# Securing Domain Controllers to Improve Active Directory Security

adsecurity.org

Sean Metcalf November 3, 2016

Active Directory security effectively begins with ensuring Domain Controllers (DCs) are configured securely. At BlackHat USA this past Summer, I spoke about AD for the security professional and provided tips on how to best secure Active Directory. This post focuses on Domain Controller security with some cross-over into Active Directory security. The blog is called ADSecurity after all…

This post covers some of the best methods to secure Active Directory by securing Domain Controllers in the following sections:

- Default Domain & Domain Controller Policies
- Creating Domain & Domain Controller Security Baseline GPOs
- Patching Domain Controllers
- Protecting Domain Controllers
- Domain Controller Recommended Group Policy Settings
- Configuring Domain Controller Auditing (Event Logs)
- Domain Controller Events to Monitor (Event Logs)
- Key Domain Controller Security Items

As with any major change to infrastructure, please test before deploying changes.

## Default Domain & Domain Controller Group Policies (GPOs)

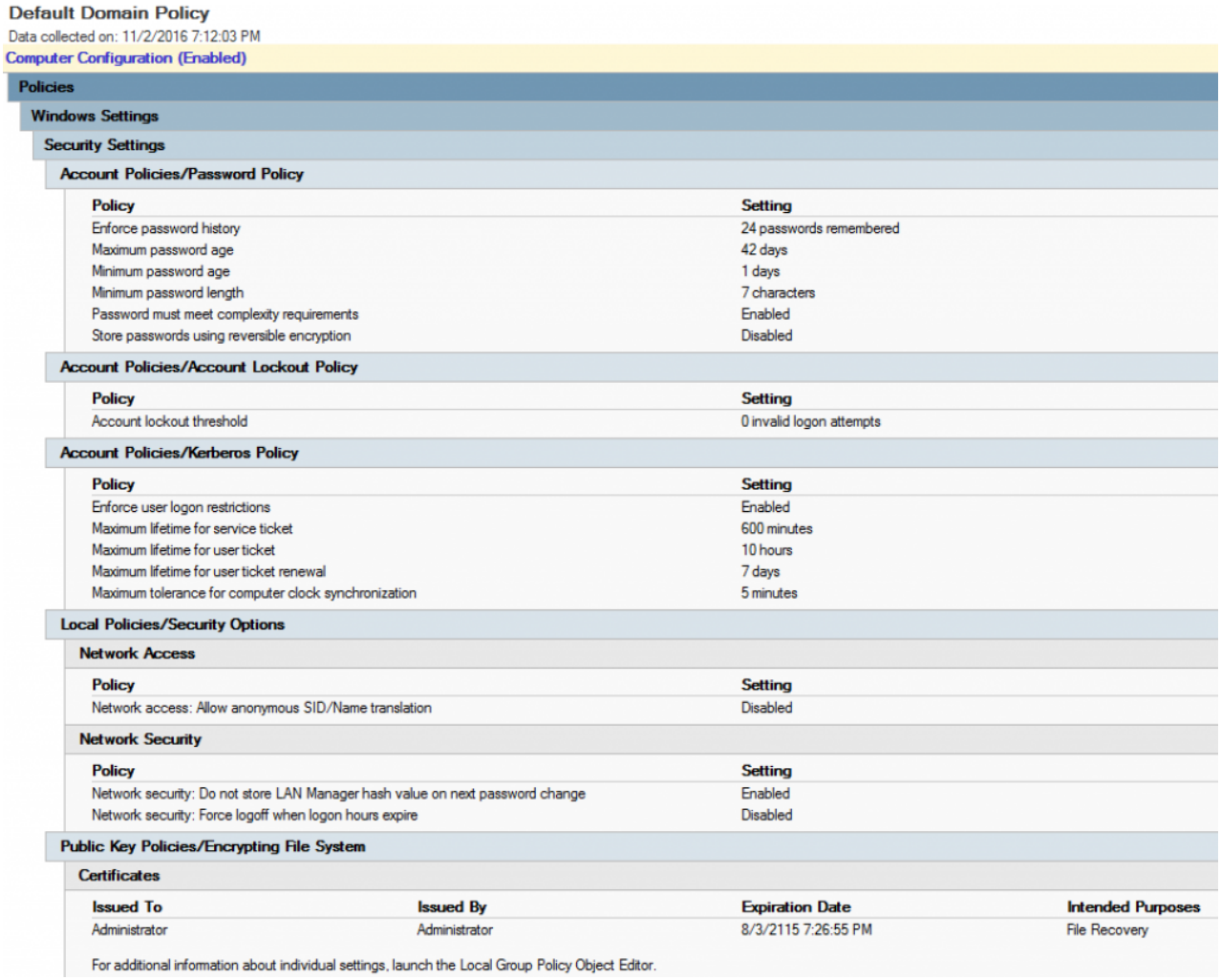
When an Active Directory domain is first created, there are two GPOs created by default:

- Default Domain Policy – GUID: {31B2F340-016D-11D2-945F-00C04FB984F9}
- Default Domain Controllers Policy – GUID: {6AC1786C-016F-11D2-945F-00C04FB984F9}

Note that these GPO GUIDs are the same for every Active Directory domain instance. This is to ensure that Windows can quickly find these GPOs and if they're deleted, they need to be restored/recreated. The Active Directory Best Practices Analyzer looks for the default GPOs to ensure they're applied correctly. GPO GUIDs are different than AD object GUIDs since some GPO GUIDs need to be the same across AD instances.

The **Default Domain Policy** should only contain the following settings:

- Password Policy
- Account Lockout Policy
- Kerberos Policy



**Default Domain Policy**

Data collected on: 11/2/2016 7:12:03 PM

**Computer Configuration (Enabled)**

**Policies**

**Windows Settings**

**Security Settings**

**Account Policies/Password Policy**

| Policy | Setting |
|---|---|
| Enforce password history | 24 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 1 days |
| Minimum password length | 7 characters |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |

**Account Policies/Account Lockout Policy**

| Policy | Setting |
|---|---|
| Account lockout threshold | 0 invalid logon attempts |

**Account Policies/Kerberos Policy**

| Policy | Setting |
|---|---|
| Enforce user logon restrictions | Enabled |
| Maximum lifetime for service ticket | 600 minutes |
| Maximum lifetime for user ticket | 10 hours |
| Maximum lifetime for user ticket renewal | 7 days |
| Maximum tolerance for computer clock synchronization | 5 minutes |

**Local Policies/Security Options**

**Network Access**

| Policy | Setting |
|---|---|
| Network access: Allow anonymous SID/Name translation | Disabled |

**Network Security**

| Policy | Setting |
|---|---|
| Network security: Do not store LAN Manager hash value on next password change | Enabled |
| Network security: Force logoff when logon hours expire | Disabled |

