application	Manual	LocalSystem	running
Computer Browser	Automatic	LocalSystem	running
Cryptographic Services	Automatic	LocalSystem	running
DCOM Server Process Launcher	Automatic	LocalSystem	running
DHCP Client	Automatic	NT AUTHORITY\NetworkService	running
Distributed File System	Manual	LocalSystem	not running
Distributed Link Tracking Client	Automatic	LocalSystem	running
Distributed Link Tracking Server	Disabled	LocalSystem	not running

Service Name	Start Method	Startup Account	State
Distributed Transaction Coordinator	Automatic	NT AUTHORITY\NetworkService	running
DNS Client	Automatic	NT AUTHORITY\NetworkService	running
Ecora Log Service for Auditor 4.1	Manual	LocalSystem	running
Ecora Monitor for Configuration Auditor 4.1	Automatic	LocalSystem	running
Ecora Policy Calculator	Automatic	LocalSystem	running
Ecora Reporting Center 2.0	Automatic	LocalSystem	running
Ecora Scheduler Service for Auditor 4.1	Automatic	LocalSystem	running
Ecora WMC Server Service for Auditor 4.1	Automatic	LocalSystem	running
Error Reporting Service	Automatic	LocalSystem	running
Event Log	Automatic	LocalSystem	running
File Replication	Manual	LocalSystem	not running
Help and Support	Automatic	LocalSystem	running
HTTP SSL	Manual	LocalSystem	running
Human Interface Device Access	Disabled	LocalSystem	not running
IIS Admin Service	Automatic	LocalSystem	running
IMAPI CD-Burning COM Service	Disabled	LocalSystem	not running
Indexing Service	Disabled	LocalSystem	not running
InstallDriver Table Manager	Manual	LocalSystem	not running
Intersite Messaging	Disabled	LocalSystem	not running
IPSEC Services	Automatic	LocalSystem	running
Kerberos Key Distribution Center	Disabled	LocalSystem	not running
License Logging	Disabled	NT AUTHORITY\NetworkService	not running
Logical Disk Manager	Automatic	LocalSystem	running
Logical Disk Manager Administrative Service	Manual	LocalSystem	not running
Messenger	Disabled	LocalSystem	not running
Microsoft Software Shadow Copy Provider	Manual	LocalSystem	not running

Service Name	Start Method	Startup Account	State
MSSQL\$AUDITOR41	Automatic	LocalSystem	running
MSSQLSERVER	Automatic	LocalSystem	running
MSSQLServerADHelper	Manual	LocalSystem	not running
Net Logon	Automatic	LocalSystem	running
NetMeeting Remote Desktop Sharing	Disabled	LocalSystem	not running
Network Connections	Manual	LocalSystem	running
Network DDE	Disabled	LocalSystem	not running
Network DDE DSDM	Disabled	LocalSystem	not running
Network Location Awareness (NLA)	Manual	LocalSystem	running
Network Provisioning Service	Manual	LocalSystem	not running
NT LM Security Support Provider	Manual	LocalSystem	not running
Performance Logs and Alerts	Automatic	NT Authority\NetworkService	not running
Plug and Play	Automatic	LocalSystem	running
Portable Media Serial Number Service	Manual	LocalSystem	not running
Print Spooler	Automatic	LocalSystem	running
Protected Storage	Automatic	LocalSystem	running
Remote Access Auto Connection Manager	Manual	LocalSystem	not running
Remote Access Connection Manager	Manual	LocalSystem	not running
Remote Desktop Help Session Manager	Manual	LocalSystem	not running
Remote Procedure Call (RPC)	Automatic	NT Authority\NetworkService	running
Remote Procedure Call (RPC) Locator	Manual	NT AUTHORITY\NetworkService	not running
Remote Registry	Automatic	NT AUTHORITY\LocalService	running
Removable Storage	Manual	LocalSystem	not running
Resultant Set of Policy Provider	Manual	LocalSystem	not running
Routing and Remote Access	Disabled	LocalSystem	not running
Secondary Logon	Automatic	LocalSystem	running

