

# Windows Server Default Configuration Procedure

Document Number:

OWNER:

SUBJECT:

Window O/S Configuration Procedure

REVISION:

0

DRAFT OWNER:

DATE ISSUED/REVISED:

PAGE:

Page 1 of 14

## Contents

	Page
1.0 PURPOSE/INTENT.....	1
2.0 SCOPE.....	2
3.0 PROCEDURE.....	2-14
4.0 MANAGEMENT APPROVAL.....	14

### 1.0 PURPOSE/INTENT

The purpose of this procedure is to provide the Information Technology Group standardized instructions on how to configure Microsoft Windows 2000 and Windows 2003 Operating Systems.

### 2.0 SCOPE

This procedure applies to all Microsoft Windows servers managed directly by the Information Technology Group.

### 3.0 PROCEDURE

#### **Server Inventory Information**

- A new Server worksheet is to be completed for the new server within a new or existing Server Documentation Workbook (See Systems & Networks Documentation Policy)

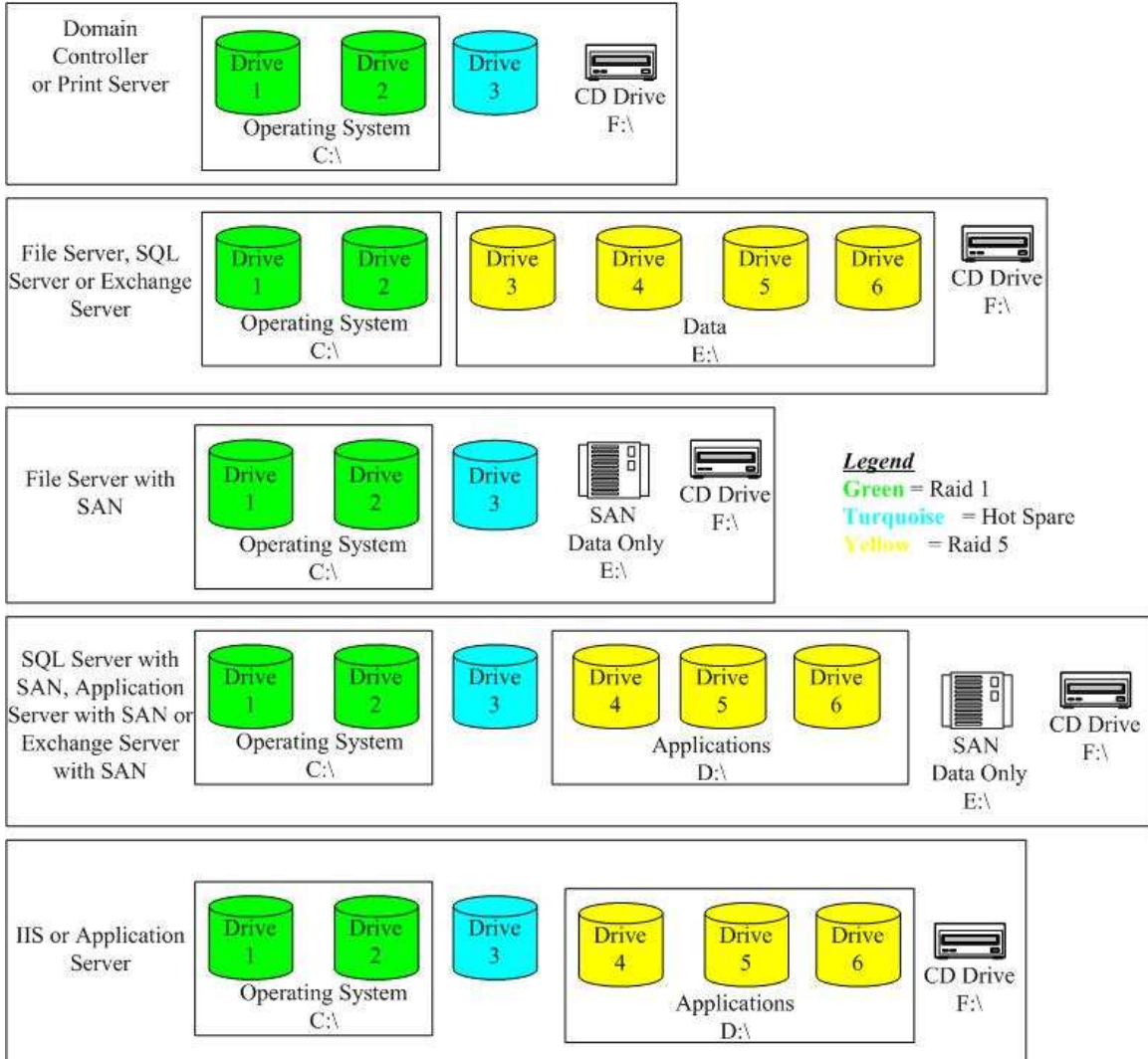
#### **Change Control**

- Submit Change control to add server to the data center

#### **Update Server Firmware and Bios**

- Use the IBM Driver website or the latest IBM UpdateXpress CD to detect the current level of system and subsystem firmware. Upgrade the BIOS, diagnostics, systems management processors, ServeRAID™, tape drives, and hard disk drives.

