InCommon Silver with Active Directory Domain Services Cookbook

⚠ This Cookbook version was written to address the InCommon Identity Assurance Profile version 1.1 that has been deprecated. The Cookbook is being updated to reflect the changes in version 1.2.

Introduction

This document is intended to aid in configuring Active Directory Domain Services (AD DS, commonly referred to as "Active Directory") to meet the requirements of the InCommon Federation's Identity Assurance Profile (IAP) for Silver level of assurance. Only sections of the IAP where there is a challenge unique to AD DS are specifically addressed. For example, sections 4.2.3.2 and 4.2.3.3 of the IAP are *not* covered in this document because issues of brute-force guessing and password entropy pose no unique challenge to AD DS; like most authentication services AD DS has controls to enable password rotation, and mitigating features like account lockout, and configuring these controls to meet those IAP sections is an exercise that requires no knowledge unique to AD DS.

This document is intended to address real-world risk mitigation in a production AD DS forest in use in a higher education environment. As with any change to a production environment, customization of recommendations for your AD DS forest and its clients, careful planning, testing, impact assessment, communication and risk mitigation of the changes deemed necessary should be a part of your implementation of the recommendations of this cookbook. AD DS likely does not stand by itself in most higher education authentication and authorization infrastructures. Other authentication components in your environment which are out of the scope of this document should also be assessed for compliance with InCommon Silver. Any institution undertaking a Silver implementation project should carefully read the InCommon Identity Assurance Profiles and the Identity Assurance Assessment Framework (both available from the Assurance section of the InCommon web site). You should thoroughly understand these documents, and determine the remediations needed in your specific environment.

The recommendations of this document are challenging to implement in a production environment, but the authors believe it is possible to implement them in a reasonable amount of time given some dedicated project resources and a good plan. The size of your AD DS deployment, the types of clients connected to it, the number of customers served (and in what capacity they are served) represent some of the variables you will need to consider when allocating staff and other resources to your AD DS risk mitigation project.

Note that to the best of our knowledge, no institution has achieved Silver certification using the approach outlined in this document. It serves as a best effort by the authors to determine what it would take to configure an AD DS environment to pass an InCommon Silver audit. The intention is to update this cookbook with real-world experience as it becomes available. If you have experience implementing the recommendations of the cookbook, please consider contributing them by sending a note to: **assurance-adsilver at incommon dot org**.

IAP sections covered in this document:

- 4.2.3.4 Stored Authentication Secrets
- 4.2.3.5 Protected Authentication Secrets
- 4.2.5.1 Resist Replay Attack
- 4.2.5.2 Resist Eavesdropper Attack
- 4.2.5.3 Secure communication

We believe that many of the approaches documented in this cookbook are applicable to all versions of AD DS from Windows Server 2003 forward (with possible exception of the IPSec approach), although the exact steps to implement them may vary. The documentation below references Windows Server 2008 R2 settings.

For more information about the InCommon Assurance program, terms and definitions, and links to the IAP and IAAF documents and the FAQ, see the Assurance Resources section

Preamble
Securing AD DS and authentication traffic is vital to achieving Silver assurance. There are two strategies that can be employed to achieve secure authentication traffic with AD DS:

- Encryption on the wire via IPSec
- Require LDAP data signing

The reader can use either of these strategies to secure authentication traffic and which is chosen is up to the reader. More about these technologies is included in the appendices.

Alternatively, you can also achieve secure authentication traffic with AD DS by using encryption on the wire via LDAPS (TLS/SSL) but that approach only works for non-Windows clients, because Windows clients require LDAP traffic for some key functionalities. You can't require LDAPS (and turn off or block LDAP) if you have any Windows clients, so we haven't included this strategy as one of the primary options. See http://support.microsoft.com/kb/832017 for details on functionalities that Windows clients have which require LDAP (which LDAPS doesn't fulfill).

4.2.3.4 Stored Authentication Secrets

AD DS Problem Statement

The language in this section requires either a salted password to be hashed, or a non-salted password to be encrypted and only un-encrypted when immediately used for authentication, or a NIST Level 3 or 4 method.

On disk, AD DS stores all passwords in a hashed form, encrypted by the Password Encryption Key (PEK). The PEK is unique on each domain controller, and the PEK itself is encrypted by the syskey. It does not concatenate passwords with a salt to increase the entropy of the hash for the purposes of mitigating the risk of a dictionary attack on a stolen copy of the password file.

In memory, AD DS stores hashes of passwords. The encryption used with these hashes varies based on the type of password. NTLMv2 passwords use HMAC-MD5, NTLM passwords use RC4, and LM passwords (if enabled) use DES.

If enabled, the algorithm AD DS uses to store LM passwords is not a true one-way function as the password can be determined from the hash because of several weaknesses in its implementation. As such, if LM password hashes are enabled (they are disabled by default after WS2008), the AD DS will not meet this part of the IAP.

Even with LM password hashes turned off, AD DS doesn't meet any of the 3 alternative methods specified in the IAP, however, there are extenuating circumstances which greatly limit the risk. In specific, because a per-domain controller PEK encrypted by a syskey is used to encrypt the hashes at rest, a stolen copy of the password file would be difficult to use, unless operated on in its in-memory form. Getting the in-memory form of the hashes would be challenging provided adequate physical, network security, and where applicable, virtual machine security is in place.

AD DS Policies or Practices to Mitigate Risk

At rest protected stored secret risk mitigation:

Additionally employing BitLocker to encrypt the volumes on the DC which store secrets would provide even greater protections against unauthorized access at rest, but is likely unnecessary to meet Silver.

Entropy risk mitigation:

NOTE: This section of the IAPs requires a salt value to be combined with a password and then hashed, with the intent of increasing the entropy of the hashed password for the purposes of preventing an offline (dictionary or “rainbow table”-based) attack on a stolen copy of the password file. We believe that the IAPs are over-prescriptive in this area, and that other strategies for increasing the entropy of stored passwords should be acceptable. The ultimate determination for this acceptability lies with each institution, their auditors, the InCommon assurance review panel, the InCommon technical advisory committee and the InCommon steering committee. Because no institution has received approval to assert the Silver Identity Assurance Qualifier (IAQ) at the time of writing, and further no institution has achieved this with AD DS in the mix, there is no way of saying whether this approach will be sufficient. Any feedback or clarification that can be added to this section over time will help more institutions achieve Silver. Please send any feedback you have on this, including and especially success stories, to assurance-adsilver at incommon dot org.

Since any salt value must be well-known to some extent in order for passwords to be successfully verified across heterogeneous systems, a well-known salt value in the form of a username, a transformed username, a time value, constant, cyclical value or any other predictable permutation, does not provide much extra entropy to the hashes in a password file. We believe that requiring passwords with a level of entropy above that required at a minimum by the IAPs (14 bits of guessing entropy, 10 bits of “min” entropy across the password store) is achievable in a practical way, and should provide total entropy (entropy of the final hash to protect against a dictionary attack) at or above the level of the IAP entropy requirements plus a well-known salt value. Exactly how much extra entropy a well-known hash value adds (for example, the username- very well-known since it’s necessarily associated at some level with the password) and therefore how much extra entropy should be required above the minimum IAP requirements to achieve the spirit, if not the letter, of the requirements, is up to each institution.

Removal of insecure stored secrets:

Steps should be taken to disable storage of the LMHASH (by running Windows 7, Server 2008, and/or setting a GPO setting "**Network security: Do not store LAN Manager hash value on next password change"** to disable storage of the LMHASH, or requiring 15 character or greater passwords, since LMHASHes cannot be applied to passwords greater than 14 characters. Note that invalidating any stored LMHASH values after making these changes will require password changes for any subject for whom Silver is to be asserted. Further protection under this section is achieved by operating Syskey management in mode 2 or 3.

Preventing the storage of longterm shared secrets in LMHASH format in conjunction with a strict password policy will mitigate risk.

To disable the storage of LM hashes of a user's passwords in the local computer's SAM database by using Local Group Policy (Windows XP or Windows Server 2003) or in a Windows Server 2003 AD DS environment by using Group Policy in AD DS, follow these steps:

1. In Group Policy, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.

2. In the list of available policies, double-click **Network security: Do not store LAN Manager hash value on next password change**.

3. Click **Enabled**, and then click **OK**.

For a discussion of password length, complexity and "entropy" calculations, see Appendix F

Other Compensating Controls

Network Intrusion Systems (NIS), client and hardware firewalls protecting Domain Controllers, e.g. Forefront Endpoint Protection, MS Security Essentials, or your institutional NIS.

Sample Management Assertion(s)

(Fill in the blanks with your campus' parameters for use with your audit staff.)

Campus AD DS stores passwords encrypted with an industry-standard encryption method at rest (NTHASH - MD4) (in the form of syskey encryption) and the passwords are hashed using an industry standard hashing algorithm. Passwords for Silver subjects must be **[x]** length with **[y]** special characters and numbers, must be changed every **[z]** days and cannot be the same as the last **[n]** passwords, or contain any subset of the user's name or login name. We believe that this provides **[b]** bits of min entropy, which is more than the 10+**[e]** bits of min entropy required by the IAPs in the form of a sufficiently entropic password plus a well-known salt value (the username, for example) which provides only **[e]** bits of extra entropy. This provides more than the minimum entropy required by the IAPs, and is better than using the minimum entropy required plus a well-known salt value. We operate Syskey in mode **[2, 3]** to further protect the stored password secrets by requiring a secret to be **[typed, supplied on a floppy disk]** during Domain Controller bootstrapping.