**Public Key Policies/Encrypting File System**

**Certificates**

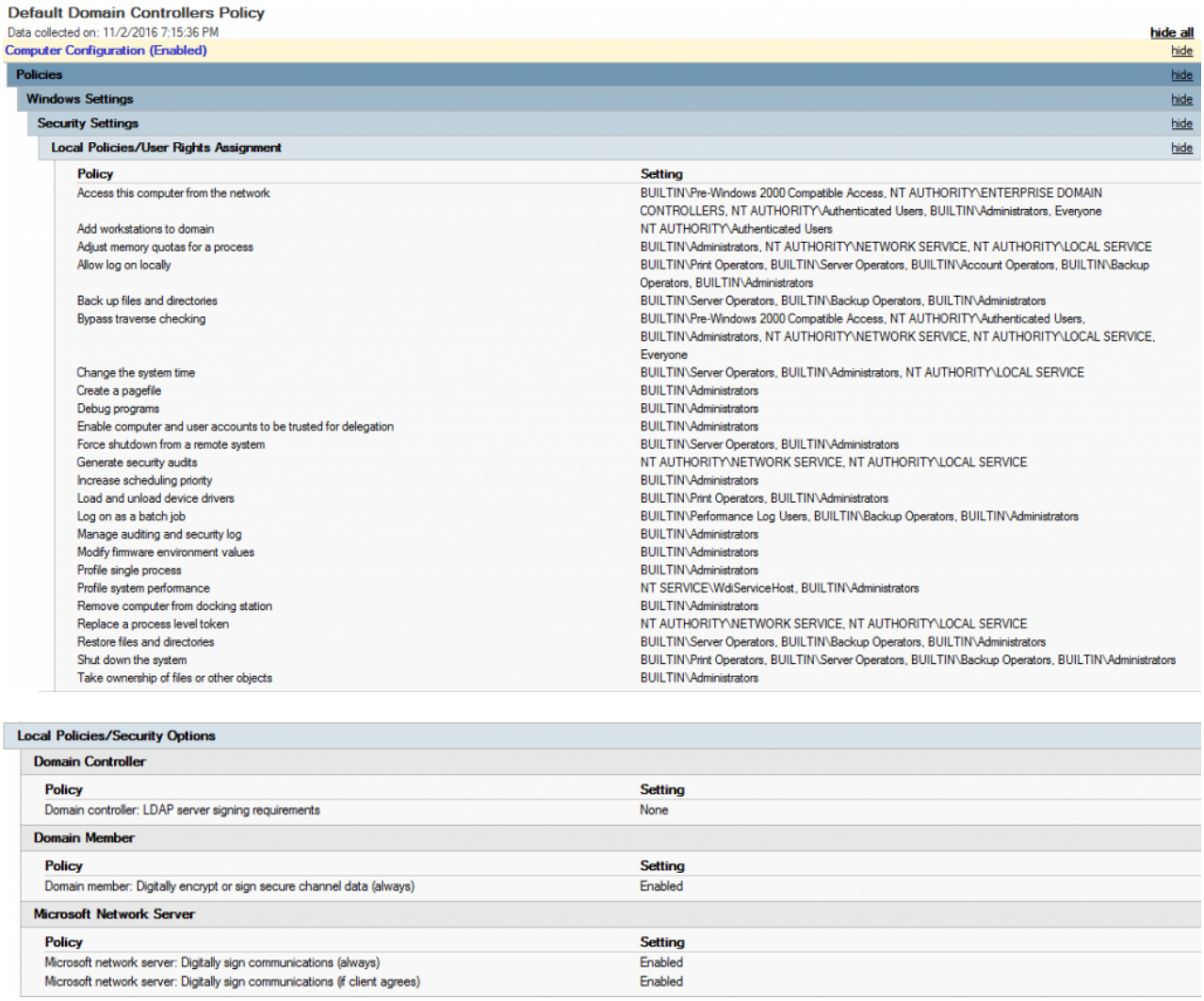
| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| Administrator | Administrator | 8/3/2115 7:26:55 PM | File Recovery |

For additional information about individual settings, launch the Local Group Policy Object Editor.

*The Default Domain Policy default settings for Windows Server 2012 R2 are shown in the above graphic.*

The **Default Domain Controllers Policy** should only contain the following settings:

- User Rights Assignment
- Security Options (some)



**Default Domain Controllers Policy**

Data collected on: 11/2/2016 7:15:36 PM — hide all

**Computer Configuration (Enabled)** — hide

**Policies** — hide

**Windows Settings** — hide

**Security Settings** — hide

**Local Policies/User Rights Assignment** — hide

| Policy | Setting |
|---|---|
| Access this computer from the network | BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone |
| Add workstations to domain | NT AUTHORITY\Authenticated Users |
| Adjust memory quotas for a process | BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE |
| Allow log on locally | BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators |
| Back up files and directories | BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators |
| Bypass traverse checking | BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, Everyone |
| Change the system time | BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE |
| Create a pagefile | BUILTIN\Administrators |
| Debug programs | BUILTIN\Administrators |
| Enable computer and user accounts to be trusted for delegation | BUILTIN\Administrators |
| Force shutdown from a remote system | BUILTIN\Server Operators, BUILTIN\Administrators |
| Generate security audits | NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE |
| Increase scheduling priority | BUILTIN\Administrators |
| Load and unload device drivers | BUILTIN\Print Operators, BUILTIN\Administrators |
| Log on as a batch job | BUILTIN\Performance Log Users, BUILTIN\Backup Operators, BUILTIN\Administrators |
| Manage auditing and security log | BUILTIN\Administrators |
| Modify firmware environment values | BUILTIN\Administrators |
| Profile single process | BUILTIN\Administrators |
| Profile system performance | NT SERVICE\WdiServiceHost, BUILTIN\Administrators |
| Remove computer from docking station | BUILTIN\Administrators |
| Replace a process level token | NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE |
| Restore files and directories | BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators |
| Shut down the system | BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators |
| Take ownership of files or other objects | BUILTIN\Administrators |

**Local Policies/Security Options**

**Domain Controller**

| Policy | Setting |
|---|---|
| Domain controller: LDAP server signing requirements | None |

**Domain Member**

| Policy | Setting |
|---|---|
| Domain member: Digitally encrypt or sign secure channel data (always) | Enabled |

**Microsoft Network Server**

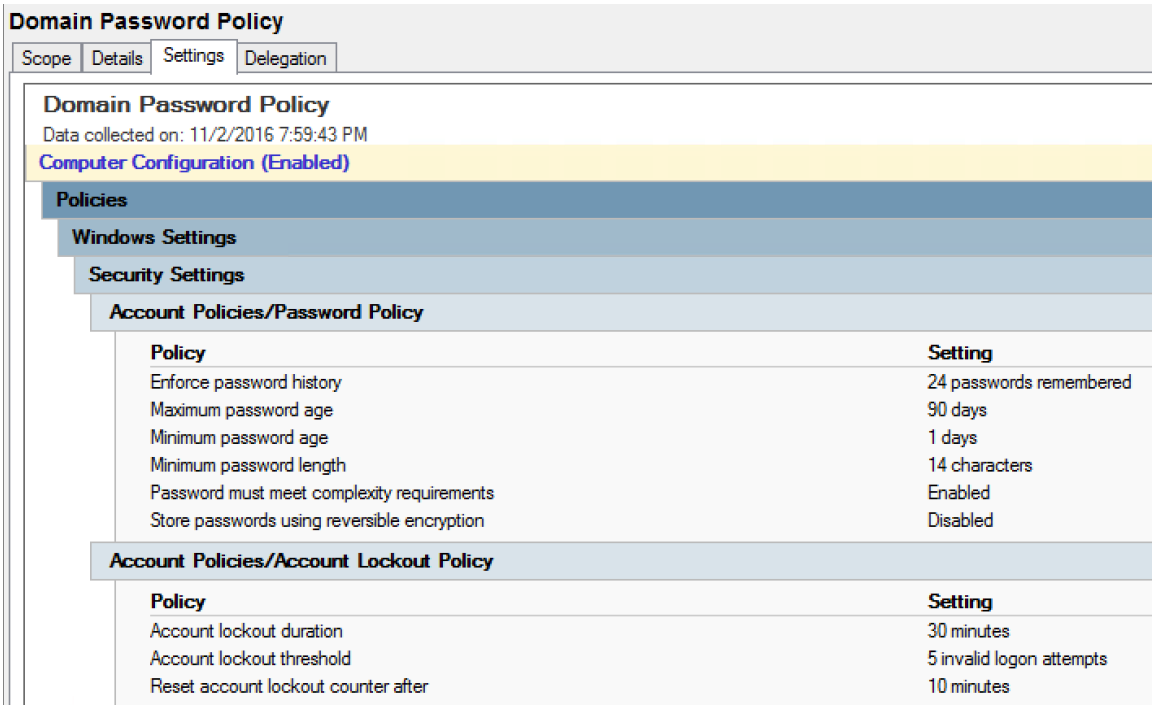
| Policy | Setting |
|---|---|
| Microsoft network server: Digitally sign communications (always) | Enabled |
| Microsoft network server: Digitally sign communications (if client agrees) | Enabled |

