**Group Policy List**

|  |  |  |  |
| --- | --- | --- | --- |
| **SL No.** | **Policy Name** | **Group Policy Objects** | **Description** |
| 1 | Password Policy | **Default Domain Policy (Global)** | Enforce password history : **3 passwords remembered**  Maximum password age : **30 days**  Minimum password age : **1 days**  Minimum password length : **8 characters**  Password meet complexity requirement : **Enabled** |
| 2 | Account Lockout Policy | Account lockout duration : **5 minutes**  Account lockout threshold : **3 invalid logon attempts**  Reset account lockout counter after : **5 minutes** |
| 3 | Automate password change notification | Interactive logon: Prompt user to change password before expiration ***(7 Days)*** |
| 4 | Prevent access to registry editing tools **(Enabled)** | **Common Restriction Global** | Disables the Windows registry editor Regedit.exe |
| 5 | Local Workstation  Windows Firewall ***(On/Off)*** | **General Policy Settings Global** | Windows Firewall is off bellow Profile  Domain Profile, Privet Profile, Public Profile  Inbound Connection Block Default  Outbound Connection Allow Default |
| 6 | Turn off AutoPlay ***(Enabled)*** | This policy setting allows you to turn off the Autoplay feature.  Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately. |
| 7 | All Removable Storage Classes: Deny Access ***(Enabled)*** | **Removable Disk Restriction Global** | Configure access to all removable storage classes.  If you enable this policy setting, no access is allowed to any removable storage class. |
| 8 | CD and DVD: Deny write access  ***(Enabled)*** | This policy setting denies write access to the CD and DVD removable storage class. |
| 9 | Desktop Wallpaper | **Desktop Personalization** | \\adds1\Desktop\_Personalization\ABC-Desktop.jpg |
| 10 | Prevent changing desktop background ***(Enabled)*** | Prevents users from adding or changing the background design of the desktop. |
| 11 | Prevent changing theme ***(Enabled)*** | This setting disables the theme gallery in the Personalization Control Panel. |
| 12 | Screen saver timeout  ***(300 Seconds)*** | Number of seconds to wait to enable the screen saver |
| 13 | Add Active Directory Group ***admin.ABC*** (IT Support) to Local Group Administrators | **Local Administration Manage NBL** | Delegation for local computer administration full Privilege |
| 14 | Add Active Directory Group ***bradm.ABC*** (Network) to Local Group Network Configuration Operator | Delegation for manage configuration of networking only |
| 15 | User Account Control: Admin Approval Mode for the Built-in Administrator account ***(Enabled)*** | **Admin-approval mode Global** | Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode |
| 16 | User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode ***(Prompt for consent for non-Windows binaries)*** |
| 17 | User Account Control: Behavior of the elevation prompt for standard users ***(Prompt for credentials)*** |
| 18 | User Account Control: Detect application installations and prompt for elevation ***(Enabled)*** |
| 19 | User Account Control: Only elevate executable files that are signed and validated ***(Disabled)*** |
| 20 | User Account Control: Use Admin Approval Mode for the built-in Administrator account **(Enabled)** |
| 21 | User Account Control: Only elevate UIAccess applications that are installed in secure locations ***(Enabled)*** |
| 22 | User Account Control: Run all administrators in Admin Approval Mode ***(Enabled)*** |
| 23 | Action: Update  Name: %userprofile%\favorites\ABC\ Home  Target Type: URL  Location: <Specify full path>  Target URL: www.abc.com | **Favorites links NBL** | ***http://www.abc.com/***  ***http://xyz.org/***  ***http://www.jkl.com.bd/*** |
| 24 | Disable changing home page settings ***(Enabled)*** | **IE Settings** | User cannot set a custom default home page. You must specify which default home page should load on the user machine  ***Homepage: http://www.abc.com/*** |
| 25 | Turn off pop-up management ***(Enabled)*** |  |
| 26 | Allow deleting browsing history on exit ***(Enabled)*** |  |
| 27 | Site to Zone Assignment List |  |
| 28 | Audit account logon events | **Local Audit Policy** | Success, Failure |
| 29 | Audit account management | Success, Failure |
| 30 | Audit directory service access | Success |
| 31 | Audit logon events | Success, Failure |
| 32 | Audit object access | Success, Failure |
| 33 | Audit policy change | Success, Failure |
| 34 | Audit privilege use | Success |
| 35 | Audit system events | Success, Failure |
| 36 | Audit: Shut down system immediately if unable to log security audits | N\A |
| 37 | Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings | N\A |
| 38 | Account Logon: Credential Validation | **Advanced Audit Policy** | Success, Failure |
| 39 | Account Management: Computer Account Management | Success, Failure |
| 40 | Account Management: Other Account Management Events | Success, Failure |
| 41 | Account Management: Security Group Management | Success, Failure |
| 42 | Account Management: User Account Management | Success, Failure |
| 43 | DS Access: Directory Service Access | Success, Failure |
| 44 | DS Access: Directory Service Changes | Success, Failure |
| 45 | Logon-Logoff: Logoff | Success |
| 46 | Logon-Logoff: Logon | Success, Failure |
| 47 | Logon-Logoff: Special Logon | Success |
| 48 | Policy Change: Audit Policy Change | Success, Failure |
| 49 | Policy Change: Authentication Policy Change | Success |
| 50 | System: Security State Change | Success, Failure |
| 51 | System: Security System Extension | Success, Failure |
| 52 | System: System Integrity | Success, Failure |
| 53 | Application: Maximum Log Size (KB). | **Audit Logs Sizes** | Recommended state is 32768 KB or greater |
| 54 | Application: Retain old events | Recommended state is Disabled |
| 55 | Security: Maximum Log Size (KB) | Recommended state is 81920KB or greater |
| 56 | Security: Retain old events. | Recommended state is disabled |
| 57 | System: Maximum Log Size (KB) | Recommended state is 32768 KB or greater |
| 58 | System: Retain old events | Recommended state is Disabled |

Audit applied for:

* Domain Controller
* Member Server
* Client

**Solutions:**

#Tools>>Group Policy Management>>Default Domain Plicy>>Edit>>>

**# Default Domain Policy (Global)**

1.Computer Configuration>>Policies>>Windows Settings>>Security Settings>>Account Policies>>Password Policy

(i) Enforce password history :Check(Define this policy settings)>>type 3>>ok

(ii)Maximum password age : Check(Define this policy settings)>>type 30>>ok

(iii)Minimum password age : Check(Define this policy settings)>>type 1>>ok

(iv)Minimum password length : Check(Define this policy settings)>>type 8>>ok

(v) Password must meet complexity requirement : Check(Define this policy settings)>>Enable>>ok

2. Computer Configuration>>Policies>>Windows Settings>>Security Settings>>Account lockout Policy

(i) Account lockout duration : Check(Define this policy settings)>>type 5>>ok

(ii) Account lockout threshold : Check(Define this policy settings)>>type 3>>ok

(iii) Reset account lockout counter after : Check(Define this policy settings)>>type 5>>ok

3. Computer Configuration>>Policies>>Windows Settings>>Security Settings>>Local Policy>>Security Options

(i) Interactive logon: Prompt user to change password before expiration : Check(Define this policy settings)>>type 7>>ok

**#Common Restriction Global**

4. User Configuration>>Policies>>Administrative Templates>>System

(i)Prevent access to registry editing tools: Enable>>ok

**#General Policy Settings Global**

5. Computer Configuration>>Policies>>Windows Settings>>Security Settings>>Windows Firewall with Advanced Security

Windows Firewall is off bellow Profile

(i)Domain Profile, Privet Profile, Public Profile:>>Windows Firewall Properties>>

a. Domain Profile= Firewall state:off

Inbound Connection: Block (default)

Outbound Connection: Allow (default)

b. Private Profile=Firewall state:off

Inbound Connection: Block (default)

Outbound Connection: Allow (default)

c.Public Profile= Firewall state:off

Inbound Connection: Block (default)

Outbound Connection: Allow (default)>>ok

6. Computer Configuration>>Policies>>Administrative Templates>>Windows Components>>AutoPlay Policies

(i) Turn off AutoPlay : Enable>>Turn off Autoplay on: All Drives

**# Removable Disk Restriction Global**

7. Computer Configuration>>Policies>>Administrative Templates>>System>>Removable Storage Access

(i) All Removable Storage Classes: Deny Access all = Enable>>ok

8. Computer Configuration>>Policies>>Administrative Templates>>System>>Removable Storage Access

(i) CD and DVD: Deny write access= Enabled>>ok

**# Desktop Personalization**

9. User Configuratione>>Policies>>Administrative Templates>>Desktop

(i) Desktop Wallpaper: Enable>>Wallpaper Name: \\adds1\Desktop\_Personalization\ABC-Desktop.jpg>>ok

10. User Configuratione>>Policies>>Administrative Templates>>Control Panel>>Personalization

(i) Prevent changing desktop backgroundL: Enabled>>ok

11. User Configuratione>>Policies>>Administrative Templates>>Control Panel>>Personalization

(i) Prevent changing theme: Enabled>>ok

12. User Configuratione>>Policies>>Administrative Templates>>Control Panel>>Personalization

(i) Screen saver timeout: Enable>>Second:300>>ok

**# Local Administration Manage NBL**

13. Tools>>Group Policy Management>>Forest>>Domain>>habibdc.com>>Group Policy Object>>ITDepartment

(i) Delegation for local computer administration full Privilege: Delegation>>Add>>Advance>>Find now>>Administrator>>Permissions: Edit settings, Delete, modify security>>ok

14. Tools>>Group Policy Management>>Forest>>Domain>>habibdc.com>>Group Policy Object>>ITDepartment

(i) ABC (Network) to Local Group Network Configuration Operator: Delegation>>Add>>Advance>>Find now>>NETWORK>>Permissions: Edit settings, Delete, modify security>>ok

