ABELMed Platform Setup Conventions

Introduction

1.1 Purpose of this document

The purpose of this document is to provide prospective ABELMed licensees and their hardware vendors with the information that they will require to prepare for the installation and operation of ABELMed. It will start with a brief overview of typical platforms, and then provide specific information that will be required to configure an ABELMed ready platform.

The ABELMed solution leverages many of the security features built into the Windows Operating system to help you meet your privacy and security responsibilities. If the platform is not prepared consistently with these conventions and recommendations it is likely to have security gaps and may not meet appropriate standards to protect health information.

The sections on configuration are moderately technical and intended primarily for the use of the hardware vendor or IT professional that will be configuring the system. These sections do not provide detailed instructions, it is expected that a competent IT professional will be familiar with these ubiquitous platforms, and understand the conventions. Some customers don't have IT professionals to help them setup their systems. They may have bought computers over the Internet or don't have local help available. For these customers we have recently added Section (6) to this document with more detailed instructions on the steps required to setup the system.

If you or your hardware vendor need clarification on any of the points, please call or email ABELSoft. We are happy to co-operate and work with you or your hardware vendor to ensure that you get all the information required to get your system setup for ABELMed.

1.2 General Platform Overview

ABELMed runs on Microsoft Windows operating systems, and uses the Microsoft SQL Server database. ABELSoft can bundle RUNTIME licenses for MS SQL Server with your ABELMed licenses. ABELMed is designed to scale from small peer-to-peer networks with few workstations, to larger domain networks in busy clinics with dedicated servers serving administrative and clinical workstations in examination rooms.

The smaller networks, with less than 5 workstations for example, can be served by a workgroup consisting entirely of computers running the Microsoft Windows 10 operating system.

On networks with 5 or more workstations, a file server with the Microsoft Windows Sever 2016 operating system is recommended. The Windows Server 2016 operating system supports larger networks and advanced features such as Active Directory security domains, disk mirroring, terminal services, as well as many other features and tools. Some practices with less than 5 workstations may still opt for a dedicated server running the server version of the operating system in order use active directory, disk mirroring, or other such features.

1.3 How to proceed

ABELSoft recommends that when looking into purchasing your hardware, operating system and other software for ABELMed that you get at least three quotes. Please make sure that you provide the ABELMed hardware "Platform Requirements" tables, and these setup conventions, so that the hardware vendor can include setup to these conventions in the price that you are quoted. Current platform requirements and setup conventions are

always available on the ABELSoft website at http://www.abelsoft.com . Some customers may opt to purchase their own hardware from vendors that do not provide setup and installation services. In such cases you may require the services of a technician who understands these setup conventions and configure the system(s) in conformance with the conventions.

If you are dealing with a hardware vendor that you have not worked with in the past, ABELSoft recommends checking references. In many areas ABELSoft can provide the names of hardware vendors who have prepared ABELMed systems in the past.

The IT person setting up the systems should read this full document before setting up the systems. The conventions are not necessarily in the order that they will be performed; rather they are grouped by subject (Servers, Database, Clients, etc.).

ABELMed Platform Setup Conventions

Server Setup Conventions

2.1 Operating system

2.1.1 Windows Server 2016 /Windows Server 2012 R2

2.1.1.1 Setup

Please conform to the following conventions when setting up a Microsoft Windows 2016 Server.

- We recommend that an Active directory domain be set up with Remote Desktop Services.
- We recommend using the NTFS file system.
- Encrypt the disks using BitLocker with AES and a 256-bit key. (Encryption is mandated by OntarioMD)
- Setup TCP/IP as the network protocol. Configure a DHCP server to assign the IP addresses to client workstations and ensure the server has a static IP address. ABELSoft recommends a router with a firewall on all high-speed Internet connections.
- Name the Server using the customer's ABELSoft client ID number. For example, if the ABELSoft customer ID number is C09999-OMG, name the server C09999. You can obtain the customer ID number by contacting ABELSoft's sales department.
- An Active directory domain is normally set up if using Windows Server 2016. With AD, user accounts only have to be set up on the server, not on each workstation.
- Create an account for each user.
- Create an **ABELMed Users** security group
- Ensure that each account has a password set. The users should change their passwords upon first login.
- Disable the guest account.
- Set a strong password for the Administrator account. Make sure that the appropriate person at the office or clinic has this password. Normally the dentist, office manager, or IT person. This may be required if an ABELSoft representative is providing technical support remotely.
- Navigate to your ABELMed installation directory. Right-click and select Properties>Security tab>select Users>uncheck Full Control.
- For remote support purposes, a high-speed internet connection is required.
- If ABELMed will ever be run on the server, set the display resolution to at least 1280x1024.
- Install the most recent service packs for the server operating system, including all critical patches and hotfixes from Microsoft.
- Turn off any CPU power saving features and disable hibernation. Screensavers are not an issue.
- Install the latest drivers for all printer(s) in the office if using Remote Desktop Services to allow for proper printer redirection.

ABELMed Platform Setup Conventions

- Install and configure any required backup programs. ABELSoft recommends the backup program bundled with Windows Server 2016, or a secure online backup service.
  Backup jobs should be configured:
    - To perform a Full System backup with System State,
    - To perform Data only backups. This will have to be setup after ABELMed is installed. ABELSoft recommends that the ABELMed folder and its sub-folders be backed up. Some backup programs have SQL plug-ins that have the ability to backup the SQL databases directly
    - To backup on a schedule. Most customers will have enough space available on media to perform a full backup with system state on a daily basis. This is recommended for small offices without an on-site IT person to ensure that all data from all applications is backed up. More sophisticated backup rotations can be set up if and when space becomes an issue.
    - A regular user will not have appropriate privileges to perform full system backups; any users that perform backups will have to be added to the Backup Operator's group.

  Important notes pertaining to backups:
    - If using an online backup service it is important to ensure that data is fully encrypted while traveling over the Internet and in storage. If you have encryption keys make sure they are kept in a safe place and that appropriate people have access to them
    - If backing up to removable media the removable media must also be encrypted. Again any passwords/encryption keys must be kept safely.
- If the customer has a high-speed Internet connection it is recommended that Automatic Updates be turned on.
- Setup the default group policy for the domain to:

  Note: Setting these policies is mandatory in order to meet OntarioMD and CCHIT/HHS certification standards however the exact numbers can be decided by each practice. Our recommended values are below. The audit policies are mandatory.
    - Maximum password age enabled for 90 days
    - Password must meet complexity requirements
    - Enable Enforce Password History set to 24
    - Account lockout duration set to 15 minutes
    - Account lockout threshold enabled for 3 attempts
    - Reset account lockout counter set to 15 minutes
    - Audit account logon events enabled for success/failure
    - Audit account management enabled for success/failure
    - Audit logon events enabled for success/failure
    - Audit object policy enabled for success/failure

- Audit policy change enabled for success/failure
- Screen saver password protected enabled for 3 minutes
- Network security: Do not store LAN Manager hash value on next password change to enabled

- If not already done by default, turn off unnecessary Services such as Messenger, IIS (If it will not be needed) and FTP. If using these services, do not allow anonymous access.
- Install and configure a reputable Anti-Virus Product. Set it up to automatically receive updates regularly. It should be configured for real-time scanning and for at least 1 full disk scan per week.

2.1.1.2 Testing

- Test Remote Desktop Services.
- Test Windows printing from all workstations, to all printers to which they will need to print.

2.1.2 Windows 10 File Server

2.1.2.1 Setup

Please conform to the following conventions when setting up a Windows 10 File server in a thick-client scenario.

- We recommend using the NTFS file system.
- Encrypt the disks using BitLocker with AES and a 256-bit key. (Encryption is mandated by OntarioMD)
- Setup TCP/IP as the network protocol. We normally configure TCP/IP to obtain an IP automatically. ABELSoft recommends a router with a firewall on all high-speed Internet connections. The router if available usually does DHCP. If there is not a router, Windows 10 will use Automatic Private IP Addressing (APIPA).
- Name the computer with the customer's ABELSoft client ID number. For example if the ABELSoft customer ID number is C09999-OMG, name the server C09999. You can obtain the customer ID number by contacting ABELSoft's sales department.
- Turn off sharing wizard/simple file sharing. Open Windows Explorer>File>Change folder and search options >Go to the view Tab>Uncheck "Use Sharing Wizard" at the bottom. While you are here also uncheck "Hide extensions for known file types". On older operating systems, this can be accessed under Tools>Folder Options.
- Create an account for ABELMed users. An account can be set up for each user, but you should be aware that this account would have to be set up on all client machines from which the user will be running ABELMed. This will require a little more ongoing maintenance to administer the accounts when you have staff changes. It is up to individual customers to decide what is best for their practice. Certified Solutions require accounts for each user.
    - Create an ABELMed Users security group
    - The ABELMed users should not be part of the Administrator group.
    - Ensure that each account has a password. The users should change their password the first time they log in.
- Disable the guest account.

ABELMed Platform Setup Conventions

- Put a strong password on the Administrator account. Make sure that the appropriate person at the office or clinic has this password. Normally the dentist, office manager, or IT person.
- Navigate to the ABELMed installation folder. Right-click and select Properties>Security tab>select Users>uncheck Full Control
- For remote support purposes, a high-speed internet connection is required.
- Set the display resolution to at least 1280x1024.
- Install the most recent service packs for the server operating system, including all critical patches and hotfixes from Microsoft.
- Turn off any CPU power saving features and disable hibernation. Screensavers are not an issue.
- Install the latest drivers for all printer(s) and any other devices and peripherals.
- Install and configure any required backup programs.
  Backup jobs should be configured:
    - To perform a Full System backup with System State,
    - To perform Data only backups. This will have to be setup after ABELMed is installed. ABELSoft recommends that the ABELMed folder and its sub-folders be backed up. Some backup programs have SQL plug-ins that have the ability to backup the SQL databases directly
    - To backup on a schedule. Most customers will have enough space available on media to perform a full backup with system state on a daily basis. This is recommended for small offices without an on-site IT person to ensure that all data from all applications is backed up. More sophisticated backup rotations can be set up if and when space becomes an issue.
    - A regular user will not have appropriate privileges to perform full system backups; any users that perform backups will have to be added to the Backup Operator's group.

  Important notes pertaining to backups:

    - If using an online backup service it is important to ensure that data is fully encrypted while traveling over the Internet and in storage. If you have encryption keys make sure they are kept in a safe place and that appropriate people have access to them
    - If backing up to removable media the removable media must also be encrypted. Again any passwords/encryption keys must be kept safely.
- If the customer has a high-speed Internet connection it is strongly recommended that Automatic Updates be turned on.
- If not already done by default, turn off unnecessary Services such as Messenger, IIS (If it will not be needed) and FTP. If using these services, do not allow anonymous access.
- Install and configure a reputable Anti-Virus Product. Set it up to automatically obtain updates regularly. It should be configured for real-time scanning and for at least 1 full disk scan per week.
- Setup the group policy to:

Note: Setting these policies is mandatory in order to meet CCHIT and OntarioMD certification standards however the exact numbers can be decided by each practice. Our recommended values are below. The audit policies are mandatory. In a Windows 10 based peer-to-peer or workgroup environment this policy must be established on each machine.

- Maximum password age enabled for 90 days
- Password must meet complexity requirements
- Enable Enforce Password History set to 24
- Account lockout duration set to 15 minutes
- Account lockout threshold enabled for 3 attempts
- Reset account lockout counter set to 15 minutes
- Audit account logon events enabled for success/failure
- Audit account management enabled for success/failure
- Audit logon events enabled for success/failure
- Audit object policy enabled for success/failure
- Audit policy change enabled for success/failure
- Screen saver password protected enabled for 3 minutes
- Network security: Do not store LAN Manager hash value on next password change to enabled

2.1.2.2 Testing

- Test Remote Desktop Services.
- Test Windows printing.

2.2 Database

2.2.1 SQL Server 2016

Install SQL Server 2016 and prerequisites before installing ABELMed. Remember to install all Service packs and hotfixes for SQL Server 2016. ABELMed uses Windows authentication.

The ABELMed installation will create the required databases and apply the required permissions for client workstations to access the data. It also creates a shortcut, under Start>All Apps>ABELMed Administration. This shortcut will run a script to automate the creation of typical maintenance schedules and backup jobs.

ABELMed Platform Setup Conventions

Client Machine Setup

3.1 Windows 10 client machine

3.1.1 Setup

Please conform to the following conventions when setting up Windows 10 client machines:

- We recommend using the NTFS file system.
- Setup TCP/IP as the network protocol. We normally configure TCP/IP to obtain an IP automatically. ABELSoft recommends a router with a firewall on all high-speed internet connections. If there is not a router, Windows 10 will use Automatic Private IP Addressing (APIPA).
- Name the computer with the customer's ABELSoft client ID number followed by a hyphen and a numeric extension. For example if the ABELSoft customer ID number is C09999-OMG, name the first client machine C09999-1, the second client machine C09999-2, and so on…
- Turn off sharing wizard/simple file sharing. Open Windows Explorer>File>Change folder and search options >Go to the view Tab>Uncheck "Use Sharing Wizard" at the bottom. While you are here also uncheck "Hide extensions for known file types". On older operating systems, this can be accessed under Tools>Folder Options.
- Create account(s) for ABELMed users. The Account names and passwords must exactly match the account(s) created on the server.
    - The users should not be part of the administrator group; they should be part of the Users group.
    - You can create a group for ABELMed users but on most systems, all regular users will be ABELMed users so the regular users group can be used instead.
    - Ensure that each account has a password. The users should change their password the first time they log in. (this will have to be done for each user on all machines).
- Disable the guest account.
- Put a strong password on the Administrator account. Make sure that the appropriate person at the office or clinic has this password. Normally the dentist, office manager, or IT person.
- Set the display resolution to at least 1280x1024.
- Install the most recent service packs for the server operating system, including all critical patches and hotfixes from Microsoft.
- Turn off any CPU power saving features and disable hibernation. Screensavers are not an issue.
- Install the latest drivers for all printer(s).
- If the customer has a high-speed Internet connection, it is recommended that Automatic Updates be turned on.
- Turn off unnecessary Services such as Messenger, IIS (If it will not be needed) and FTP. If using these services do not allow anonymous access. Note that some practices use ABEL's case presentation software & will need IIS.

- Install and configure a reputable Anti-Virus Product. Set it up to automatically obtain updates regularly. It should be configured for real-time scanning and for at least 1 full disk scan per week.

3.1.2 Testing

- Test Windows printing from all workstations.
- Make sure that the client machine can connect to the server and access shares created on the server. If you create test shares, please remember to remove them when you are through.

ABELMed Platform Setup Conventions

Compatibility and setup with Firewalls, Anti-Virus and Security Suites

4.1 Setting up Firewall Appliances

The specific instructions for setting up Firewalls vary with make and model and often require certified specialists. Most ABELMed communication is internal on the LAN with some exceptions for Lab and prescription communication. In multi-site installations additional ports may have to be opened up to allow ABELMed communication. Specific requirements on such communication vary widely depending on the specific architecture of your setup. The following table details the types of communication used by ABELMed and what ports may have to be opened up.

Service or Function	Port	Protocol	Reason required
MS SQL	1433 **incoming**	TCP	To communicate with the SQL server. Do not open this port up to the Internet. If clients and servers are separated by a firewall port on the LAN, or a software firewall, this port may need to be opened locally.
File and Printer sharing Windows NetBIOS	139 **incoming** 445 **incoming** 137 **incoming** 138 **incoming**	TCP TCP UDP UDP	To save data to and retrieve data from the file share. Do not open these ports up to the Internet. If clients and servers are separated by a firewall port on the LAN, or a software firewall, these ports may need to be opened locally.
ABELMed licensing	5093 **incoming**	UDP	Only when thick clients with floating licenses are operating through the firewall without a VPN.
ABELMed Portal	1506 **incoming**	TCP	If subscribed to ABELMed portal.
Thin Client / Terminal Services[1]	3389 **incoming**	TCP	To run the Remote Desktop Client control.
HTTP/HTTPS	80 **outgoing** 443 **outgoing**	TCP TCP	If the physicians require Internet access for clinical research then the physician would typically access information by visiting web sites with a browser. The articles would typically be in html, pdf, or word format. Occasionally the information would be delivered as a chargeable or restricted service over an SSL secured web site.
HTTP/HTTPS	80 **incoming** 443 **incoming**	TCP TCP	For remote support (to customers with an Internet connection) ABELSoft uses a tool called GoToAssist (http://www.gotoassist.com).No ports need be kept open to allow incoming traffic on the firewall as the session is initiated inside by the customer going to ABELSoft's web site (http://www.abelmed.com) and following the link to the remote support server website (http://www.gotoassist.com/sb/abelsoft) to enter the appropriate session code. Many firewalls only block incoming traffic, and allow outgoing connections on all ports. In cases where outgoing traffic is also restricted the customer will require outgoing access on ports 80 (TCP) & 443 (TCP) to connect to the remote support session. The full session from the form where the session code is entered is encrypted using 128 bit SSL encryption. Port 443 is also used for communication with Lab Interface & Surescripts Interface.
FTP/SFTP	22 **outgoing**	TCP	Electronic claims submission
NTP/SNTP	123 **outgoing**	UDP	Client/server workstation time synchronization.

[1] – This port is optional. Terminal Services communication is on port 3389/TCP. In the event that Terminal Services/ Remote Desktop is used to run ABELMed PM-EMR remotely client software then these ports must be opened on the firewall. However if the Remote Desktop session is run within a VPN connection this is not necessary. ABELSoft recommends the VPN approach to any customers operating ABELMed PM-EMR over a high speed Internet connection.

4.2 Anti-Virus

It is not practical for ABELSoft to test large numbers of Anti-virus programs, as there are many such programs on the market. We routinely check several of the more popular AV utilities with the latest version of ABELMed. We post our findings in the table below. Always check the online version of this document to ensure that you are reading our most recent findings.

ABELSoft does NOT exclude our program or data areas from scanning on production systems. Such exclusions should not be necessary.

The following products have been tested with ABELMed ver. 12

Product	Results	Workaround steps if required
Symantec Endpoint Protection 12	No Known Problems	n/a
Microsoft Security Essentials	Does not install to Windows Server 2016/2012 R2.	n/a
Windows Defender	No known problems. Ships with Windows 10, Windows Server 2012R2/2016.	
Kaspersky Small Office Security 3	Built-in firewalling and network heuristics cause problems with MS SQL and ABELMed licensing.	Add appropriate exceptions in firewall, exclude ABELMed application from heuristic scanning.
Avast	File scanner causes problems with ABELMed executables during launch.	Add exclusions for ABELMed executables.

Table last Updated December 24th, 2015 – check website for most recent version.

4.3 Known problems with Firewalls and steps to mitigate

ABELSoft does not perform regular testing with the various software firewalls included with many consumer Internet security suites. ABELSoft recommends routers or firewall appliances at the perimeter. Some people prefer software-based firewalls as well. Such devices might be desirable on larger networks where threats from within the perimeter protection are more likely. In such cases ABELSoft recommends the Windows Firewall included with all recent Microsoft operating systems. The following has been found to work.

Product	Results	Workaround required

Microsoft Windows Firewall	Tested. Client unable to get license.	Must add exceptions in firewall for all required ports. See table at end of document for required ports.
Norton Internet Security	Limited testing in the field.	Must add exceptions in firewall for all required ports. See table at end of document for required ports.
Kaspersky Small Office Security 3	Extensive testing	Must add exceptions in firewall for all required ports. See table at end of document for required ports.

ABELMed Platform Setup Conventions

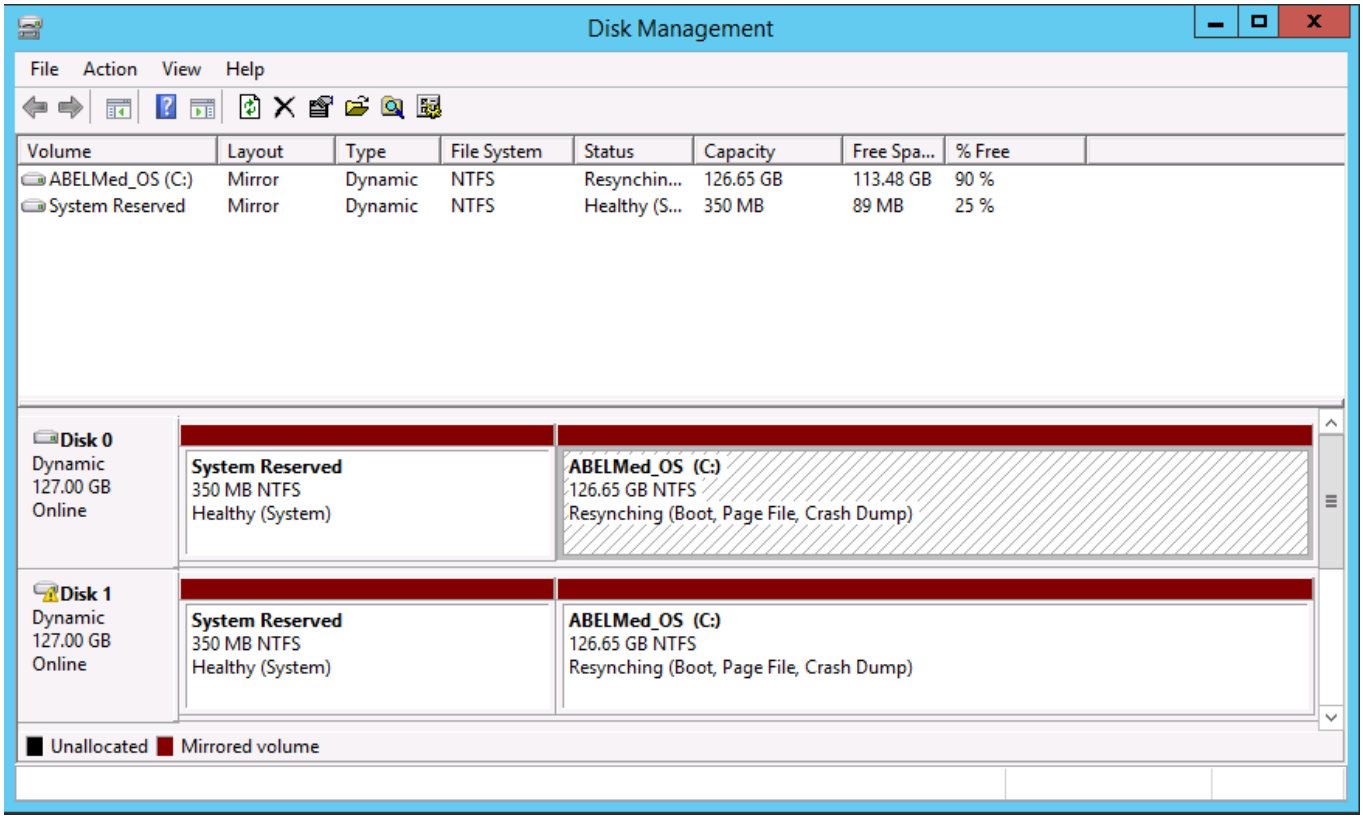
Protecting Health Information and system Reliability

5 Standards to Protect Data and Increase System Reliability

One of the strongest advantages of operating on industry standard platforms such as Microsoft Windows based operating system on Intel (or compatible) hardware platforms is that there are many technologies available that can be leveraged to increase the reliability of your system, reduce downtime, and protect your data. This section briefly discusses a few of these options that ABELSoft recommends that you consider implementing.

5.1 Disk Mirroring and RAID Arrays

The risk of data loss in the event of a server hard disk failure is mitigated by Windows ability to mirror the disks. In the event of a disk failure the remaining disk continues to work until such a time as it is convenient to replace the failed disk and re-establish the mirror set.



5.2 Backups

In the event of data corruption, hard disk failure, or other failure that results in the loss of access to the EMR, ABELSoft would have to recover the client's most recent backup(s). ABELSoft users typically use the Backup Utility for Windows that is supplied with Windows Server 2016, but ABELMed has the flexibility to work with most backup programs and backup services on the market should the customer prefer. Detailed backup & recovery procedures are provided in the ABELMed manual.

5.3 Encryption

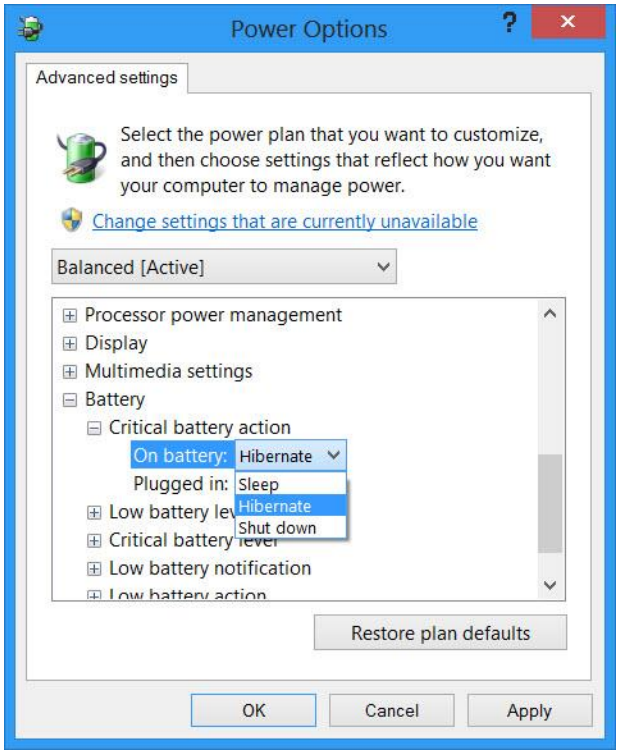
Strong encryption is required on any disks containing PHI. 256bit AES is the current standard. Computer hard disks, removable backup media, and media that data is exported to all need to be encrypted. There is more information on the MyABEL.com site https://www.myabel.com/MedicalCDN/DataEncryption .

5.4 Multi Factor Authentication

ABELMed leverages the industry standard Microsoft Windows operating system for authentication, password rules, etc. There are several products available that provide two factor authentication for Windows logins. Given the very sensitive nature of Protected Health Information, and the high risk and cost of privacy breaches, we recommend implementing one of these technologies to strengthen security around user authentication in your practice.

5.5 Uninterruptable Power Supplies

The risk of data loss in the event of a power outage that extends beyond the capacity of the battery, to provide adequate power, is mitigated by Windows' built in ability to monitor power status & UPS battery state. Windows can be configured to notify users and perform an orderly shutdown, preventing data loss.



5.6 Updates

The importance of installing Windows Updates

Most Windows updates include security updates. Security vulnerabilities can be exploited by malware or hackers. These types of situations are regularly identified in various parts of Windows – ActiveX, Internet Explorer and .Net Framework are just examples. These vulnerabilities are eliminated by Windows updates.

Other updates address other bugs and issues in Windows. Even though they are not responsible for security vulnerabilities, they might impact the stability of your Operating System, or impact applications you are using.

Windows Updates also come with new features, while patching some known issues.

Most computers should have Windows Updates set up to “Install Updates Automatically”, which is the recommended setting. However, you also have the option of manually checking for updates if preferred.

5.7 Security Monitoring

ABEL recommends business grade router/firewall appliances that have features like Intrusion Detection and Intrusion Prevention capability IDS/IPS. While having such appliances in place helps it is best not to “set it and forget it”. Ideally monitoring and checking of alerts and logs, both appliance and computer logs, should be a regular ongoing practice. This allows detection follow-up and adjustment when required. When such activity is performed regularly and properly documented, incidents can be quickly detected and acted upon. There will be no question that you have been performing your “due diligence” should a breach occur. Most practices do not have suitable expertise on staff to review these alerts and logs. Third party Managed Detection and Response (MDR) services are recommended for this role.

5.8 Additional Technologies

ABELMed PM - EMR has been designed work on the Microsoft Windows platform. These platforms have many such features incorporated into the operating system. The Windows platform also interoperates with many third party products, both hardware and software, that can be used to mitigate risk and protect data. The level of fault tolerance can be configured to match the requirements of the health care provider.

In addition to hardware and software solutions there are many services available to help protect your Windows system. These include such services as Online Data Backups as well as Remote Monitoring and Administration. ABELSoft can help you with such services.

ABELMed Platform Setup Conventions

Appendix A - Detailed Steps on the security settings described above

This section provides detailed steps for configuration of the security settings and group policy settings mentioned above for technicians or customers who may not be familiar with them. Steps may vary slightly depending on OS version.

6.1 Creating ABELMed Users Group and User Accounts

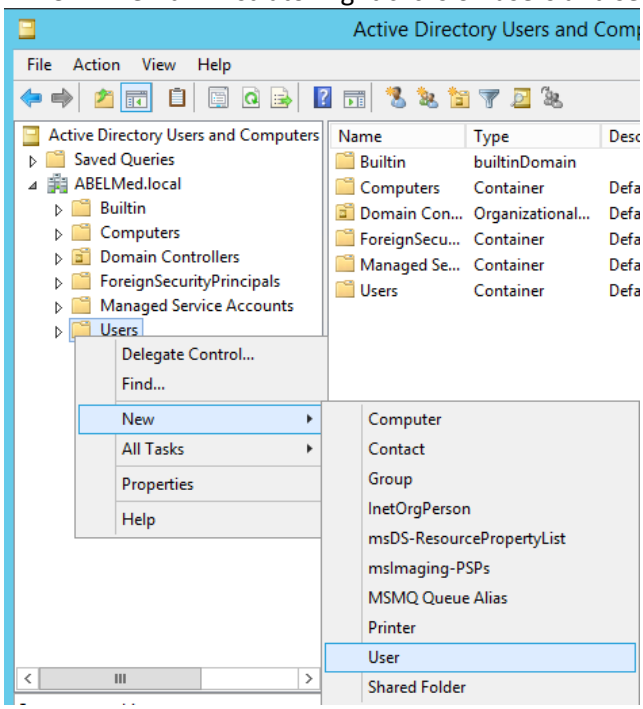
This section covers the initial user setup that would normally be performed by the hardware vendor or IT department before ABELSoft comes out to do the installation. The ABELMed administrator will set these users up as members in ABELMed and configure the appropriate levels of privilege in ABELMed. Ongoing administration including deletion and modification of user accounts is covered in the ABELMed user's manual.

Initially we recommend that an ABELMed Users Group be setup.

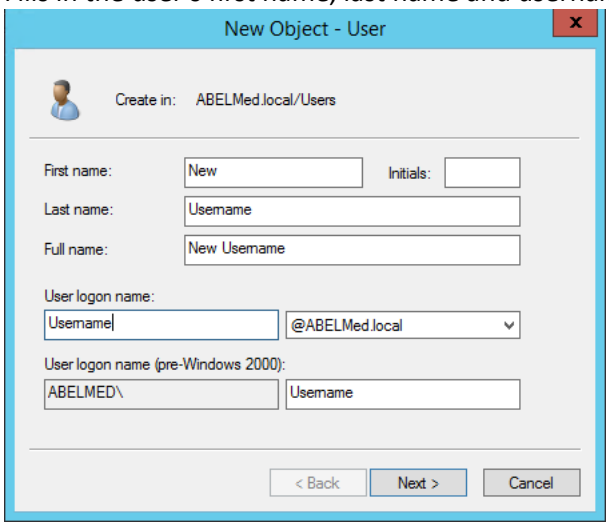
1. Log in on the server.
2. Select **Start> Active Directory Users & Computers**
3. Right click on users and selects **New > Group** from the pop out menus
4. Fill in the group name ABELMed Users
5. The Scope of the Group is normally the **Domain local**
6. The Type of Group is **Security**

Each user is set up in Windows with a username matching the member's username in the ABELMed Authentication Manager. The typical steps on a Windows 2016 Server would be as follows:

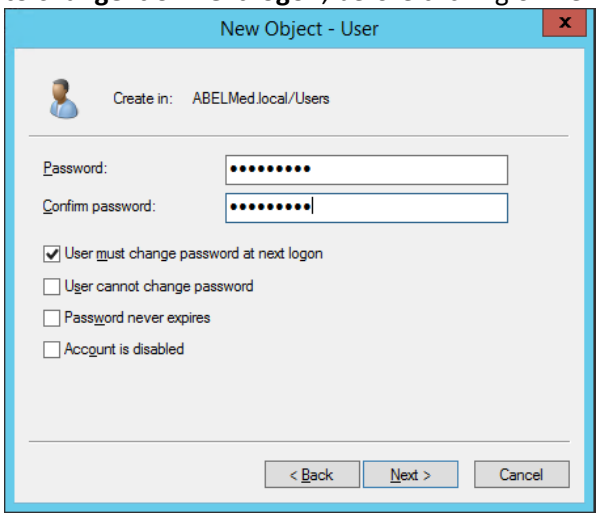
1. Log in on the server.
2. Select **Start> Active Directory Users & Computers**
3. The Administrator right clicks on users and selects **New > User** from the pop out menus



4. Fills in the user's first name, last name and username then click on next.

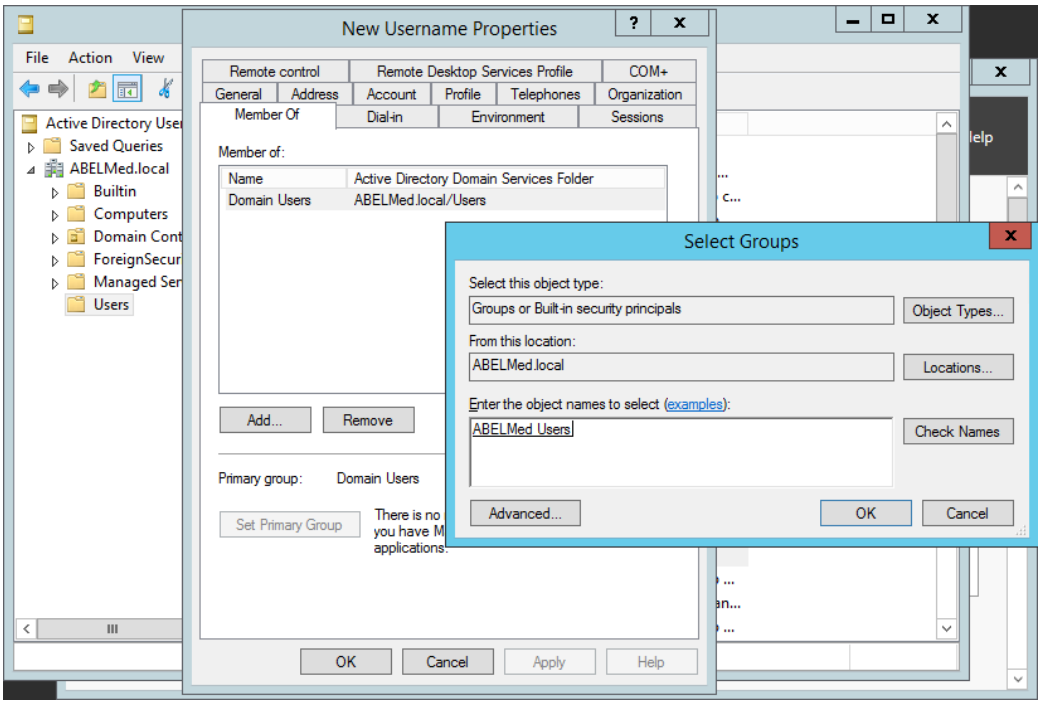


5. The initial password would be entered by the administrator twice, **checking the option to force the user to change it on next logon**, before clicking on next, and then **finish** to create the user.

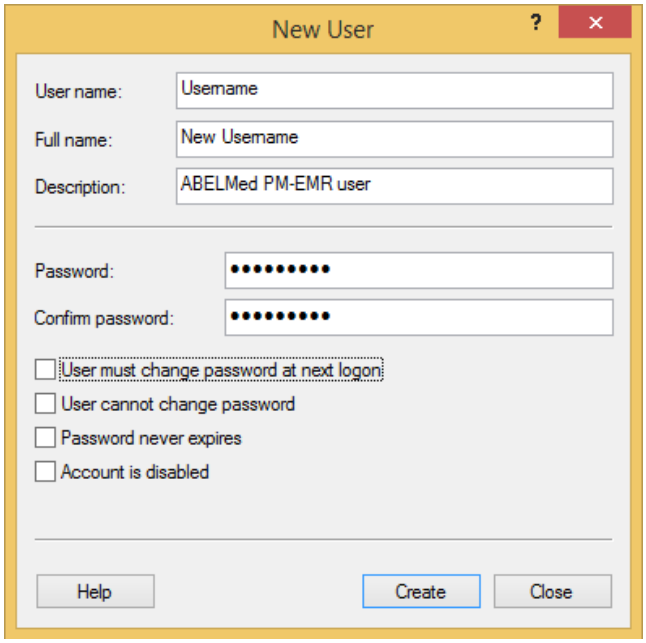


6. The user would then be added to the ABELMed Users group. By double clicking on the new username, clicking on the Member Of tab, clicking in the Add button, typing in the group name, clicking on the Check Names button, and OK

ABELMed Platform Setup Conventions



On a small standalone or peer-peer network with a Windows 10 based file server, the steps would be similar only they will be performed under computer Management. Right click on My Computer, select Manage, expand System Tools, Local Users & Groups, right click on Groups, select New Group and then add the group and user in the same way as described above. Add the user to the appropriate ABELMed Users group when finished. On a small network such as this the user must be created identically on each workstation.