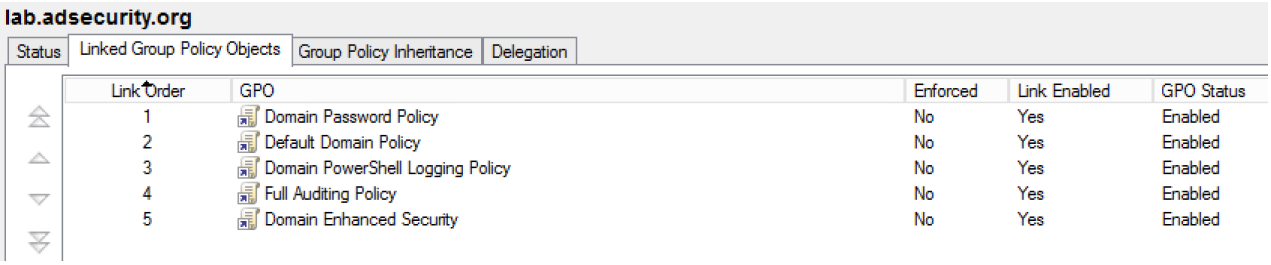
*The Default Domain Controllers Policy default settings for Windows Server 2012 R2 are shown in the above graphics.*

## Creating Domain & Domain Controller Security Baseline GPOs

It is very tempting to put customized settings into the default GPOs. Please resist this urge since it's better to layer additional security in new GPOs (and easier for change management).

Note that the domain password policy is effectively the GPO with the highest link order linked to the domain, so it's possible to create a new GPO with custom password policy settings, link to the domain, and move the link order to 1 (as shown in the following graphics).




With that said, many organizations simply customize the password policy in the Default Domain Policy GPO which is fine (and was required back in the Windows 2000 and 2003 Server days). Just don't add new settings to this GPO; keep it clean.

The default password policy settings in the Default Domain Policy GPO leave a lot to be desired. I recommend tightening these up to make them more secure. If there are accounts that require less restrictive requirements, use Fine-Grained Password Policy to provide more lax password settings for exceptions.

- Enforce Password History: 24 (the default is fine)
- Maximum Password Age: 60 – 180 depending on organizational requirements and minimum password length.
- Minimum Password Age: 1

  Set this to be 1 or higher so users can't simply keep cycling their new password until they roll through the password history to get back to their favorite password.

- Minimum Password Length: 14
  Fun fact: the only acceptable values set via the Group Policy Management Console (GPMC) are the numbers 0 through 14. Manually setting the associated Group Policy settings files in SYSVOL is an unsupported way to set a higher value.
  The better idea is to set it to 14 here, then use a Fine Grained Password Policy to apply to a group and ensure the users you want this setting to apply to are in this group.
- Password must meet complexity requirements: Enabled
- Store passwords using reversible encryption: Disabled
  If this is set to enabled, any user that changes their password while this setting is enabled has their password stored in the AD database (NTDS.dit file) in a way that can be reversed (as opposed to only hashed) which means the user's password can be extracted.
- Account lockout duration: 1 – 90 minutes
  Set to some value to mitigate password guessing attempts
- Account lockout threshold: 5 – 20 invalid logon attempts
  Set to configure how many invalid logon attempts are required before locking the account.
- Reset account lockout counter after: 5 – 60 minutes
  Set to configure how long until the account is automatically unlock without requiring help desk assistance.

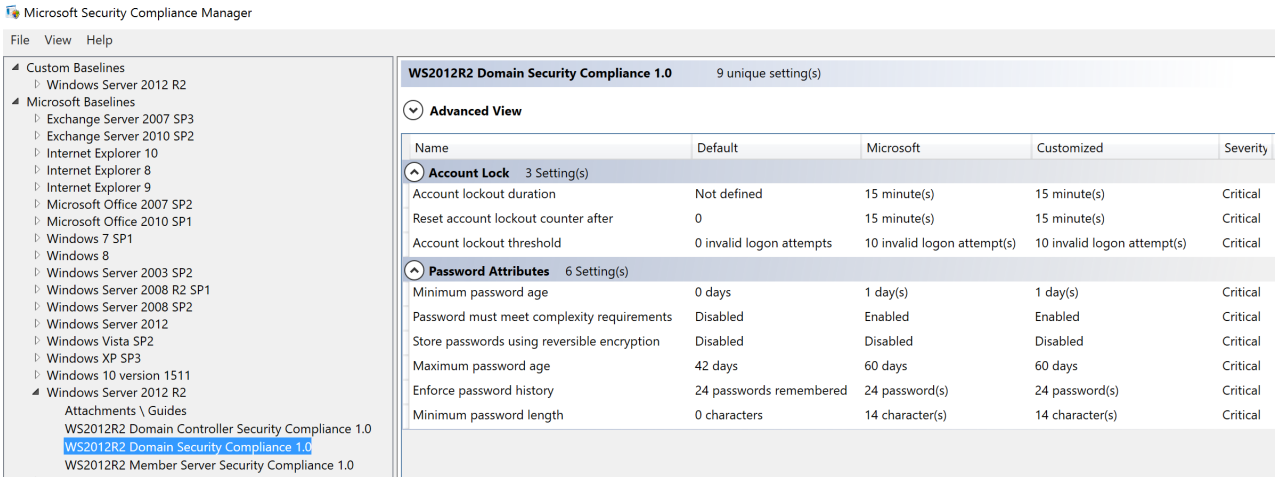
The first step is to create two new GPOs (these are examples, call them whatever you like):

