FacetWin File and Printer Sharing Connections

UNIX Server Requirements: (Updated 2024/12/31)

You must be using FacetWin Version 40u (Build 513) or later on the UNIX server, This contains the latest improvements for working with the newer Windows operating systems. Must upgrade to the current FacetWin release to take advantage of the latest improvements and optimizations.

DO NOT UNINSTALL!! Just install right over the current version.

FacetWin has four types of user security for file and print services. All of the methods require that the user name used to logon to the Windows PC is the same as the user name on the UNIX server. The only exception is when the FacetWin "alias" feature is used to map one or more PC user names to a different UNIX user name.

The following are the four security methods for file and print services:

NT SERVER Security Method: (Not Windows 11, 24H2)

In the facetwin.cfg configuration file, the NT SERVER security method is indicated by the line:

pass_security=\\nt_server_ip_address

where nt_server_ip_address is the IP address of the primary password authentication Windows Server.

All of the other pass_security lines should be commented out.

NTLMSSP Security Method:

To use the NTLMSSP method with FacetWin, set “pass_security=NTLMSSP” in the facetwin.cfg file.

All of the other pass_security lines should be commented out.

Run “fct_encrypt -b” on the Linux/Unix server to build the "fctpasswd" file when new users have been added to the “/etc/passwd” file.

The user password must be set in the “/usr/facetwin/fctpasswd” file by running “fct_encrypt username” for each user.

LANMAN Security Method: (Not Windows 11, 24H2)

To use the LANMAN method with FacetWin, set “pass_security=LANMAN” in the facetwin.cfg file.

All of the other pass_security lines should be commented out.

Run “fct_encrypt -b” on the Linux/Unix server to build the "fctpasswd" file when new users have been added to the “/etc/passwd” file.

The user password must be set in the “/usr/facetwin/fctpasswd” file by running “fct_encrypt username” for each user.

RHOST Security Method:

To use the RHOST method with FacetWin set “pass_security=RHOST” in the “facetwin.cfg” file on the Linux/Unix server.

All of the other pass_security lines should be commented out.

The RHOST security method is not used very often, because it requires fixed IP

addresses and a clear understanding of the “/etc/hosts”, "$HOME/.rhosts" and

"/etc/hosts.equiv" files. For information on these files see the UNIX man pages for hosts, hosts.equiv and rhosts.

The PC or Windows Server names must be resolvable by the UNIX system.

UNIX Security Method:

To use UNIX security method with FacetWin set “pass_security=UNIX” in the facetwin.cfg file.

All of the other pass_security lines should be commented out.

Windows Computer Requirements:

FacetWin File and Printer sharing works with only SMBv1!!

The SMB1.0/CIFS Client must be enabled on ALL Windows Computers.

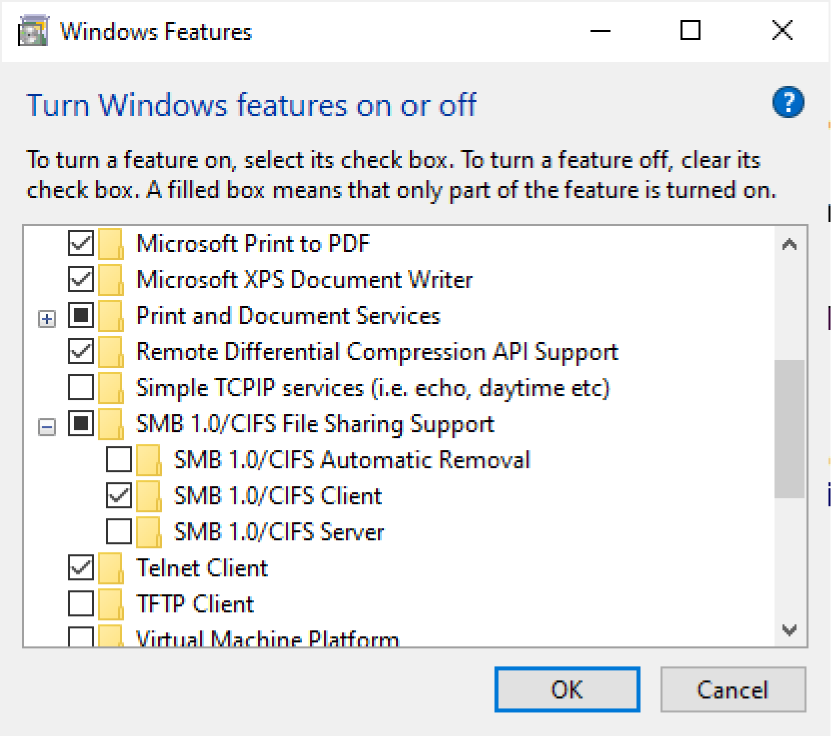
1) Press the Windows key on the keyboard, type "Turn Windows Features", press Enter.