**□ Drive Configuration**



<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  <b>Page 3 of 10</b>
	<b>Revision: 0</b>	

## Windows Server Setup

- Use the IBM Server Configuration CD and the Windows Server CD with the latest service pack slip streamed to install the NOS and drivers on the server.
- Primary partition size for Operating System installation varies per server. Please see the Drive Configuration section for more detail
- Format the partition using the NTFS file system
- Install Windows Server to the default directory
  - Windows 2000 C:\WINNT
  - Windows 2003 C:\Windows
- Personalize Your Software
  - Name {Your Company Name}
  - Organization {YOUR COMPANY NAME}
- Licensing Modes
  - Per Seat , Per Device or Per User - each computer must have its own Client Access License
- Computer Name (See Server Standard Naming Convention Document)
- Password
  - Use the current local administrator password.
- Components
  - This section applies during the install of Windows 2000 Server Only
  - Accessories and Utilities
    - Accessibility Wizard Uncheck
    - Accessories Check
    - Communications Uncheck
    - Games Uncheck
    - Multimedia Uncheck
  - Indexing Service Uncheck
  - Internet Information Server Uncheck
  - Management and Monitoring Tools
    - Check Network Monitoring Tools Check
  - Script Debugger Uncheck
  - Terminal Services
    - Client Creator Files Uncheck
    - Enable Terminal Services Check
- Terminal Services Setup
  - Remote Administration Mode
  - Some application servers need to run in Application Server Mode
- Networking Settings
  - ALL SERVERS HAVE A STATIC ADDRESS
- Join Workgroup (This will be changed later)
- Reboot

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  Page 4 of 10
	<b>Revision: 0</b>	

**Update Windows Drivers**

- Using the IBM Drivers website or the latest IBM UpdateExpress CD now will detect the current level of device drivers and upgrade them. SCSI controllers, Ethernet controllers, video controllers, systems management processors, ServeRAID™

**Stop and Disable unnecessary services**

- Alerter
- Automatic Updates
- Clipboard
- Computer Browser
  - Domain Controllers have this service on
  - Remote sites with no DC must have at least one server with this service on
- Distributed File System
- Distributed Link Tracking Client
- Distributed Link Tracking Server
- Fax Service
- Internet Connection Sharing
- IPSEC Services
- License Logging Service
- Messenger
- Netmeeting Remote Desktop Sharing
- Network DDE
- Network DSDM
- Network Location Awareness (Windows 2003 Only)
- Print Spooler
  - Only Turn this off if the server will not be a print server
  - Metaframe servers need this on
- Telnet
- Wireless Configuration (Windows 2003 Only)
- 

**Install Windows Server Recovery Console**

- Insert the Windows Server CD you used to install the Operating System
- Go to Start
- Run
- Type X:\i386\WINNT32.exe /cmdcons (x = cd drive letter)

**Install Symantec Antivirus Corporate Edition**

- Install the latest Symantec AntiVirus CLIENT version.
- See the Symantec AntiVirus Configuration document.

**Audit Settings**

MMC -> Local Security Policy

<i>Windows Server 2000 &amp; 2003</i>		
<i>Policy</i>	<i>Success</i>	<i>Failure</i>
Audit Account Logon Events	X	X
Audit Account Management	X	X
Audit Directory Services Access		X
Audit Logon Events	X	X

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>
	<b>Revision: 0</b>	<b>Page 5 of 10</b>

Audit Object Access		X
Audit Policy Change	X	X
Audit Privilege Use	X	X
Audit Process Tracking		X
Audit System Events	X	X

User Manager for Domains -> Policies -> Audit

<b>Windows NT 4.0</b>		
<b>Policy</b>	<b>Success</b>	<b>Failure</b>
Logon and Logoff	X	X
File and Object Access		X
Use of User Rights	X	X
User and Group Management	X	X
Security Policy Changes	X	X
Restart, Shutdown, and System	X	X
Process Tracking		X

## Log Settings

On both Windows 2000 and Windows NT 4.0 the log settings shown below can be set using the Event Viewer application.