4.2.3.5 Protected Authentication Secrets

AD DS Problem Statement
This section has three requirements:

- All stores involving secrets must meet operational requirements
- Transmission of secrets that are the same as those used in IdP applications must be protected
- Non-IdP applications should protect the secrets

The first requirement means that any store that stores these credentials, even if it is not the immediate verfier used by the IdP operation, is subject to the operational requirements in section 4.2.8 and also the requirements for stored secrets in 4.2.3.4.

The second requirement requires secrets for credentials which might be the same as those used in an IdP verification event in the context of a Silver assertion (not only in the context of such an assertion, but anywhere these credentials are used) to be sent via protected channels whether during initial provisioning, password set or reset, between verifiers, or between (IdP and other, non-IdP) applications and verifiers.

The third requirement, in the context of AD DS, means that AD DS computer clients and servers should not expose the secrets either via insecure storage or transmission. If application servers leverage the AD DS to proxy authentication, then the practices around how those application servers handle secrets is of concern.

These three requirements boil down to expanding the storage requirements and establishing transmission requirements around password secrets.

So in the context of AD DS, the transmission requirements mean that the domain to which Silver subject passwords are provisioned must comply with the requirements of these sections, and password traffic must take place via *protected channels. Protected channels* are defined in the IAAF as: "industry-standard cryptographic methods to provide integrity and confidentiality protection, resistance to replay and man-in-the-middle attacks, and mutual authentication." LDAP data signing or IPSec are examples of a protected channel, and is an acceptable method of password transmission for AD DS. According to our interpretation of this passage, Kerberos and NTLMv2 are also acceptable (see 4.2.5.1, 4.2.5.2 and 4.2.5.3, below).

In order to meet the requirements of this section of the IAP, policies must also be in place to require secure communications with AD DS *and any other verifier containing Silver usernames and passwords or an alternative credential that enable Silver credential issuance.* In the context of AD DS, there are two areas of concern:

- If the AD DS domain accepts alternative credentials (via the altSecurityIdentity mechanism) such as a cross-realm Kerberos trust or the use of an X.509 certificate to validate identity, then those external services and stores are subject to the requirements of section 4.2.8 and 4.2.3.4 if the alternate credentials are allowed to be used in the context of a Silver authentication event. To clarify: if you allow an X.509 certificate to be used for authentication to AD DS, but your IdP requires username and password, and does not allow use of the X.509 certificate for Silver authentication, the X.509 certificate and its storage and transmission is not in-scope for the purposes of 4.2.8 and 4.2.3.4. Conversely, if the X.509 certificate is allowed or required by the IdP for the Silver authentication, then it is fully in-scope.
- If clients cache credentials to enable automated logon, then the store of those cached credentials are subject to the requirements of section 4.2.8 and 4.2.3.4. There is a great diversity of possible client cache mechanisms, so analyzing all of those is outside what can be addressed here, however, the most common client cache in an AD DS environment, the Windows Credential Manager, relies on the Data Protection API which generally meets the standards.

AD DS Policies or Practices to Mitigate Risk
AD DS storage mitigation:

Ensure that any AD DS forest(s) and domain(s) that contain "silver" usernames and passwords meet the operational requirements of section 4.2.8, protect their secrets appropriately via complex hashed passwords and appropriate use of syskey, and specifically only allow connections via SSL/TLS, Kerberos, and possibly NTLMv2. Use the following GPO and/or firewall settings and syskey mode(s) **[2, 3]** to ensure this behavior.

AD DS transmission mitigation:

There are several possible alternate solutions:

- Require signed LDAP traffic by setting the following GPO setting: **Domain Controller: LDAP Server signing requirements=Enabled**
  Note: This may require deploying an additional GPO setting to clients, "**Network security: LDAP client signing requirements**", and require third party applications to be reconfigured to use SSL/TLS or signed SASL binds. This may have an adverse effect on the ability of Mac OS X and other clients to authenticate using the AD DS, so care must be taken in an enterprise setting when testing and communicating this change. http://support.microsoft.com/kb/823659 discusses some possible incompatibilities with doing this and Appendix B discusses one solution for Mac OS X clients.
- Use IPSec policies to force LDAP (port 389) traffic to be encrypted. Steps for creating an IPSec policy are documented on Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc730656.aspx

Application proxy authentication mitigation:

Ensure that applications that leverage your AD DS meet both the storage mitigation and transmission mitigation requirements.