- Baseline Domain Security Policy
- Baseline Domain Controller Security Policy

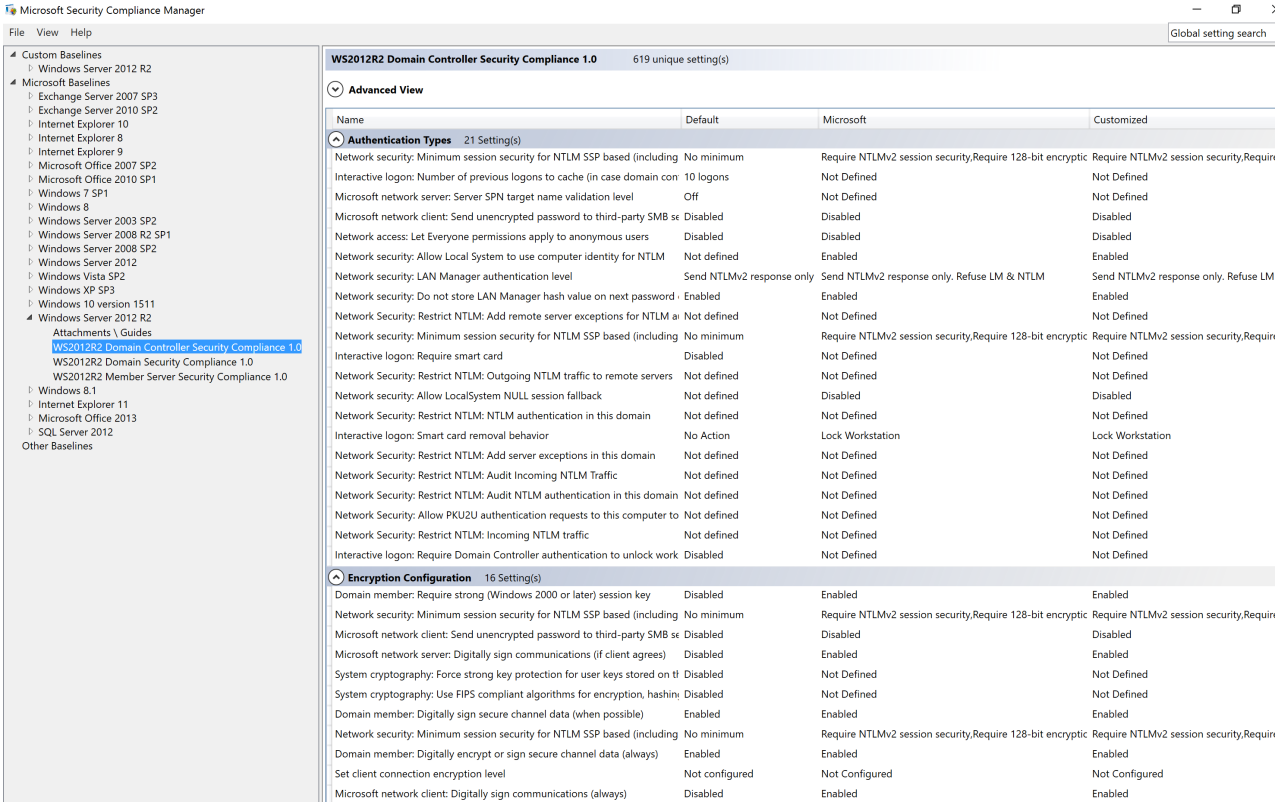
The Baseline Domain Security Policy should contain settings that apply to the entire domain.
The best way to create a secure Domain Policy and a secure Domain Controller Policy is to download the Microsoft Security Compliance Manager (currently at version 4.0) and select "Security Compliance" option under the operating system version for which you want to create the security baseline GPOs. Review the options, change as needed, and export as a GPO Backup (folder). Create a new empty GPO in the domain and "Import Settings" from the SCM GPO backup so the new GPO has the same settings as the SCM export. Then apply this GPO to your Domain Controllers . This will improve your DC security baseline if you have minimal security settings already configured, especially if you have no existing workstation GPO.

Most of the settings included are identified and described in the "Protecting Domain Controllers" & "Recommended Group Policy Settings" sections further down in this post.

*Microsoft SCM Domain Security Compliance Policy*
*(review settings and test before deploying)*




*Microsoft SCM Domain Controller Security Compliance Policy*




If one of the templates includes FIPS compliant encryption, validate whether or not you need it set since Microsoft doesn't recommend this as of 2014. If you are unsure if you need it, don't enable it. FIPS compatible encryption can actually cause problems. Some government systems require it, but please test extensively with applications first.

As part of developing your Security Baseline, there are several large organizations that have spent time and money determining what's "secure":

- DoD STIG: http://iase.disa.mil/stigs/os/windows
- Australian Information Security Manual: http://www.asd.gov.au/infosec/ism/index.htm
- CIS Benchmarks: https://benchmarks.cisecurity.org/downloads/browse/?category=benchmarks.os.window

If you already have a GPO configuring workstation security, you can compare what you have to the SCM generated “Security Compliance” GPO using Microsoft’s Policy Analyzer.

There are two different schools of thought for Group Policies, one is to use as few GPOs as possible filing up each one with as many like settings as possible and the other is to use separate GPOs for each purpose. I tend to fall in the middle. Use separate GPOs for major configuration settings: Windows Workstation Configuration, Windows Server Configuration, User Configuration, etc. In addition to these, configure additional GPOs with a few new settings for testing.

## Patching Domain Controllers

Important servers need to be patched as soon as possible when critical security patches are released. The concern centers around “what if I apply a patch and it breaks something?” which is a valid one. Mitigating concerns around breaking operations and ensuring security patches are applied promptly is a delicate balance, certainly more art than science.

- Apply patches to a subset of Domain Controllers first to let them “bake” for a period of time, then apply to another set, and then install the patch on all of them. One popular approach is to apply the patch(es) to even numbered DCs at first, and then deploy to odd numbered DCs.
- Apply critical security patches first. Any security patch labelled “critical” and applies to DCs needs to be installed as soon as possible. This includes any kind of Remote Code Execution (RCE), AD privilege escalation, and similar.
- Ensure that any service installed on a DC is properly patched as well. Domain Controllers frequently host DNS, so a vulnerable DNS service running on a DC could be exploited to compromise the Active Directory domain.
- Ensure that servers should be fully patched before promoting to be a DC (issues like MS14-068 make this critical).

## Protecting Domain Controllers

Domain Controller security, and in many ways Active Directory security, is based on the Windows version installed on the Domain Controllers. This is why it’s important to run the current Windows version on Domain Controllers – newer versions of Windows server have better security baked in and improved Active Directory security features.

Some of the Active Directory Domain Functional Level security features are listed here by Windows version:

**Windows Server 2008 R2 Domain Functional Level:**

- Kerberos AES encryption support
  Enables possibility of removing RC4 HMAC Kerberos encryption from supported types. Note that Windows 7 & Windows Server 2008 R2 no longer support Kerberos DES encryption.
- Managed Service Accounts
  AD controls the service account password.
- Authentication Mechanism Assurance.
  Users receive additional group membership when authentication with smartcard

**Windows Server 2012 Domain Functional Level:**

**Windows Server 2012 R2 Domain Functional Level:**

- Authentication Policies & Silos
  Protect privileged accounts limiting where they can logon to.
- Protected Users Security Group
  - PDC set to Windows 2012 R2 to create the group
  - Protected Users Host Protection (Win 8.1/2012R2) Prevents:
    - Authentication by using NTLM, Digest Authentication, or CredSSP.
    - Cached credentials
    - DES or RC4 encryption types in Kerberos pre-authentication.
    - Account delegation.
  - Protected Users Domain Enforcement Prevents:
    - NTLM authentication.
    - DES or RC4 encryption types in Kerberos pre-authentication.
    - Be delegated with unconstrained or constrained delegation.
    - Renew the Kerberos TGTs beyond the initial four-hour lifetime.

**Windows Server 2016 New Security Features:**

- Privileged Access Management – support for a separate bastion (admin) forest
- Microsoft Passport

Only approved software should be installed on Domain Controllers from trusted sources. This includes installing the Windows OS from a trusted source.

Domain Controllers should have the Windows firewall enabled and configured to prevent internet access. Most of the time, Domain Controllers do not have a good reason for direct internet access.

Ideally, there should be no software or agents installed on Domain Controllers since each additional program installed potentially provides another attack pathway. Every agent or service installed provides that application owner the potential ability to run code on a Domain Controller. If the patch infrastructure manages all workstations, servers, and Domain Controllers, it only takes the compromise of a single patch infrastructure admin to

compromise the Active Directory environment. This is why Domain Controllers and administrative workstations/servers require their own management infrastructure separate from the rest of the enterprise since shared system management can provide a path to domain compromise. Domain Controllers and admin workstations/servers should have their own patching infrastructure like Windows Server Update Services (WSUS).

The best way to protect Active Directory is to limit domain level administrative privileges. This includes limiting access to Domain Controllers, specifically logon and administrative rights. The following User Rights Assignments should be configured to enforce least privilege for Domain Controllers via Group Policy:

- Logon as a batch job: Not Defined
- Deny log on as a batch job: Guests
- Allow log on locally: Administrators
- Allow log on through Remote Desktop Services: Administrators
- Access this computer from the network: Administrators, Authenticated Users, Enterprise Domain Controllers
- Backup file and directories: Administrators (Backup Operators if a backup agent is required)
- Restore file and directories: Administrators (Backup Operators if a backup agent is required)
- Add workstations to domain: Administrators
- Bypass traverse checking: Not Defined
- Deny access to this computer from the network: Guests, NT AUTHORITY\Local Account
- Devices: Prevent users from installing printer drivers: Enabled
- Log on as a service: [only specific accounts that require this right should be listed here]
- Domain controller: Allow server operators to schedule tasks: Disabled
- Deny log on through Remote Desktop Services: Guests, NT AUTHORITY\Local Account
- Devices: Prevent users from installing printer drivers: Enabled
- Shut down the system: Administrators

## Domain Controller Recommended Group Policy Settings

This section outlines recommended security settings for Domain Controllers, many of which are described and set in the Microsoft security baseline in SCM.
Please fully test these settings before applying.

### Enable NTLM Auditing

Restrict NTLM: Audit Incoming NTLM Traffic: Enable auditing for all accounts

> This policy setting allows you to audit incoming NTLM traffic.
> This policy is supported on at least Windows 7 or Windows Server 2008 R2.
> Note: Audit events are recorded on this computer in the “Operational” Log located under the Applications and Services Log/Microsoft/Windows/NTLM.

Restrict NTLM: Audit NTLM authentication in this domain: Enable all

> This policy setting allows you to audit NTLM authentication in a domain from this domain controller.
> This policy is supported on at least Windows Server 2008 R2.
> Note: Audit events are recorded on this computer in the “Operational” Log located under the Applications and Services Log/Microsoft/Windows/NTLM.

**LAN Manager authentication level: Send NTLMv2 response only. Refuse LM & NTLM**

By default, this configuration is set to “Send NTLMv2 response only”**.**
In the Microsoft Security Compliance Manager, Microsoft recommends this configuration be set to “Send NTLMv2 response only. Refuse LM & NTLM.” This recommendation stands; however, many environments are still using NTLMv1 authentication, so it may be necessary to enable NTLM authentication auditing to identify how NTLM authenticaiton is used in the enterprise.

LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2.

LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:

- Join a domain
- Authenticate between Active Directory forests
- Authenticate to down-level domains
- Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP)
- Authenticate to computers that are not in the domain

The possible values for the Network security: LAN Manager authentication level setting are:

- Send LM & NTLM responses
- Send LM & NTLM — use NTLMv2 session security if negotiated
- Send NTLM responses only
- Send NTLMv2 responses only
- Send NTLMv2 responses only\refuse LM
- Send NTLMv2 responses only\refuse LM & NTLM
- Not Defined

The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows:

- Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
- Send LM & NTLM – use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
- Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.

> - Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
> - Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).
> - Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication).
>
> These settings correspond to the levels discussed in other Microsoft documents as follows:
>
> - Level 0 – Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
> - Level 1 – Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
> - Level 2 – Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
> - Level 3 – Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
> - Level 4 – Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2.
> - Level 5 – Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2).

**Lsass.exe audit mode: Enabled**
Enable “Lsass.exe audit mode” to identify what programs may be blocked when enabling LSA Protection.
Review the following events to identify potential issues before enabling LSA Protection:

- Event 3065: This event records that a code integrity check determined that a process (usually lsass.exe) attempted to load a particular driver that did not meet the security requirements for Shared Sections. However, due to the system policy that is set, the image was allowed to load.

- Event 3066: This event records that a code integrity check determined that a process (usually lsass.exe) attempted to load a particular driver that did not meet the Microsoft signing level requirements. However, due to the system policy that is set, the image was allowed to load.

> You can configure this setting to enable the auditing of Lsass.exe so that you can evaluate feasibility of enabling LSA protection.  You can use the audit mode to identify LSA plug-ins and drivers that will fail to load in LSA Protection mode. While in the audit mode, the system will generate event logs, identifying all of the plug-ins and drivers that will fail to load under LSA if LSA Protection is enabled. The messages are logged without blocking the plug-ins or drivers.
>
> If you enable this setting, Lsass.exe audit mode is enabled and event are generated in the event log.
>
> If you disable or do not configure this setting, Lsass.exe audit mode is disabled and event are not generated in the event log.

**Enable LSA Protection: Enabled**
Prior to enabling this setting on Domain Controllers, enable “Lsass.exe audit mode” to identify what programs may be blocked.

> Use this setting to configure additional protection for the Local Security Authority (LSA) process to prevent code injection that could compromise credentials.
>
> On x86-based or x64-based devices that use Secure Boot and UEFI, a UEFI variable is set in the UEFI firmware when LSA protection is enabled by using the registry key. When the setting is stored in the firmware, the UEFI variable cannot be deleted or changed in the registry key. The UEFI variable must be reset.
>
> x86-based or x64-based devices that do not support UEFI or Secure Boot are disabled, cannot store the configuration for LSA protection in the firmware, and rely solely on the presence of the registry key. In this scenario, it is possible to disable LSA protection by using remote access to the device.
>
> If you enable this setting, LSA protection is enabled.
> If you disable or do not configure this setting, LSA protection is not enabled.

**Domain member: Require strong (Windows 2000 or later) session key: Enabled**
The default is “Disabled”.

> Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems.
> Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)
>
> When this policy setting is enabled, a secure channel can only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key.
> To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. If communication to non-Windows 2000–based domains is required, Microsoft recommends that you disable this policy setting.

**Network security: Minimum session security for NTLM SSP based (include secure RPC) servers: Require NTLMv2 session security, Require 128-bit encryption**

The default setting is “No Minimum”.
In the Microsoft Security Compliance Manager, Microsoft recommends this configuration is set to “Require NTLMv2 session security, Require 128-bit encryption” to improve NTLM security.

> This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.
>
> The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:
>
> - Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.
> - Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.
> - Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.
> - Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.
> - Not Defined.

**Network security: Minimum session security for NTLM SSP based (include secure RPC) clients: Require NTLMv2 session security, Require 128-bit encryption**

The default setting is “No Minimum”.
In the Microsoft Security Compliance Manager, Microsoft recommends this configuration is set to “Require NTLMv2 session security, Require 128-bit encryption” to improve NTLM security.

> This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI.
>
> The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:
>
> - Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.
> - Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.
> - Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.
> - Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.
> - Not Defined.

**Microsoft network server: Digitally sign communications (if client agrees): Enabled**
The default setting is Disabled.

> Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.
> SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.
>
> This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled.
> Note  Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment.

**Microsoft network server: Digitally sign communication (always): Enabled**
**Microsoft network client: Digitally sign communication (always): Enabled**

Both of these settings are configured as “Disabled” by default.

> Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.
> SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.
>
> This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments.
>
> Note  When Windows Vista–based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the “Microsoft network client and server: Digitally sign communications (four related settings)” section in Chapter 5 of the Threats and Countermeasures guide.

**Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled**
The default setting is “Disabled”.

> An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.
>
> This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment.
> The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide.

**WDigest Authentication (disabling may require KB2871997): Disabled**
WDigest Authentication is disabled by default on Windows Server 2012 R2 and newer, so this setting enforces this setting.

