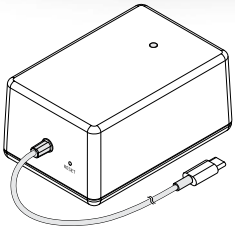
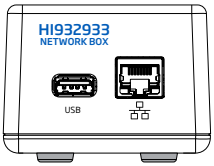
INSTRUCTION MANUAL





HI932 Supplemental Manual

SMB and FTP Configuration & Data Sharing

HI932 Automatic Titrator firmware versions 2.2.2 and higher

HI932933 Network Box firmware version 1.0.2 and higher

Hanna Instruments Inc., 584 Park East Drive, Woonsocket, RI 02895 USA
www.hannainst.com

Dear Customer,

Thank you for choosing a Hanna Instruments® product.
Please read this instruction manual carefully before using this instrument as it provides the necessary information for correct use of this instrument and a precise idea of its versatility.

If you need additional technical information, do not hesitate to e-mail us at tech@hannainst.com.
Visit www.hannainst.com for more information about Hanna Instruments and our products.

This manual has been written as supplement for MAN932 **Automatic Potentiometric Titrator** running software version 2.2.2 (and higher) and HI932933 **Network Box** running software version 1.0.2 (and higher), and contains the necessary information to configure and use FTP and SMB data sharing.

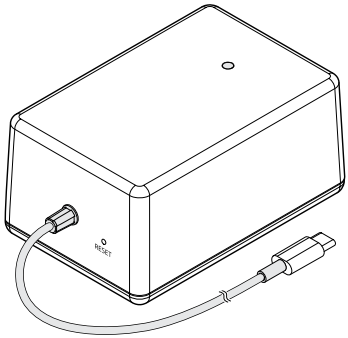
Network Security

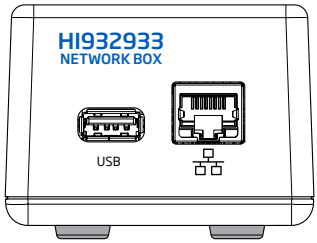
Users must secure their own network connections and access points.
Hanna Instruments accepts no responsibility for any network security breaches or incidental damages arising from network intrusions.
Always consult internal IT department and follow established network security best practices.

TABLE OF CONTENTS

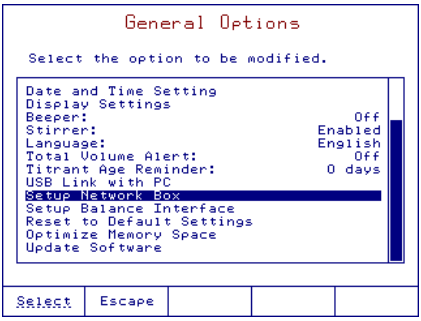
1. TITRATOR SETUP

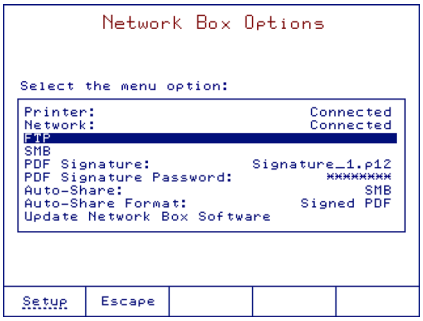
The HI932933 Network Box needs to be connected to the HI932 Automatic Titrator.



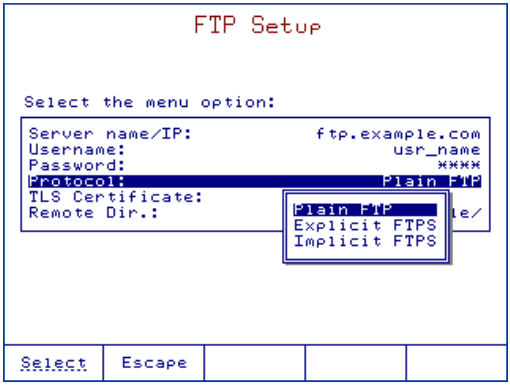


1. Press the [General Options] key.
2. Use the ∧ and ∨ keys to navigate to "Setup Network Box" and press [Select].
3. Use **FTP** or **SMB** and press [Setup].





1.1. FTP SETUP



The network configuration needed to connect HI932 Titrator to an FTP network share requires the following inputs:

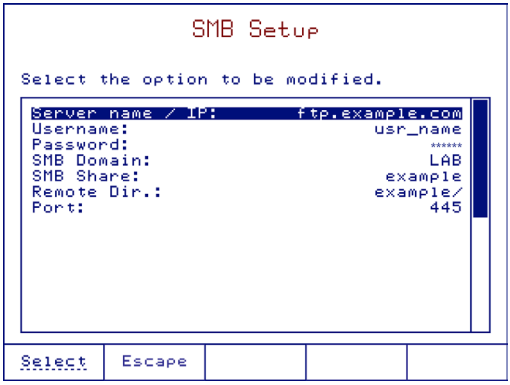
- **Server name /IP address**
  Fill in server name or IP address where server is located.
- **Username**
  Fill in specific username for the server.
- **Password**
  Enter user password for the server.
- **Protocol**
  Select required FTP protocol (Plain FTP/Explicit FTPS/Implicit FTPS).
- **TLS Certificate**
  TLS/SSL certificates are external certificates for FTPS, used to secure in-transit data during file transfer. TLS certificates are imported and installed from the USB device.
- **Remote Dir.**
  Enter remote directory path, i.e. folder path name located on server host.

The transition from unsecured to secured FTP file transfers is based on port selection and TLS certificate availability.

- Standard (Plain) FTP transfer operates without a TLS certificate and uses Port 21. Communication is plain text and unencrypted.
- Explicit FTPS transfer requires a TLS certificate, uses Port 21, and operates via secure (encrypted) connection.
- Implicit FTPS transfer requires a TLS certificate, uses Port 990 and operates via secure (encrypted) connection.

Note: *For details on FTP configuration and certificate loading please refer to* ***HI932 User Manual****:*
section: 2.3.13. Network Box Setup > FTP Setup > Import TLS Certificate

1.2. SMB SETUP



The network configuration needed to connect HI932 Titrator to an SMB network share requires the following inputs:

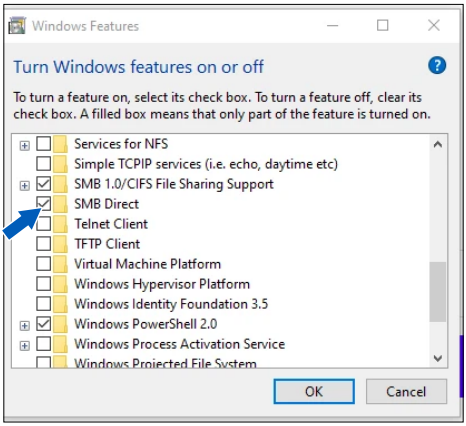
- **Server name /IP address**
  Fill in the name of the PC hosting the SMB share.
  See 2.2. SMB Server Folder Setup.
- **Username** and **Password**
  Fill in SMB network credentials used to access the PC.
  See 2.1.5. Create User Account and Password.
- **SMB Domain**
  The workgroup name of the PC.
  See 2.3.1. Find Workgroup Name.
- **SMB Share folder**
  The name of the shared folder on the host PC.
  See 2.2. SMB Server Folder Setup.
- **Remote Dir**
  Optional sub-folder of the SMB share.
  For instance, if Remote Dir. is HI932, the files will be transferred to \\ **PC- Name\SMB-Folder**\HI932\...)
- **Port**
  Port 445 for SMB transfer

