**Old ass checklist from 2014 but still has some useful information**

**Table of Contents:**

* Before You Start

1. Clear DNS Cache
2. View Hidden Files
3. Stopping Network Shares
4. User and Group Configuration
5. Malwarebytes
6. Removing Unwanted Software
7. Firewall
8. Policies
9. Services
10. Remote Desktop
11. Automatic Updating
12. Processes and Open Ports
13. Alternate Data Streams
14. Removing Programs from Startup
15. Adding and Removing Windows Components
16. Anti-Virus
17. User Account Control Configuration
18. Disable Dump File Creation
19. Creating a Restore Point
20. Saved Windows Credentials
21. Internet Options
22. Power Settings
23. Data Execution Prevention
24. Malicious and Outdated Drivers
25. Rootkit Scanning
26. CCleaner
27. Microsoft Security Baseline Analyzer
28. Service Packs
29. Updating via the Control Panel
30. Final Thoughts
31. Appendix

***CAREFULLY CONSIDER THE DEPENDENCIES OF SERVICES YOU HAVE TO RUN, ALWAYS BACKUP CONFIGS***

1. **Clear the DNS Cache**
   1. Open up a command prompt by clicking the **Start** button and typing *cmd*
   2. Right click the **cmd.exe** icon, Run as administrator, and the command prompt window should open up
   3. Type *ipconfig /flushdns*
   4. Hit enter
   5. Type *notepad C:\Windows\System32\drivers\etc\hosts*
   6. Hit enter. Delete any lines that don’t start with #
2. **Enable Viewing of Hidden Files**
   1. Go to **My Computer**, and then go to **View**. Select **Change folder and Search Options**
   2. Go to the **View** tab
   3. Select the **Show hidden files and folders**
   4. Uncheck the **Hide extensions for known**
   5. Uncheck the **Hide protected OS files**
   6. Uncheck the **Hide empty drives...**
3. **Stop Network Shares**
   1. Open the **Start** menu, and type in *cmd*
   2. **Do not hit enter**. Right click, and choose **Run as Administrator**
   3. Now, if User account control menu pops up, click yes
   4. Type in *net share*
      1. This lists all the active shares from your computer, we are going to kill these now
   5. Type *net share /delete INSERT NAME OF NET SHARE HERE*
      1. If the name includes a **$**, that means the share is hidden. Yes you should still delete it, and you have to include the dollar sign in the name to delete it
   6. Delete every share that is listed
      1. **IPC$** will be restarted on boot up, this can’t be changed, and won’t be counted for points ever anyways. The other two default shares are C$ and ADMIN$
4. **User and Group Configuration**
   1. Go to **Start**, type *MMC*, hit enter
   2. Now, go to **File**, **Add/Remove Snap-ins**, scroll down and choose **Local Users and Groups**
   3. Find the users that do not matchup with those in the readme, or default users
      1. Default users are **Administrator**, and **Guest**
   4. Make sure, check again
   5. Now delete them. **Right click** the desired user, and click **Delete**. If a prompt comes up that says **Do you want to delete the users files?** Click **Yes**.
   6. We need to rename the guest account (and possibly the Administrator, see below)
      1. Check to see if you are working on the default administrator account. Click **Start**, then on the top right, your username should be displayed. If you are using the default **Administrator**, do NOT change his name. If you are not, rename the **Administrator** account
   7. **Right click** the desired user, and click **Rename**. Don’t make it guessable, like your name or something. Make it completely random
   8. We also need to disable the **Guest** account. **Right click** that account, and click **Disable**
   9. Set a password for the remaining user accounts you did not delete
      1. Make this password 8 characters, with 1 number and 1 special letter !@#$%^ etc.
   10. Now, go to the **Groups** page
   11. Open the **Administrators** group
   12. Double check each entered username with the readme
       1. If something doesn’t belong, remove it
5. **Install MalwareBytes and Process Explorer, and Run MalwareBytes**
   1. First, go to the google doc’s site. In case you don’t have it, or are too lazy to look it up, here is the link to the google docs page- <https://drive.google.com/#folders/0B7FKJ-QDh83GQUFYeDd6cE9lMW8>
      1. To download something, **Right Click** it and click **Download**
   2. Now, go to the Malware folder, then download **MalwareBytes Installer.exe**
   3. We also need **Process Explorer**. Go to the **Processes** folder, and download **Procexp.exe**
   4. On **MalwareBytes**, when it gives you the option to update, do it
      1. It may say the installer is out of date, just go along with it. Download and install the newer install version, then Install it.
   5. When it finishes installing, uncheck the **Enable Malwarebytes PRO edition** or whatever it is, we don’t need that.
   6. Select the **Full Scan**, then click **Scan**
   7. Scan the **C drive** only

Whiles the Malwarebytes is running, we have to do other stuff, so come back to step g when malwarebytes is done scanning

* 1. When the scan finishes, select the **Show Results** button, and then make sure each box is selected, and click remove selected.

1. **Remove Software**
   1. Go to **Control Panel** (click **Start**, then type *Control Panel*. Click on the **Control Panel** icon)
   2. Now, under the **Programs** menu, there should be a submenu called **Uninstall a program**. Click it.
   3. Now, uninstall every program in the list EXCEPT **MalwareBytes, Microsoft Visual C++**, or **Microsoft .NET** since we installed it. If **CCleaner** or something like that was installed already, uninstall it now
   4. If you get an error saying access is denied, or the program is in use go to **Processes and Open Ports** to end the process
   5. Some programs are installed, but hidden with a registry key. You need to open up the registry by clicking **Start** and typing **regedit**
   6. Once you are in the registry, go to **HKEYLOCALMACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall**
      1. This contains a complete list of the software that is installed on the system
   7. Look for programs that do not correspond with those in the **Uninstall List** in the **Control Panel**
   8. Google these programs to make sure they are legitimate- I doubt CyberPatriot will hide things in there, but you can never be sure
2. **Firewall**
   1. Click **Start,** then type *MMC*  and click it.
   2. Click File, then **Add/Remove Snap-ins.**
   3. Scroll down, then add in the **Windows Firewall with Advanced Security**
   4. On the homepage, go to **Windows Firewall Properties**
   5. There will be three tabs- **Domain**, **Private**, and **Public**
      1. Each correspond with the type of network you are on. When you connect to a new network, Windows 7 will prompt you to choose- Home, Public, or Work network. This will decide firewall settings for that network.
      2. Domain= Work, Private= Home, Public=Public
   6. Go through each of the three tabs and make sure the firewall is **on**
   7. Make sure **Inbound Connections** are **Blocked** by default, and **Outbound Connections** are **Allowed** for each of the three profiles
   8. For each of the three sections, go to **Logging**, then **Customize**
   9. Select the Yes for both **Log dropped** & **Logged Successful** **Packets**
   10. Increase the **Log Size Limit** according to available disk space
   11. Make sure you do this for each profile!!
   12. Now, in the left pane, double click the **Windows Firewall with Advanced Security**
   13. Click on Inbound rules- These rules dictate who can connect to your computer
   14. Look for potentially malicious rules
   15. Disable and **File and Printer Sharing** rules
       1. To disable a rule, **Right Click** the rule and check **Disable**
   16. Disable **Remote Assistance** and **Remote Desktop** rules
   17. Disable any other **Remote** rules
   18. Disable **SNMP or SMTP** rules, unless the readme says you need them
3. **Policies**
   1. Open up the **MMC**
   2. Add in the **Group Policy Object Editor**  Snap-in
      1. If the computer doesn’t have GPOE, then you either need to update it, or it is home basic, in which just skip this step. Although I doubt you will get a home basic image.
   3. A few things to note- **READ THESE BEFORE YOU START**
      1. In the policy list, I’m not going to include Network and Local Service. **IF YOU SEE THESE IN THE LIST, DO NOT REMOVE THEM**
      2. **DO NOT REMOVE THE CYBERPATRIOT SCORING BOT USER FROM ANYTHING**
      3. **Even if it says no one, DO NOT REMOVE NETWORK/LOCAL SERVICE FROM ANYTHING**
   4. Configure the Policies as you see Below

|  |  |
| --- | --- |
| **Password Policy** |  |
| Enforce Password History | 8 |
| Maximum Password Age | 14 |
| Minimum Password Age | 8 |
| Minimum Password Length | 8 |
| Password must meet… | Enabled |
| Store Passwords using… | Disabled |
|  |  |
| **Account Lockout Policy** |  |
| Account Lockout Duration | 10 |
| Account Lockout Threshold | 7 |
| Reset Account Lockout Counter… | 10 |
|  |  |
| **User Rights Assignment** |  |
| Access credential manager as a… | Admin |
| Access this computer from the network | No One |
| Act as part of the OS | No One |
| Add workstation to domain | No One |
| Adjust memory quotas for a process | No One |
| Allow logon locally | Admin |
| Allow logon through RDS | No One |
| Backup files/directories | Admin |
| Bypass traverse checking | No One |
| Change the system time | No One |
| Change the time zone | No One |
| Create a page file | No One |
| Create a token object | Admin |
| Create global objects | Admin |
| Create permanent shared objects | No One |
| Create symbolic links | Admin |
| Debug programs | No One |
| Deny access to this computer… | No One |
| Deny logon as a batch job | No One |
| Deny logon as a service | No One |
| Deny logon locally | No One |
| Deny logon through RDS | No One |
| Enable computer and User Accounts… | Admin |
| Force shutdown from a remote system | No One |
| Generate security audits | No One |
| Impersonate a client after authentication | No One |
| Increase a process working set | No One |
| Increase scheduling priority | Admin |
| Load and unload device drivers | Admin |
| Lock pages in memory | Admin |
| Logon as a batch job | No One |
| Logon as a service | No One |
| Manage auditing and Security log | Admin |
| Modify an object label | Admin |
| Modify firmware environment values | Admin |
| Perform volume maintenance tasks | Admin |
| Profile single process | Admin |
| Profile system performance | Admin |
| Remove computer from docking station | Admin |
| Replace a process level token | Admin |
| Restore files and directories | Admin |
| Shutdown the system | Admin |
| Synchronize directory service data | Admin |
| Take Ownership of files… | Admin |
|  |  |
| **Security Options** |  |
| Admin Account | If you are logged on as the default Admin, enabled. If not, Disabled |
| Guest Account | Disabled |
| Limit Local use of Blank Passwords | Enabled |
| Rename Admin account | If you are logged on as the default Admin, do not rename it If not, rename it |
| Rename Guest account | Rename it |
| Audit the access of… | Enabled |
| Audit the use of… | Enabled |
| Force audit policy… | Enabled |
| Shutdown the machine if unable to log security audits | Disabled |
| Machine access restrictions | Not Defined |
| Machine launch restrictions | Not Defined |
| Allow undock without having to logon | Disabled |
| Allowed to format and eject removable media | Admin only |
| Prevent users from installing printer drivers | Enabled |
| Prevent CD-ROM access | Enabled |
| Restrict floppy access | Enabled |
| Allow server operators to schedule tasks | Disabled |
| LDAP Server signing requirements | Require it |
| Refuse machine account password changes | Enabled |
| Digitally encrypt or sign secure channel data | Enabled for all of them |
| Disable machine account password changes | Enabled |
| Maximum machine password age | 13 days |
| Require strong (Windows 2000 or later) session key | Enabled |
| Display user information when the session… | Do not Display user information |
| Do not display last user name | Enabled |
| Do not require CTRL + ALT + DEL | Disabled |
| Message Text for users attempting to logon | leave blank |
| Message Title for users attempting to logon | leave blank |
| Number of previous logons to cache | 0 |
| Prompt user to change password before expiration | 8 days |
| Require domain controller authentication… | Disabled |
| Require smart card | Disabled |
| Smart card removal behavior | No action |
| Digitally sign communications | Disabled |
| Send unencrypted passwords to 3rd party SMB servers | Disabled |
| Amount of Idle time before suspending session | 45 minutes |
| Digitally sign communications | Disabled |
| Disconnect clients when logon hour expires | Disabled |
| Server SPN target name | Leave it alone |
| Allow Anonymous SID/Name Translation | Disabled |
| Do not allow anonymous enumeration of SAM accounts | Enabled |
| Do not allow anonymous enumeration of SAM accounts and shares | Enabled |
| Do not allow storage of passwords… | Enabled |
| Let everyone permissions apply to anonymous users | Disabled |
| Name pipes that can be accessed anonymously | Disabled |
| Remotely accessible ANYTHING | Remove all text |
| Restrict anonymous access | Enabled |
| Shares that can be accessed anonymously | Delete everything |
| Sharing and security | Classic |
| Allow local system to use… | Disabled |
| Allow local system to null session fallback | Leave alone |