Other Compensating Controls
If one or more of these settings would cause undue hardship in your community, risk mitigation via active network monitoring for the inappropriate activity (for example, LDAP binds in the clear) and following up with the responsible parties may be acceptable. In any event, active monitoring for these events is probably advisable. The institution should adopt security policies requiring secure communication of subject passwords by all applications that use them, and enforce this policy through monitoring and audit. This section specifically requires institutional policy around security requirements for authentication events. This policy, its details and enforcement are outside the scope of this document. Additionally, active network monitoring, auditing and following up with non-compliant parties may provide mitigation of risk, and appropriate GPO settings may further help to facilitate implementation of these policies.

Sample Management Assertion(s)

The institution's AD DS domain controllers are operated within the constraints placed on them by sections 4.2.5.1, 4.2.5.2., 4.2.5.3 and 4.2.8 (see assertions for the respective sections.) We have set forest-wide group policies **[place list of GPOs here]** that prevent unsecured binds and authentication via NTLMv1.

And/Or:
We actively monitor for unsecured authentication events on our network using the following intrusion detection system monitoring profiles **[place list of profiles here]** and follow up with any sources of unsecured authentication activity. We further monitor for usernames and passwords traversing the network in the clear from sources such as forms-based web page logins, and follow up with the sources of these events.

And:
We have an institutional policy requiring secure communication of authentication events for institutional network IDs: **[put link to institutional policy here]**. This policy is enforced by **[responsible party]** using **[audits, education, IDS rules, etc.]**

4.2.5.1 Resist Replay Attack

AD DS Problem Statement

AD DS allows a wide range of authentication methods by default, not all of which meet the requirement of preventing a replay attack from being successful. In particular, basic LDAP binds (in the clear) would allow harvesting of subject passwords if messages passing between a subject and verifier (AD DS domain controller) are intercepted, and NTLMv1 as a challenge-handshake authentication protocol does not provide strong resistance to replay attack. Other methods such as Kerberos, NTLMv2 and secure LDAP binds or LDAP binds using SSPI/Kerberos do provide resistance to replay attack, so a way to prevent or mitigate risk of the weaker authentication methods is desirable in an AD DS deployment.

AD DS Policies or Practices to Mitigate Risk

LM mitigation:

Set domain GPOs in any/all domains where Silver subject credentials can be stored/are provisioned that prevent use of NTLMv1 and prevent storage of LMHASHes. Set a workstation GPO at a domain level that prevents workstation storage of LMHASHes. See Microsoft TechNet: http://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx for an exhaustive discussion of the LanManCompatibilityLevel setting and how to set it. LanManCompatibilityLevel = 5 for domain controllers is what is being suggested here, and LanManCompatibilityLevel = 3 on all AD DS clients.

Additionally or alternatively, require Silver subject passwords/phrases to be >= 15 characters to prevent storage of cryptographically weak LMHASH values.

Note that invalidating any stored LMHASH values after making the above changes will require password changes for any subject for whom Silver is to be asserted.

Basic LDAP bind and LM mitigation:

There are two strategies that can be employed to secure all authentication (and non-authentication) traffic with AD DS:

- Encryption on the wire via IPSec
- Require LDAP data signing

If you choose LDAP data signing, you must configure "Domain controller: LDAP server signing requirements: Enabled", which will cause AD DS domain controllers to require all clients to negotiate signed LDAP traffic. http://support.microsoft.com/kb/823659 discusses some possible incompatibilities with doing this--also see Appendix B.

If you choose IPSec, you must require that all authentication traffic be encrypted using IPSec. This depends on forest functional level (must be Windows Server 2008 forest functional level); if lower OS DCs exist in a domain, then the least common denominator is used.

Kerberos mitigation:

Replay attacks are a concern for Kerberos environments. The risk can be mitigated by reducing the time skew allowed. More details are available here:

1. http://technet.microsoft.com/en-us/library/cc784130(WS.10).aspx
2. http://users.tkk.fi/u/autikkan/kerberos/AIWSC03_kerberos_replay_attacks.pdf

Other Compensating Controls

Have your IT security office or equivalent set up Intrusion Detection System (IDS) rules to monitor for NTLMv1 and/or basic binds in the clear and notify any services or sources of this traffic to your AD DS domain controllers, reduce traffic over time, then enact GPO-based policies as described above, and /or use institutional policy to stipulate use of secure authentication methods with your AD DS authentication service and any supplicant services (such as requiring SSL for web sites that use forms for logins, that authenticate against your AD DS.) Follow up policy with audits of services, especially those that exhibit noncompliant behavior.