6.2 Installing Remote Desktop Services

This section will provide detailed steps on how to install and configure Remote Desktop Services on the Windows Server 2016 Operating system.

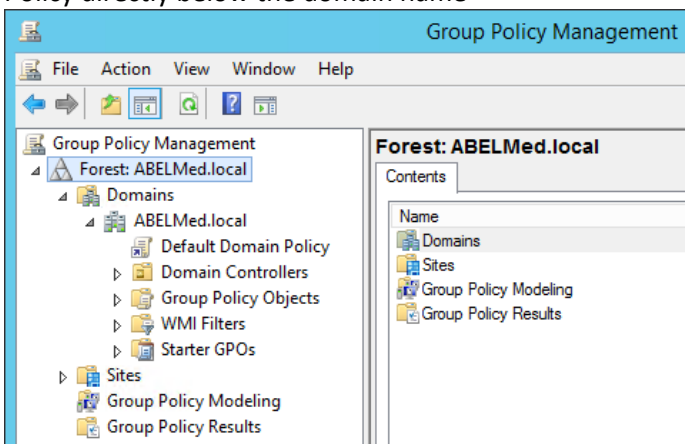
1. Open Server Manager by clicking the Server and Toolbox icon beside the start menu:

2. Under **Manage**, click **Add Roles and Features**.
3. On the **Before You Begin** page of the Add Roles Wizard, click **Next**.
4. On the **Installation Type** page, select the **Remote Desktop Services Installation** check box, and then click **Next**.
5. On the **Select Deployment Type** page, click **Quick Start**.
6. On the **Select Deployment Scenario** page, select the **Session-based desktop deployment**.
7. On the **Select a Server** page, choose your server from the server pool and click **Next**.
   On the **Confirm Selections** page, click **Restart the destination server automatically if required**, and then click **Deploy**.
8. Once the server restarts, go back into **Server Manager, Add Roles and Features,** and select **Remote Desktop Licensing** from below the **Remote Desktop Services** section. Click **Next** twice, then click **Install**.
9. After the server restarts, the remaining steps of the installation finish. When the **Installation Results** page appears, confirm that installation of the RD Session Host role service succeeded.

6.3 Password Policies

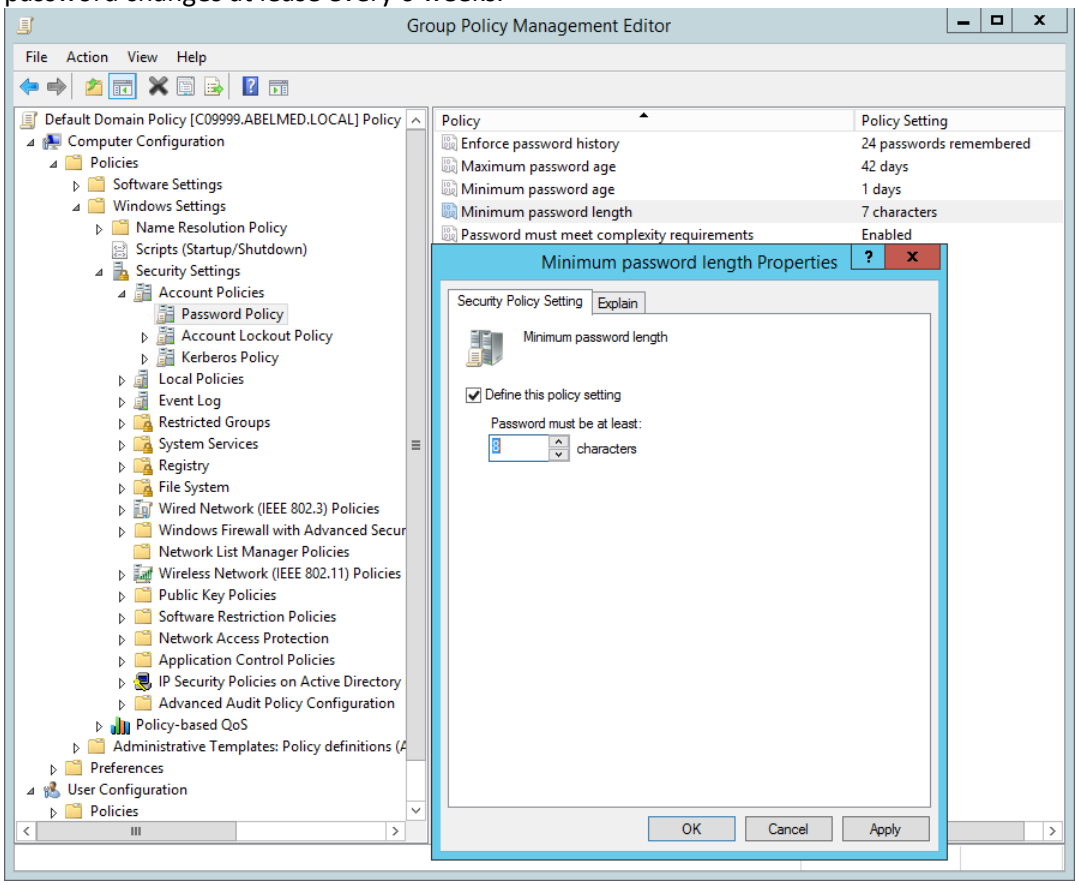
The following steps describe how to set the group policy to ensure password length & complexity rules are enabled in Windows Server 2016.

1. Click on the Windows Start button.
2. Type **Group Policy Management**.
3. Click **Group Policy Management**.
4. In Group Policy Management, expand the tree view in the left column so you can see the Default Domain Policy directly below the domain name