### Application Log

Maximum Log Size 30720 KB\*  
When Maximum Log size is reached: Overwrite events as needed

### Security Log

Maximum Log Size 30720 KB\*  
When Maximum Log size is reached: Overwrite events as needed

### System Log

Maximum Log Size 30720 KB\*  
When Maximum Log size is reached: Overwrite events as needed

\* - Older NT based systems lacking disk space may be set as appropriate. Maximum log size must be no less than 1024 KB on any system.

## Miscellaneous Log Related Settings

Printers Folder -> File -> Server Properties -> Advanced Tab

Uncheck 'Log Spooler Information Events' and 'Notify when remote documents are printed'

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  <b>Page 6 of 10</b>
	<b>Revision: 0</b>	

## Account Rights & Privileges

1. Domain and Local Administrator account passwords are never to be given to anyone outside of {Your Company Name} Information Technology Group.
2. Field users are never to be a member of the Domain Admin or any Administrators group. If these rights are needed, they are supplied through site administrator credentials to be supplied to the appropriate personnel at the facility.
3. All passwords for the Domain Admin, all Local administrators, and the SiteAdmin account are to be documented and provided to the Manager of Network Services. Any changes to the above passwords are to be documented and provided to the Manager of Network Services on a timely basis.
4. The built-in Administrator account is to be renamed to 'ITADMIN' and a new account created with the name 'Administrator'. The newly created 'Administrator' account is to be given only guest privileges.
5. Verify NetAdmin account exists. (DO NOT MODIFY IF IT DOES) If it does not exist, create it in the local SAM context with the following properties and email an account creation notice to corporate.
  - a. Username: NetAdmin
  - b. Full Name: \*\*\* DO NOT TOUCH \*\*\*
  - c. Description: Corporate Network Administrator Account
  - d. Password: temppassword
  - e. Set 'Password Never Expires' right
  - f. Group Membership: Domain\Domain Admins, Domain\Administrators, Server\Administrators (Set primary group to Domain Admins)
  - g. No profile or login script should be assigned
6. Service Accounts should be created for servers required to be logged in with specific credentials and/or rights (e.g. ABC\_SERVICE account for ABC Application) or for the purpose of running an application service with a specific identity and/or rights (e.g. Inventory App COM object or BackupExec Service) subject to the following parameters:
  - a. The Service account should be created locally on the server (local SAM) for which it will be used and given ONLY the necessary rights on that server (i.e. Logon as a service, Administrator group membership, etc.) to perform the function for which it had been created.
  - b. The Service Account should have a descriptive user name associating it with the service and/or application for which it will be used.
  - c. The service account must have a unique password and the password must never be identical or similar to the user name
  - d. If domain-based resources are to be accessed, a matching account can be created on the domain (same user name and password), however, the account should be given no more rights on the domain than a generic user. (i.e. Domain Users group, resource specific groups, etc.)

## Security Settings

### General Security Settings

1. All servers capable of such must display the warning banner as approved by the {YOUR COMPANY NAME} Legal department. Verbiage is provided here:
  - a. Caption is "\*\*\*\*\* WARNING \*\*\*\*\*"
  - b. Text is "This is a privately owned system and is not for public use or access. Access is restricted to authorized personnel only."
2. A Screen Saver (or some other software mechanism) should be configured on the server to automatically lock the workstation after no more than 10 minutes.
3. All Windows Servers must comply with the {YOUR COMPANY NAME} Antivirus Policy. Virus definition files must be centrally managed. Real time file system protection must be enabled. Complete scans must be completed weekly. Any deviation from the {YOUR COMPANY NAME} Antivirus Policy must be approved by IT Management.

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  Page 7 of 10
	<b>Revision: 0</b>	

4. All unnecessary services and applications (e.g. IIS, FTP, SMTP, TFTP servers) should be un-installed from the server. If un-installation is not possible, the service and/or application should be disabled from use and all capabilities of launching automatically be disabled or removed.