Increase auditing of logon activites on domain controllers to detect replay attack attempts. More details are available on Microsoft TechNet: http://technet.microsoft.com/en-us/library/dd772658(WS.10).aspx

Sample Management Assertion(s)

Kerberos V uses a replay cache to protect against replay attack. When combined with an appropriate account lockout policy, this provides mitigation against replay attack since even in the unlikely event that someone hijacked a session by eavesdropping and replaying before the session originator had a chance to respond, repeated collisions between attacker and subject authentication should cause repeated account lockout, which should trigger a helpdesk call on the part of the subject. When combined with adequate password complexity from section 4.2.3.3 this makes it highly improbable an attacker could conduct a successful replay attack under section 4.2.5.1.

Secure LDAP binds using TLS are encrypted so are protected and acceptable. Likewise, requiring LDAP data signing encrypts the password data so are protected and acceptable.

Basic LDAP binds using SSPI for security that require Kerberos are acceptable because they use Kerberos for authentication, covered under the first paragraph of this assertion.

NTLMv2 is acceptable because it uses a fine-grained time value in the hashing process that the client must use to respond to the server challenge, to mitigate risk of a replay attack.

We disable NTLMv1 and basic unsecured LDAP binds by setting Group Policy Object settings **[x, y]**

4.2.5.2 Resist Eavesdropper Attack

AD DS Problem Statement

AD DS allows a wide range of authentication methods by default, not all of which meet the requirement of preventing an eavesdropper from gaining knowledge of a subject's secret in transit between the subject and verifier (AD DS domain controller). In particular, basic LDAP binds (in the clear) would allow harvesting of subject passwords if messages passing between a subject and verifier (AD DS domain controller) are intercepted, and NTLMv1 as a challenge-handshake authentication protocol does not provide strong resistance to a brute force attack. To be clear: in meeting the requirements of this section, mitigating NTLMv1 and LM traffic is not enough. You must also address the risk of LDAP binds in the clear. Other methods such as Kerberos, NTLMv2 and secure LDAP binds or LDAP binds using SSPI/Kerberos do provide resistance to eavesdropping or brute force attack, so a way to prevent or mitigate risk of the weaker authentication methods is desirable in an AD DS deployment.

AD DS Policies or Practices to Mitigate Risk

LM and NTLMv1 eavesdropper mitigation:

Set domain GPOs in any/all domains where Silver subject credentials can be stored/are provisioned that prevent use of NTLMv1 and prevent storage of LMHASHes. Set a workstation GPO at a domain level that prevents workstation storage of LMHASHes. See the following Microsoft TechNet article http://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx for an exhaustive discussion of the LanManCompatibilityLevel setting and how to set it. LanManCompatibilityLevel = 5 for domain controllers is what is being suggested here, and LanManCompatibilityLevel = 3 on all AD DS clients.

Additionally or alternatively, require Silver subject passwords/phrases to be >= 15 characters to prevent storage of weak LMHASH. As of Server 2008 R2, require signed LDAP binds, which will cause AD DS domain controllers to drop non-tunneled connections.

Note that invalidating any stored LMHASH values after making the above changes will require password changes for any subject for whom Silver is to be asserted.

All eavesdropper mitigation:

There are two strategies that can be employed to prevent eavesdropper attacks with AD DS:

- Encryption on the wire via IPSec
- Require LDAP data signing

If you choose LDAP data signing, you must configure "Domain controller: LDAP server signing requirements: Enabled", which will cause AD DS domain controllers to require all clients to negotiate signed LDAP traffic. http://support.microsoft.com/kb/823659 discusses some possible incompatibilities with doing this--also see Appendix B.

If you choose IPSec, you must require that all authentication traffic be encrypted using IPSec (with Authentication Header (AH) and Layer 2 Tunneling Protocol (L2TP)). This depends on forest functional level (must be Windows Server 2008 forest functional level); if previous versions of Windows Server OS domain controllers exist in a domain, then the least common denominator is used for forest functional level.

Other Compensating Controls

Have your IT security office or equivalent set up Intrusion Detection System (IDS) rules to monitor for NTLMv1 and/or basic binds in the clear and notify any services or sources of this traffic to your AD DS domain controllers, reduce traffic over time, then enact GPO-based policies as described above, and /or use institutional policy to stipulate use of secure authentication methods with your AD DS authentication service and any supplicant services (such as requiring SSL for web sites that use forms for logins, that authenticate against your AD DS.) Follow up policy with audits of services, especially those that exhibit noncompliant behavior.

Sample Management Assertion(s)

Secure LDAP binds using TLS are encrypted so are protected and acceptable.Likewise, requiring LDAP data signing encrypts the password data so are protected and acceptable.