2) The “Turn Windows features on or off” dialog box appears.

3) Expand SMB1.0/CIFS File Sharing Support, remove check in box SMB1.0/CIFS Automatic Removal, check box SMB1.0/CIFS **Client**.

4) Click OK.

Windows 10/11:



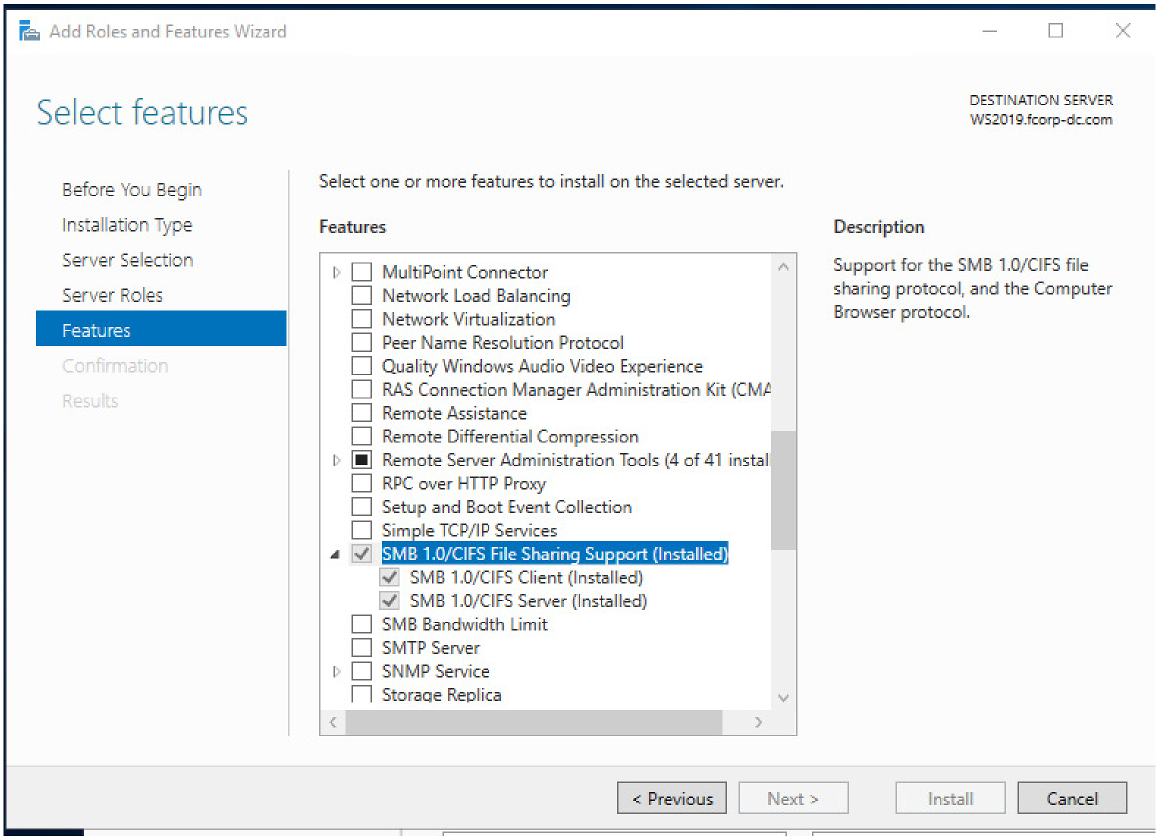
Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Microsoft Print to PDF
- ☑ Microsoft XPS Document Writer
- ⊞ ■ Print and Document Services
- ☑ Remote Differential Compression API Support
- □ Simple TCPIP services (i.e. echo, daytime etc)
- ⊟ ■ SMB 1.0/CIFS File Sharing Support
  - □ SMB 1.0/CIFS Automatic Removal
  - ☑ SMB 1.0/CIFS Client
  - □ SMB 1.0/CIFS Server
- ☑ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform

Windows 2019 Server:



Select one or more features to install on the selected server.

Features

- □ MultiPoint Connector
- □ Network Load Balancing
- □ Network Virtualization
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ RAS Connection Manager Administration Kit (CMA
- □ Remote Assistance
- □ Remote Differential Compression
- ■ Remote Server Administration Tools (4 of 41 instal
- □ RPC over HTTP Proxy
- □ Setup and Boot Event Collection
- □ Simple TCP/IP Services
- ☑ SMB 1.0/CIFS File Sharing Support (Installed)
  - ☑ SMB 1.0/CIFS Client (Installed)
  - ☑ SMB 1.0/CIFS Server (Installed)
- □ SMB Bandwidth Limit
- □ SMTP Server
- □ SNMP Service
- □ Storage Replica

Description

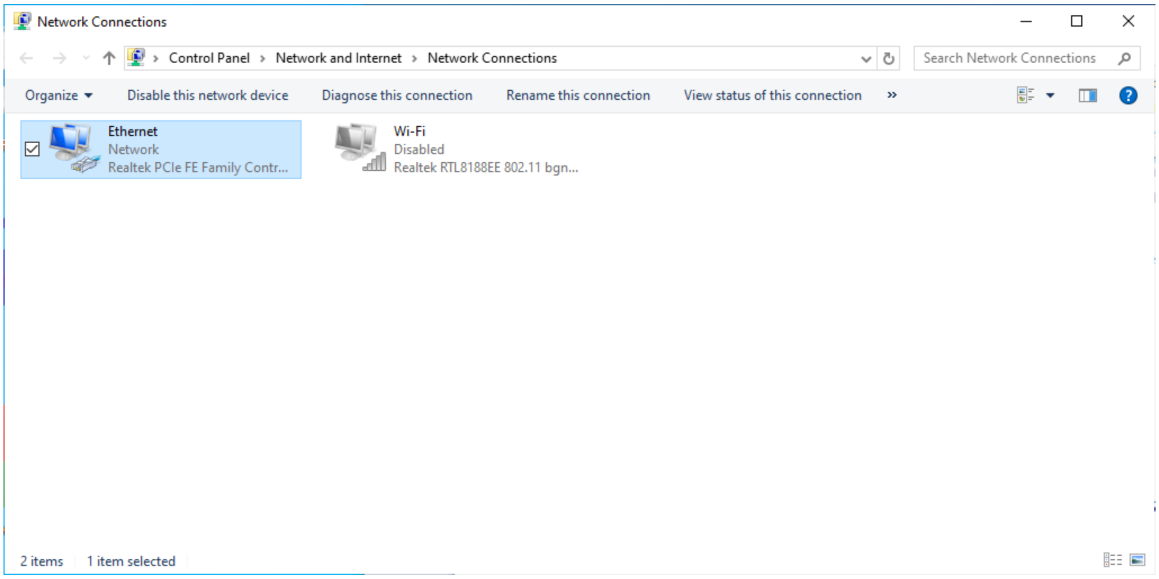
Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.