2. SMB SERVER SETUP (WINDOWS 11)

2.1. PREREQUISITE STEPS

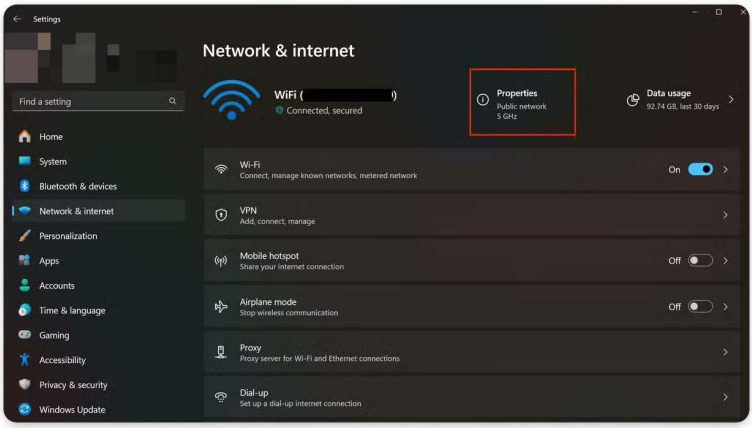
2.1.1. Windows Features

1. Press Windows key (⊞) and search: "`Turn Windows features on or off`".
2. Scroll down and enable ☑ "`SMB Direct`".

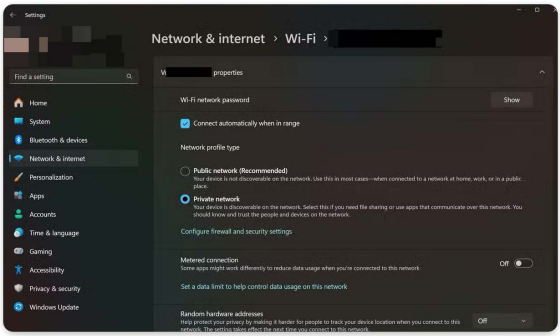


2.1.2. Private Nework Profile

1. Press the Windows key (⊞) and type "`Settings`".
2. Click on the "`Settings`" shortcut.
3. Click "`Network & Internet`" in the left sidebar.
4. Select active connection type at the top ("`Wi-Fi`" or "`Ethernet`").
5. Click on the connected network's [Properties] tab.



6. Select ⦿ **Private network** under "Network profile type".

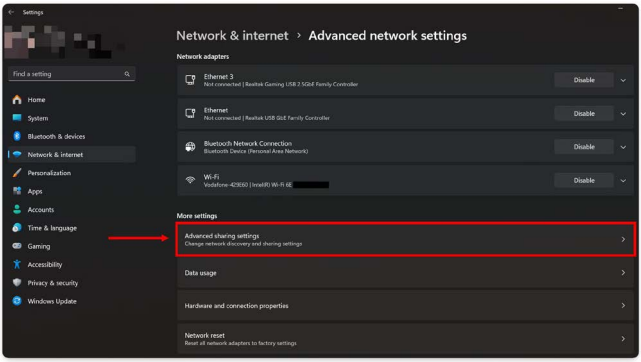


- If current network is set to public (default setting), users are asked whether they want to enable network discovery for all public networks or change current network to private.
  Choose "No, make the network I am connected to a private network".
- If network discovery is off, a warning banner will pop-up. Click the yellow banner and select "Turn on network discovery and file sharing".
  Administrator permissions are required to apply this change.

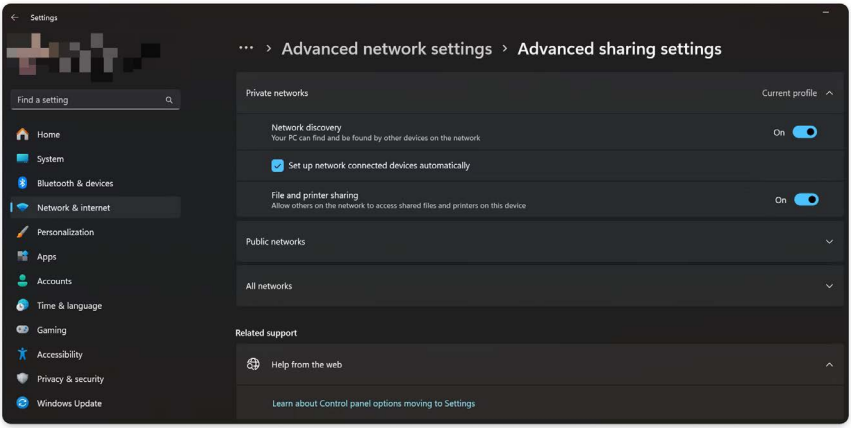
2.1.3. Advanced Sharing Settings

- [Enable Network Discovery]
  Allows the Windows PC to broadcast its presence and see other devices on the local subnet. Otherwise, the titrator might fail to locate or verify the computer's hostname/IP address on the network.
- [Enable File and Printer Sharing]
  Starts the background Windows services responsible for listening to incoming SMB traffic.
  The host PC will completely ignore or reject any incoming file transfer requests, if "Enable File and Printer Sharing" is turned off, even if SMB Direct has been enabled.

1. Press Windows key (⊞) and search "Advanced sharing settings". Next, click on the shortcut.
   Alternatively, go to [Settings] → [Network & internet] → [Advanced network settings] → [Advanced sharing settings].

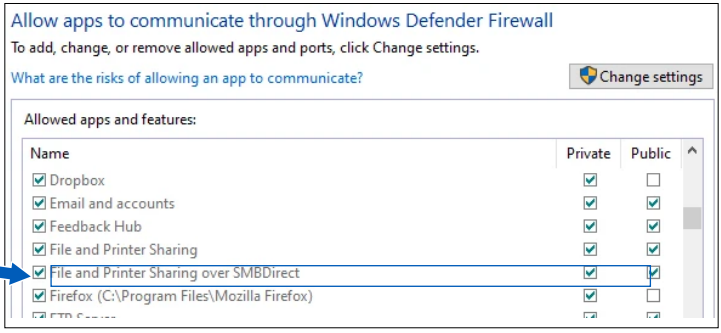


2. Click the "Private networks" dropdown to expand the section.
   - Toggle the switch to **On** for "Network discovery".
   - Toggle the switch to **On** for "File and printer sharing".



2.1.4. Firewall Settings

1. Press Windows key (⊞) and search "Allow an app through Windows Firewall".
2. Press **Enter** key.
3. Click the [Change settings] button at the top right.
   Administrator permissions are required to apply this change.
4. Scroll down the list and enable ☑ "File and Printer Sharing over SMBDirect".
   Ensure the checkbox under the "Private" column on the right is also checked.
5. Click [OK] to save changes.

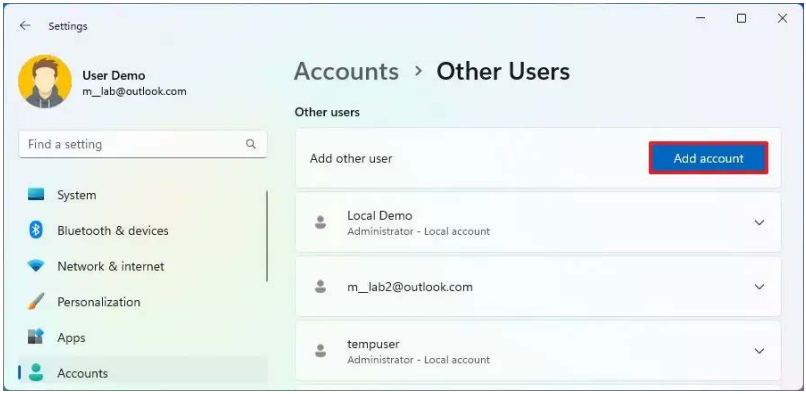


2.1.5. Create User Account and Password

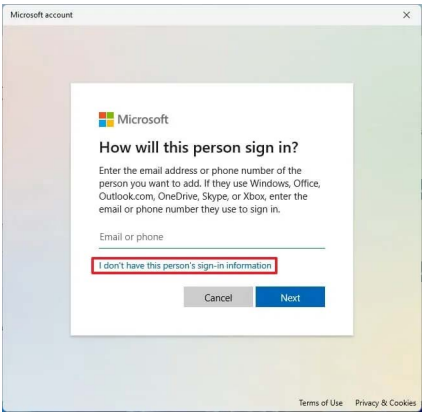
To connect HI932 Automatic Titrator to a PC's SMB server, create a local user account (ex. **user1**) directly on the Windows PC. The HI932 Titrator uses these exact username and password credentials to log in and transfer reports on the network share.