Basic LDAP binds using SSPI for security that require Kerberos V are acceptable, because it is not possible to gain useful knowledge of the subject's secret from the messages exchanged during a Kerberos V authentication event.

NTLMv2 is acceptable because it uses a challenge-handshake authentication protocol that hashes the username and password together with a random salt in the response to the server challenge using MD5 to prevent a successful dictionary attack against the password in transit.

We disable NTLMv1 and basic unsecured LDAP binds by setting Group Policy Object settings **[x, y]**

The use of RADIUS with PEAP-MS-CHAPv2 is acceptable because PEAP establishes a TLS tunnel to protect the MS-CHAPv2 messages communicated between the RADIUS client and server.The use of MS-CHAPv2 alone is not acceptable as is it known to be cryptographically weak.

4.2.5.3 Secure communication

AD DS Problem Statement
While this section is focused at communication between the *Subject* and *IdP*, not the IdP and *Verifier*, it naturally extends to AD DS if AD DS is your source of credential verification, or (peripherally, via section 4.2.3.5) to AD DS if your Silver subject credentials are provisioned in AD DS or transit it in any way. As such, the requirements for section 4.2.3.5 cover this section of the IAP with regard to AD DS.

AD DS Policies or Practices to Mitigate Risk
See other sections of this document for acceptable strategies to mitigate risk in this context.

Other Compensating Controls
See other sections of this document for acceptable compensating controls.

Sample Management Assertion(s)
AD DS is not explicitly within the scope of this section of the IAP, but it follows that communication between AD DS and other systems should be appropriately protected. Management assertions in section 4.2.3.5 provide documentation of these protections.

Appendix A - Known Issues With NTLMv1 Disabled/LMHASH Storage Turned Off

Put any known issues/affected systems here, along with how you solved the problem, if possible.

See http://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx for an exhaustive discussion of the LanManCompatibilityLevel setting.

By default, Windows XP and earlier clients aren't compatible with DCs that have LanManCompabilityLevel=5. This means you must get all older Windows clients reconfigured. Domain joined computers can be easily addressed with group policy. Non-domain joined computers will require manual configuration or a script you provide.

Appendix B - Known Issues With Requiring Signed LDAP Binds

Put any known issues/affected systems here, along with how you solved the problem, if possible.

Cisco TMS doesn't support LDAPS. This is an application that integrates with AD DS to provide identity and access management. No resolution. Maybe newer versions will provide LDAPS support. Unclear if Cisco TMS supports LDAP signing.

While the Mac OS GUI claims it will enable LDAP signing by default, in practice, it doesn't. However, if you use Apple's dsconfigad command line tool with the switch "-packetencrypt ssl", you can tell the Mac OS to use LDAPS (i.e. employ LDAP over TLS/SSL). This protects Mac OS clients authentication traffic. This dsconfigad option can be used at the time of Mac computer domain join or it can be used after domain join to mitigate this issue.

Appendix C - Operational Considerations, Practices, Processes For Syskey Mode 2/3 Management

Put any known issues, operational considerations, process changes, etc., along with how you solved any problems here, if possible.

Appendix D - Definitions and Background

IPSec
Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over IP networks through the use of cryptographic security services. The Microsoft Windows implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPSec working group.

IPSec establishes trust and security from a source IP address to a destination IP address. The only computers that must know about the traffic being secured are the sending and receiving computers. Each computer handles security at its respective end with the assumption that the medium over which the communication takes place is not secure. Computers that only route data from source to destination are not required to support IPsec unless firewall-type packet filtering or network address translation (NAT) is performed between the two computers.

You can use the IP Security Policy snap-in to create, edit, and assign IPsec policies on a local computer and remote computers.

Kerberos
Kerberos is an authentication protocol which works on the basis of "tickets" to allow nodes on a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication - both the subject and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may employ public key cryptography by utilizing asymmetric keys during certain phases of authentication. (from Wikipedia)

LDAPS
LDAPS refers to encrypted LDAP communication achieved either by using an SSL tunnel (via LDAPv2) or by using the LDAPv3 Transport Layer Security (TLS) extension. Which method is used depends on what the client supports. The default port associated with LDAPS traffic is 636, and for AD DS global catalog traffic is port 3269. Strictly speaking, the term LDAPS was deprecated with LDAPv2, but in common usage it is also used to refer to TLS based encrypted LDAP traffic.