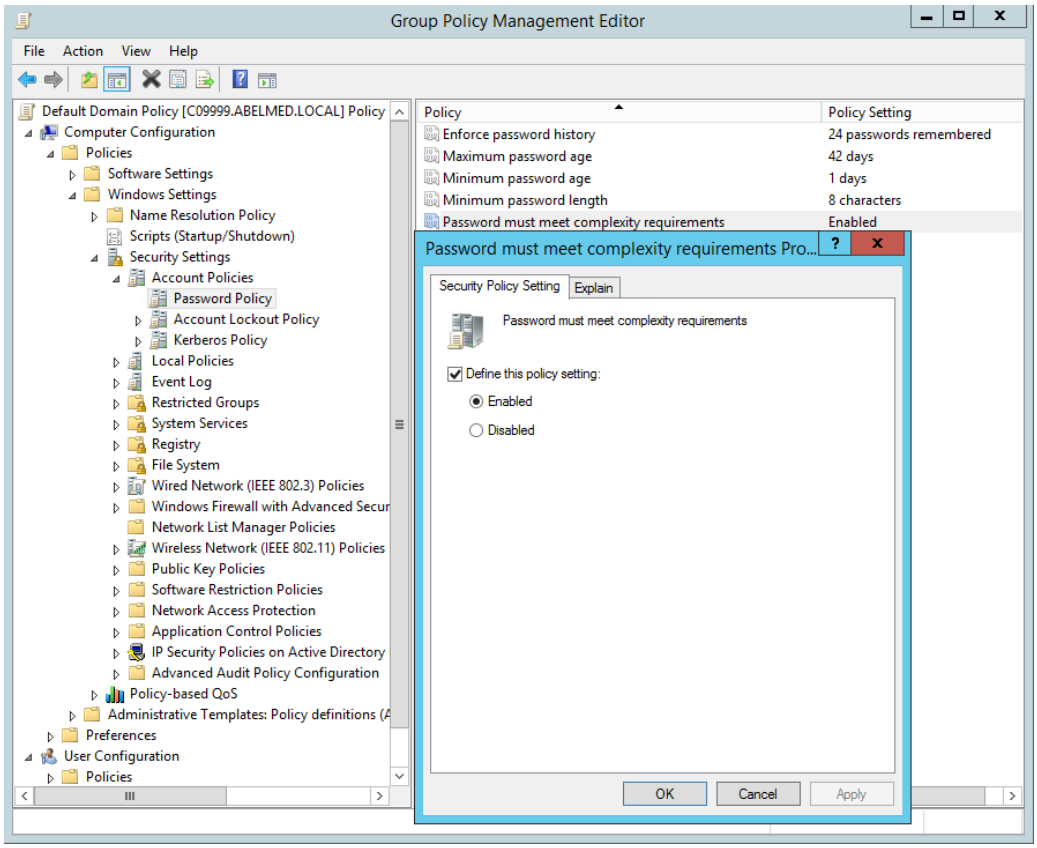


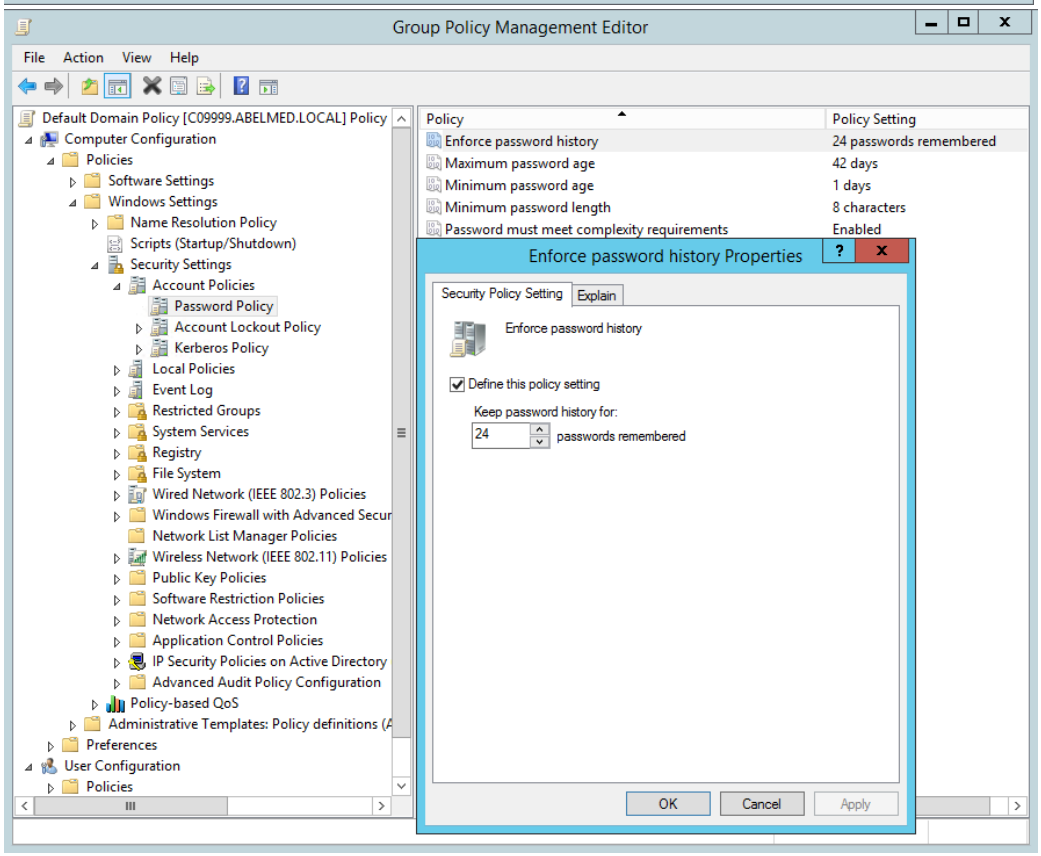
5. Right-click on Default Domain Policy and select Edit from the drop down menu.

6. In the Group Policy Window, click the “+” to expand Computer Configuration.
7. Click the “+” to expand Policies.
8. Click the “+” to expand Windows Settings.
9. Click the “+” to expand Security Settings.
10. Click the “+” to expand Account Policy
11. Click on Password Policy.
12. ABELSoft recommends that several Policies be set here:
    a. **Minimum Password length** should be set at 8 or more characters
    b. **Password must meet complexity requirements** should be defined and enabled. This will mandate additional criteria beyond the standard Windows case sensitive password
    c. **Enforce password history** should be set to help prevent passwords from being reused. We suggest the maximum value of 24 be used.
    d. The above Policy would be ineffective if users could quickly cycle through passwords until they can reuse them. A **Minimum password age** of 30 days will prevent such abuse.
    e. A password age of 90 Days will ensure quarterly password changes. This would be the longest ABELSoft would recommend. Some offices like a **Maximum password age** of 42 days to ensure password changes at lease every 6 weeks.

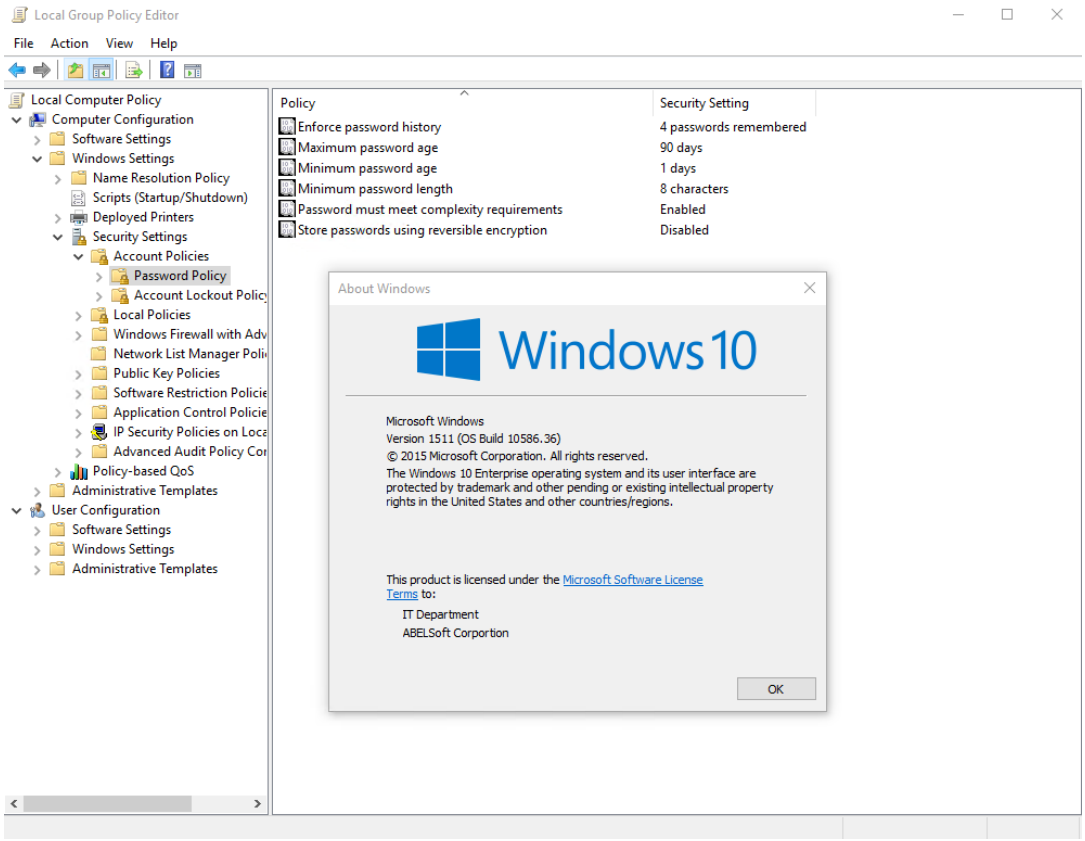


ABELMed Platform Setup Conventions





Similar Policies can be applied to Standalone or small peer-peer networks using the Local Computer Policy provided by Windows 10. The Administrator can achieve access to the policy by clicking on Start > Typing in GPEdit.msc > and clicking on OK. The diagram below shows that the same settings are available there.