Service Name	Start Method	Startup Account	State
Security Accounts Manager	Automatic	LocalSystem	running
Server	Automatic	LocalSystem	running
Shell Hardware Detection	Automatic	LocalSystem	running
Smart Card	Manual	NT AUTHORITY\Local Service	not running
Special Administration Console Helper	Manual	LocalSystem	not running
SQLAgent\$AUDITOR41	Manual	LocalSystem	not running
SQLSERVERAGENT	Manual	LocalSystem	not running
System Event Notification	Automatic	LocalSystem	running
Task Scheduler	Automatic	LocalSystem	running
TCP/IP NetBIOS Helper	Automatic	NT AUTHORITY\Local Service	running
Telephony	Manual	LocalSystem	not running
Telnet	Disabled	NT AUTHORITY\Local Service	not running
Terminal Services	Manual	LocalSystem	running
Terminal Services Session Directory	Disabled	LocalSystem	not running
Themes	Disabled	LocalSystem	not running
Uninterruptible Power Supply	Manual	NT AUTHORITY\Local Service	not running
Virtual Disk Service	Manual	LocalSystem	not running
VMware Descheduled Time Accounting Service	Manual	LocalSystem	not running
VMware Tools Service	Automatic	LocalSystem	running
Volume Shadow Copy	Manual	LocalSystem	not running
WebClient	Disabled	NT AUTHORITY\Local Service	not running
Windows Audio	Disabled	LocalSystem	not running
Windows Firewall/Internet Connection Sharing (ICS)	Disabled	LocalSystem	not running

Service Name	Start Method	Startup Account	State
Windows Image Acquisition (WIA)	Disabled	NT AUTHORITY\Local Service	not running
Windows Installer	Manual	LocalSystem	not running
Windows Management Instrumentation	Automatic	LocalSystem	running
Windows Management Instrumentation Driver Extensions	Manual	LocalSystem	not running
Windows Time	Automatic	NT AUTHORITY\Local Service	running
Windows User Mode Driver Framework	Manual	NT AUTHORITY\Local Service	not running
WinHTTP Web Proxy Auto-Discovery Service	Manual	NT AUTHORITY\Local Service	not running
Wireless Configuration	Automatic	LocalSystem	running
WMI Performance Adapter	Manual	LocalSystem	not running
Workstation	Automatic	LocalSystem	running
World Wide Web Publishing Service	Automatic	LocalSystem	running

18 Scheduled Tasks

Table with all scheduled tasks and their status is presented below:

Table 26. Scheduled tasks for LAB1.COM/MBRSRV5.LAB1.COM

Task name	Schedule	Next run time	Last run time	Status	Last result	Creator
EcoraAuditor41_Consolidated Change Log_Ad Hoc_B384718E71 30402597D336B4 B9682934.job	not scheduled	never	never		0x0	SYSTEM

Task name	Schedule	Next run time	Last run time	Status	Last result	Creator
EcoraAuditor41_D ocumentation Report_ test_9F122AD72F 32463D881DAFD 60E46D044.job	not scheduled	never	never		0x0	SYSTEM
EcoraAuditor41_D ocumentation Report_SQL_400 11487F5644B1CA CA989F6C6A2C8 30.job	not scheduled	never	02/12/2008 16:03		0x0	SYSTEM
EcoraAuditor41_E coraAuditor4.1_ WIN - Collect and Document All Systems - Daily_18014E0D2 6F74502848B3F8 BD11DFC85.job	not scheduled	never	02/13/2008 12:35		0x0	SYSTEM
EcoraAuditor41_E coraAuditor4.1_A D - Collect and Document - Full - AD Hoc_28A77B38E7 8743028FACB9C2 B7B5E15D.job	not scheduled	never	02/14/2008 14:30		0x0	SYSTEM
EcoraAuditor41_F act-Finding Report_Ad Hoc_E9E00335A8 BD4E989F9AE6EA 1B639FB6.job	not scheduled	never	never		0x0	SYSTEM

Task EcoraAuditor41_Consolidated Change Log_Ad
Hoc_B384718E7130402597D336B4B9682934.job

- Run path for task: **C:\Program Files\Ecora\Auditor41\bin\auditor.exe**
- Folder for starting task: **default**
- Task comments: **Task scheduled by Ecora Software**
- Who will be run scheduled task: **LAB1\administrator**

- Task is **enabled**
- Run only if logged on: **disabled**

AllSchedules_STScheduleVector: ***NULL***

Show multiple schedules: **disabled**

Settings

- Delete the task if it is not scheduled to run again: **disabled**
- Stop the task if it runs for: 72 h 00 min
- Idle Time
 - Only start if idle for a least: **disabled**
 - If not been idle that long, retry for up to: **disabled**
 - Stop task if computer ceases to be idle: **disabled**
- Power Management
 - Don't start task if computer is running on batteries: **disabled**
 - Stop if battery mode begins: **disabled**
 - Wake the computer to run this task: **disabled**

Permissions

Table 27. Task permissions

Account	NTFS Permissions
BUILTIN\Administrators (alias)	Allow - Main(Full).
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).