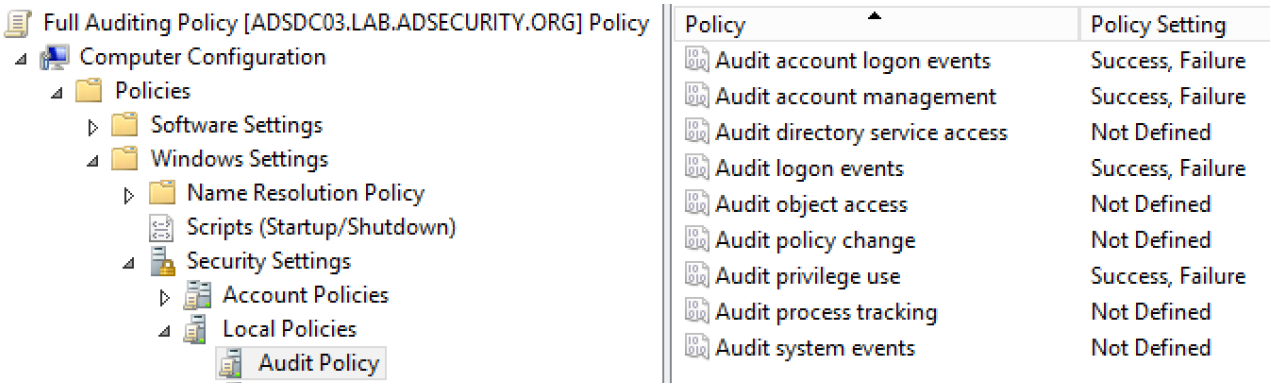
> WDigest leaves user's plaintext-equivalent passwords in Lsass.exe memory, which leaves the password vulnerable to Pass-the-Hash and other credential theft attacks.
>
> When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. Microsoft recommends disabling WDigest authentication unless it is needed.
>
> If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server.
>
> Update KB2871997 must first be installed to disable WDigest authentication using this setting in Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012.
>
> Enabled: Enables WDigest authentication.
>
> Disabled (recommended): Disables WDigest authentication. For this setting to work on Windows 7, Windows 8, Windows Server 2008 R2 or Windows Server 2012, KB2871997 must first be installed.
>
> For more information, see http://support.microsoft.com/kb/2871997 and http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx .

*HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential REG_DWORD:0*

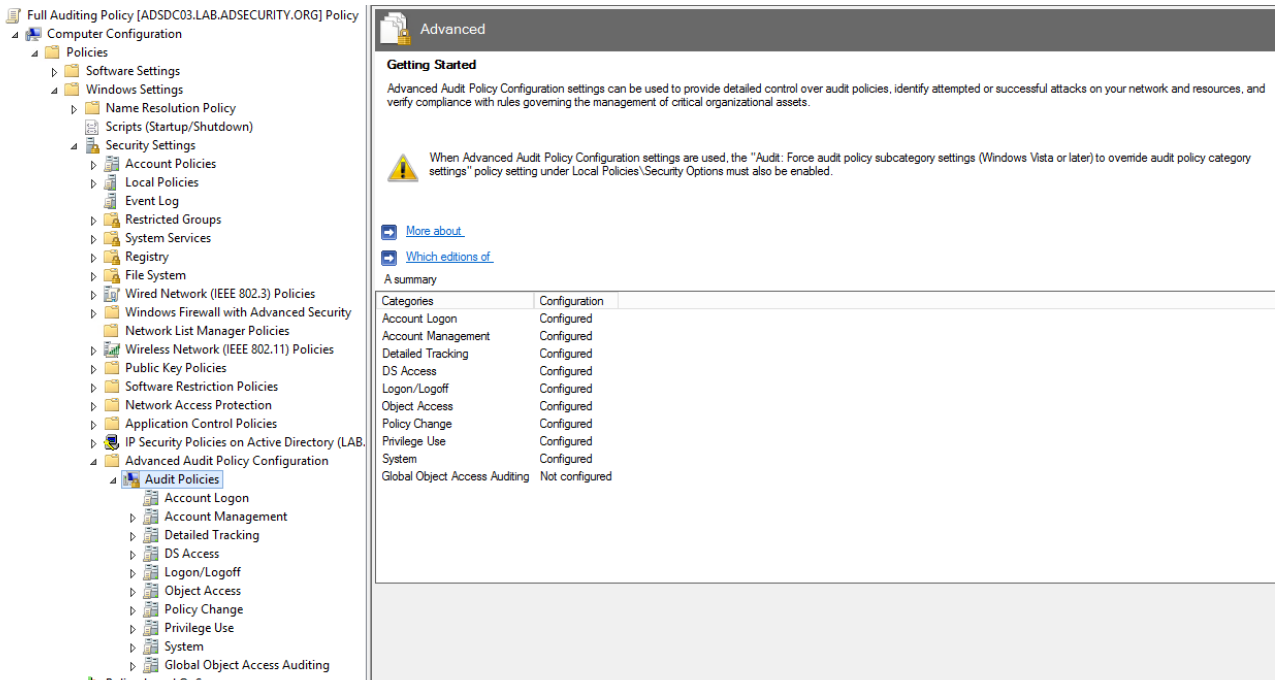
## Configuring Domain Controller Auditing (Event Logs)

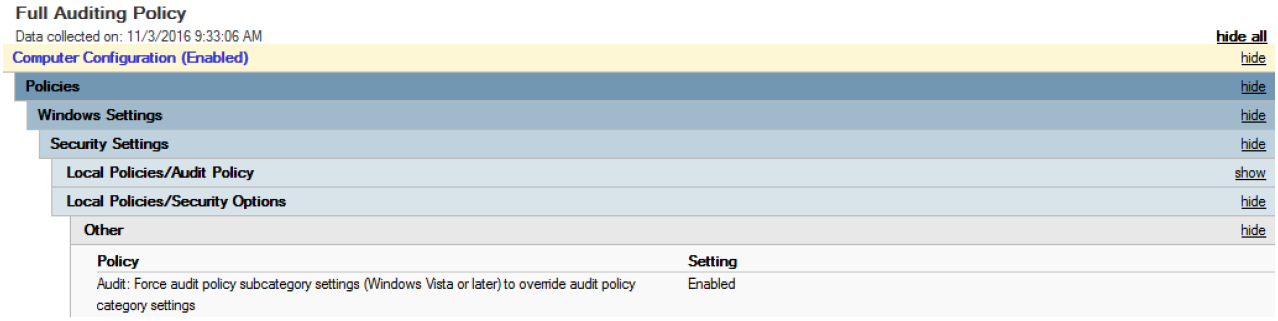
Securing Domain Controllers is only one part of Active Directory security. Another is being able to detect anomalous activity which starts with logging.

Prior to Windows Server 2008, Windows auditing was limited to 9 items.



Starting with Windows Vista & Windows Server 2008, Windows auditing is expanded to 57 items.