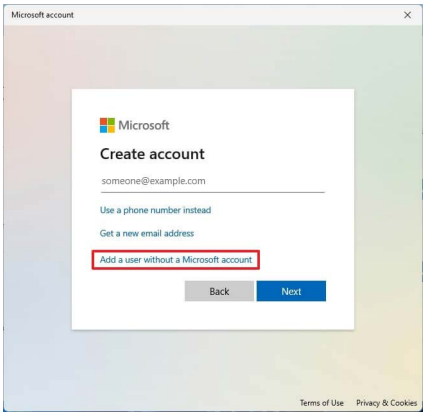
Note: *Existing users can also be used to access the PC's SMB server. Please consult local IT department for support when setting up users and permissions.*

1. Press windows key (⊞) and type "Other users".
2. Click on the "Add, edit, or remove other users" system setting.
3. Under the "Other users" section, click the [Add account] button next to "Add other user".



4. In the Microsoft popup, click "I don't have this person's sign-in information".
5. Click "Add a user without a Microsoft account".





6. Fill in the desired "User name" and "Password" fields.
7. Complete the mandatory Security Questions.
8. Click [Next] to finalize creating the local account.

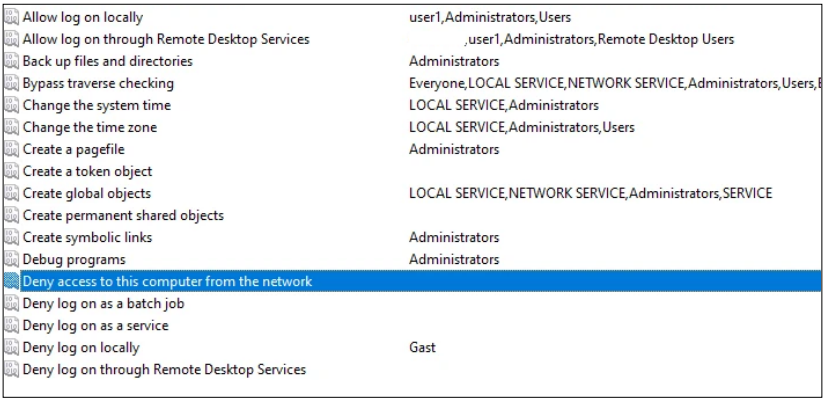
9. Grant "Administrator Rights" for HI932 Titrator, to be able to create and save files to network drives.
   Note: *If the titrator user lacks administrative folder-writing privileges, network file saving will fail.*
   9.1. While still on the "Other users" page, click on the newly created account name to expand it.
   9.2. Click the [Change account type] button.
   9.3. Open the "Account type" dropdown menu and select "Administrator".
   9.4. Click [OK] to apply the changes.
10. After user creation, log into the created Windows account to setup the local user.

2.1.6. Security Policy

Note: *The steps below require Windows 11 Pro or Enterprise and may require elevated administrator permissions. Please consult local IT department for support.*

1. Press the Windows key (⊞) and locate "Local Security Policy".
2. Navigate to and click on "Local Policies".
3. Navigate to and click on "User Rights Assignment".
4. Edit policy.
   - Double-click "Allow log on through Remote Desktop Services".
   - Click [Add User or Group].
     » Type the exact user name (see 2.1.5. Create User Account and Password).
     » Click [Check Names] then [OK].
   - Double-click "Deny log on through Remote Desktop Services"
     » Ensure the specific user account assigned to the titrator is not listed here.

     Note: *Do not remove default system or administrator groups, as this creates security risks.*
   - Ensure "Deny access to this computer from the network" is not active.
     » The user's name sharing the files should not be listed here.



User access via remote access (i.e sending files from titrator) should now be enabled.