Task EcoraAuditor41_Documentation Report _
test_9F122AD72F32463D881DAFD60E46D044.job

- Run path for task: **C:\Program Files\Ecora\Auditor41\bin\auditor.exe**
- Folder for starting task: **default**
- Task comments: **Task scheduled by Ecora Software**
- Who will be run scheduled task: **LAB1\administrator**
- Task is **enabled**
- Run only if logged on: **disabled**

AllSchedules_STScheduleVector: ***NULL***

Show multiple schedules: **disabled**

Settings

- Delete the task if it is not scheduled to run again: **disabled**
- Stop the task if it runs for: 72 h 00 min
- Idle Time
 - Only start if idle for a least: **disabled**
 - If not been idle that long, retry for up to: **disabled**
 - Stop task if computer ceases to be idle: **disabled**

- Power Management
 - Don't start task if computer is running on batteries: **disabled**
 - Stop if battery mode begins: **disabled**
 - Wake the computer to run this task: **disabled**

Permissions

Table 28. Task permissions

Account	NTFS Permissions
BUILTIN\Administrators (alias)	Allow - Main(Full).
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).

Task EcoraAuditor41_Documentation

Report_SQL_40011487F5644B1CACA989F6C6A2C830.job

- Run path for task: **C:\Program Files\Ecora\Auditor41\bin\auditor.exe**
- Folder for starting task: **default**
- Task comments: **Task scheduled by Ecora Software**
- Who will be run scheduled task: **LAB1\administrator**
- Task is **enabled**
- Run only if logged on: **disabled**

AllSchedules_STScheduleVector: ***NULL***

Show multiple schedules: **disabled**

Settings

- Delete the task if it is not scheduled to run again: **disabled**
- Stop the task if it runs for: 72 h 00 min
- Idle Time
 - Only start if idle for a least: **disabled**
 - If not been idle that long, retry for up to: **disabled**
 - Stop task if computer ceases to be idle: **disabled**
- Power Management
 - Don't start task if computer is running on batteries: **disabled**
 - Stop if battery mode begins: **disabled**
 - Wake the computer to run this task: **disabled**

Permissions

Table 29. Task permissions

Account	NTFS Permissions
BUILTIN\Administrators (alias)	Allow - Main(Full).
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).

Task EcoraAuditor41_EcoraAuditor4.1_WIN - Collect and Document All Systems - Daily_18014E0D26F74502848B3F8BD11DFC85.job

- Run path for task: **C:\Program Files\Ecora\Auditor41\bin\auditor.exe**
- Folder for starting task: **default**
- Task comments: **Task scheduled by Ecora Software**
- Who will be run scheduled task: **LAB1\administrator**
- Task is **enabled**
- Run only if logged on: **disabled**

AllSchedules_STScheduleVector: ***NULL***

Show multiple schedules: **disabled**

Settings

- Delete the task if it is not scheduled to run again: **disabled**
- Stop the task if it runs for: 72 h 00 min
- Idle Time
 - Only start if idle for a least: **disabled**
 - If not been idle that long, retry for up to: **disabled**
 - Stop task if computer ceases to be idle: **disabled**
- Power Management
 - Don't start task if computer is running on batteries: **disabled**
 - Stop if battery mode begins: **disabled**
 - Wake the computer to run this task: **disabled**

Permissions

Table 30. Task permissions

Account	NTFS Permissions
BUILTIN\Administrators (alias)	Allow - Main(Full).
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).

Task EcoraAuditor41_EcoraAuditor4.1_AD - Collect and Document - Full - AD Hoc_28A77B38E78743028FACB9C2B7B5E15D.job

- Run path for task: **C:\Program Files\Ecora\Auditor41\bin\auditor.exe**
- Folder for starting task: **default**
- Task comments: **Task scheduled by Ecora Software**
- Who will be run scheduled task: **LAB1\administrator**
- Task is **enabled**
- Run only if logged on: **disabled**

AllSchedules_STScheduleVector: ***NULL***

Show multiple schedules: **disabled**

Settings

- Delete the task if it is not scheduled to run again: **disabled**
- Stop the task if it runs for: 72 h 00 min
- Idle Time
 - Only start if idle for a least: **disabled**
 - If not been idle that long, retry for up to: **disabled**
 - Stop task if computer ceases to be idle: **disabled**
- Power Management
 - Don't start task if computer is running on batteries: **disabled**
 - Stop if battery mode begins: **disabled**
 - Wake the computer to run this task: **disabled**

Permissions

Table 31. Task permissions

Account	NTFS Permissions
BUILTIN\Administrators (alias)	Allow - Main(Full).
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).