Reboot the computer.

Windows Network Connections Properties:

Press the Windows key on the keyboard, type "View network connections", press Enter.

The “Network Connections” dialog box appears.

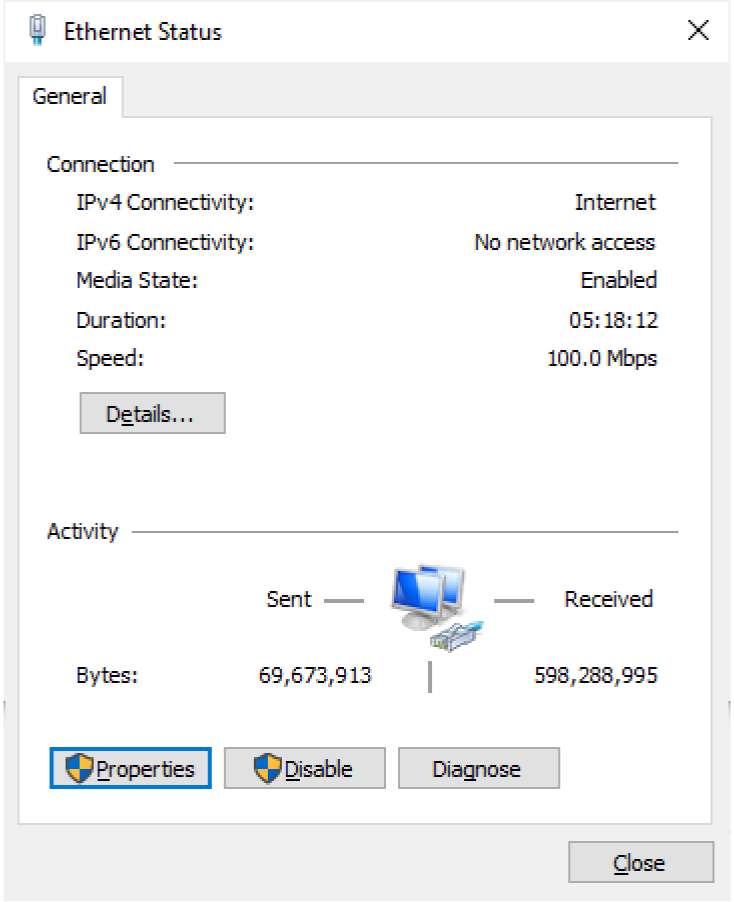

Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
»

☑ Ethernet
Network
Realtek PCIe FE Family Contr...

Wi-Fi
Disabled
Realtek RTL8188EE 802.11 bgn...

2 items | 1 item selected

Select the network connection being used. The Ethernet Status screen appears.



IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 05:18:12
Speed: 100.0 Mbps