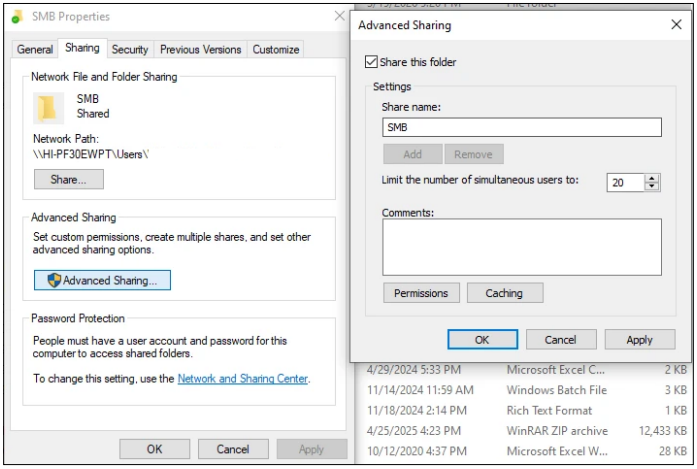
Notes:

- *To avoid any issues, review the firewall settings to ensure* **port 445** *is not blocked.*
- *Consult with IT department, if there are any issues.*

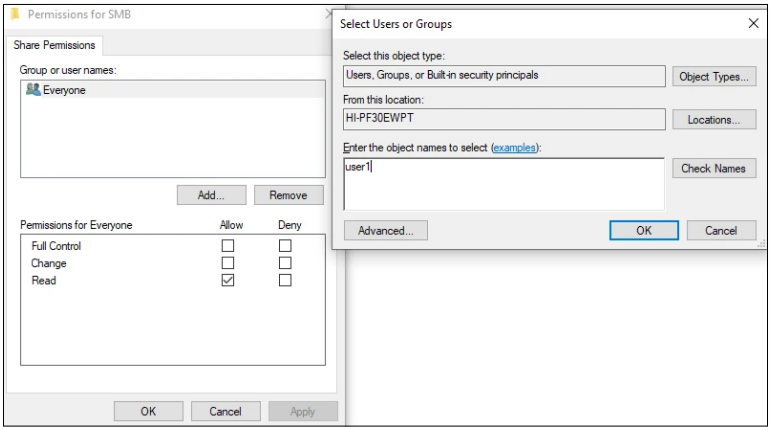
2.2. SMB SERVER FOLDER SETUP

1. Create a new folder in the desired location (ex. SMB folder in Documents).

2. Share the created folder on the network.
   2.1. Right click on the folder and press [Properties].
   2.2. Go to "Sharing" tab and press [Share].



   2.3. Add the created local user (ex. **user1**), change permissions to "Read/Write", and press [Share].
   2.4. Press [Advance Sharing...].
   2.5. Press [Permissions] then [Add...].
   2.6. Type the user name (see 2.1.5. Create User Account and Password) .
   2.7. Click on [Check Names] followed by [OK].



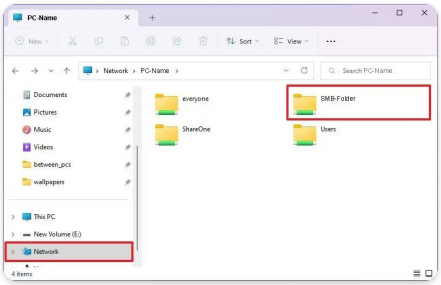
2.8. Check ☑ **Allow** for all permissions of **user1** and **Everyone** users.
2.9. Press [Apply] followed by [OK].
2.10. Close Advanced Sharing window with [Apply], then press [OK].

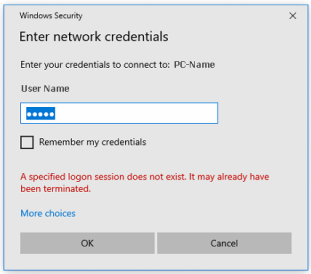
Network path will be updated to the name of the computer and the shared folder name.
The SMB server is now set up. (e.g. **PC-Name\SMB-Folder**\).