Task EcoraAuditor41_Fact-Finding Report_Ad Hoc_E9E00335A8BD4E989F9AE6EA1B639FB6.job

- Run path for task: **C:\Program Files\Ecora\Auditor41\bin\auditor.exe**
- Folder for starting task: **default**
- Task comments: **Task scheduled by Ecora Software**
- Who will be run scheduled task: **LAB1\administrator**
- Task is **enabled**
- Run only if logged on: **disabled**

AllSchedules_STScheduleVector: ***NULL***

Show multiple schedules: **disabled**

Settings

- Delete the task if it is not scheduled to run again: **disabled**
- Stop the task if it runs for: 72 h 00 min
- Idle Time
 - Only start if idle for a least: **disabled**
 - If not been idle that long, retry for up to: **disabled**
 - Stop task if computer ceases to be idle: **disabled**
- Power Management
 - Don't start task if computer is running on batteries: **disabled**
 - Stop if battery mode begins: **disabled**
 - Wake the computer to run this task: **disabled**

Permissions

Table 32. Task permissions

Account	NTFS Permissions
BUILTIN\Administrators (alias)	Allow - Main(Full).
NT AUTHORITY\SYSTEM (well-known group)	Allow - Main(Full).

19 Security Settings

The following sections list computer security settings.

19.1 Account Policies

19.1.1 Password Policy (unconfigured options are not shown)

Table 33. Password Policy

Policy	Security Setting	Overridden By
Enforce password history	24 passwords remembered	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum password age	42 days	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Minimum password age	1 days	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Minimum password length	9 characters	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Password must meet complexity requirements	Enabled	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Store passwords using reversible encryption	Disabled	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}

19.1.2 Account Lockout Policy (unconfigured options are not shown)

Table 34. Account Lockout Policy

Policy	Security Setting	Overridden By
Account lockout threshold	0 invalid logon attempts	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}

19.1.3 Kerberos Policy (unconfigured options are not shown)

Table 35. Kerberos Policy

Policy	Security Setting	Overridden By
Enforce user logon restrictions	Enabled	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum lifetime for service ticket	600 minutes	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum lifetime for user ticket	10 hours	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}

19.2 Local Policies

19.2.1 Audit Policy (unconfigured options are not shown)

Table 36. Audit Policy

Policy	Security Setting	Overridden By
Audit account logon events	Success	
Audit account management	No Auditing	
Audit directory service access	No Auditing	

Policy	Security Setting	Overridden By
Audit logon events	Success	
Audit object access	No Auditing	
Audit policy change	No Auditing	
Audit privilege use	No Auditing	
Audit process tracking	No Auditing	
Audit system events	No Auditing	

19.2.2 User Rights Assignment (unconfigured privilege levels are not shown)

Table 37. User Rights

Privilege Level	Accounts	Overridden By
Access this computer from the network	BUILTIN\Backup Operators (alias) BUILTIN\Power Users (alias) BUILTIN\Users (alias) BUILTIN\Administrators (alias) MBRSRV5\ASPNET (user) MBRSRV5\IWAM_MBRsrv5 (user) MBRSRV5\IUSR_MBRsrv5 (user) Everyone (well-known group)	
Adjust memory quotas for a process	BUILTIN\Administrators (alias) MBRSRV5\IWAM_MBRsrv5 (user) NT AUTHORITY\NETWORK SERVICE (well-known group) NT AUTHORITY\LOCAL SERVICE (well-known group)	
Allow log on locally	BUILTIN\Backup Operators (alias) BUILTIN\Power Users (alias)	