LMHASH
LM hash, **LanMan**, or **LAN Manager hash** was the primary hash that Microsoft Windows versions prior to Windows NT used to store subject passwords. Support for the legacy LAN Manager protocol continued in later versions of Windows for backwards compatibility, but was recommended by Microsoft to be turned off by administrators; as of Windows Vista, the protocol is disabled by default, but continues to be used by some non-Microsoft CIFS implementations. (from Wikipedia)

NTLM/NTLMv2
NTLM (**NT LAN Manager**) is a suite of Microsoft security protocols that provides authentication services. NTLM is the successor to the authentication protocol in Microsoft LAN Manager (LANMAN), an older Microsoft product, and attempts to provide backwards compatibility with LANMAN. NTLM version two (NTLMv2), which was introduced in Windows NT 4.0 SP4 (and natively supported in Windows 2000), enhances NTLM security by hardening the protocol against many spoofing attacks, and adding the ability for a server to authenticate to the client. (from Wikipedia)

SYSKEY
A tool used to configure the startup key, a random, 128-bit, symmetric cryptographic key created at system startup and used to encrypt all of the user`s symmetric cryptographic keys. Use SysKey with a password shared between two individuals (person A knows the first 8 charaters, person B knows the second 8 chracters). The steps for configuring SysKey are here:http://technet.microsoft.com/en-us/library/cc773183(WS.10).aspx

Appendix E- InCommon Assurance Framework Terminology

Credential Issuance
Credential Issuance is the process that binds the credential to the subject and enables the credential to be used by the subject. This process may or may not actually add the records associated with the credential to systems. With Windows AD DS, this may be accomplished by creating and enabling the user account, and conveying the password to the subject via a registration process that complies with the subject registration and credential issuance requirements of the IAP

Credential Revocation
Credential Revocation is the process that removes the binding of the credential from the subject and renders the credential non-usable by the subject. This process may or may not actually remove the records associated with the credential from systems. With Windows AD DS, this may be accomplished multiple ways:

- disabling the user account
- giving the user account an account expiration value in the past
- changing the password on the user account to a value unknown to the user (note that this is only acceptable as a temporary method of revocation--one of the other methods must be used before your password entropy/brute force period is exceeded)
- deleting the user account
- moving the user account to a directory which is configured to prevent Silver authentication, such as a correctly configured Active Directory Lightweight Directory Services (AD-LDS).

Appendix F - Password Entropy - Calculating it, what's needed, what's "good enough," etc.

While this topic is not specifically within the scope of this cookbook, it plays a big role in brute force and dictionary attacks against your credential store. NIST SP 800-63 Appendix A contains a lengthy discussion of Claude Shannon's notion of information entropy and complexity as it applies to passwords. We'll leave that discussion to that document. Here, we'll say that there are any number of ways to reach the required 1:16384 chance of guessing a password during its active life, and the 14 bits of entropy, against a targeted guessing attack, that are required by the Silver IAP. You can have longer, complex passwords that are active for a longer time, shorter, less complex passwords that are active for a shorter time, with more or less aggressive account lockout policies, etc. SP 800-63, the IAP document and an entropy calculation spreadsheet, such as http://www.infoworld.com/sites/all/themes/ifw/downloads/passwordcalc096.zip are good reference documents.

Appendix G - FAQ

(Please add any FAQ/Q&A type things you can think of with regard to AD DS here- if you have a question, please add it, and if you have an answer, please add it. They don't necessarily have to come in pairs, but we'll try to collaboratively fill in the blanks for each other.)

Caveat: We are not auditors, and we aren't the InCommon arbitration board, the TAC, or the steering committee (and we aren't even close to being FICAM.) So, take these Q&As as they are intended, as a best effort interpretation. These statements largely remain to be vetted by auditing/achievement of Silver.

Q: What is within scope for services based on AD DS? In other words, if I have AD DS on my campus, and the passwords are the same as passwords used by my IdP (even if the IdP doesn't directly authenticate against AD DS,) do I have to be concerned with the security of authentication events for every dependent service?

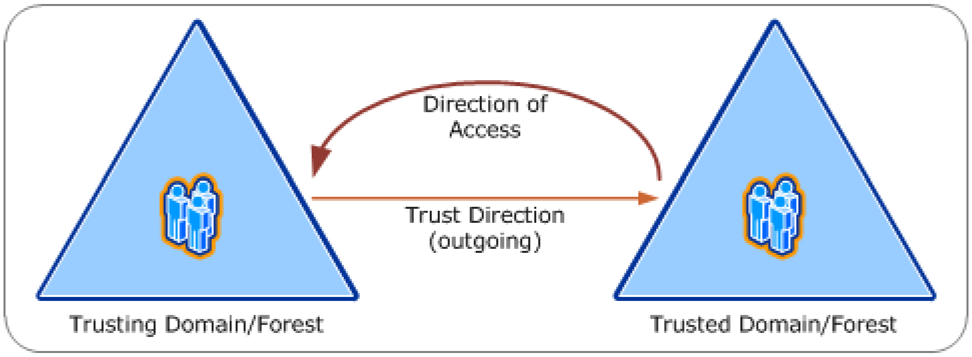
A: You should use common sense and best security practices in your assessment of the situation at your institution. Silver is Silver, it's not Gold or Platinum. If there are strategies you can use to detect direct simple binds to AD DS and prevent NTLMv1 connections, those are good things to do. You should probably have a strategy for following up with people doing simple binds and asking them not to do that. You may want to consider spot auditing owners of any kind of service ID that does any kind of authentication with your AD DS implementation, to make sure they aren't doing things like exposing passwords via unprotected forms authentication on web sites, etc. You can probably use a combination of institutional authentication policy, monitoring processes (such as intrusion detection system rules that look for simple LDAP binds) and spot checks to mitigate this risk adequately.