Bytes: 69,673,913 | 598,288,995

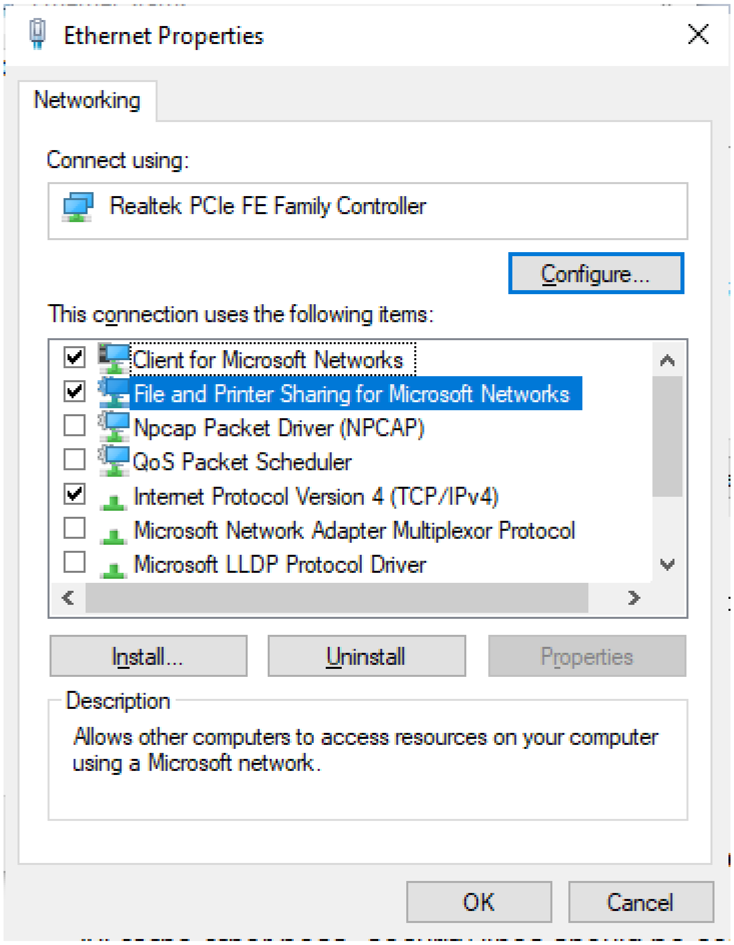
Click on the "Properties" button. The "Ethernet Properties" screen appears.

1) Uncheck "Internet Protocol Version 6 (TCP/IPv6)" properties box.

2) Check the "Client for Microsoft Networks" properties box.

3) Check the "File and Printer Sharing for Microsoft Networks" properties box.

4) Check "Internet Protocol Version 4 (TCP/IPv4)" properties box.



Connect using:

Realtek PCIe FE Family Controller

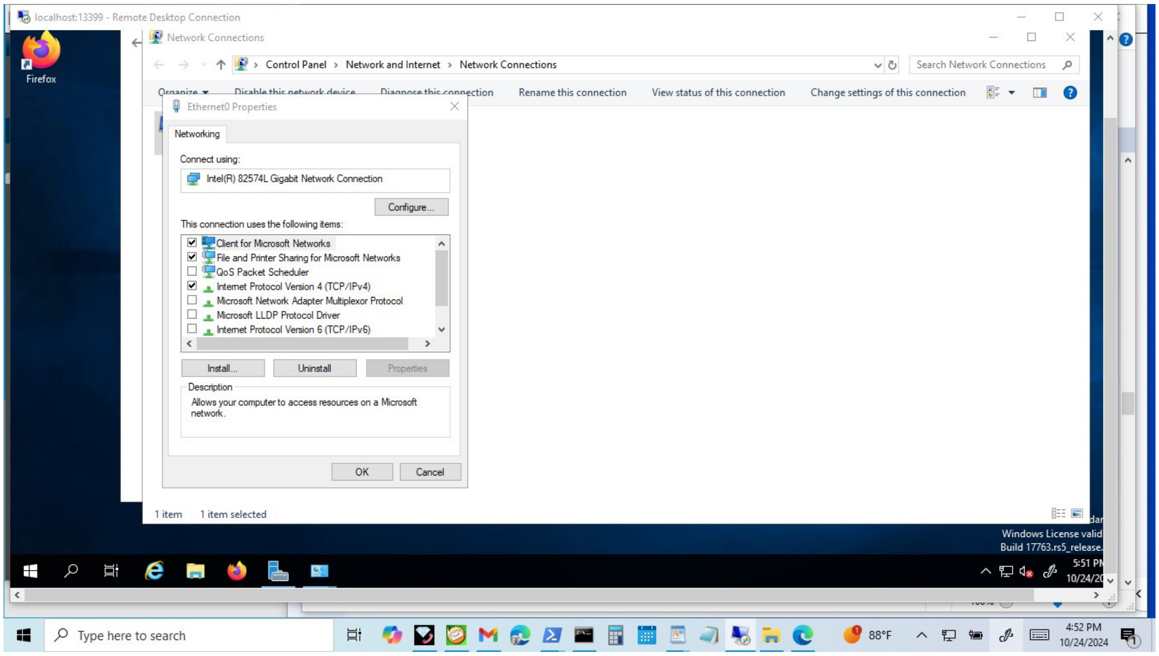
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Npcap Packet Driver (NPCAP)
- ☐ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☐ Microsoft LLDP Protocol Driver

Description

Allows other computers to access resources on your computer using a Microsoft network.

Windows 2019 Server:


localhost:13399 - Remote Desktop Connection
Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Firefox
1 item
1 item selected
Windows License valid
Build 17763.rs5_release.
5:51 PM
Type here to search
88°F
4:52 PM
10/24/2024

Ethernet0 Properties

Networking

Connect using:

Intel(R) 82574L Gigabit Network Connection

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☐ Microsoft LLDP Protocol Driver
- ☐ Internet Protocol Version 6 (TCP/IPv6)

Install... Uninstall Properties

Description

Allows your computer to access resources on a Microsoft network.

OK Cancel

Changes needed on the client Windows PC to use the LANMAN security method with the "gpedit.msc" Windows 10: (Not Windows 11, 24H2)

Administrative Tools->

Local Security Policy->

Local Policies->

Security Options->

- Network security: LAN Manager authentication level:

  Send LM & NTLM - use NTLMv2 session security if negotiated

- Microsoft Network Client: Digitally sign communications (if server agrees): Disabled

- Microsoft Network Client: Digitally sign communications (always): Disabled

Changes needed on the client Windows PC to use the LANMAN security method with the Registry since the "gpedit.msc" is not available on Microsoft Windows Home Edition: (Not Windows 11, 24H2)

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LmCompatibilityLevel"=dword:00000001

- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
\LanManWorkStation\parameters]
"RequireSecuritySignature"=dword:00000000

- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters]
"EnableSecuritySignature"=dword:00000000

The registry can automatically be updated with this "***LANMAN.reg***" file. It should be downloaded unmodified by your browser, and then double-clicked on to update your registry. There are also clues Batch and PowerShell scripts to verify the reguired Registry settings.

http://db.facetcorp.com/evals/facetwin/fwt/registry

Apply change and then reboot Windows computer.

Changes needed on the client Windows PC to use the NTLMSSP security method with the "gpedit.msc" Windows 10/11 Pro:

Administrative Tools->

Local Security Policy->

Local Policies->

Security Options->

- Network security: LAN Manager authentication level:

  Send NTLMv2 response only

- Microsoft Network Client: Digitally sign communications (if server agrees): Disabled
- Microsoft Network Client: Digitally sign communications (always): Disabled

Changes needed on the client Windows PC to use the NTLMSSP security method with the Registry since the "gpedit.msc" is not available on Microsoft Windows Home Edition:

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LmCompatibilityLevel"=dword:00000003
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters]
"RequireSecuritySignature"=dword:00000000
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters]
"EnableSecuritySignature"=dword:00000000

The registry can automatically be updated with this "***NTLMSSP.reg***" file. It should be downloaded unmodified by your browser, and then double-clicked on to update your registry. There are also clues Batch and PowerShell scripts to verify the reguired Registry settings.

http://db.facetcorp.com/evals/facetwin/fwt/registry

Apply change and then reboot Windows computer.

Changes needed on the client Windows PC to use the RHOST security method with the "gpedit.msc" Windows 10/11 Pro:

Administrative Tools->

Local Security Policy->

Local Policies->

Security Options->

- Network security: LAN Manager authentication level:

  Send NTLMv2 response only
- Microsoft Network Client: Digitally sign communications (if server agrees): Disabled
- Microsoft Network Client: Digitally sign communications (always): Disabled

Changes needed on the client Windows PC to use the RHOST security method with the Registry since the "gpedit.msc" is not available on Microsoft Windows Home Edition:

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] "LmCompatibilityLevel"=dword:00000003
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters] "RequireSecuritySignature"=dword:00000000
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters] "EnableSecuritySignature"=dword:00000000

The registry can automatically be updated with this "***RHOST.reg***" file. It should be downloaded unmodified by your browser, and then double-clicked on to update your registry. There are also clues Batch and PowerShell scripts to verify the reguired Registry settings.

http://db.facetcorp.com/evals/facetwin/fwt/registry

Apply change and then reboot Windows computer.

Changes needed on the client Windows PC to use the UNIX security method with the "gpedit.msc" Windows 10/11 Pro:

Administrative Tools->

Local Security Policy->

Local Policies->

Security Options->

- Microsoft network client: Send unencrypted passwords to third-party SMB servers: Enabled
- Microsoft Network Client: Digitally sign communications (if server agrees): Disabled
- Microsoft Network Client: Digitally sign communications (always): Disabled
- Network security: LAN Manager authentication level:

  Send LM & NTLM - use NTLMv2 session security if negotiated

Changes needed on the client Windows PC to use the UNIX security method with the Registry since the "gpedit.msc" is not available on Microsoft Windows Home Edition:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanmanWorkStation \parameters]"EnablePlainTextPassword"=dword:00000001
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters] "EnableSecuritySignature"=dword:00000000
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \LanManWorkStation\parameters] "RequireSecuritySignature"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] "LmCompatibilityLevel"=dword:00000001

The registry can automatically be updated with this "***UNIX.reg***" file. It should be downloaded unmodified by your browser, and then double-clicked on to update your registry. There are also clues Batch and PowerShell scripts to verify the reguired Registry settings.

http://db.facetcorp.com/evals/facetwin/fwt/registry

Apply change and then reboot Windows computer.

Changes needed on the client Windows PC to use the NT_SERVER security method with the "gpedit.msc" Windows 10/11 Pro: (Not Windows 11, 24H2)

Administrative Tools->

Local Security Policy->

Local Policies->

Security Options->

- Network security: LAN Manager authentication level:

  Send LM & NTLM - use NTLMv2 session security if negotiated
- Microsoft Network Client: Digitally sign communications (if server agrees): Disabled
- Microsoft Network Client: Digitally sign communications (always): Disabled

Changes needed on the client Windows PC to use the NT_SERVER security method with the Registry since the "gpedit.msc" is not available on Microsoft Windows Home Edition: (Not Windows 11, 24H2)

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
  "LmCompatibilityLevel"=dword:00000001
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
  \LanManWorkStation\parameters]
  "RequireSecuritySignature"=dword:0000000
- [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
  \LanManWorkStation\parameters]
  "EnableSecuritySignature"=dword:00000000

The registry can automatically be updated with this "***NT_SERVER.reg***" file. It should be downloaded unmodified by your browser, and then double-clicked on to update your registry. There are also clues Batch and PowerShell scripts to verify the reguired Registry settings.

http://db.facetcorp.com/evals/facetwin/fwt/registry

Apply change and then reboot Windows computer.

If Logon fails, view the Windows Logon Failures:

To view only the list of login events and not every security event that has been detected, you can filter just Audit Failures.

1) Right click on Start on the Taskbar (Window Icon)

2) Select Event Viewer

3) Expand the Windows Logs and select Security.

4) Select Filter Current Log… in the right sidebar.

5) Click down arrow next to Keywords, check box "Audit Failures" to view.

6) Select OK.

Now you will be able to view your filter of Audit Failures in the Event Viewer.

The best way to check Windows Event Logs on Windows Servers is through the Event Viewer. You can launch it from the Server Manager using the following steps:

1) Click on the top Tools menu button.

2) Search the list for Event Viewer.

3) Double click on it to open it .