1. **Services**
   1. Open up services by clicking **Start**, then typing *MMC*. Click the MMC icon
   2. Now, click **File**, then **Add/Remove Snap-in**.
   3. Add in the **Services Snap-in,** then click finish and ok
   4. Sort by name, and cross reference with the default services. If you find a service not on this list and are unsure about it, just google it, or follow the steps below
      1. ***DO NOT DELETE ANYTHING TO DO WITH CP, CYBERPATRIOT, SCORING BOT, SAIC etc. Do not even touch them.***
      2. For other services, **Right Click**, go to **Properties**, and check the **Path to Executable**. It should be on the default page.
      3. Find the executable file, by putting the location into the **Start** menu, but make sure you don’t accidently run it!
      4. Check the date it was installed. If it was in the Summer of 2009, the executable should be ok. If you are still unsure, just google the name of the executable. You will know it is an executable file, because it will end with .exe
   5. Default services that are not necessary. IF THE README SAYS OTHERWISE GO BY THE README
   6. Here are the Default Services, and their recommended settings for a Windows 7 box-

|  |  |
| --- | --- |
| **Service Name** | **Required Configuration (CHANGE TO THIS ONE!!)** |
| ActiveX Installer | Disabled |
| Adaptive Brightness | Disabled |
| Application Experience | Manual |
| Application Identity | Manual |
| Application Information | Manual |
| Application Layer Gateway Service | Disabled |
| Background Intelligent Transfer Service | Manual |
| Base Filtering Engine | Automatic |
| BitLocker Drive Encryption Service | Manual |
| Bitlock Level Backup Engine Service | Disabled |
| Bluetooth Support Service | Disabled |
| Certificate Propagation | Disabled |
| CNG Key Isolation | Manual |
| COM+ Event System | Manual |
| COM+ System Application | Manual |
| Computer Browser | Manual |
| Credential Manger | Manual |
| Cryptographic Services | Automatic |
| DCOM Server Process Launcher | Automatic |
| Desktop Window Manager Session Manager | Automatic |
| DHCP Client | Automatic |
| Diagnostic Policy Service | Disabled |
| Diagnostic Service Host | Disabled |
| Diagnostic System Host | Disabled |
| Disk Defragmenter | Disabled |
| Distributed Link Tracking Client | Manual |
| Distributed Transaction Coordinator | Manual |
| DNS Client | Automatic |
| Encrypting File System | Manual |
| Extensible Authentication Protocol | Manual |
| Fax | Disabled |
| Function Discovery Provider Host | Manual |
| Function Discovery Resource Publication | Manual |
| Group Policy Client | Automatic |
| Health Key and Certificate Management | Manual |
| HomeGroup Listener | Disabled |
| HomeGroup Listener | Disabled |
| Human Interface Device Access | Disabled |
| IKE and AuthIP IPsec Keying modules | Manual |
| Interactive Services Detection | Disabled |
| Internet Connection Sharing | Disabled |
| IP Helper | Manual |
| IPsec Policy Agent | Manual |
| KtmRm for Distributed Transaction Coordinator | Disabled |
| Link-Layer Topology Discovery Mapper | Manual |
| Microsoft .NET Framework NGEN v2.0 | Manual |
| Microsoft iSCSI Initiator Service | Disabled |
| Microsoft Software Shadow Copy Provider | Disabled |
| Multimedia Class Scheduler | Disabled |
| Net.Tcp Port Sharing Service | Disabled |
| Netlogon | Disabled |
| Network Access Protection Agent | Manual |
| Network Connections | Manual |
| Network List Service | Manual |
| Network Location Awareness | Manual |
| Network Store Interface Service | Automatic |
| Parental Controls | Disabled |
| Peer Name resolution Protocol | Disabled |
| Peer Networking Grouping | Disabled |
| Peer Networking Identity Manager | Disabled |
| Performance Logs & Alerts | Manual |
| Plug and Play | Disabled |
| PnP-X IP Bus Enumerator | Disabled |
| PNRP Machine Name Publication Service | Disabled |
| Portable Device Enumerator Service | Disabled |
| Power | Automatic |
| Print Spooler | Disabled |
| Problem Reports and Solutions Control Panel Support | Manual |
| Program Compatibility Assistant Service | Manual |
| Protected Storage | Manual |
| Quality Windows Audio Video Experience | Disabled |
| Remote Access Auto Connection Manager | Disabled |
| Remote Access Connection Manager | Disabled |
| Remote Desktop Configuration | Disabled |
| Remote Desktop Services | Disabled |
| Remote Procedure Call (RPC) | Automatic |
| Remote Procedure Call (RPC) Locator | Manual |
| Remote Registry  RIP Routing | ^^ Dis-Disabled |
| Routing and Remote Access | Disabled |
| RPC Endpoint Mapper | Automatic |
| Secondary Logon | Disabled |
| Secure Socket Tunneling Protocol Service | Disabled |
| Security Accounts Manager | Automatic |
| Security Center | Automatic |
| Server | Manual |
| Shell Hardware Detection | Disabled |
| Smart Card | Disabled |
| Smart Card Removal Policy | Disabled |
| SNMP Trap | Disabled |
| Software Protection | Automatic |
| SPP Notification Service | Manual |
| SSDP Discovery | Disabled |
| Superfetch | Manual |
| System Event Notification Service | Automatic |
| Tablet PC Input Service | Disabled |
| Task Scheduler | Disabled |
| TCP/IP NetBIOS Helper | Disabled |
| Telephony | Disabled |
| Telnet | Disabled |
| Themes | Manual |
| Thread Ordering Server | Manual |
| TP AutoConnect Service | Disabled |
| TP VC Gateway Service | Disabled |
| TPM Base Services | Disabled |
| UPnP Device Host | Disabled |
| User Profile Service | Automatic |
| Virtual Disk | Manual |
| VMware Snapshot Provider | Manual |
| VMware Tools | Automatic |
| Volume Shadow Copy | Disabled |
| WebClient | Disabled |
| Windows Audio | Disabled |
| Windows Audio Endpoint Builder | Disabled |
| Windows Backup | Manual |
| Windows Biometric Service | Disabled |
| Windows CardSpace | Disabled |
| Windows Color System | Disabled |
| Windows Connect Now | Disabled |
| Windows Defender | Automatic |
| Windows Driver Foundation | Manual |
| Windows Error Reporting Service | Manual |
| Windows Event Collector | Disabled |
| Windows Event Log | Automatic |
| Windows Firewall | Automatic |
| Windows Font Cache | Disabled |
| Windows Image Acquisition | Disabled |
| Windows Installer | Manual |
| Windows Management Instrumentation | Automatic |
| Windows Media Player Network Sharing Service | Disabled |
| Windows Modules Installer | Manual |
| Windows Presentation Foundation | Disabled |
| Windows Remote Management | Disabled |
| Windows Search | Automatic |
| Widows Time | Manual |
| Windows Update | Automatic |
| WinHTTP Web Proxy AutoDiscovery Service | Disabled |
| Wired Autoconfig | Manual |
| WLAN AutoConfig | Manual |
| WMI Performance Adapter | Disabled |
| Workstation | Automatic |
| WWAN AutoConfig | Manual |

The following are common, but not default Windows Services. Disable all of the following, **unless the readme says otherwise!**

* + 1. SMTP
    2. Bonjour
    3. Remote Access Auto Connection manager
    4. Remote Access Connection manager
    5. Remote Desktop Config
    6. Remote Desktop services
    7. Remote Registry
    8. RIP routing
    9. World Wide Web Publishing service- This means you have IIS server running
    10. NetMeeting Remote Desktop Sharing
    11. Simple File Sharing
    12. SSDP Discovery Service
    13. Windows Messenger Service

1. **Remote Desktop**
   1. Right click **My Computer**  and go to properties
   2. Go to the **Remote** tab
   3. Go to the **Advanced** button
   4. Uncheck **Allow this computer to be controlled…**
   5. Now, uncheck **Allow remote assistance connections…**
   6. Apply, and ok
      1. Depending on the type of Windows 7 you have, there will be different check marks. Make sure you read them before you uncheck them.
2. **Turn on Automatic Updating**
   1. Click **Start** and type *Control* Panel. Open it up
   2. Then Go to the **System and Security** tab
   3. Go to the **Windows Update** menu
   4. On the lefthand side, click **Change Settings**
   5. Choose **Install Updates Automatically**
      1. If it is time based, make sure you don’t have it set so it will interrupt your image
3. **Processes and Open Ports**
   1. Open ports are one of the most important things to check- because hard to find programs will almost always open ports.
   2. Open up a command prompt, and type *netstat –ano*
      1. This will list the port number, the IP, and the PID
   3. Now, we need **Process Explorer**
      1. Go to the **Downloads** folder, and click on **Procexp.exe**.
         1. It will ask you to agree, just click **Yes**
   4. Click on the **Options** menu, then select **Verify Image Signatures**. This will ensure that an executable actually is made by who they say. They can fake the creator/signature.
   5. Now, go to the **View** tab, and click on **Select Columns**. Make sure the following are selected:
      1. **PID**
      2. **Company Name**
      3. **Verified Signature**
      4. **Image Path**
   6. Now, we need to figure out what Processes open which Ports
   7. Cross reference the **Open Ports’ PID** with the **PID’s from Process Explorer**. These are normal **Default Windows Processes**-
      1. **System Idle Process**
      2. **System**
      3. **Smss.exe**
      4. **Crss.exe**
      5. **Services.exe**
      6. **Winnit.exe**
      7. **SearchIndexer.exe**
      8. **Lsass.exe**
      9. **Winlogon.exe**
      10. **Dwm.exe**
      11. **Svchost.exe (YOU NEED TO CHECK ALL OF THESE BECAUSE A LOT OF MALWARE LIKES TO HIDE UNDER THIS PROCESS NAME!)**
      12. **Explorer.exe**
   8. Make sure you have cross referenced each the **PID’s** from the **Command Prompt** and **Process Explorer**
   9. If you are unsure if a process is malicious or not, look at the company name, and the Verified Signature. If it is a **SVChost** with **Microsoft** Company name and it is verified, then it is OK. However, we don’t want all products from **Microsoft Corporation**, such as a **Telnet Server**, or SMTP server running (Unless the readme says so.) If you are unsure, google it.
   10. To end a malicious or unneeded process, the first thing you need to do is write down the Path. This will be important later on
   11. Now, we need to right click the process, and select **Kill Process**. This will stop the **Process** from running.
   12. However, our job is not done yet, we need to delete the .exe file that was running the process. Take note that you do **NOT** need to do this for verified Microsoft Corporation products, like Telnet or SMTP. However, make sure you have disabled the service
   13. Take the file path (I really, really hope you wrote it down…) and click **Start** and copy it in to the search bar. Be careful not to accidently run the .exe file again.
   14. We need to delete the file, so go into the folder containing the file, and hold down the **SHIFT + DELETE** keys. This will permanently delete the file, instead of just sending it to the recycle bin.
   15. Triple check to make sure you want to delete it
   16. Click **Yes**
   17. Rinse and repeat until you have checked all of the **processes**
4. **Alternate Data Streams (ADS)** 
   1. ADS is alternate data streams. It is a vulnerability in the way NTFS works, so files can hide themselves. We have to get a scanner to remove it
   2. Get the **ADSspy** from the google docs. It is on the Cyber Toolkit main page
   3. Install **ADSspy**
   4. Select **Full Scan (all NTFS drives)** so it scans the whole box. This will let you know what streams come up, and you can remove them from there. You can skip ahead to the next step while it is scanning the image.
5. **Remove Programs from Startup**.
   * 1. Go to **Run** (Windows Key + R)
     2. Type *msconfig*
     3. Go to the **Startup** tab
        1. Only these should be listed:
           1. Any type of **VMware** software
           2. **Malwarebytes** if you installed it yourself
           3. Anything **Cyberpatriot** or **Scoring Bot** related
        2. We don’t need anything else.
        3. Write down the name, and the location of the file. Then, follow #11 to find out if it is malicious. If it’s something like **Netcat**, **bfk**, **nc**, **ncat**, **telnet**, an alarm should go off in your head. You need to uncheck these immediately
        4. Disable the startup things you don’t need- See list above
     4. This makes it so that the program doesn’t restart when we turn the computer off and on again
6. **Adding/Removing Windows Components**
   1. Open up a Control Panel
   2. Go to the **Programs** menu, then click on **Programs and Features**
   3. On the left pane, select **Turn Windows Features On or Off**
   4. Turn off these features, unless the readme says otherwise-
      1. **Games**
      2. **Internet Information Services**
      3. **Internet Information Services Hostable Web Core**
      4. **Media Features**
      5. **Print and Document Services**
      6. **SNMP**
      7. **Telnet Client**
      8. **Telnet Server**
      9. **TFTP Client/Server**
      10. **Windows PowerShell**
      11. **XPS Services**
      12. **XPS Viewer**
   5. Basically, this is a host machine, and shouldn’t be running any servers, or have any reason for any of this.
7. **Installing an Anti-Virus**
   1. Download the **AVG installer.exe** from the google docs, in the **Antivirus** folder
   2. Install **AVG.** Choose **Basic Protection**, and **Custom Install**
      1. Uncheck each box from the custom install, we don’t want any of their bloatware
      2. Uncheck each box from the **Component Selection**
      3. Finish Installing it
8. **User Account Control Configuration**
   1. Click **Start** and type *Control Panel.*
   2. Go to the **System and Security** option
   3. Under the **Action Center**, select **Change User Account Control** **settings**.
   4. Now, move the bar all the way up. This ensures that no programs can get elevated rights without your permission. It gets annoying I know, but it could be the difference between making it to national finals and not.
   5. Make sure you click **OK** and don’t just exit out of the screen, otherwise it will not save it.
9. **Disable Dump File Creation**
   1. Open up the **Control Panel**
   2. Go to **System**
   3. Click **Advanced**
   4. Now click **Startup/Recovery**
   5. Click **Settings**
   6. Change value for **Write Debugging Information** to **None**
10. **Creating a Restore Point**
    1. Right click **My Computer** and go to **Properties**
    2. Go to the **System Protection** tab
    3. Click on the **Configure** button
    4. Click **Turn on system protection**
    5. Set the Max usage to **2 GB**
    6. Click **OK**
    7. Now, click on the **Create** button
    8. Type a description to Create the restore point
    9. Click **Create**
    10. Click **OK**
11. **Saved Windows Credentials**
    1. Go to the **Control Panel,** then click the **User Accounts and Family Safety** option
    2. Click **Manage your credentials**
    3. Delete all the credentials, there should be no entry in any box
    4. Double check to make sure you have removed both Windows AND Web credentials
12. **Internet Options Settings**
    1. Open **Internet Explorer**,
    2. Select the **tools** menu, then select **Internet Options**
    3. Make sure the homepage is set to google.com
    4. Go to **Browsing History Settings**
       1. Select the **Never** option on the first tab
    5. Check the **Delete browsing history on exit** tab
    6. Go to the **Security tab**, and ramp up the security level for **each zone** to be high
    7. Go to the **Privacy tab**, and ramp up the security level to **Block all Cookies**
    8. Go to the **Content tab**, and **Clear the SSL Slate**
    9. Go to **Autocomplete Settings**, and remove all of the checkboxes
    10. **Delete** the **Autocomplete history**, and go to the managed passwords to make sure nothing is in there
    11. Select apply and then OK
13. **Power Settings**
    1. Go to the **Control Panel** and go to **System and Security**
    2. Go to the **Power Options** menu
    3. Select the **Require a Password on Wakeup**
    4. Select the **Require a password**
    5. Save changes
14. **Data Execution Prevention**
    1. Go to the **Control Panel**, and go to the Top right corner. Change **View by:** to **Small Icons**
    2. Then, look for the **Performance Icon**
    3. Now, go to **Adjust Visual Effects** option
    4. Navigate to the **Data Execution Prevention** tab
    5. Select **Turn on DEP for all programs and services except those I select (don’t put any in there)**
    6. Apply and ok
15. **Malicious Drivers**
    1. Download the tool **Uniblue DriverScanner**
    2. Install the tool
    3. Scan the system- this will let you know if any drivers are out of date, and if there are any malicious drivers on the system. Update them as recommended by the program
16. **GMER scan**
    1. GMER scans for rootkits on the system which is great. Get it from the google docs, in the **Rootkits** folder
    2. Run the GMER scan, and remove any programs that it turns up
17. **CCleaner**
    1. Get CCleaner installer from the **Malware** folder in google docs
    2. Download and install CCleaner with the recommended settings
    3. On the **Intelligently Scan for Cookies to keep** popup menu, click **No**
    4. Click **Analyze** and let CCleaner run
    5. Check all of the boxes it turns up, and click **Run Cleaner**
    6. Now, go to the **Registry** Tab, and click **Scan for Issues**
    7. Let it scan, then click all the boxes, and say **Fix Selected Issues**
    8. Click **Yes**, and save the .reg file when it comes up
18. **Microsoft Baseline Security Analyzer scan**
    1. Get MBSA from the google docs, under the **Malware** folder
    2. Install MBSA using recommended settings
    3. Startup MBSA, and click **Scan a Computer**
    4. Find out what MBSA says your image is not good with, and fix it

DO NOT TURN OFF YOUR COMPUTER WHEN IT IS INSTALLING UPDATES. MAKE SURE YOU ARE PLUGGED IN

1. **Service Packs**
   1. Get the Services packs from the Google Docs, in the **Service Packs** folder. Make sure you have selected the right operating system
   2. Install the service pack by double clicking it and let it run.
2. **Updating via Control Panel**
   1. Open up the **Control Panel**, and click **System and Security**
      1. You may have the other version, just click **Windows Update**
      2. Under **Windows Update**, click **Check for Updates**.
      3. Install all of the required updates
3. **Final Thoughts:**
4. This checklist should get you through all of the Windows 7 images through finals. XP and Server a slightly different, but if you don’t have any other checklists to follow, you can use this one and still get probably a 100% on xp (Locations for stuff is different, but you can figure it out), and server probably an 80 or 90%, because of server roles and securing an IIS/FTP server. This should get you guys at least to semi-finals, if you follow it (and if you have a reliable linux dude).

**Appendix**

You can use this command in the PowerShell to find files modified after 12/7/12 and output it into a text file. Then, use this to search for media in the results, and you will probably find the prohibited media files on the system.

**cd /**

**get-childitem -recurse | where-object {$\_.lastwritetime -gt "12-07-2012"} > "Files Modified after 2012.txt"**

**Remember to Remove Welcome Screen**

* 1. Open up the **Control Panel**
  2. Go to **User Accounts**
  3. Click **Change the way users log on or off**
  4. Uncheck **Use Welcome Screen**
  5. Click **Save** and exit

Here is a list of a bunch of important registry keys. Use them wisely, don’t go into the registry if you don’t know what you are doing. I included some shortcuts to make it shorter.

HKLM- HKEY Local Machine

HKCU- HKEY Current User

HKCR- HKEY Classes Root

HKU- HKEY Users

HKCC- HKEY Current Config

CCS- Current Control Set

CV- Current Version

|  |  |
| --- | --- |
| Registry Key | What it does |
| HKLM/SYSTEM/CCS/Control/Session Manager/Memory Management | Contains Page file information |
| HKLM/SOFTWARE/Microsoft/Windows/CV/Uninstall | Contains a full list of software installed on the system |
| HKLM/System/CCS/Services/LanmanServer/Parameters/AutoShareServer | Shows hidden shared files |
| HKLM/SYSTEM/CCS/Services/CDROM | Change to 1 to disable auto-play |
| HKLM/Software/Microsoft/Windows/CV/Run | Shows Programs on startup |
| HKCU/Software/Microsoft/Windows/CV/Run | Shows programs on startup |
| HKLM/System/CCS/Services/RasMan/Parameters | Add value named "DisabledSavedPassword", set it to 1 to disabled windows saving passwords |
| HKLM/Software/Microsoft/WindowsNT/CV/Winlogon/Cachedlogonscount | Set to 0 to disable cached logons |
| HKLM/System/CCS/Control/Print/Printers/DefaultSppolDirectory | Change the location of the print spooler file |
| HKLM/System?CCS/Services/Servicename | When the service is being launched by a svchost.exe, it will be in a particular service group, which is then launched by that SVChost. |
| HKLM/Software/Microsoft/WindowsNT/CV/Svchost | Under this key you will find various groups in which each contain multiple services that will be launched when the group is loaded by svchost.exe |
| HKLM/System/CCS/Services/servicename/Parameters/ServiceDLL | The value of the ServiceDLL key is the actual file we want to be concerned with |
| HKLM/SYSTEM/CCS001/Enum/Root | This contains a subkey called LEGACY\_svcname. These entries should be deleted as well, but you may have to change the permissions to delete them |
| HKLM/SYSTEM/CCS002/Enum/Root | This contains a subkey called LEGACY\_svcname. These entries should be deleted as well, but you may have to change the permissions to delete them |
| HKLM/Software/Microsoft/WindowsNT/CV/Winlogon | The UserInit key specifies which programs should be launched right after a user logs into windows. The default program for this key is C:\Windows\System32\Userinit.exe. Userinit.exe is a program that restores your profile, fonts, colors, etc. for your username. It is possible to add further programs that will launch from this key by separating the programs with a comma. For example: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit =C:\windows\system32\userinit.exe,c:\windows\badprogram.exe. This will make both programs launch when you log in and is a common place for Trojans, hijackers, and spyware to launch from. |
| HKLM/SOFTWARE/Microsoft/Windows/CV/ShellServiceObjectDelayLoad | This Registry value contains values in a similar way as the Run key does. The difference is that instead of pointing to the file itself, it points to the CLSID's InProcServer, which contains the information about the particular DLL file that is being used. The files under this key are loaded automatically by Explorer.exe when your computer starts. Because Explorer.exe is the shell for your computer, it will always start, thus always loading the files under this key. These files are therefore loaded early in the startup process before any human intervention occurs. |
| HKCU/Software/Microsoft/CV/Explorer/runMRU- | Most Recently User run commands |
| HKCU/Software/Microsoft/Windows/CV/Explorer/RecentDocs | Recently opened documents with Windows Explorer |
| HKCU/Software/Microsoft/Windows/CV/Explorer/ComDlg32/OpensaveMRU | Keeps a list of recently opened saved files |
| HKCU/Software/Microsoft/Windows/CV/Explorer/ComDlg32/LastVistitedMRU | More information on recently opened files |
| HKCU/Software/Microsoft/Search Assistant/ACMRU | Contains recent search terms using Windows default search |
| HKCU/Software/Microsoft/Windows/CV/Explorer/UserAssist | Contains 2GUID subkeys. Each contains a list of system objects like control panel and shortcuts that a user has accessed |
| HKLM/System/Controlset00x/Enum/USBSTOR | Stores the contest and DID values of any USB device connected to the system |
| HKCU/Software/Microsoft/Windows/ShellNoRoam/MUICache | Shows Programs that have been run on the system |
| HKCU/Software/Classes/LS/Software/Microsoft/Windows/Shell/MUICache | Shows Programs that have been run on the system |
| HKCU/Software/Microsoft/Windows/CV/Explorer/MapNetworkDriveMRU | Contains a list of mapped network drives |
| HKCU/Software/Microsoft/Protected Storage System Provider | Windows protected Storage. Is used to store private info, like passwords |
| HKCU/Microsoft/Windows/CV/Explorer/WWQ | Contains recent Windows searches |
| HKCU/Software/Microsoft/WS/ProcessedSearch-Roots/0003/Default | Contains recent Windows searches |
| HKCU/Software/Microsoft/Windows/CV/Applets/Regedit | Shows Last accessed registry key |
| HKCU/Software/Microsoft/Office/10.0/Word/Data | Shows recent word files |
| HKCU/Software/Microsot/Office/10.0/Excel/Recent Files | Recent Excel files |
| HKCU/Software/Microsoft/Office/10.0/PowerPoint/Recent File List | Shows recent PowerPoint files |
| HKCU/Software/Microsoft/MediaPlayer/Player/RecentFileList | Recent Windows Media Player files |
| HKLM/SOFTWARE/Microsoft/WZCSVC/Parameters/Interfaces | Connected to Wireless Networks |
| HKCU/Software/Microsoft/Windows/CV/ExplorerComputerDescriptions | Recent Computers connected |
| HKCU/Software/Microsoft/Internet Explorer/Download Directory | Default download directory |
| HKCU/Software/Microsoft/IE/INtelliForms/SPW | Auto Complete Passwords |
| HKLM/UID/Software/Skype/PluginManger | Displays country, language, and recent user |
| HKLM/SOFTWARE/Microsoft/WindowsNT/CV/NetworkList/Nla/Wireless | Displays any wireless networks the computer has connected to |
| HKU/UID/Software/Adobe/AcrobatReader/9.0/AVGeneral/RecentFiles | Shows recent Adobe Reader files |
| HKU/SID/Software/WindRAR/ArcHIstory | Recent WinRAR files |
| HKU/UID/Software/Microsoft/Windows/CV/Explorer/RD/.gif | shows recent .gif files |
| HKU/UID/Software/Microsoft/Windows/CV/Explorer/RD/.jpg | Shows recent .jpg files |
| HKU/UID/Software/Microsoft/Windows/CV/Explorer/RD/.txt | Shows recent text files |
| HKLM/System/MountedDevices | Contains a list of mounted devices |
| HKCU/Software/Microsoft/Command Processor | Contains a registry value called autorun which should contain a command that is automatically executed each time cmd.exe is run |
| HKLM/Software/Microsoft/Comand Processor | Contains a registry value called autorun which should contain a command that is automatically executed each time cmd.exe is run |
| HKLM/System/CCS001/Services/pnpsvc | Manually remote a service |
| HKLM/SYSTEM/CCS002/Service/pnpsvc | Manually remove a service |

Here are some important commands in the command prompt:

|  |  |
| --- | --- |
| Command | What it does |
| Dir /s <name> | Searches the current directory for the file name |
| cd <Path> | change directory to a certain path |
| cd / | Changes directory to C:\ |
| dir | displays the contents of the current directory |
| mkdir <name> | Makes a directory |
| openfiles | Displays files that are open in a remote machine |
| prompt <name> | Creates a new prompt with the name |
| rename | Renames a file or folder |
| sc | Configure services |
| cls | clear the command prompt |
| cmd | opens a new instance of command prompt |
| convert | Convert the drive from FAT to NTFS |
| del <filename> | delete the files |
| Netstat -ano | Lists the open ports and PID's |
| Tasklist /SVC /FO Table | Lists the running tasks in a table format |
| Taskkill <PID> /F /T | Force kills the process and all sub-processes |
| Taskkill /IM <NAME> | Kills the task via image name |
| schtasks | lists the scheduled tasks on the system |
| schtasks /Delete <TASKNAME> | Delete a certain scheduled task |
| schtasks /End <TASKNAME | Ends the running of a certain scheduled task |
| schtasks /ShowSid <NAME | Shows the SID of a certain scheduled task |
| sc start <Servicename> | Starts the selected Service |
| sc pause <Servicename> | Pauses the selected service |
| sc stop <Servicename> | stops the selected service |
| net share | Displays the shared folders on the system |
| net share /delete <name> | Deletes the selected share |
| net accounts /Forceloggoff:NO | Does not force logoff when the permitted hours expire |
| net accounts /minpwlen:8 | Sets the minimum password length to 8 |
| net accounts /maxpwage: 14 | Sets the maximum password age to 14 days |
| net accounts /minpwage:7 | Sets the minimum password age to 7 |
| net localgroup | displays local groups on the system |
| net user eagle2120 password | Sets the password for eagle2120 to password |
| net user eagle2120 /delete | Deletes the user eagle2120 |
| net user eagle2120 /ACTIVE:No | Disables the user eagle2120 |
| net user bob password /add | creates a user "bob" with a password of password |

Make sure this is the absolute last thing you have to do. This will totally lock down your box, including your ability to use it, so make sure it is totally done with everything else

Administrative Templates-

Control Panel

Regional/Language Options

Restrict the UI language Windows uses for all logged on users: Enabled- English

Force selected system UI language to overwrite the User UI language: Disabled

User Accounts

Apply the default user logon picture to all users: Enabled

Network

BITS

Do not allow the BITS client to use Windows Branch Cache: Enabled

Do not allow the computer to act as a BITS peer-caching client: Enabled

Do not allow the computer to act as a BITS peer-caching server: Enabled

Allow BITS peer-caching: Disabled

Time-out for inactive BITS jobs: 1 Day

Limit the maximum network bandwidth for BITS background transfers: Enabled, 0

Limit the maximum network bandwidth: Enabled, 1

Set up a maintenance schedule to limit the maximum bandwidth...: Disabled

Set up a work schedule to limit the maximum network bandwidth...: Disabled

Limit the BITS Peer-cache size: Enabled, 1

Limit the age of files in the BITS peer-cache: Enabled, 1

Limit the maximum BITS job download time: Enabled, 1

Limit the maximum number of files allowed in a BITS job: Enabled, 1

Limit the maximum number of BITS jobs for this computer: Enabled, 1

Limit the maximum number of BITS jobs for each user: Enabled, 1

Limit the Maximum number of ranges that can be added to the file in a BITS job: Enabled, 1