## Install all available Windows Server Service Packs and Critical Updates

- Windows NT 4.0
  - Service Pack 6a
  - All Post-SP6a hotfixes
- Windows 2000
  - Service Pack 4
  - All Post-SP4 hotfixes
- Windows 2003
  - Service Pack 2
  - All Post-SP2 hotfixes

## Network Configuration

- Configure Network Adapter
  - Advanced Tab
    - Link Speed & Duplex
      - Auto Detect
    - Power Management
      - Disable
- Network Connection Properties
  - Check the *Show icon in taskbar when connected* check box
  - Internet Protocol (TCP/IP) - This information varies per site.
    - IP Address
    - Subnet Mask
    - Default Gateway
    - DNS Servers
      - DNS 1
      - DNS 2
    - The Domain Suffix will be filled in when you join the domain.
    - Wins Servers
      - Local WINS Server IP Address First
      - WINS 1
      - WINS 2
      - Uncheck Enable LMHOSTS lookup
      - Enable NetBIOS over TCP/IP

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  Page 8 of 10
	<b>Revision: 0</b>	

**Join Active Directory Domain**

- System Properties
  - Computer Name
    - Create computer account in AD in relevant OU
    - Change member of domain to
      - {Your Company Name}.com
    - Provide Credentials that have permissions to join computers to the target domain
    - Reboot

**Install ServeRAID Manager Software**

- Install the ServeRaid Manager
- **Do not Install as a service**
- Destination Folder                      Accept Default

**Install Windows Server Resource Kit**

- Windows 2000
  - Typical Install
  - Do Not install ActivePerl
- Windows 2003
  - Select All Defaults

**Install Veritas BackupExec Backup Software**

- Install from the latest media purchased with the server.
- Configure according to the Backup & Disaster Recovery Policy

**Local Security Policy**

- Windows 2000
  - Local Policies
    - Security Options
      - Additional restrictions for Anonymous Connections
        - No Access without explicit anonymous permissions
        - Domain Controllers need to be set to Relay of Default Permissions
      - LAN Manager Authentication
        - Send LM & NTLM – use NTLM2 session security if negotiated
      - Enable Digitally Sign Server Communication (when possible)
- Windows 2003
  - Local Policies
    - Security Options
      - Network Access
        - Enable Do not allow Anonymous Enumeration of Sam Accounts and Shares
        - Domain Controllers
          - Disable Do not allow Anonymous Enumeration of Sam Accounts and Shares
          - Disable Do not allow Anonymous Enumeration of Sam Accounts
      - System Settings
        - Optional Subsystems
          - Delete Posix

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  <b>Page 9 of 10</b>
	<b>Revision: 0</b>	

## **Post Software Install Configurations**

- Device Manager – Make sure there are no errors in the device manager. Install drivers as necessary to correct any issues
- Edit Boot.ini
  - /3gb switch –
    - Use only if you have 3gb of memory and are using Advanced Server
    - <http://support.microsoft.com/default.aspx?scid=kb;en-us;328882>

multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Server" /fastdetect /3GB

- Reset boot.ini to Read-Only when done
- Configure Print Server Properties
  - Un-check Log Spooler Information Events
  - Un-check Notify when remote documents are printed
- Terminal Services Configuration
  - Sessions
    - End Disconnected session 5 min
    - Idle Session Limit 2 hours.
  - Client Settings -
    - Connection
      - Uncheck Use connection settings from user settings
      - Uncheck Connect client drives at logon
      - Uncheck Connect client printers at logon
      - Uncheck Default to main client printer
    - Disable the Following
      - Check Drive Mapping
      - Check Windows Printer Mapping
      - LPT Port Mapping
      - COM port mapping
      - Clipboard Mapping
      - Audio Mapping
  - Network Adapter
    - Set to main production adapter
  - Server Settings
    - Disable Active Desktop
    - Check Restrict each user to one session
- System Properties
  - Remote
    - Check Allow users to connect remotely
  - Advanced
    - Startup and Recovery
      - Time to display list of operating systems 5 seconds
- Add/Remove Windows Components – Windows 2003 Only
  - Accessories and Utilities
    - Uncheck Accessibility Wizard
    - Uncheck Communications
  - Management and Monitoring Tools
    - Check Network Monitor Tools
- Disk Performance – Windows 2000 Only
  - Open a command prompt
  - Type Diskperf –y

<b>Windows Server Default Configuration Procedure</b>	<b>Document Number:</b>	<b>Page No:</b>  Page 10 of 10
	<b>Revision: 0</b>	

- Reboot

**Applications & Services Installation Procedures**

- If this server is to host the WINS name resolution service, please follow the WINS Configuration Procedure document.
- If SQL server is being installed on this server, please follow the SQL Server 2000 Configuration Procedure document.
- If this server is to be an SMTP relay or utilize the SMTP service for a hosted application, please follow the SMTP Configuration document.

**4.0 APPROVAL**

<b>6.0 APPROVAL SIGN-OFF</b>		
<b>Role</b>	<b>Responsibility</b>	<b>Name/Function</b>
Owner	Correctness and completeness	
Reviewed by	Review of correctness and completeness	
Reviewed by	Review of correctness and completeness	
Reviewed by	Review of correctness and completeness	
Approved by	Adoption of policy within department	