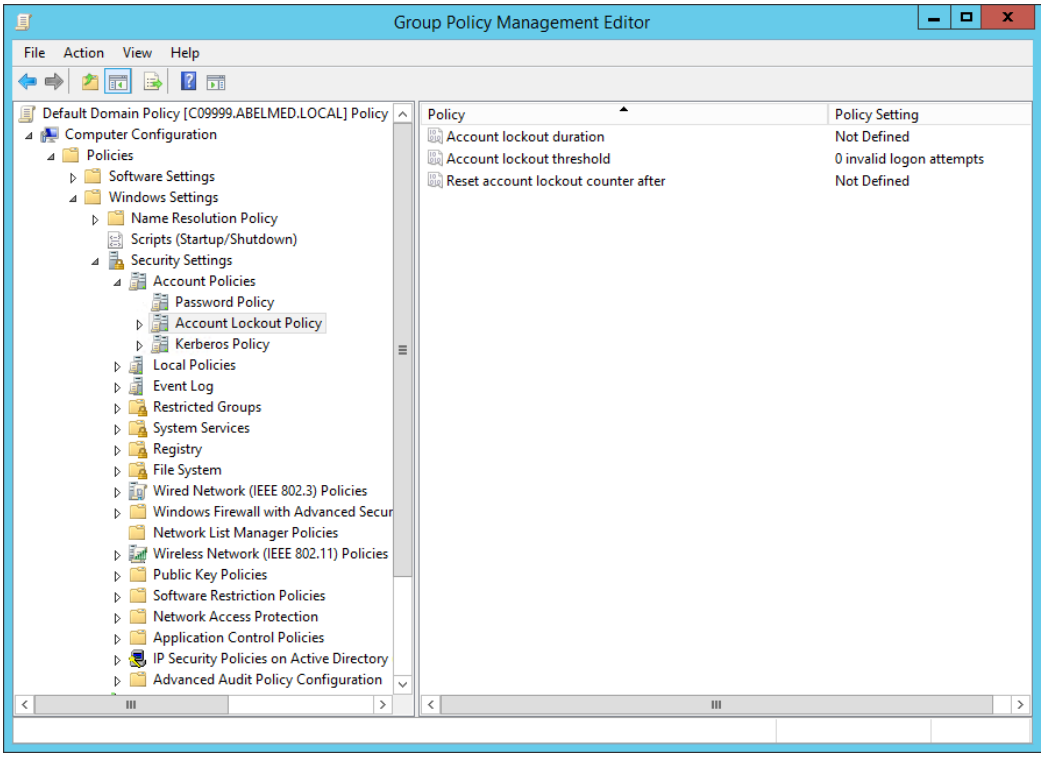


6.4 Account Lockout Policies

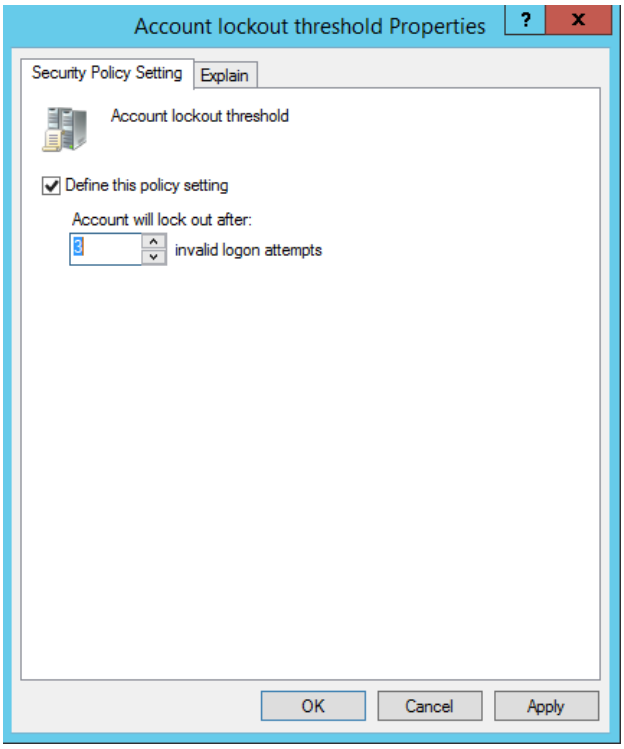
ABELMed relies on Microsoft Windows to provide the authentication, and on Microsoft Windows Group Policy to control the behavior of the system on failures to authenticate. The following steps show how to configure a typical account lockout policy. This example shows how to set a lockout after 3 invalid login attempts, set the lockout duration to 3 days, and reset the lockout counter daily (So that 3 failed login attempts in a day would lock the user account for 3 days, unless an administrator manually unlocked the account. Manual unlocking can be performed by the administrator as shown at the end of this section.

1. Click on the Windows Start button.
2. Select Administrative Tools.
3. Click Group Policy Management.
4. In Group Policy Management, expand the tree view in the left column so you can see the Default Domain Policy directly below the domain name

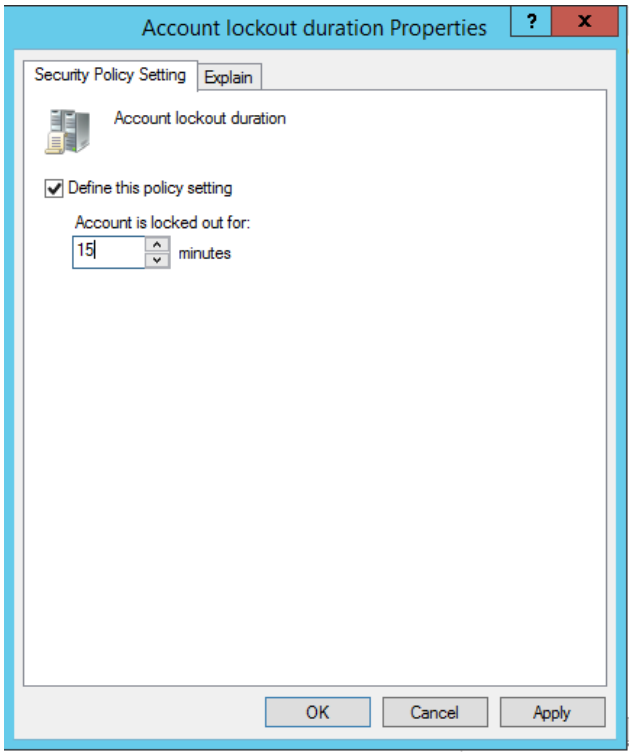
5. Right-click on Default Domain Policy and select Edit



6. Click the “+” to expand Windows Settings.
7. Click the “+” to expand Security Settings.
8. Click the “+” to expand Account Policies.
9. Select Account Policy Lockout
10. Double-click Account lockout threshold

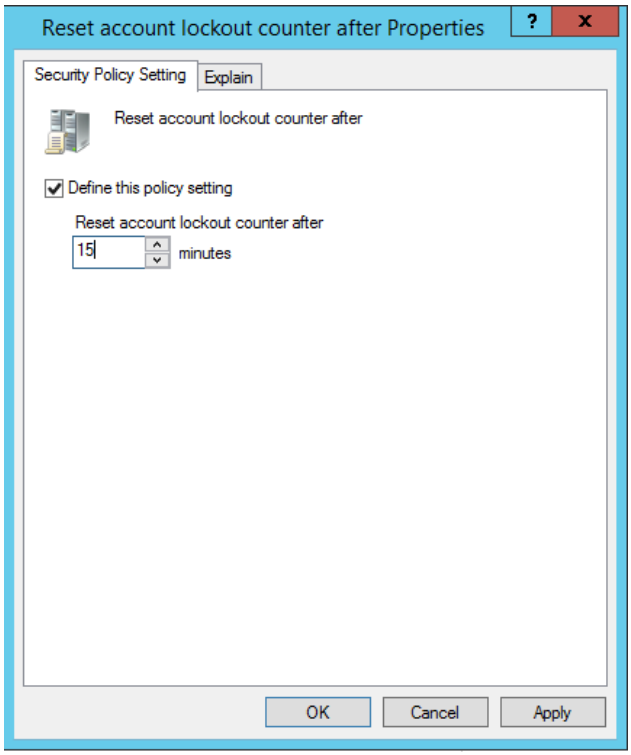


11. Change the value of "Account will lock out after:" to 3 invalid logon attempts.
12. Click OK.
13. Double-click Account lockout duration.



14. Type in the value 15 minutes.
15. Click OK.

16. Double-click on Reset account lockout counter after.



17. Type in the value 15 minutes.
18. Click on OK.
19. Click the X in the upper right of the Group Policy window.

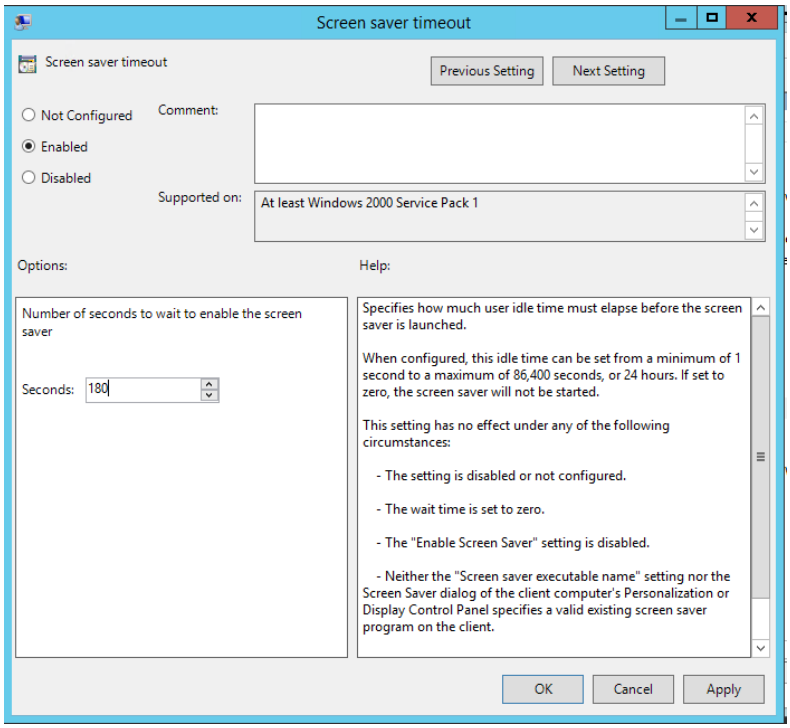
6.5 Inactivity timeout and lock

ABELMed leverages Microsoft Windows technologies that lock a system upon detection of inactivity. The procedure is described below.

ABELSoft prescribes Windows 10 for secure use workstations. In these cases ABELMed PM - EMR and operating system logon security is integrated (i.e., Single sign-on methodology). These workstations can be set in Windows to automatically lock after a defined period of inactivity at the workstation by specifying the screen-saver to be the native Windows 10 password “logon” screen-saver. These settings can be enforced and “locked-down” with an enforced group policy for groups of stations or users or individual stations or users.

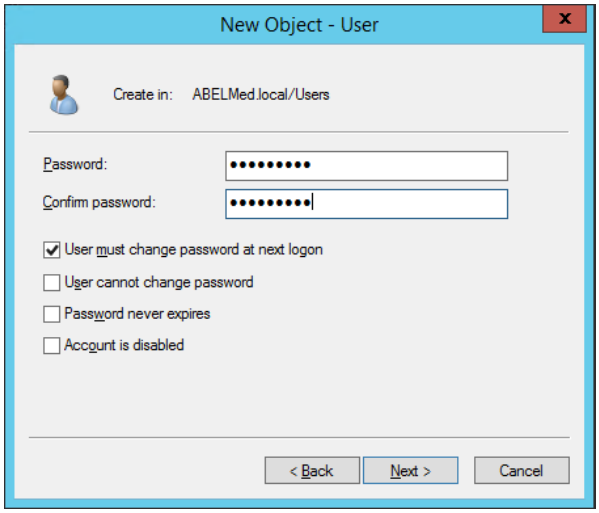
Like the Password and Account Lockout Policies these settings are best made in Group Policy. Follow the Steps in the previous two steps to enter group Policy. The screen saver timeout Policies are set at User Configuration>Administrative Templates>Control Panel>Personalization>Screen Saver Timeout

Suggested value is 180 seconds (3 minutes). Some users find this to be too low. We suggest trying 3 minutes, and if it causes many problems this value can always be increased later (with permission from the appropriate physicians or other authorities).