Branch Cache

Turn on Branch Cache: Disabled

Set Branch Cache distributed Cache mode: Disabled

Set Branch Cache HOsted Cache Mode: Disabled

Configure Branch Cache for Network Files: Disabled

Set percentage of Disk space used for client computer cache: Enabled, 1

DNS Client

Allow DNS Suffix Appending to Unqualified Multi-Label...: Disabled

Connection-Specific DNS Suffix: Not configured

Primary DNS Suffix Devolution Level: Not configured

DNS Servers: Not configured

Primary DNS Suffix: Not Configured

Register DNS records with connection-specific DNS suffix: Not Configured

Register PTR Records: Not configured

Dynamic Update: Enabled

Replace Addresses in Conflicts: Not Configured

Registration Refresh Interval: Enabled, 1000

TTL Set in the A and PTR record: Enabled, 300

DNS Suffix Search List: Not configured

Update Security Level Update Top Level Domain Zones: Enabled

Primary DNS Suffix Devolution: Enabled

Turn off Multicast Name Resolution: Enabled

Lanman Server

Hash Publication for BranchCache: Disabled

Link-Layer Topology Discovery

Turn on Mapper I/O driver: Not configured

Turn on Responder driver: Not configured

Microsoft Peer-to-Peer Network

Disable password strength validation for Peer Grouping: Disabled

Turn off Microsoft Peer-toPeer networking services: Enabled

Global Clouds

Turn off Multicast Bootstrap: Enabled

Turn off PNRP cloud creation: Enabled

Set PNRP cloud to resolve only: Enabled

Set the Seed Server: Not configured

Link-Local Clouds

Turn off Multicast Bootstrap: Enabled

Turn off PNRP cloud creation: Enabled

Set PNRP cloud to resolve only: Enabled

Set the Seed Server: Not configured

Site-Local Clouds

Turn off Multicast Bootstrap: Enabled

Turn off PNRP cloud creation: Enabled

Set PNRP cloud to resolve only: Enabled

Set the Seed Server: Not configured

Network Connections

Windows

Domain Profile

Allow local program exceptions: Not configured

Define inbound program exceptions: Not configured

Protect all network Connections: Enabled

Do not allow exceptions: Not configured

Allow inbound file and printer sharing...: Disabled

Allow ICMP exceptions: Not configured

Allow logging: Enabled

Prohibit Notifications: Disabled

Allow local port exceptions: Not configured

Define inbound port exceptions: Not configured

Allow inbound remote administration...: Disabled

Prohibit unicast response to multicast...: Not configured

Allow inbound UPnP framework...: Disabled

Standard Profile

Allow local program exceptions: Not configured

Define inbound program exceptions: Not configured

Protect all network Connections: Enabled

Do not allow exceptions: Not configured

Allow inbound file and printer sharing...: Disabled

Allow ICMP exceptions: Not configured

Allow logging: Enabled

Prohibit Notifications: Disabled

Allow local port exceptions: Not configured

Define inbound port exceptions: Not configured

Allow inbound remote administration...: Disabled

Prohibit unicast response to multicast...: Not configured

Allow inbound UPnP framework...: Disabled

Windows Firewall: Allow authenticated IPsec bypass: Disabled

Prohibit installation and configuration of network bridge on..: Disabled

Do not show the local access only icon: Not Configured

Route all traffic through the internal network: Disabled

Prohibit use of Internet Connection Firewall on your...: Disabled

Prohibit use of ICS on your DNS domain network: Enabled

Require domain users to elevate when setting a network location: Enabled

Network Connectivity Status Indicator

Corporate DNS Probe Host Address: Not configured

Corporate DNS Probe Host Name: Not configured

Corporate Site Prefix List: Not configured

Corporate Website Probe URL: Not configured

Domain Location Determination URL: Not configured

Offline Files

Sub-folders always available offline: Disabled

Administratively assigned offline files: Disabled

Configure Background Sync: Not configured

Limit Disk Space used by Offline Files: Enabled, 1, 1

Non-Default Server Disconnect Actions: Not configured

Default Cache Size: Not configured

Allow or Disallow use of Offline Files feature: Disabled

Encrypt the Offline Files cache: Enabled

Event Logging level: Enabled, 3

Exclude Files from being cached: Not configured

Files not cached: Not configured

Action on server disconnect: Not configured

Prevent use of Offline Files folder: Enabled

Remove Make Available Offline: Enabled

Prohibit Make Available Offline for these files and folders: Enabled

Turn off reminder balloons: Enabled

Enable Transparent Caching: Disabled

At logoff, delete local copy of user's offline files: Enabled

Turn on economical application of administratively...: Disabled

Reminder balloon frequency: Disabled

Initial reminder balloon lifetime: Disabled

Reminder balloon lifetime: Disabled

Configure slow-link mode: Not configured

Configure slow link speed: Not configured

Synchronize all offline files before logging off: Disabled

Synchronize all offline files when logging on: Disabled

Synchronize offline files before suspend: Disabled

QoS Packet Scheduler

DSCP value of conforming packets

Best effort service type: Not configured

Controlled load service type: Not configured

Guaranteed Service type: Not configured

Network control service type: Not configured

Qualitative service type: Not configured

DSCP value of non-conforming packets

Best effort service type: Not configured

Controlled load service type: Not configured

Guaranteed Service type: Not configured

Network control service type: Not configured

Qualitative service type: Not configured

Layer-2 priority value

Best effort service type: Not configured

Controlled load service type: Not configured

Guaranteed Service type: Not configured

Network control service type: Not configured

Non-conforming packets: Not configured

Qualitative service type: Not configured

Limit outstanding packets: Not configured

Limit reservable Bandwidth: Not configured

Set timer resolution: Not configured

SNMP

Communities: Disabled

Permitted Mangers: Disabled

Traps for public community: Disabled

SSL Configuration Settings

SSL Cipher Suite Order: Disabled

TCPIP Settings

IPv6 Transition Technologies

6to4 Relay Name: Not configured

6to4 Relay name Resolution interval: Not configured

6to4 state: Not configured

IP-HTTPS state: Not Configured

ISATAP Router Name: Not configured

ISATAP State: Not configured

Teredo Client Port: Not configured

Teredo default qualified: No configured

Teredo Refresh Rate: Not configured

Teredo Server Name: Not configured

Teredo State: Not configured

Parameters

Windows Scaling Heuristics State: Not configured

Windows Connect Now

Configuration of wireless setting using Windows...: Not configured

Prohibit Access of the Windows connect now wizards: Enabled

Printers

Add Printer Wizard- Network Scan page (Managed network): Not configured

Add Printer Wizard- Network Scan Page (Unmanaged Network): Not configured

Allow Print Spooler to accept client connections: Disabled

Allow printers to be published: Disabled

Allow pruning of published printers: Disabled

Always render print jobs on the server: Disabled

Automatically publish new printers in the AD: Disabled

Check published state: Not configured

Computer Location: Enabled

Custom support URL in the Printers folder's left pane: Disabled

Directory pruning interval: Not configured

Directory pruning priority: Not configured

Directory pruning retry: Not configured

Disallow installation of printers using kernel-mode drivers: Enabled

Execute print drivers in isolated processes: Disabled

Extend Point and Print connection to Windows Update: Enable

Log directory pruning retry events: Enabled

Only use package point and print: Enabled

Override print driver execution compatibility settings...: Enabled

Package Point and print- approved servers: Not configured

Point and Print restrictions: Not configured

Pre-populate printer search location text: Disabled

Printer browsing: Disabled

Prune printers that are not automatically republished: Disabled

Web-based printing: Disabled

System

Credentials Delegation

Allow delegating default credentials: Disabled

Allow delegating default credentials with NTLM-only...: Disabled

Allow delegating fresh credentials: Disabled

Allow delegating fresh credentials with NTLM-only server...: Disabled

Allow delegating saved credentials: Disabled

Allow delegating saved credentials with NTLM-only: Disabled

Deny delegating default credentials: Enabled

Deny delegating fresh credentials: Enabled

Deny delegating saved credentials: Enabled

Device Installation

Device Installation Restrictions

Allow Administrators to override Device Installation...: Enabled

Allow installation of devices that match any of these...: Disabled

Allow installation of devices using drivers that match...: Disabled

Display a custom message title when device installation is...: Disabled

Display a custom message when installation is prevented...: Disabled

Prevent installation of devices not described by other...:Enabled

Prevent installation of devices that match any of these...: Disabled

Prevent installation of devices using drivers that match...: Disabled

Prevent installation of removable devices: Enabled

Time to force reboot when required...: Disabled

Allow remote access to the Plug and Play interface: Disabled

Configure device installation time-out: Enabled, 300

Do not send a Windows error report when a generic...: Enabled

Prevent creation of a system restore point during...: Enabled

Prevent device metadata retrieval from the Internet: Enabled

Prevent Windows from sending an error report when...: Enabled

Prioritize all digitally signed drivers equally during...: Enabled

Specify search order for device driver source locations: Disabled

Turn off "found new hardware" balloons during device...: Enabled

Device Redirection Restrictions

Prevent redirection of devices that match any of these...: Not configured

Prevent redirection of USB devices: Enabled

Disk NV Cache

Turn off Boot and Resume Optimizations: Enabled

Turn off Cache Power Mode: Enabled

Turn off Non-volatile Cache Feature: Enabled

Turn off solid state mode: Enabled

Disk Quotas

Apply policy to removable media: Enabled

Default quota limit and warning level: Not configured

Enable disk quotas: Enabled

Enforce disk quota limit: Not configured

Log event when quota limit exceeded: Enabled

Log event when quota warning level exceeded: Enabled

Distributed COM

Application Compatibility

Allow local activation security check exemptions: Disabled

Define Activation Security Check exemptions: Disabled

Driver Installation

Allow non-administrators to install drivers for these...: Disabled

Turn off Windows Update device driver search prompt: Disabled

Enhanced Storage Access

Allow Enhanced Storage certificate provisioning: Enabled

Allow only USB root hub connected Enhanced Storage...: Disabled

Configure list of Enhanced Storage devices usable on...: Disabled

Configure list of IEEE 1667 silos usable on your computer: Not configured

Do not allow non-Enhanced storage removable devices: Enabled

Do not allow password authentication of Enhanced storage...: Disabled

Lock enhanced storage when the computer is locked: Enabled

File system

NTFS

Do not allow compression on all NTFS volumes: Enabled

Do not allow encryption on all NTFS volumes: Disabled

Enable NTFS pagefile encryption: Enabled

Short name creation options: Not configured

Disable delete notifications on all volumes: Enabled

Selectively allow the evaluation of a symbol link: Disabled

Folder Redirection

Use localized sub-folder names when redirection...: Disabled

Group Policy

Allow Cross-Forest User Policy and Roaming User Profiles: Disabled

Always use local ADM files for Group Policy Object Editor: Disabled

Disallow interactive users from generating RSOP...: Enabled

Disk Quota policy processing: Not configured

EFS recovery policy processing: Not configured

Folder Redirection policy processing: Not configured

Group Policy Refresh interval for computers: Enabled, 180, 20

Group Policy refresh interval for domain controllers: Enabled, 180, 20

Group policy slow link detection: Disabled

Internet Explorer Maintenance policy processing: Not configured

IP Security policy processing: Not configured

Registry policy processing: Not configured

Remove users ability to invoke machine policy refresh: Enabled

Scripts policy processing: Not configured

Security policy processing: Not configured

Software Installation policy processing: Not configured

Startup policy processing wait time: Not configured

Turn off background refresh of Group Policy: Disabled

Turn off Local Group Policy objects processing: Not configured

Turn off RSOP logging: Disabled

User Group Policy loopback processing mode: Not configured

Wired Policy processing: Not configured

Wireless policy processing: Not configured

Internet Communication Management

Internet Connection Settings

Turn off access to all windows update features: Disabled

Turn off Automatic Root Certificates Update: Disabled

Turn off downloading of print drivers over HTTP: Enabled

Turn off Event Viewer "Events.asp" links: Enabled

Turn off handwriting personalization data sharing: Enabled

Turn off handwriting recognition error reporting: Enabled

Turn off Help and Support Center "Did you know?" content: Disabled

Turn off Help and Support Center Microsoft...: Disabled

Turn off Internet Connection Wizard if URL connection...: Enabled

Turn off Internet download for Web publishing and online...: Enabled

Turn off Internet File Association Service: Enabled

Turn off printing over HTTP: Enabled

Turn off Registration if URL connection is referring to ...: Enabled

Turn off Search companion content file updates: Enabled

Turn off "Order prints" picture task: Enabled

Turn off the "Publish to web" task for files and folders: Enabled

Turn off the Windows messenger customer experience: Enabled

Turn off Windows Error Reporting: Enabled

Turn off Windows Network Connectivity Status indicator..: Not configured

Turn off Windows update device driver searching: Disabled

Restrict Internet communication: Disabled

iSCSI

General iSCSI

Do not allow additional session logins: Enabled

Do not allow changes to initiator iqn name: Enabled

iSCSI Security

Do not allow changes to initiator CHAP secret: Enabled

Do not allow connections without IPsec: Enabled

Do not allow sessions without mutual CHAP: Enabled

Do not allow sessions without one way CHAP: Enabled

iSCSI Target Discovery

Do not allow adding new targets via manual configuration: Enabled

Do not allow manual configuration of discovered targets: Enabled

Do not allow manual configuration of iSNS servers: Enabled

Do not allow manual configuration of target portals: Enabled

Kerberos

Define host name-to-Kerberos realm mappings: Not configured

Define interoperable Kerberos V5 realm settings: Not configured

Require strict KDC validation: Enabled

Require strict target SPN match on Remote Procedure Calls: Enabled

Use forest search order: Enabled

Locale Services

Disallow changing of geographic location: Enabled

Disallow selection of Custom Locales: Enabled

Disallow user override of locale settings: Enabled

Restrict system locales: Enabled, en-US

Restrict user locales: Enabled en-US

Logon

Always use classic logon: Enabled

Always use custom logon background: Disabled

Always wait for the network at computer start-up and logon: Not configured

Assign a default domain for logon: Disabled

Do not process the legacy run list: Enabled

Do not process the run once list: Enabled

Don't display the Getting Started welcome screen at logon: Enabled

Exclude credential providers: Not configured

Hide entry points for Fast User switching: Enabled

Run these programs at user logon: Disabled

Turn off Windows Start-up Sound: Enabled

Net Logon

DC Locator DNS Records

Allow cryptography algorithms compatible with Windows...:

Contact PDC on logon failure:

Expected dial-up delay on logon

Final DC discovery retry settings for background callers:

Initial DC discovery retry settings for background callers:

Log file debug output level:

Maximum DC discovery retry interval settings for...:

Maximum Log file size:

Negative DC discovery cache setting:

Netlogon share compatibility:

Positive Periodic DC Cache Refresh for background:

Positive Periodic DC Cache Refresh for non-background:

Scavenge Interval:

Site Name:

Sysvol Share compatibility:

Performance Control Panel

Turn off access to the OEM and Microsoft branding section:

Turn off access to the performance center core section:

Turn off access to the solutions to performance problems:

Power Management

Button Settings

Select the Lid Switch Action on battery: Not Configured

Select the Lid Swtich Action Plugged in: Not Configured

Select the Power button Action on battery: Not Configured

Select the Power button action Plugged in: Not Configured

Select the sleep button action on battery: Not Configured

Select the sleep button action Plugged in: Not Configured

Select the start menu power button action on battery: Not Configured

Select the start menu power button action Plugged in: Not Configured

Hard Disk Settings

Turn off the hard disk on battery: Enabled, 150

Turn off the hard disk Plugged in: Enabled, 150

Notification Settings

Critical Battery Notification Action: Not Configured

Critical Battery Notification Level: Not Configured

Low Battery Notification Action: Not Configured

Low Battery Notification Level: Not Configured

Reserve Battery Notification Level: Not Configured

Turn off Low Battery User notification: Not Configured

Sleep Settings

Allow Applications to Prevent Automatic Sleep on battery: Disabled

Allow Applications to Prevent Automatic Sleep Plugged in: Disabled

Allow Automatic Sleep with Open Network Files on battery: Not Configured

Allow Automatic Sleep with Open Network Files Plugged in: Not Configured

Allow standby States when sleeping on battery: Not Configured

Allow standby states when sleeping Plugged in: Not Configured

Require a Password when a computer wakes on battery: Enabled

Require a Password when a computer wakes Plugged in: Enabled

Specify the System Hibernate Timeout on battery: Enabled, 600

Specify the System Hibernate Timeout Plugged in: Enabled, 600

Specify the System Sleep Timeout on battery: Enabled, 600

Specify the System Sleep Timeout Plugged in: Enabled, 600

Specify the Unattended Sleep Timeout on battery: Enabled, 450

Specify the Unattended Sleep Timeout Plugged in: Enabled, 450

Turn off Hybrid Sleep on battery: Not Configured

Turn off Hybrid Sleep Plugged in: Not Configured

Turn on the ability for Applications to prevent sleep...: Disabled

Turn on the ability for applications to prevent sleep...: Disabled

Video and Display Settings

Reduce Display Brightness on battery: Enabled, 180

Reduce Display Brightness Plugged in: Enabled, 180

Specify the Display Dim Brightness on battery: Enabled, 180

Specify the Display Dim Brightness Plugged in: Enabled, 180

Turn off Adaptive Display Timeout on battery: Enabled, 240

Turn off Adaptive Display Timeout Plugged in: Enabled, 240

Turn off the display on battery: Enabled, 300

Turn off the display Plugged in: Enabled, 300

Turn on Desktop Background Slideshow on battery: Enabled, 250

Turn on Desktop Background Slideshow Plugged in: Enabled, 250

Select and Active Power Plan: Not configured

Specify a Custom Active Power Plan: Not configured

Recovery

Allow restore of system to default state: Enabled

Remote Assistance

Allow only Vista or later connections: Enabled

Customize Warning Messages: Not configured

Offer Remote Assistance: Disabled

Solicited Remote Assistance: Disabled

Turn on bandwidth optimization: Disabled

Turn on session logging: Enabled

Remote Procedure Call

Ignore Delegation failure: Disabled

Minimum Idle connection Timeout for RPC/HTTP: Not configured

Propagation of extended error information: Not configured

Restrictions for Unauthenticated RPC clients: Enabled, Auth. w/o Exceptions

RPC Endpoint Mapper Client Authentication: Enabled

RPC Troubleshooting State Information: Enabled, None

Removable Storage Access

Allow removable storage classes: Deny all access: Not configured

All removable storage: Allow direct access in remote sessions: Disabled

CD and DVD: Deny execute access: Not configured

CD and DVD: Deny read access: Not configured

CD and DVD: Deny write access: Not configured

Custom Classes: Deny read access: Not configured

Custom Classes: Deny write access: Not configured

Floppy Drives: Deny execute access: Not configured

Floppy Drives: Deny read access: Not configured

Floppy Drives: Deny write access: Not configured

Removable Disks: Deny execute access: Not configured

Removable Disks: Deny read access: Not configured

Removable Disks: Deny write access: Not configured

Tape Drives: Deny execute access: Not configured

Tape Drives: Deny read access: Not configured

Tape Drives: Deny write access: Not configured

Time to force reboot: Not configured

WDP Devices: Deny read access: Not configured

WDP Devices: Deny write access: Not configured

Scripts

Allow logon scripts when NetBIOS or WINS is disabled: Disabled

Maximum wait time for Group Policy scripts: Not configured

Run logon scripts synchronously: Not configured

Run startup scripts asynchronously: Not configured

Run startup scripts visible: Enabled

Run Windows PowerShell scripts at computer startup...: Not configured

Run Windows PowerShell scripts at first user logon, logoff: Not configured

Shutdown Options

Turn off automatic termination of applications...: Disabled

System Restore

Turn off Configuration: Not configured

Turn off System Restore: Disabled

Troubleshooting and Diagnostics

Application Compatibility Diagnostics

Notify blocked drivers: Enabled

Detect application failures caused by deprecated COM...: Enabled, All

Detect application failures caused by deprecated Windows..: Enabled, All

Detect application installation failures: Enabled

Detect application installer that need to be run as...: Enabled, All

Detect applications unable to launch installers under UAC: Enabled, All

Corrupted File Recovery

Configure Corrupted File Recovery Behaviour: Not configured

Disk Diagnostic

Disk Diagnostic: Configure custom alert text: Not configured

Disk Diagnostic: Configure execution level: Not configured

Fault Tolerant Heap

Configure Scenario execution level: Not configured

Microsoft Support Diagnostic Tool

MSDT: Turn on MSDT interactive communication with Support..: Disabled

MSDT: Restrict tool download: Enabled

MSDT: Configure execution level: Disabled

MSI corrupted file recovery

Configure MSI corrupted file recovery behavior: Not configured

Scheduled Maintenance

Configure Scheduled Maintenance behavior: Not configured

Scripted Diagnostics

Troubleshooting: Allow users to access online...: Disabled

Troubleshooting: Allow users to access and run...: Disabled

Configure Security Policy for Scripted Diagnostics: Enabled

Windows Boot Performance Diagnostics

Configure Scenario Execution level: Not configured

Windows Memory Leak Diagnosis

Configure Scenario Execution level: Not configured

Windows Performance PerfTrack

Enable/Disable Perftrack: Disabled

Windows Resource Exhaustion Detection and Resolution

Configure Scenario Execution level: Not configured

Windows Shutdown Performance Diagnostics

Configure Scenario Execution level: Not configured

Windows Standby/Resume Performance Diagnostics

Configure Scenario Execution level: Not configured

Windows System Responsiveness Performance Diagnostics

Configure Scenario Execution level: Not configured

Diagnostics: Configure scenario retention: Not configured

Diagnostics: Configure scenario execution level: Not configured

Trusted Platform Module Services

Configure the list of blocked TPM commands: Not configured

Ignore the default list of blocked TPM commands: Not configured

Ignore the local list of blocked TPM commands: Not configured

Turn on TPM backup to Active Directory Domain Services: Not configured

User Profiles

Add the administrator’s security group to roaming user...: Enabled

Delete user profiles older than a specified number...: Enabled, 29

Do not check for user ownership of Roaming Profile Folders: Not configured

Delete cached copies of roaming profiles: Enabled

Do not forcefully unload the user’s registry at user logoff: Disabled

Do not detect slow network connections: Enabled

Prompt user when a slow network connection is detected: Not configured

Leave Windows only installer and Group Policy Software...: Disabled

Only allow local user profiles: Enabled

Set roaming profile path for all users logging on...: Not configured

Timeout for dialogue boxes: Not configured

Do not log users on with temporary profiles: Enabled

Maximum retries to unload and update user profile: Not configured

Prevent Roaming Profile changes from propagating...: Enabled

Wait for remote user profile: Enabled

Slow network connection Timeout for user profiles: Not configured

Background upload of a roaming user profile's registry...: Not configured

Set maximum wait time for the network if a user has...: Not configured

Windows File Protection

Hide the file scan progress window: Disabled

Limit Windows File Protection cache size: Enabled, 50

Set Windows File Protection scanning: Not configured

Specify Windows File Protection cache location: Not configured

Windows HotStart

Turn off Windows HotStart: Not configured

Windows Time Service

Time Providers

Configure Windows NTP Client: Not configured

Enable Windows NTP Client: Not configured

Enable Windows NTP Server: Not configured

Global Configuration Settings: Not configured

Windows Components

ActiveX Installer Service

Approved Installation Sites for ActiveX Controls:

ActiveX installation policy for sites in trusted zones:

Application Compatibility

Prevent access to 16-bit applications: Enabled

Remove Program Compatibility: Not configured

Turn off Application Telemetry: Not configured

Turn off Application Compatibility Engine: Enabled

Turn off Program Compatibility Assistant: Enabled

Turn off Program Inventory: Not configured

Turn off SwitchBack Compatibility Engine: Enabled

Turn off Problem Steps Recorder: Enabled

AutoPlay

Turn off Autoplay: Enabled

Don't set the always do this check-box: Enabled

Turn off Autoplay for non-volume devices: Enabled

Default behavior for AutoRun: Not configured

Backup

Client

Prevent backing up to local disks: Enabled

Prevent backing up to network location: Enabled

Prevent backing up to optical media: Enabled

Prevent the user from running the Backup Status and...: Enabled

Turn off restore functionality: Enabled

Turn off the ability to back up data files: Enabled

Turn off the ability to create a system image: Enabled

Server

Allow only system backup: Enabled

Disallow locally attached storage as backup target: Enabled

Disallow network as backup target: Enabled

Disallow optical media as backup target: Enabled

Disallow run-once backups: Enabled

Biometrics

Allow domain users to log on using biometrics: Disabled

Allow the use of biometrics: Disabled

Allow users to log on using: Disabled

Timeout for fast user switching events: Not configured

BitLocker Drive Encryption

Fixed Data Drives

Allow access to BitLocker-protected...: Not configured

Choose how BitLocker-protected fixed drives...: Not configured

Configure use of passwords for fixed data drives: Not configured

Configure use of smart cards on fixed data drives: Not configured

Deny write access to fixed drives not protected...: Not configured

Operating System Drives

Allow enhanced PINs for startup: Not configured

Choose how BitLocker-protected...: Not configured

Configure minimum PIN length for startup: Not configured

Configure TPM platform validation profile: Not configured

Require additional authentication startup: Not configured

Require additional authentication at start-up...: Not configured

Removable Data Drives

Allow access to BitLocker-protected...: Not configured

Choose how BitLocker-protected removable: Not configured

Configure use of passwords for removable data drives: Not configured

Configure use of smart cards on removable data drives: Not configured

Control use of BitLocker on removable drives: Not configured

Deny write access to removable drives not protected...: Not configured

Choose default folder for recovery password: Not configured

Choose drive encryption method and cipher strength: Not configured

Prevent memory overwrite on restart: Not configured

Provide the unique identifiers for your organization: Not configured

Store BitLocker recovery information in Active Directory...: Not configured

Validate smart card certificate usage rule compliance: Not configured

Credential User Interface

Enumerate administrator accounts on elevation: Disabled

Require trusted path for credential entry: Enabled

Desktop Gadgets

Override the More Gadgets link: Enabled

Restrict unpacking and installation of gadgets that...: Enabled

Turn off desktop gadgets: Enabled

Turn off user-installed desktop gadgets: Enabled

Desktop Windows Manager

Windows Frame Coloring

Do not allow color changes: Enabled

Specify a default color: Not configured

Do not allow desktop composition: Enabled

Do not allow Flip3D invocation: Enabled

Do not allow windows animations: Enabled

Digital Locker

Do not allow Digital Locker to run: Enabled

Event Forwarding

Configure the server address, refresh interval...: Not configured

ForwarderResourceUsage: Not configured

Event Log Service:

Application

Backup log automatically when full: Enabled

Log Access: Not configured

Log File Path: Not configured

Max Log Size: Enabled, 2046

Retain old events: Enabled

Security

Backup log automatically when full: Enabled

Log Access: Not configured

Log File Path: Not configured

Max Log Size: Enabled, 2046

Retain old events: Enabled

Setup

Backup log automatically when full: Enabled

Log Access: Not configured

Log File Path: Not configured

Max Log Size: Enabled, 2046

Retain old events: Enabled

System

Backup log automatically when full: Enabled

Log Access: Not configured

Log File Path: Not configured

Max Log Size: Enabled, 2046

Retain old events: Enabled

Event Viewer

Events.asp program: Not configured

Events.asp program command line parameters: Not configured

Events.asp URL: Not configured

Game Explorer

Turn off downloading of game information: Enabled

Turn off game updates: Enabled

Turn off tracking of last play time...: Enabled

HomeGroup

Prevent the computer from joining a HomeGroup: Enabled

Internet Explorer

Accelerators

Deploy default Accelerators: Not configured

Deploy non-default Accelerators: Not configured

Turn off Accelerators: Enabled

Use Policy Accelerators: Enabled

Application Compatibility

Enable cut copy...