*Note that "Audit: Force audit policy subcategory settings" should be set to "Enabled" to enforce them when normal audit settings are often configured.*

Use AuditPol to validate auditing settings: ***auditpol.exe /get /category:****

## Auditing Subcategories to Events

| Auditing Subcategory | Event IDs |
|---|---|
| Audit Audit Policy Change | 4719: System audit policy was changed.<br>**4908**: Special Groups Logon table modified. |

| | |
|---|---|
| Audit Authentication Policy Change | 4706: A new trust was created to a domain.<br>4707: A trust to a domain was removed.<br><br>**4713**: Kerberos policy was changed.<br><br>**4716**: Trusted domain information was modified.<br><br>4717: System security access was granted to an account.<br><br>4718: System security access was removed from an account.<br><br>**4739**: Domain Policy was changed.<br><br>4865: A trusted forest information entry was added.<br><br>4866: A trusted forest information entry was removed.<br><br>**4867**: A trusted forest information entry was modified.<br><br>4706: A new trust was created to a domain.<br><br>4707: A trust to a domain was removed. |
| Audit Computer Account Management | **4741**: A computer account was created.<br>**4742**: A computer account was changed.<br><br>4743: A computer account was deleted. |
| **Audit DPAPI Activity** | **4692**: Backup of data protection master key was attempted.<br>4693: Recovery of data protection master key was attempted.<br><br>4695: Unprotection of auditable protected data was attempted. |
| Audit Kerberos Authentication Service | **4768**: A Kerberos authentication ticket (TGT) was requested<br>**4771**: Kerberos pre-authentication failed<br><br>4772: Kerberos authentication ticket request failed |
| Audit Kerberos Service Ticket Operation | **4769**: A Kerberos service ticket (TGS) was requested<br>4770: A Kerberos service ticket was renewed |
| Audit Logoff | 4634: An account was logged off. |

| | |
|---|---|
| Audit Logon | **4624**: An account was successfully logged on.<br>**4625**: An account failed to log on.<br><br>**4648**: A logon was attempted using explicit credentials. |
| Audit Other Account Logon Events | **4648**: A logon was attempted using explicit credentials<br>4649: A replay attack was detected.<br><br>4800: The workstation was locked.<br><br>4801: The workstation was unlocked.<br><br>5378: The requested credentials delegation was disallowed by policy. |
| **Audit Other Object Access Events** | **4698: A scheduled task was created.**<br>**4699: A scheduled task was deleted.**<br><br>**4702: A scheduled task was updated.** |
| Audit Process Creation | **4688**: A new process has been created. |
| Audit Security Group Management | **4728**: A member was added to a security-enabled global group.<br>4729: A member was removed from a security-enabled global group.<br><br>**4732**: A member was added to a security-enabled local group.<br><br>4733: A member was removed from a security-enabled local group.<br><br>4735: A security-enabled local group was changed.<br><br>4737: A security-enabled global group was changed.<br><br>4755: A security-enabled universal group was changed.<br><br>**4756**: A member was added to a security-enabled universal group.<br><br>4757: A member was removed from a security-enabled universal group.<br><br>4764: A group’s type was changed. |

| | |
|---|---|
| Audit Security System Extension | **4610**: An authentication package has been loaded by the Local Security Authority.<br>**4611**: A trusted logon process has been registered with the Local Security Authority.<br><br>**4697**: A service was installed in the system. |
| **Audit Sensitive Privilege Use** | **4672: Special privileges assigned to new logon.**<br>**4673: A privileged service was called.**<br><br>**4674: An operation was attempted on a privileged object.** |
| Audit Special Logon | **4964**: Special groups have been assigned to a new logon. |
| Audit User Account Management | **4720**: A user account was created.<br>**4722**: A user account was enabled.<br><br>**4723**: An attempt was made to change an account's password.<br><br>4724: An attempt was made to reset an account's password.<br><br>4725: A user account was disabled.<br><br>4726: A user account was deleted.<br><br>**4738**: A user account was changed.<br><br>4740: A user account was locked out.<br><br>**4765**: SID History was added to an account.<br><br>**4766**: An attempt to add SID History to an account failed.<br><br>4767: A user account was unlocked.<br><br>**4780**: The ACL was set on accounts which are members of administrators groups.<br><br>**4794**: An attempt was made to set the Directory Services Restore Mode. |

## Recommended DC Auditing

- Account Logon
  - Audit Credential Validation: Success & Failure
  - Audit Kerberos Authentication Service: Success & Failure
  - **Audit Kerberos Service Ticket Operations: Success & Failure**

- Account Management
  - Audit Computer Account Management: Success & Failure
  - Audit Other Account Management Events: Success & Failure
  - Audit Security Group Management: Success & Failure
  - Audit User Account Management: Success & Failure
- Detailed Tracking
  - Audit DPAPI Activity: Success & Failure
  - Audit Process Creation: Success & Failure
- DS Access
  - Audit Directory Service Access: Success & Failure
  - Audit Directory Service Changes: Success & Failure
- Logon and Logoff
  - Audit Account Lockout: Success
  - Audit Logoff: Success
  - Audit Logon: Success & Failure
  - **Audit Special Logon: Success & Failure**
- System
  - Audit IPsec Driver: Success & Failure
  - Audit Security State Change: Success & Failure
  - Audit Security System Extension: S&F Audit System Integrity : S&F

## Baseline Domain Controller Events to Log

This list should be the basis for event IDs logged on Domain Controllers as well as what type of information these provide.

| EventID | Description | Impact |
|---|---|---|
| 4768 | Kerberos auth ticket (TGT) was requested | Track user Kerb auth, with client/workstation name. |
| **4769** | User requests a Kerberos service ticket | Track user resource access requests & Kerberoasting |
| **4964** | Custom Special Group logon tracking | Track admin & “users of interest” logons |
| **4625/4771** | Logon failure | Interesting logon failures.  4771 with 0x18 = bad pw |
| 4765/4766 | SID History added to an account/attempt failed | If you aren’t actively migrating accounts between domains, this could be malicious |
| 4794 | DSRM account password change attempt | If this isn’t expected, could be malicious |
| 4780 | ACLs set on admin accounts | If this isn’t expected, could be malicious |

| | | |
|---|---|---|
| 4739/643 | Domain Policy was changed | If this isn't expected, could be malicious |
| 4713/617 | Kerberos policy was changed | If this isn't expected, could be malicious |
| 4724/628 | Attempt to reset an account's password | Monitor for admin & sensitive account pw reset |
| 4735/639 | Security-enabled local group changed | Monitor admin/sensitive group membership changes |
| 4737/641 | Security-enabled global group changed | Monitor admin/sensitive group membership changes |
| 4755/659 | Security-enabled universal group changed | Monitor admin & sensitive group membership changes |
| 5136 | A directory service object was modified | Monitor for GPO changes, admin account modification, specific user attribute modification, etc. |

Domain Controller Events to Monitor (Event Logs)

Here's a large list of Domain Controller Events to monitor:

- 4610 – An authentication package has been loaded by the Local Security Authority.
- 4611 – A trusted logon process has been registered with the Local Security Authority.
- 4616 – The system time was changed.
- 4624 – An account was successfully logged on.
- 4625 – An account failed to log on.
- 4634 – An account was logged off.
- 4648 – A logon was attempted using explicit credentials
- 4649 – A replay attack was detected.
- 4672 – Special privileges assigned to new logon.
- 4673 – A privileged service was called.
- 4674 – An operation was attempted on a privileged object.
- 4688 – A new process has been created.
- 4689 – A process has exited.
- 4692 – Backup of data protection master key was attempted.
- 4693 – Recovery of data protection master key was attempted.
- 4695 – Unprotection of auditable protected data was attempted.
- 4697 – A service was installed in the system.
- 4698 – A scheduled task was created.
- 4699 – A scheduled task was deleted.
- 4702 – A scheduled task was updated.

- 4706 – A new trust was created to a domain.
- 4707 – A trust to a domain was removed.
- 4713 – Kerberos policy was changed.
- 4716 – Trusted domain information was modified.
- 4717 – System security access was granted to an account.
- 4718 – System security access was removed from an account.
- 4719 – System audit policy was changed.
- 4720 – A user account was created.
- 4722 – A user account was enabled.
- 4723 – An attempt was made to change an account's password.
- 4724 – An attempt was made to reset an account's password.
- 4725 – A user account was disabled.
- 4726 – A user account was deleted.
- 4727 – A security-enabled global group was created.
- 4728 – A member was added to a security-enabled global group.
- 4729 – A member was removed from a security-enabled global group.
- 4730 – A security-enabled global group was deleted.
- 4731 – A security-enabled local group was created.
- 4732 – A member was added to a security-enabled local group.
- 4733 – A member was removed from a security-enabled local group.
- 4734 – A security-enabled local group was deleted.
- 4735 – A security-enabled local group was changed.
- 4737 – A security-enabled global group was changed.
- 4738 – A user account was changed.
- 4739 – Domain Policy was changed.
- 4740 – A user account was locked out.
- 4741 – A computer account was created.
- 4742 – A computer account was changed.
- 4743 – A computer account was deleted.
- 4754 – A security-enabled universal group was created.
- 4755 – A security-enabled universal group was changed.
- 4756 – A member was added to a security-enabled universal group.
- 4757 – A member was removed from a security-enabled universal group.
- 4758 – A security-enabled universal group was deleted.
- 4759 – A security-disabled universal group was created.
- 4760 – A security-disabled universal group was changed.
- 4764 – A group's type was changed.
- 4765 – SID History was added to an account.
- 4766 – An attempt to add SID History to an account failed.
- 4767 – A user account was unlocked.
- 4768 – A Kerberos authentication ticket (TGT) was requested
- 4769 – A Kerberos service ticket was requested
- 4770 – A Kerberos service ticket was renewed
- 4771 – Kerberos pre-authentication failed
- 4772 – Kerberos authentication ticket request failed

- 4774 – An account was mapped for logon.
- 4775 – An account could not be mapped for logon.
- 4776 – The domain controller attempted to validate the credentials for an account
- 4777 – The domain controller failed to validate the credentials for an account
- 4780 – The ACL was set on accounts which are members of administrators groups.
- 4782 – The password hash for an account was accessed.
- 4793 – The Password Policy Checking API was called.
- 4794 – An attempt was made to set the Directory Services Restore Mode.
- 4800 – The workstation was locked.
- 4801 – The workstation was unlocked.
- 4816 – RPC detected an integrity violation while decrypting an incoming message.
- 4817 – Auditing settings on an object were changed.
- 4865 – A trusted forest information entry was added.
- 4866 – A trusted forest information entry was removed.
- 4867 – A trusted forest information entry was modified.
- 4904 – An attempt was made to register a security event source.
- 4905 – An attempt was made to unregister a security event source.
- 4907 – Auditing settings on object were changed.
- 4908 – Special Groups Logon table modified.
- 4944 – The following policy was active when the Windows Firewall started.
- 4964 – Special groups have been assigned to a new logon.
- 5024 – The Windows Firewall Service has started successfully.
- 5025 – The Windows Firewall Service has been stopped.
- 5030 – The Windows Firewall Service failed to start.
- 5031 – The Windows Firewall Service blocked an application from accepting incoming connections on the network.
- 5033 – The Windows Firewall Driver has started successfully.
- 5034 – The Windows Firewall Driver has been stopped.
- 5035 – The Windows Firewall Driver failed to start.
- 5038 – Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
- 5148 – The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
- 5149 – The DoS attack has subsided and normal processing is being resumed.
- 5150 – The Windows Filtering Platform blocked a packet.
- 5151 – A more restrictive Windows Filtering Platform filter has blocked a packet.
- 5152 – The Windows Filtering Platform blocked a packet.
- 5153 – A more restrictive Windows Filtering Platform filter has blocked a packet.
- 5154 – The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
- 5155 – The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
- 5168 – SPN check for SMB/SMB2 failed.
- 5378 – The requested credentials delegation was disallowed by policy.

- 6144 – Security policy in the group policy objects has been applied successfully.

Expanded information on these events is available for download (DC-Events.xlsx or DC-Events.csv). The xlsx file includes hyperlinks.
Information in the csv/xlsx files includes:

- EventID
- Activity Logged
- Audit Category
- Auditing Subcategory
- OS Support
- Event Volume

Note that many of these are high volume, so evaluate by priority prior to ingesting in your SIEM of choice.

Microsoft provides guidance for Auditing

## Key Domain Controller Security Items

- Member servers should be fully patched before promoting to be a DC (issues like MS14-068 make this critical).
- You may be tempted to move Domain Controllers out of the default Domain Controllers OU, but don't do it. Domain Controllers in other OUs may receive different custom delegation and GPO settings.
- Create a new GPO for Domain Controller security (and link to the Domain Controllers OU).
- Run the Active Directory Best PRactices Analyzer every year to ensure Doamin and Domain Controller configuration is consistent. There are a number of best practice checks performed when run that identify potential issues.
- All patching and updating of DCs should be done separately from workstations and servers – meaning different updating architecture. Many organizations use WSUS to patch DCs and SCCM to patch everything else.
- Ensure that out-of-band (OOB) management passwords (DSRM password) are changed regularly & securely stored.
- Configure sub-category auditing and set to to be enforced via GPO ("Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings"). This way you have the security events you need to track changes and AD activity. Run "auditpol.exe /get /category:*" on the server to confirm proper auditing is enabled.
- Limit DC agents to the most critical, preferably none since every agent that's added to a DC provides another pathway to AD compromise. If an agent is necessary, whoever manages that product should be treated as a Domain Admin.
- If you have virtual DCs (and who doesn't?), treat the virtual admins as a Domain Admin.

- Configure the PDC to automatically synchronize time via GPO (https://blogs.technet.microsoft.com/nepapfe/2013/03/01/its-simple-time-configuration-in-active-directory/).
- Minimal groups (& users) with DC admin/logon rights.
- Change the default domain Administrator account at least 1x/year, preferably 2x.
- Change the KRBTGT account password at least 1x/year, preferably 2x. Each time, the password should be changed once, wait for replication (or the next day), and then change again (https://blogs.microsoft.com/microsoftsecure/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/).
- Configure AppLocker on DCs to only allow authorized applications to run. There shouldn't be much that runs on a DC, so this should be relatively easy.
- Set all admin accounts to "sensitive & cannot be delegated".
- Minimize the groups (& users) with DC admin/logon rights.
- Reduce/remove accounts & groups in Domain Admins, especially service accounts.
- Leverage admin workstations & admin tiering to protect admin accounts (https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/securing-privileged-access-reference-material)
- Only run software & services to support AD.
- Validate scheduled tasks & scripts.
- Add admin accounts to "Protected Users" group (requires Windows Server 2012 R2 Domain Controllers, 2012R2 DFL for domain protection).
- Default domain Administrator & KRBTGT password should be changed every year & when an AD admin leaves.
- Remove trusts that are no longer necessary & enable SID filtering as appropriate.
- All domain authentication should be set (when possible) to: "Send NTLMv2 response only\refuse LM & NTLM."
- Block internet access for DCs, servers, & all administration systems.
- Monitor scheduled tasks on sensitive systems (DCs, etc).

## References:


- Microsoft Security Documents: https://technet.microsoft.com/en-us/security/dn785092
- Best Practices for Securing Active Directory: https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
- Securing Active Directory: An Overview of Best Practices (Word doc download) https://www.microsoft.com/en-us/download/details.aspx?id=38815
- From the "Best Practices for Securing Active Directory" document, Securing Domain Controllers: https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack
- Microsoft Virtual Academy: Defending Active Directory Against Cyberattacks https://mva.microsoft.com/en-US/training-courses/defending-active-directory-against-cyberattacks-16327?l=Gj8k5XsSC_2004300474

- Recommended Auditing: https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
- The US government spends a lot of time putting together a secure baseline for different Operating Systems. I look at the security settings they recommend as a starting point and will sometimes lower the security they recommend (depending on the customer requirements) https://www.stigviewer.com/stig/windows_server_2012_2012_r2_domain_controller/
- There's also a STIG for Active Directory (2008 only for StigViewer.com): https://www.stigviewer.com/stig/active_directory_domain/