**# Admin-approval mode Global**

15. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Admin Approval Mode for the Built-in Administrator account>>Check(Define this policy settings)>>Enable>>ok

16. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode>>Check(Define this policy settings)>>Prompt for consent for non-Windows binaries>>ok

17. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Behavior of the elevation prompt for standard users>>Check(Define this policy settings)>>Prompt for credentials>>ok

18. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Detect application installations and prompt for elevation >>Check(Define this policy settings)>>Enabled>>ok

19. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Only elevate executable files that are signed and validated>>Check(Define this policy settings)>>Disabled>>ok

20. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Admin Approval Mode for the Built-in Administrator account>>Check(Define this policy settings)>>Enable>>ok

21. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Only elevate UIAccess applications that are installed in secure locations>>Check(Define this policy settings)>>Enable>>ok

22. Computer Configuration>>Policies>>Windows Seettings>>Security Settings>>Local Policies>>Security Options

(i) User Account Control: Run all administrators in Admin Approval Mode>>Check(Define this policy settings)>>Enable>>ok

**# Favorites links NBL**

23. User Configuration > Preferences > Windows Settings > Shortcuts

Action: Update

Name: %userprofile%\favorites\ABC\ Home

Target Type: URL

Location: <Specify full path>

Target URL: www.abc.com

**# IE Settings**

24. User Configuration>>Policies>>Administrative Templates>>Windows Components>>Internet Explorer

(i) Disable changing home page settings>>Enabled>>Homepage: http://www.abc.com/>>ok

25. User Configuration>>Policies>>Administrative Templates>>Windows Components>>Internet Explorer

(i) Turn off pop-up management >>Enabled>>ok

26. User Configuration>>Policies>>Administrative Templates>>Windows Components>>Internet Explorer>>Delete Browsing History

(i) Allow deleting browsing history on exit>>Enabled>>ok

27. User Configuration>>Policies>>Administrative Templates>>Windows Components>>Internet Explorer>>Internet Control Panel>>Security Page

(i) Site to Zone Assignment List>>Enable>>Enter the zone assignments here>>ok

**#Local Audit Policy**

28. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit account logon events>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

29. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit account management>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

30. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit directory service access >>Check(Define these policy settings)>>Check(Success)>>ok

31. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit logon events>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

32. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit object access>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

33. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit policy change>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

34. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit privilege use >>Check(Define these policy settings)>>Check(Success)>>ok

35. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Audit Policy

(i) Audit system events>>Check(Define these policy settings)>>Check(Success, Failure)>>ok

36. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Security Options

(i) Audit: Shut down system immediately if unable to log security audits>>N/A

37. Computer Configuration>>Windows Settings>>Security Settings>>Local Policies>>Security Options

(i) Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

**# Advanced Audit Policy**

38. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Account Logon

(i) Account Logon: Audit Credential Validation>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

39. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Account Management

(i) Account Management: Audit Computer Account Management>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

40. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Account Management

(i) Account Management: Audit Other Account Management Events>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

41. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Account Management

(i) Account Management: Audit Security Group Management>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

42. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Account Management

(i) Account Management: User Account Management>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

43. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>DS Access

(i) DS Access: Audit Directory Service Access>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

44. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>DS Access

(i) DS Access: Directory Service Changes>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

45. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Logon/Logoff

(i) Logon-Logoff: Audit Logoff>>Check(Define these policy settings)>>Check(Sucess)>>ok

46. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Logon/Logoff

(i) Logon-Logoff: Audit Logon>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

47. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Logon/Logoff

(i) Logon-Logoff: Special Logon>>Check(Define these policy settings)>>Check(Sucess)>>ok

48. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Policy Change

(i) Policy Change: Audit Audit Policy Change>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

49. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>Policy Change

(i) Policy Change: Audit Authentication Policy Change>>Check(Define these policy settings)>>Check(Sucess)>>ok

50. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>System

(i) System: Audit Security State Change>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

51. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>System

(i) System: Audit Security System Extension>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

52. Computer Configuration>>Windows Settings>>Security Settings>>Advanced Audit Policy Configuration>>System

(i) System: Audit System Integrity>>Check(Define these policy settings)>>Check(Sucess, Failure)>>ok

**# Audit Logs Sizes**

53. Computer Configuration>>Policies>>Windows Settings>>Security Settings>>Event Log

(i) Maximum Application Log Size>>Check(Define these policy settings)>>32768 KB>>ok

54. Application: Retain old events=Recommended state is Disabled

55. Computer Configuration>>Policies>>Administrative Templates>>Windows Components>>Event Log Service>>Security

(i) Specify the Maximum Log Size (KB)>>Enable>>81920KB>>ok

56. Security: Retain old events.=Recommended state is disabled

57. Computer Configuration>>Policies>>Administrative Templates>>Windows Components>>Event Log Service>>System

(i) Maximum Log Size (KB)>>Enable>>32768 KB>>ok

58. System: Retain old events=Recommended state is Disabled