Q: What is the security boundary for an AD DS deployment?

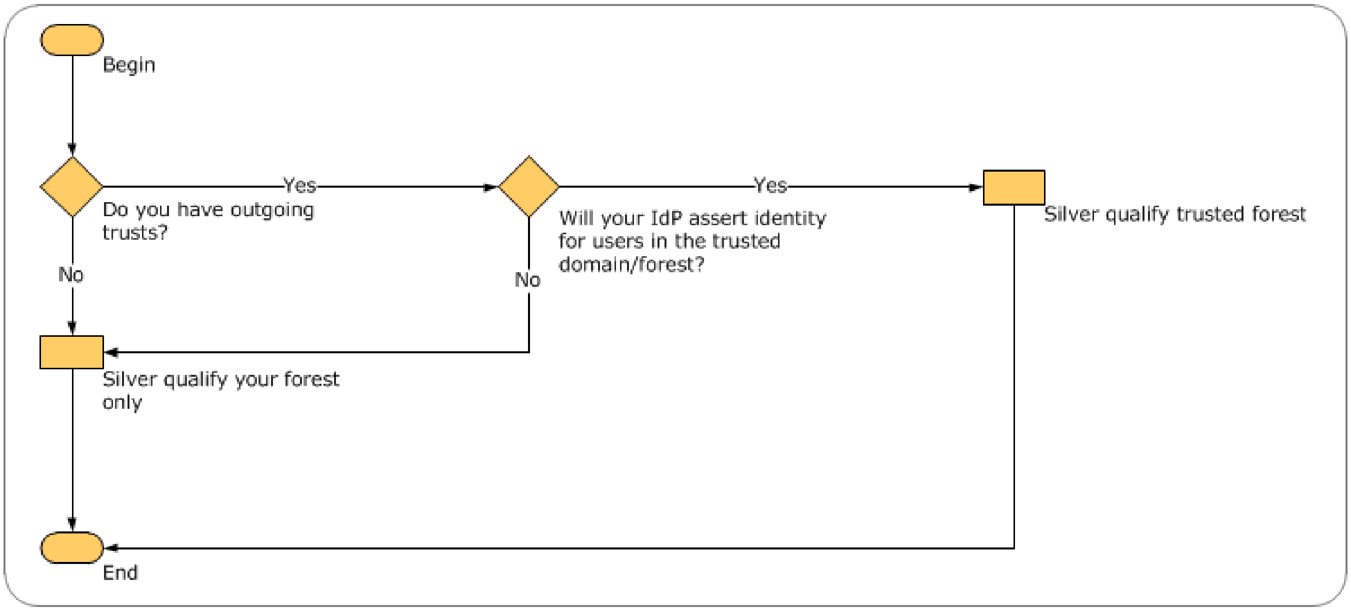
A: The security boundary is the forest, unless you have a domain or forest trust and you are the trust*ing* domain/forest. If you have a trust, and your IdP asserts identity for principals in the trusted domain or forest, then both forests are in-scope. For more information, see figures 1 and 2, below.

Figures

1 Basics of AD DS trusts (diagram by Brian Desmond)



2 Decision Flowchart for AD DS Domain/Forest Trust and Silver Compliance (diagram by Brian Desmond)


Begin
Do you have outgoing trusts?
Yes
No
Will your IdP assert identity for users in the trusted domain/forest?
Yes
No
Silver qualify trusted forest
Silver qualify your forest only
End

Version History

2011 May 5 - Initial work within the CIC CIOs Identity Management working group

2011 July 20 - CIC IdM Draft

2011 August 15 - InCommon Wiki Draft

2012 January 11 - InCommon Public Review Draft 1

2012 February 13 - Version 1.0

2012 March 26 - Version 1.1 (Post-IAM Online Feedback)

2012 August 9 - Minor changes to note that many of the approaches in the cookbook work from Windows Server 2003 forward