All Processes: Disabled

Internet Explorer Processes: Disabled

Process list: Disabled

Browser menus

Turn off print menu: Enabled

Compatibility View

Include updated web site lists from Microsoft: Disabled

Turn off compatibility view: Enabled

Turn off compatibility view button: Enabled

Turn on Internet Explorer 7 standards...: Disabled

Turn on Internet Explorer Standards...: Disabled

Use policy list of Internet explorer 7 sites: Disabled

Use policy list of quirks mode sites: Not configured

Corporate Settings

Code Download

Prevent setting of the code download...: Not configured

Delete Browsing History

Configure Delete Browsing history...: Enabled

Disable configuring history: Enabled

Prevent Deleting ActiveX Filtering...: Enabled

Prevent Deleting Cookies: Enabled

Prevent Deleting Download History: Enabled

Prevent Deleting Favorites Site Data: Enabled

Prevent Deleting Form Data: Enabled

Prevent Deleting InPrivate filtering data: Enabled

Prevent Deleting passwords: Enabled

Prevent Deleting Passwords: Enabled

Prevent Deleting Temporary Internet Files: Enabled

Prevent Deleting web sites that the user has...: Enabled

Prevent the deletion of temporary internet files...: Enabled

Turn off delete browsing history functionality: Enabled

Internet Control Panel

Advanced Page

Allow active content from CDs to run...: Disabled

Check for server certificate revocation:

Turn off ClearType: Enabled

Do not allow resetting Internet Explorer settings:

Check for signatures on downloaded programs:

Allow third-party browser extensions: Disabled

Turn on Caret Browsing support: Not configured

Use HTTP 1.1: Not configured

Allow Install on Demand Internet Explorer: Disabled

Allow Install on Demand except Internet Explorer: Disabled

Automatically check for Internet Explorer updates: Disabled

Allow software to run or install even if the signature...: Disabled

Play animations in web pages: Disabled

Play sounds in web pages: Disabled

Play videos in web pages: Disabled

Turn off profile assistant: Enabled

Use HTTP 1.1 through proxy connections: Not configured

Do not save encrypted pages to disk: Enabled

Turn off encryption support: Disabled

Empty Temporary Internet Files folder when...: Enabled

Security Page

Intranet Sites: Include all the local...: Disabled

Locked-Down Internet Zone...: Enabled

Internet Zone Template: Enabled, High

Locked-Down Intranet Zone...: Enabled, High

Intranet Zone: Enabled, High

Locked-Down Local Machine Zone...: Enabled, High

Local Machine Zone Template: Enabled, High

Locked-Down Restricted Sites Zone...: Enabled, High

Restricted Sites Zone Template: Enabled, High

Locked-Down Trusted Sites Zone...: Enabled, High

Trusted Sites Zone Template: Enabled, High

Turn on Warn about certificate address...: Enabled

Intranet Sites: Include all sites that...: Disabled

Intranet Sites: Include all network paths: Disabled

Site to Zone Assignment list: Not configured

Turn on automatic detection of the Intranet: Disabled

Turn on Notification bar notification for...: Disabled

Disable the Advanced Page: Enabled

Disable the Connections page: Enabled

Disable the Content page: Enabled

Disable the General page: Enabled

Disable the Privacy page: Enabled

Disable the Programs page: Enabled

Disable the Security page: Enabled

Send internationalized domain names: Not configured

Use UTF-8 for mail-to links: Disabled

Prevent ignoring certificate errors: Enabled

Internet Settings

Advanced

Browsing

Go to an Intranet site for a single...: Disabled

Multimedia

Enable alternative codecs in HTML5 media...: Disabled

Searching

Prevent configuration of search from the...: Enabled

Prevent configuration of top result search...: Enabled

AutoComplete

Turn of Windows Search AutoComplete: Enabled

Component Updates

Help Menu > about IE

Prevent the configuration of cipher strength...: Enabled

Periodic checks...

Turn off changing the URL to be displayed...: Enabled

Turn off configuring the update check....: Enabled

Privacy

Disable toolbars and extensions when...: Enabled

Do not collect InPrivate...: Enabled

InPrivate Filtering threshold: Enabled, 3

Tracking protection threshold: Not configured

Turn off InPrivate Browsing: Enabled

Turn off filtering: Enabled

Turn off tracking protection: Enabled

Security Features

Add-on management

Add-on list: Not configured

All processes: Enabled

Deny all add-ons unless specifically...: Enabled

Process list: Not configured

AJAX

Enable native XMLhttprequest support: Disabled

Maximum number of connections per...: Not configured

Maximum number of connections per...: Not configured

Turn off Cross Document messaging: Enabled

Turn off the XDomain request object: Enabled

Binary Behavior security restriction

Admin-approved behaviors: Disabled

All processes: Enabled

Install binaries signed by...: Disabled

Internet Explorer Processes: Enabled

Process list: Not configured

Consistent mime handling

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Local machine zone lockdown security

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Mime sniffing safety feature

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

MK protocol Security restriction

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Network protocol lockdown

Restricted protocols per security zone

Internet Zone restricted protocols: Not configured

Intranet zone restricted protocols: Not configured

Local machine zone restricted protocols: Not configured

Restricted sites zone restricted protocols: Not configured

Trusted sites zone restricted protocols: Not configured

All processes: Enabled

Internet Explorer Processes: Enabled

Process List: Not configured

Notification bar

All processes: Not configured

Internet Explorer processes: Disabled

Process list: Not configured

Object caching protection

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Prevention from zone elevation

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Restrict ActiveX install

All processes: Not configured

Internet Explorer processes: Enabled

Process list: Not configured

Restrict file download

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Scripted windows security restrictions

All processes: Enabled

Internet Explorer processes: Enabled

Process list: Not configured

Turn off Data Execution Prevention: Disabled

Turn off data URI support: Enabled

Toolbars

Customize Command labels: Not configured

Hide the command bar: Enabled

Hide the status bar: Enabled

Lock all toolbars: Enabled

Set location of Stop and Refresh buttons: Not configured

Show tabs on a separate row: Enabled

Turn off developer tools: Enabled

Turn off toolbar upgrade tool: Enabled

Use large icons for command buttons: Not configured

Add a specific list of search providers to the user's...: Disabled

Allow Internet Explorer 8 shutdown behavior: Disabled

Automatically enable newly installed add-ons: Disabled

Configure new tab page default behavior: Enabled, New tab page

Customize User Agent String: Not configured

Disable add-on performance notifications: Enabled

Disable Automatic Install of Internet Explorer...: Enabled

Disable Browser Geolocation: Enabled

Disable changing Automatic Configuration settings: Enabled

Disable changing connection settings: Enabled

Disable changing proxy settings: Enabled

Disable changing secondary home page settings: Enabled

Disable Import/Export Settings wizard: Enabled

Disable Periodic Check for Internet Explorer...: Enabled

Disable Per-User Installation of ActiveX Controls: Enabled

Disable showing the splash screen: Enabled

Disable software update shell notification...: Enabled

Do not allow users to enable or disable add-ons: Enabled

Enforce Full Screen mode: Enabled

Make proxy settings per machine...: Enabled

Only use the ActiveX Installer service for installation...: Enabled

Pop-up allow list: Disabled

Prevent fix settings functionality: Enabled

Prevent bypassing SmartScreen filter warnings: Enabled

Prevent Internet Explorer search box from displaying: Enabled

Prevent participation in the Customer Experience...: Enabled

Prevent users from bypassing SmartScreen...: Enabled

Restrict changing the default search provider: Enabled

Security Zones: Do not allow users to add...: Enabled

Security Zones: Do not allow users to change policies: Enabled

Security Zones: Use only machine settings: Enabled

Set tab process growth: Not configured

Turn off ability to pin sites: Enabled

Turn off ActiveX opt-in Prompt: Enabled

Turn off configuration of default behavior of new tab...: Enabled

Turn off configuration of tabbed browsing pop-up behavior: Enabled

Turn off configuration of windows reuse: Enabled

Turn off Crash Detection: Enabled

Turn off displaying the Internet Explorer Help Menu: Enabled

Turn off Favorites bar: Enabled

Turn off managing Phishing filter: Enabled

Turn off Managing pop-up allow list: Enabled

Turn off managing pop-up filter level: Enabled

Turn of managing SmartScreen filter...: Enabled

Turn of managing SmartScreen filter...: Enabled

Turn off page zooming functionality: Enabled

Turn off pop-up management: Enabled

Turn off Quick Tabs functionality: Enabled

Turn off Reopen Last Browsing Session: Enabled

Turn off suggestions for all user-installed providers: Enabled

Turn off tabbed browsing: Enabled

Turn off the activation of quick pick menu: Enabled

Turn off the auto-complete feature for web addresses: Enabled

Turn off the security settings check feature: Disabled

Turn on ActiveX Filtering: Enabled

Turn on compatibility logging: Enabled

Turn on menu bar by default: Disabled

Turn on suggested sites: Disabled

Internet Information Services

Prevent IIS installation: Enabled

Location and Sensors

Turn off location: Enabled

Turn off location scripting: Enabled

Turn off sensors: Enabled

NetMeeting

Disable remote Desktop Sharing: Enabled

Network Projector

Network projector port settings: Not configured

Turn off connect to a network...: Enabled

Online Assistance:

Turn off Active Help: Enabled

Parental Controls

Make Parental control panel visible...: Disabled

Presentation Settings

Turn off Windows Presentation Settings: Enabled

Remote Desktop Session

RD Licensing

License Server security group: Enabled

Prevent license upgrade: Enabled

Remote Desktop connection Client

Allow .rdp files from unknown publishers: Disabled

Allow .rdp files from valid publishers...: Disabled

Configure server authentication for...: Enabled, Do not connect...

Do not allow passwords to be saved: Enabled

Prompt for credentials on the client computer: Enabled

Specify SHA1 thumbprints of certificates...: Not configured

Remote Desktop Session Host

Connections

Allow users to connect remotely using Remote Desktop..: Disabled

Automatic reconnection: Disabled

Configure keep-alive connection...: Not configured

Deny logoff an administrator...: Enabled

Limit number of connections: Not configured

Restrict Remote Desktop Services Users...: Enabled

Set rules for remote control of Remote...: Enabled, No remote..

Device and Resource Redirection

Allow audio and video playback...: Disabled

Allow audio recording redirection: Disabled

Allow time zone redirection: Disabled

Do not allow clipboard redirection: Enabled

Do not allow COM port redirection: Enabled

Do not allow drive redirection: Enabled

Do not allow LPT port redirection: Enabled

Do not allow smart card device redirection: Enabled

Do not allow supported Plug and Play...: Enabled

Limit audio playback quality: Not configured

Licensing

Hide notifications about RD licensing problems...: Enabled

Set the Remote Desktop licensing mode: Enabled, Per user

Use the specified Remote Desktop...: Not configured

Printer Redirection

Do not allow client printer redirection: Enabled

Do not set default client printer to be...: Enabled

Specify RD session host server fall-back...: Disabled

Use remote desktop easy print printer driver first: Disabled

Profiles

Limit the size of the entire roaming user...: Not configured

Set path for remote Desktop Services...: Not configured

Set Remote Desktop Services User Home Directory: Not configured

Use mandatory profiles on the RD session host: Disabled

RD Connection Broker

Configure RD connection broker farm name:

Configure RD connection broker server name:

Join RD connection broker:

Use IP Address redirection:

Remote Sessions Environment

Always show desktop on connection: Enabled

Enforce removal of Remote Desktop Wallpaper: Not configured

Limit maximum color depth: Disabled

Limit maximum display resolution: Disabled

Limit maximum number of monitors: Disabled

Optimize visual experience for...: Not configured

Remove disconnect option from shutdown...: Enabled

Remote Windows Security item from start menu: Enabled

Set compression algorithm for RDP data: Not configured

Start a program on connection: Disabled

Security

Always prompt for a password upon connection: Enabled

Do not allow local administrator to customize...: Enabled

Require secure RPC communication: Enabled

Require use of specific layer for remote...: Not configured

Require user authentication for remote...: Enabled

Server authentication certificate template: Not configured

Set client connection encryption level: Enabled, High

Session Time Limits

Set time limit for active but idle Remote...: Enabled, 15

Set time limit for active remote desktop...: Not configured

Set time limit for disconnected sessions: Enabled, 10

Terminate session when time limits are...: Enabled

Temporary Folders

Do not delete temp folders upon exit: Disabled

Do not use temporary folders per session: Enabled

RSS Feeds

Turn off addition and removal of feeds...: Enabled

Turn off background sync for feeds...: Enabled

Turn off download of enclosures: Enabled

Turn off feed and web slices discovery: Enabled

Turn off the feed list: Enabled

Turn on basic authentication over HTTP: Disabled

Search

OCR

Force TIFF IFilter to perform OCR for every...: Enabled

Select OCR languages from a code page: Not configured

Add primary intranet search location: Not configured

Add secondary intranet search locations: Not configured

Allow indexing of encrypted files: Disabled

Allow use of diacritics: Not configured

Control rich previews for attachments: Not configured

Default excluded paths: Not configured

Default indexed paths: Not configured

Disable indexer back off: Enabled

Do not allow web search: Enabled

Enable indexing of online delegate mailboxes: Disabled

Enable indexing of uncached exchange folders: Disabled

Enabled throttling for online mail indexing: Disabled

Indexer data location: Not configured

Prevent adding UNC locations to index from...: Enabled

Prevent adding user-specific locations to All locations...: Enabled

Prevent automatically adding shared folders to the...: Enabled

Prevent clients from querying the index remotely: Enabled

Prevent customization of indexed locations in the...: Enabled

Prevent displaying advanced indexing options in...: Enabled

Prevent indexing certain paths: Not configured:

Prevent indexing email attachments: Enabled

Prevent indexing files in offline files cache: Enabled

Prevent indexing Microsoft Office Outlook: Enabled

Prevent indexing public folders: Enabled

Prevent indexing certain file types: Not configured

Prevent indexing when running on battery power: Not configured

Prevent unwanted iFilters and protocol handlers: Enabled

Preview pane location: Disabled

Set large or small icon view in desktop search results: Disabled

Stop indexing in the event of limited hard drive space: Enabled

Security Center

Turn on Security Center: Enabled

Shutdown Options

Timeout hung logon sessions during shutdown: Not configured

Turn off legacy remote shutdown interface: Enabled

Smart Card

Sound Recorder

Do not allow sound recorder to run: Enabled

Tablet PC

Accessories

Do not allow Inkball to run: Enabled

Do not allow printing to Journal Note Writer: Enabled

Do not allow sniping tool to run: Enabled

Do not allow Windows Journal to be run: Enabled

Cursors

Turn off pen feedback: Enabled

Handwriting Personalization

Turn off automatic learning: Enabled

Hardware Buttons

Prevent back-ESC mapping: Enabled

Prevent launch an application: Enabled

Prevent press and hold: Enabled

Turn off hardware buttons: Enabled

Input Panel

Disable text prediction: Enabled

For tablet pen input, don’t show the input...: Enabled

For touch input, don’t show the input panel icon: Enabled

Include rarely used Chinese, Kanji, or Hanja...: Enabled

Prevent Input Panel tab from appearing: Enabled

Switch to the PRC gestures: Enabled

Turn off AutoComplete integration with Input...: Enabled

Turn off password security in Input Panel: Disabled

Turn off tolerant and Z scraped scratch-out...: Not configured

Pen Flicks Learning

Prevent Flicks learning mode: Enabled

Pen UX Behaviors

Prevent flicks: Enabled

Tablet PC Pen Training

Turn off Tablet PC Pen training: Enabled

Touch Input

Turn off Tablet PC touch input: Enabled

Turn off Touch Panning: Enabled

Task Scheduler

Hide Advanced Properties checkbox in Add Scheduled...: Enabled

Hide Property Pages: Enabled

Prevent Task run or End: Enabled

Prohibit Browse: Enabled

Prohibit Drag-and-Drop: Enabled

Prohibit new task creation: Enabled

Prohibit Task deletion: Enabled

Windows Anytime Upgrade

Prevent Windows Anytime Upgrade from...: Enabled

Windows Calendar

Turn off Windows Calendar: Enabled

Windows Color System

Prohibit installing or uninstalling color profiles: Enabled

Windows Customer Support

Allow Corporate redirection of Customer...: Disabled

Tag Windows Customer Experience Improvement...: Disabled

Windows Defender

Check for New signatures before scheduled scans: Enabled

Configure Microsoft SpyNet Reporting: Not configured

Turn off real-time monitoring: Disabled

Turn off routinely taking action: Enabled

Turn off windows defender: Disabled

Turn on definition updates through both...: Not configured

Turn on definition updates through both...: Not configured

Windows Error Reporting Service

Advanced Error Reporting Settings

Configure corporate windows error reporting: Not configured

Configure report archive: Not configured

Configure report queue: Not configured

Default application reporting settings: Not configured

List of applications to always report errors...: Disabled

List of applications to be excluded: Disabled

List of applications to never report errors for: Not configured

Report OS errors: Disabled

Report unplanned shutdown events: Disabled

Consent

Configure default consent: Disabled

Customize consent settings: Not configured

Ignore custom consent settings: Not configured

Configure Error Reporting: Not configured

Disable Logging: Disabled

Disable Windows Error Reporting: Enabled

Display Error Notification: Disabled

Do not send additional data: Enabled

Prevent display of the user interface for...: Enabled

Windows Explorer

Previous Versions

Disable binding directly to IPropertySetStorage...: Not configured

Set a support web page link: Disabled

Turn off Data execution Prevention for Explorer: Disabled

Turn off heap termination on corruption: Disabled

Turn off numerical sorting in Windows Explorer: Enabled

Turn off shell protocol protected mode: Disabled

Verify old and new folder redirection targets...: Disabled

Windows Installer

Allow admin to install RDS session:

Always install with elevated privileges:

Baseline file cache maximum size: Not configured

Cache transforms in secure location on workstation: Enabled

Disable IE security prompt for windows installer...: Disabled

Disable logging via package settings: Enabled

Disable windows installed: Disabled

Enable user control over installs: Enabled

Enable user to browse for source while elevated: Disabled

Enable user to patch elevated products: Enabled

Enforce upgrade to component rules: Enabled

Logging: Not configured

Prohibit Flyweight patching: Not configured

Prohibit non-admins from applying vendor signed...: Enabled

Prohibit Patching: Enabled

Prohibit removal of updates: Enabled

Prohibit rollback: Disabled

Prohibit use of restart manager: Enabled

Prohibit user installs: Enabled

Remove browse dialogue box for new source: Enabled

Turn off creation of System restore checkpoints: Enabled

Windows Logon Options

Disable or enable software secure attention sequence: Enabled

Display information about previous logons during user...: Disabled

Report when logon server was not available during...: Disabled

Windows Mail

Turn off the communities features: Enabled

Turn off Windows Mail application: Enabled

Windows Media Center

Do not allow Windows Media Center to run: Enabled

Windows Media Digital Rights Management

Prevent Windows Media DRM Internet Access: Enabled

Windows Media Player

Do not show first use dialogue boxes: Enabled

Prevent automatic Updates: Disabled

Prevent Desktop shortcut creation: Enabled

Prevent media sharing: Enabled

Prevent Quick launch toolbar shortcut creation: Enabled

Prevent Video smoothing: Enabled

Windows Messenger

Do not allow Windows Messenger to be run: Enabled

Do not automatically start Windows Messenger initially: Enabled

Windows Mobility Center

Turn off Windows Mobility Center: Enabled

Windows Reliability Analysis

Configure Reliability WMI Providers: Not configured

Windows Remote Management

WinRM Client

Allow Basic authentication: Disabled

Allow CredSSP authentication: Enabled

Allow unencrypted traffic: Disabled

Disallow digest authentication: Enabled

Disallow Kerberos Authentication: Disabled

Disallow Negotiate authentication: Enabled

Trusted hosts: Not configured

WinRM Server

Allow automatic configuration of listeners: Disabled

Allow basic authentication: Disabled

Allow CredSSP authentication: Enabled

Allow unencrypted traffic: Disabled

Disallow Kerberos authentication: Disabled

Disallow Negotiate authentication: Enabled

Specify channel binding token hardening level: Not configured

Turn on Compatibility HTTP listener: Not configured

Turn on Compatibility HTTPS listener: Not configured

Windows Remote Shell

Allow Remote shell access: Disabled

Max Concurrent User: Not configured

Specify idle timeout: Not configured

Specify maximum amount of memory in MB per shell: Not configured

Specify maximum number of processes per shell: Not configured

Specify maximum number of remote shells per user: Not configured

Specify shell timeout: Not configured

Windows SideShow

Delete data from devices running Microsoft firmware...: Enabled

Require a PIN to access data on devices running...: Enabled

Turn off automatic wake: Enabled

Turn off Windows SideShow: Enabled

Windows System Requirements

Set the Email IDs to which notifications are sent: Disabled

Set the SMTP Server used to send notifications: Disabled

Set the Time interval in minutes for logging account data: Not configured

Turn on Accounts for WSRM: Disabled

Windows Update

Allow automatic updates immediate installation: Disabled

Allow non-admins to receive update notifications: Disabled

Allow signed updates from an intranet Microsoft...: Disabled

Automatic Updates detection frequency: Not configured

Configure Automatic Updates: Not configured

Delay Restart for scheduled installations: Not configured

Do not adjust default option to install updates and...: Enabled

Do not display install updates and shutdown potion in...: Enabled

Enable client-side targeting: Disabled

Enabling Windows Update Power Management...: Disabled

No auto-restart with logged on users for scheduled...: Enabled

Re-prompt for restart with scheduled installations: Not configured

Reschedule Automatic updates scheduled installations: Not configured

Specify intranet Microsoft update service location: Disabled

Turn on recommended updates via Automatic Updates: Enabled

Turn on Software Notifications: Disabled

DONE!!