6.6 Make sure that user can change their own password

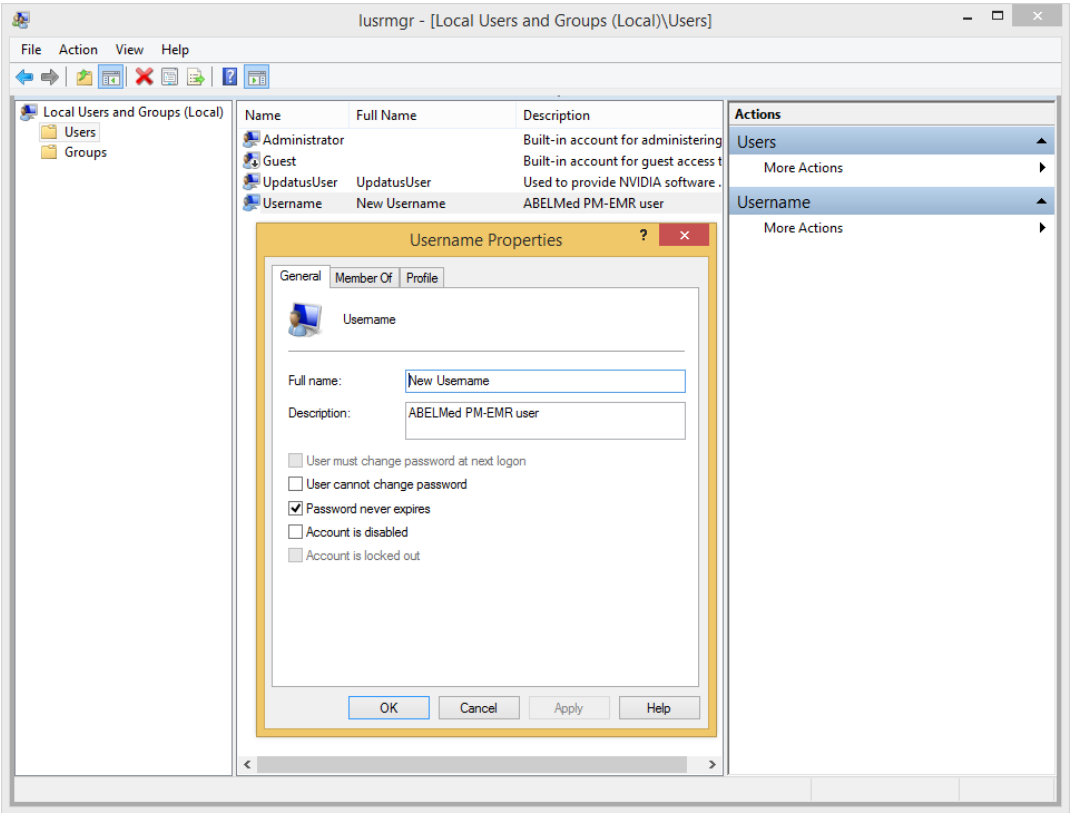
On a Windows 2016 domain when the administrator creates the user account, the administrator determines whether the user will have the appropriate level of privilege to change their own password. The screen capture below shows the default setting where **User cannot change password** is **UNCHECKED**. This setting cannot be selected when **User must change password at next logon** is selected, therefore the setting is already correct for new accounts with **User must change password at next logon selected**.



For existing accounts you should manually check to make sure that **User cannot change password** is unchecked. you can get to this setting by clicking on **Start>Administrative Tools>Active Directory Users & Computers**

>double click on users> double click on the appropriate user > Click on the account tab checkboxes will be in the account options area.

Similarly, if a Windows 2016 domain does not exist, when the administrator creates the user account in Windows 10, the administrator determines whether the user will have the appropriate level of privilege to change their own password. The screen capture below shows the default setting where "User cannot change password" is UNCHECKED.



6.7 Setup NTP/SNTP Time Synchronization

Explanation of NTP time synchronization can be found on the Microsoft website
http://support.microsoft.com/kb/816042

ABELMed Platform Setup Conventions

We are including excerpts on the specific setup steps required here. We strongly recommend an external time source as documented here, rather than the internal time source that is also mentioned in the same Microsoft article.

Configuring the Windows Time service to use an external time source

To configure an internal time server to synchronize with an external time source, follow these steps:

1. Change the server type to NTP. To do this, follow these steps:
    a. Click the **Start button**, type **regedit**, and then click **OK**.
    b. Locate and then click the following registry subkey:

        HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type

    c. In the right pane, right-click **Type**, and then click **Modify**.
    d. In **Edit Value**, type **NTP** in the **Value data** box, and then click **OK**.

Set AnnounceFlags to 5. To do this, follow these steps:

. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags

a. In the right pane, right-click **AnnounceFlags**, and then click **Modify**.
b. In **Edit DWORD Value**, type **5** in the **Value data** box, and then click **OK**.

Enable NTPServer. To do this, follow these steps:

. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer

a. In the right pane, right-click **Enabled**, and then click **Modify**.
b. In **Edit DWORD Value**, type **1** in the **Value data** box, and then click **OK**.

Specify the time sources. To do this, follow these steps:

. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

a. In the right pane, right-click **NtpServer**, and then click **Modify**.

b. In **Edit Value**, type *Peers* in the **Value data** box, and then click **OK**.

Note *Peers* is a placeholder for a space-delimited list of peers from which your computer obtains time stamps. Each DNS name that is listed must be unique. You must append **,0x1** to the end of each DNS name. If you do not append **,0x1** to the end of each DNS name, the changes made in step 5 will not take effect.

Select the poll interval. To do this, follow these steps:

. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval

a. In the right pane, right-click **SpecialPollInterval**, and then click **Modify**.

b. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for the number of seconds that you want between each poll. A recommended value is 900 Decimal. This value configures the Time Server to poll every 15 minutes.

Configure the time correction settings. To do this, follow these steps:

. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPosPhaseCorrection

. In the right pane, right-click **MaxPosPhaseCorrection**, and then click **Modify**.

a. In **Edit DWORD Value**, click to select **Decimal** in the **Base** box.

b. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for a reasonable value, such as 1 hour (3600) or 30 minutes (1800). The value that you select will depend upon the poll interval, network condition, and external time source.

c. Locate and then click the following registry subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNegPhaseCorrection

d. In the right pane, right-click **MaxNegPhaseCorrection**, and then click **Modify**.

e. In **Edit DWORD Value**, click to select **Decimal** in the **Base** box.

f. In **Edit DWORD Value**, type *TimeInSeconds* in the **Value data** box, and then click **OK**.

Note *TimeInSeconds* is a placeholder for a reasonable value, such as 1 hour (3600) or 30 minutes (1800). The value that you select will depend upon the poll interval, network condition, and external time source.

Quit Registry Editor.

At the command prompt, type the following command to restart the Windows Time service, and then press ENTER:

net stop w32time && net start w32time

6.8 Disable LMHash

Modern Windows systems use a very secure system called Kerberos for secure authentication. Passwords are not directly stored or transmitted. Standards based hashes(MD4) are stored in encrypted databases, and only hashes of passwords are ever transmitted. Windows systems also have components that support backward compatibility to older less secure authentication systems, specifically one component called LANManager. ABELSoft recommends that you turn off such compatibility so that password hashes are not stored or transmitted using these older vulnerable standards. The following instructions tell how to disable the LMHash

Implement the NoLMHash Policy by Using Group Policy

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 10 or Windows Server 2016) or in a Windows Server 2016 Active Directory environment by using Group Policy in Active Directory, follow these steps:

1. In Group Policy, expand **Computer Configuration**, expand **Policies**, 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**.

ABELMed Platform Setup Conventions

Appendix B – Security and Auditing Checklist

This checklist is provided to help you systematically perform the recommended security setup. Make copies of the pages for more than 5 workstations.

Practice Name: _____ ABEL ID:_____ Date:_____

Security Requirements	Server	Workstation 1	Workstation 2	Workstation3	Workstation 4	Workstation 5
Machine Name						
Encrypt Drive(s)						
Enforce password history enabled						
Maximum password age enabled for 90 days						
Minimum password length set to 8 characters enabled						
Password must meet complexity requirements						
Account lockout duration set to 15 minutes						
Account lockout threshold enabled for 3 attempts						
Reset account lockout counter set to 15 minutes						
Audit account logon events enabled for success/failure						
Audit account management enabled for success/failure						
Audit logon events enabled for success/failure						
Audit object access enabled for success/failure						
Audit policy change enabled for success/failure						

ABELMed Platform Setup Conventions

Screen saver password protected enabled for 3 minutes						
Remote Access enabled/configured						
Time synchronization configured						
Firewall rules created 1. MS SQL – 1433 2. MS SQL – 1434 3. NetBIOS – 139 4. Microsoft DS – 445 5. NetBIOS – 137 6. NetBIOS – 138 7. SSL – 443 8. RDP – 3389						
Backup software installed/configured to backup 1. Application data 2. Security credentials 3. Log/audit files						
Backup and archive files are encrypted						
Antivirus software installed						
No conflict between ABELMed and installed antivirus software						
VPN software installed/configured						
Uninterruptable Power Supply 1. Setup 2. Software installed						
Configure & Test Multi-Factor Authentication if implementing it						
Physical security of server/desktop						

I verify that ABELSoft's security and auditing checklist has been completed as indicated above.

IT Technician Name: _____

IT Technician Signature: _____