Enable SMB Signing via GPO

What is SMB

The Server Message Block protocol (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network

How does the SMB protocol work?

The SMB protocol enables applications and their users to access files on remote servers, as well as connect to other resources, including printers, mailslots and named pipes. SMB provides client applications with a secure and controlled method for opening, reading, moving, creating and updating files on remote servers. The protocol can also communicate with server programs configured to receive SMB client requests.

Known as a response-request protocol, the SMB protocol is one of the most common methods used for network communications. In this model, the client sends an SMB request to the server to initiate the connection. When the server receives the request, it replies by sending an SMB response back to the client, establishing the communication channel necessary for a two-way conversation.

The SMB protocol operates at the application layer but relies on lower network levels for transport. At one time, SMB ran on top of Network Basic Input/Output System over Transmission Control Protocol/Internet Protocol (NetBIOS over TCP/IP, or NBT) or, to a lesser degree, legacy protocols such as Internetwork Packet Exchange or NetBIOS Extended User Interface. When SMB was using NBT, it relied on ports 137, 138 and 139 for transport. Now, SMB runs directly over TCP/IP and uses port 445.

Today, communications with devices that do not support SMB directly over TCP/IP require the use of NetBIOS over a transport protocol such as TCP/IP.

Microsoft Windows operating systems (OSes) since Windows 95 have included client and server SMB protocol support. The Linux OS and macOS also provide built-in support for SMB. In addition, Unix-based systems can use Samba to facilitate SMB access to file and print services.

What is SMB signing?

SMB signing (also known as security signatures) is a security mechanism in the SMB protocol. SMB signing means that every SMB message contains a signature that is generated by using the session key. The client puts a hash of the entire message into the signature field of the SMB header.

It is worth noting that if SMB signing is enabled and required on the server and disabled on the client, or vice-versa, the connection will fail and the machines won’t be able to talk over SMB. These instances of protocol mismatch should not happen if you’ve uniformly applied the GPO settings to all machines in your environment (make sure to take into account any machines not joined to the domain and therefore not receiving Group Policy).

To configure:

Create the following GPO from your Group Policy Management

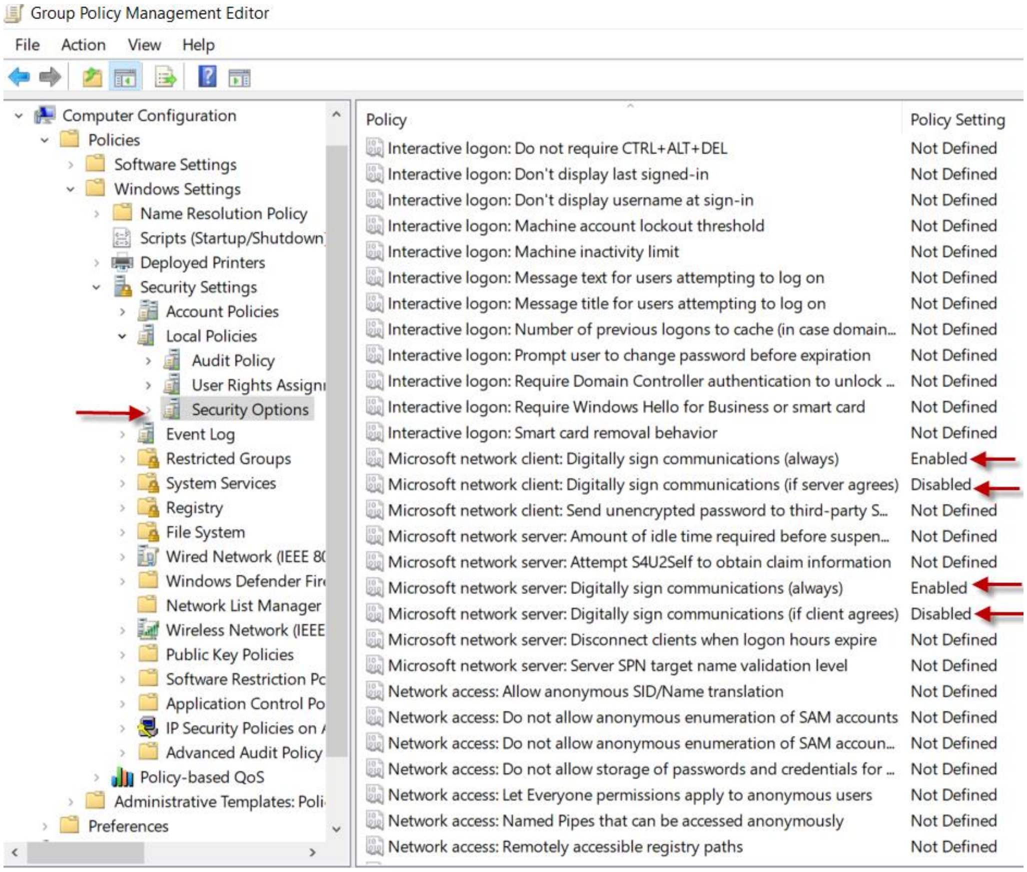
Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options ->

Microsoft network client: Digitally sign communications (always) > ENABLED

Microsoft network client: Digitally sign communications (if server agrees) > DISABLED

Microsoft network server: Digitally sign communications (always) > ENABLED

Microsoft network server: Digitally sign communications (if client agrees) > DISABLED



Policy	Policy Setting
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Not Defined
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock ...	Not Defined
Interactive logon: Require Windows Hello for Business or smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Disabled
Microsoft network client: Send unencrypted password to third-party S...	Not Defined
Microsoft network server: Amount of idle time required before suspen...	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Do not allow anonymous enumeration of SAM accoun...	Not Defined
Network access: Do not allow storage of passwords and credentials for ...	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Not Defined
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined