**GPO Settings**

Right click on Default Domain Policy and click Import Settings…

* Be sure to remap some settings to map to local domain - e.g. Domain Admins@cyberdragons.edu

**Computer Configuration/Policies/WindowsSettings/SecuritySettings…**

**/Account Policies/Password Policy**

Maximum password age **0**

Minimum password age **0**

**/Account Policies/Account Lockout Policy**

To Do Account lockout duration **5 minutes**

To Do Account lockout threshold **10 invalid logon attempts**

To Do Reset account lockout counter after **5 minutes**

**/Account Policies/Kerberos Policy**

To Do Enforce user logon restrictions **Enabled**

To Do Maximum lifetime for service ticket **600 minutes**

To Do Maximum lifetime for user ticket **10 hours**

To Do Maximum lifetime for user ticket renewal **7 days**

To Do Maximum tolerance for computer clock synchronization **5 minutes**

**/Local Policies/Audit Policy**

To Do Audit account logon events **Success, Failure**

To Do Audit account management **Success, Failure**

To Do Audit directory service access **Success, Failure**

To Do Audit logon events **Success, Failure**

To Do Audit object access **Success, Failure**

To Do Audit policy change **Success, Failure**

To Do Audit privilege use **Success, Failure**

To Do Audit process tracking **None**

To Do Audit system events **None**

**/Local Policies/Security Options/User Rights Assignment**

To Do Deny access to the computer from the network: **Guest, Local account, Local account and member of Administrators group**

**/Local Policies/Security Options**

To Do Accounts: Local Administrator account status **Disabled**

To Do Accounts: Local Guest account status **Disabled**

To Do Accounts: Limit local account use of blank passwords to console logon only **Enabled**

To Do Accounts: Rename administrator account **“ludwig”**

To Do Accounts: Rename guest account **"yoo"**

To Do Accounts: Block Microsoft Accounts **Enabled**

To Do Domain member: Digitally encrypt secure channel data (when possible) **Enabled**

To Do Domain member: Digitally sign secure channel data (when possible) **Enabled**

To Do Domain member: Disable machine account password changes **Disabled**

To Do Domain member: Maximum machine account password age **30 days**

To Do Domain member: Require strong (Windows 2000 or later) session key **Enabled**

To Do Interactive logon: Message title for users attempting to log on: **GPO MSG**

To Do Interactive logon: Message text for users attempting to log on: **GPO APP**

To Do Interactive logon: Number of Previous logons to cache **1**

To Do Microsoft network client: Digitally sign communications (if server agrees) **Enabled**

To Do Microsoft network client: Send unencrypted password to third-party SMB servers **Disabled**

To Do Network security: LAN Manager auth. lvl **Send NTLMv2 response only\refuse NTLM & LM**

To Do Network security: Do not store LAN Manager hash value on next password chg **Enabled**

To Do Restrict NTLM: Incoming Traffic **Enable**

To Do Network access: Do not allow anon enumeration of SAM accounts and shares **Enabled**

To Do Network access: Do not allow anon enumeration of SAM accounts **Enabled**

To Do  Network Access: Remotely Accessible Registry paths and sub paths **Disabled**

To Do Network access: Allow anon SID/name translation **Disabled**

To Do Network Access: Let everyone permissions apply to anonymous users: **Disabled**

**/Event Log**

To Do Prevent local guests group from accessing application log **Enabled**

To Do Prevent local guests group from accessing security log **Enabled**

To Do Prevent local guests group from accessing system log **Enabled**

**/System Services**

To Do WinHTTP Web Proxy Autoconfiguration - **Disabled**

**/Windows Firewall with Advanced Security**

To Do Enforce default settings (Inbound connections not matching a rule blocked/outbound allowed)

* Policy allows local policies to be created/applied
* Logs all allowed and blocked connections

**/Application Control Policies/AppLocker/Script Rules**

To Do Deny any scripts running from %OSDRIVE%\Users\\* Directory

**/Advanced Audit Policy Configuration**

To Do Enforce a number of settings for logging Success/Failure under

* Account Management
* Logon/Logoff
* Policy Change
* System

**Administrative Templates**

**/Network/DNSClient**

To Do Turn off Multicast Name Resolution – set to enabled

**/System/GroupPolicy**

r

To Do Group Policy refresh interval for computers **5min / 5min**

To Do Group Policy refresh interval for domain controllers **5min / 0 min**

To Do Configure Security Policy Processing - **Enabled and Process even if no changes**

**/Windows Components/Windows Update**

To Do Configure Automatic Updates - Autodownload and Notify

To Do (optional - if needed/desired) Specify intranet Microsoft update service location - <http://192.168.9.13:8530> for both

**/Windows Components/Remote Desktop Services/Remote Desktop Session Host\Sec.**

To Do Set client connection encryption level **Client Compatible**

**Computer Configuration/Policies/Preferences/Windows Settings**

**/Registry**

To Do Disable SMBv1

Registry subkey: **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**

Registry entry: SMB1

REG\_DWORD: 0 = Disabled

REG\_DWORD: 1 = Enabled

To Do Disable WPAD

Disable WPAD via Group Policy by deploying the following:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad

New DWORD (32-Bit Value) called “WpadOverride” and set to “1”

To Do Cleartext storage of creds:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest

· If the UseLogonCredential value is set to **0**, WDigest will not store credentials in memory.

· If the UseLogonCredential value is set to **1**, WDigest will store credentials in memory.

\*\*Requires some patches be installed

* 2984972 for supported editions of Windows 7 and Windows Server 2008 R2
* 2984976 for supported editions of Windows 7 and Windows Server 2008 R2 that have update [2592687 (Remote Desktop Protocol (RDP) 8.0 update)](http://support.microsoft.com/kb/2592687) installed. Customers who install update 2984976 must also install update 2984972.
* 2984981 for supported editions of Windows 7 and Windows Server 2008 R2 that have update [2830477 (Remote Desktop Connection (RDC) 8.1 client update)](http://support.microsoft.com/kb/2830477) installed. Customers who install update 2984981 must also install update 2984972.
* 2973501 for supported editions of Windows 8, Windows Server 2012, and Windows RT.

*From <*[*https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997*](https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997)*>*