Privilege Level	Accounts	Overridden By
	BUILTIN\Users (alias) BUILTIN\Administrators (alias) MBRSRV5\IUSR_MBRsrv5 (user)	
Allow logon through Terminal Services	BUILTIN\Remote Desktop Users (alias) BUILTIN\Administrators (alias)	
Back up files and directories	BUILTIN\Backup Operators (alias) BUILTIN\Administrators (alias)	
Bypass traverse checking	BUILTIN\Backup Operators (alias) BUILTIN\Power Users (alias) BUILTIN\Users (alias) BUILTIN\Administrators (alias) Everyone (well-known group)	
Change the system time	BUILTIN\Power Users (alias) BUILTIN\Administrators (alias) NT AUTHORITY\LOCAL SERVICE (well-known group)	
Create a pagefile	BUILTIN\Administrators (alias)	
Create global objects	NT AUTHORITY\SERVICE (well-known group) BUILTIN\Administrators (alias)	
Debug programs	BUILTIN\Administrators (alias)	
Deny access to this computer from the network	MBRSRV5\SUPPORT_388945a0 (user)	
Deny logon through Terminal Services	MBRSRV5\ASPNET (user)	

Privilege Level	Accounts	Overridden By
Deny to log on locally	MBRSRV5\ASPNET (user) MBRSRV5\SUPPORT_388945a0 (user)	
Force shutdown from a remote system	BUILTIN\Administrators (alias)	
Generate security audits	NT AUTHORITY\NETWORK SERVICE (well-known group) NT AUTHORITY\LOCAL SERVICE (well-known group)	
Impersonate a client after authentication	NT AUTHORITY\SERVICE (well-known group) BUILTIN\Administrators (alias) MBRSRV5\ASPNET (user) MBRSRV5\IIS_WPG (alias)	
Increase scheduling priority	BUILTIN\Administrators (alias)	
Load and unload device drivers	BUILTIN\Administrators (alias)	
Log on as a batch job	LAB1\Administrator (user) MBRSRV5\ASPNET (user) MBRSRV5\IIS_WPG (alias) MBRSRV5\IWAM_MBR5RV5 (user) MBRSRV5\IUSR_MBR5RV5 (user) MBRSRV5\SUPPORT_388945a0 (user) NT AUTHORITY\LOCAL SERVICE (well-known group)	
Log on as a service	MBRSRV5\ASPNET (user) NT AUTHORITY\NETWORK SERVICE (well-known group) NT AUTHORITY\SYSTEM (well-known group)	
Manage auditing and security log	BUILTIN\Administrators (alias)	

Privilege Level	Accounts	Overridden By
Modify firmware environment values	BUILTIN\Administrators (alias)	
Perform volume maintenance tasks	BUILTIN\Administrators (alias)	
Profile single process	BUILTIN\Power Users (alias) BUILTIN\Administrators (alias)	
Profile system performance	BUILTIN\Administrators (alias)	
Remove computer from docking station	BUILTIN\Power Users (alias) BUILTIN\Administrators (alias)	
Replace a process level token	MBRSRV5\IWAM_MBRsrv5 (user) NT AUTHORITY\NETWORK SERVICE (well-known group) NT AUTHORITY\LOCAL SERVICE (well-known group)	
Restore files and directories	BUILTIN\Backup Operators (alias) BUILTIN\Administrators (alias)	
Shut down the system	BUILTIN\Backup Operators (alias) BUILTIN\Power Users (alias) BUILTIN\Administrators (alias)	
Take ownership of files or other objects	BUILTIN\Administrators (alias)	

19.2.3 Security Options (unconfigured options are not shown)

Table 38. Security Options

Policy	Security Setting	Overridden By
Accounts: Limit local account use of blank passwords to console logon only	Enabled	
Audit: Audit the access of global system objects	Disabled	
Audit: Audit the use of Backup and Restore privilege	Disabled	
Audit: Shut down system immediately if unable to log security audits	Disabled	
Devices: Allow undock without having to log on	Enabled	
Devices: Allowed to format and eject removable media	Administrators	
Devices: Prevent users from installing printer drivers	Enabled	
Devices: Restrict CD-ROM access to locally logged-on user only	Disabled	
Devices: Restrict floppy access to locally logged-on user only	Disabled	
Devices: Unsigned driver installation behavior	Warn but allow installation	
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	
Domain member: Digitally sign secure channel data (when possible)	Enabled	

Policy	Security Setting	Overridden By
Domain member: Disable machine account password changes	Disabled	
Domain member: Maximum machine account password age	30 days	
Domain member: Require strong (Windows 2000 or later) session key	Disabled	
Interactive logon: Do not display last user name	Disabled	
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	
Interactive logon: Message text for users attempting to log on		
Interactive logon: Message title for users attempting to log on		
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	
Interactive logon: Prompt user to change password before expiration	14 days	
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	
Interactive logon: Require smart card	Disabled	
Interactive logon: Smart card removal behavior	No Action	
Microsoft network client: Digitally sign communications (always)	Disabled	

Policy	Security Setting	Overridden By
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	
Microsoft network server: Amount of idle time required before suspending session	15 minutes	
Microsoft network server: Digitally sign communications (always)	Disabled	
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	
Microsoft network server: Disconnect clients when logon hours expire	Enabled	
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	
Network access: Let Everyone permissions apply to anonymous users	Disabled	
Network access: Named Pipes that can be accessed anonymously	COMNAP COMNODE SQL\QUERY SPOOLSS	

Policy	Security Setting	Overridden By
	NETLOGON LSARPC SAMR BROWSER	
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	
Network access: Shares that can be accessed anonymously	COMCFG DFS\$	

Policy	Security Setting	Overridden By
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	
Network security: Do not store LAN Manager hash value on next password change	Disabled	
Network security: LAN Manager authentication level	Send NTLM response only	
Network security: LDAP client signing requirements	Negotiate signing	
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	0	
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	0	
Recovery console: Allow automatic administrative logon	Disabled	
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	
Shutdown: Allow system to be shut down without having to log on	Disabled	
Shutdown: Clear virtual memory pagefile	Disabled	
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	
System objects: Default owner for objects created by members of the Administrators group	Administrators group	

Policy	Security Setting	Overridden By
System objects: Require case insensitivity for non-Windows subsystems	Enabled	
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	
System settings: Optional subsystems	Posix	
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	

20 Terminal server

Terminal server is enabled. See subitems to get an information.

20.1 Terminal server configuration

Product version: **5.2**

Mode: **remote administration server**

Delete temporary folders on exit: **yes**

Use temporary folders per session: **yes**

Licensing: **remote desktop for administration**

Active desktop: **enable**

Permission compatibility: **full security**

Restrict each user to one session: **no**

Session directory: **disable**

20.2 Connection RDP-Tcp

General:

- Type: **Microsoft RDP 5.2**
- Transport: **tcp**
- Comment:

- Encryption level: **client compatible**
- Use standard windows authentication: **disabled**

Logon settings:

Terminal server **uses client-provided logon information.**

Always prompt for password: **disabled**

Sessions:

Override user session timeout settings: **disabled**

Override user session limit or broken connection settings: **disabled**

Override user reconnection settings: **disabled**

Environment:

Override initial program settings: **disabled**

Disable wallpaper: **yes**

Remote control:

Remote control: **use remote control with default user settings**

- Require user's permission: **yes**
- Level of control: **interact with the session**

Client settings:

Use connection settings from user settings: **enabled**

Limit maximum color depth: **enabled**

- Color depth: **16 bit**

Disable the following:

- Drive mapping: **no**
- Windows printer mappings: **no**
- LPT port mappings: **no**
- COM port mapping: **no**
- Clipboard mapping: **no**
- Audio mapping: **yes**

Network adapter:

- Network adapter: **all network adapters configured with this protocol**
- Number of connections: **unlimited**

Security:

- Name: **BUILTIN\Administrators**
- Type: **allow**
- Permissions: **full control**
-
- Name: **BUILTIN\Remote Desktop Users**
- Type: **allow**

- Permissions: **user access**
-
- Name: **NT AUTHORITY\LOCAL SERVICE**
- Type: **allow**
- Permissions: **special permissions**
- **Special Permissions:**
 - Query information: **allow**
 - Set information:
 - Reset:
 - Remote control:
 - Logon:
 - Logoff:
 - Message: **allow**
 - Connect:
 - Disconnect:
 - Virtual channels:
- Name: **NT AUTHORITY\NETWORK SERVICE**
- Type: **allow**
- Permissions: **special permissions**
- **Special Permissions:**
 - Query information: **allow**
 - Set information:
 - Reset:
 - Remote control:
 - Logon:
 - Logoff:
 - Message: **allow**
 - Connect:
 - Disconnect:
 - Virtual channels:
- Name: **NT AUTHORITY\SYSTEM**
- Type: **allow**
- Permissions: **full control**
-

21 WINS Server

NULL

* Attributes for this topic have been suppressed *