2.3. TEST SMB SERVER ACCESS

Use another computer on the same network to log in:

1. Type the Network Path.
   1.1. Open **File Explorer**.
   1.2. Type the network path into the address bar ([\\PC-Name\SMB-Folder\]) and press [Enter].
   1.3. Type the network user password when prompted and press [Enter].
   In some cases, users may be prompted to enter their pin. Press [More Choices] and sign in using user name and password credentials to log into the local PC.





2. Use the Command Terminal.
   2.1. Open the [Start menu], type `"cmd"`, then press [Enter].
   2.2. Type the command below, then press [Enter].
   `"net use \\PC-Name\SMB-Folder /user:user1 * "`
   2.3. Type the network user password when prompted, then press [Enter].
   2.4. To reconnect the mapped drive after a reboot, type the command below, then press [Enter].
   `"net use Z: \\PC-Name\SMB-Folder /user:user1 * /persistent:yes"`
   2.5. Type the network user password when prompted, then press [Enter].

Notes:

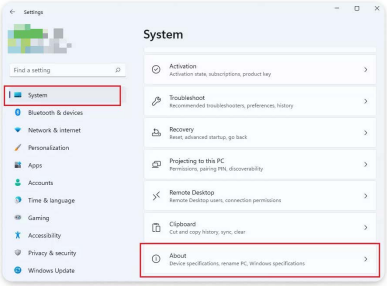
- *Replace* `"PC-Name", "SMB-Folder", "user1"` *with actual names.*
- `"Z"` *is the drive letter you want to assign to the mapped network drive.*

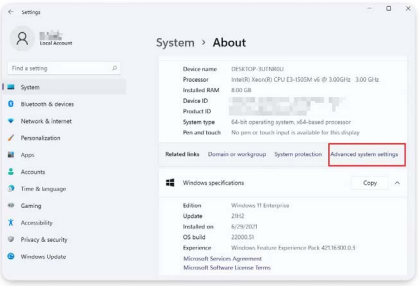
3. Map a Network Drive.
   3.1. Open File Explorer and click on `"This PC"` in the left sidebar.
   3.2. In the top ribbon, click on the three dots (Windows 11) or the Computer tab (Windows 10).
   3.3. Select [Map network drive]. Choose a drive letter from the drop-down menu.

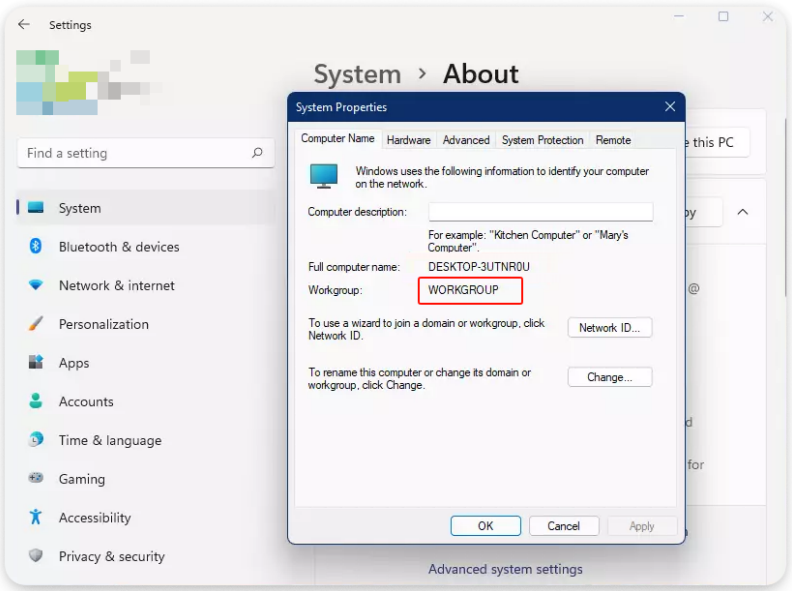
3.4. In the folder box, type the network path (e.g. **PC-Name****SMB-Folder**\).
3.5. Check [Connect using different credentials] to enter a specific username and password.
3.6. Check [Reconnect at sign-in] to automatically reconnect.
3.7. Click [Finish].
3.8. Type the network user password when prompted, then press [Enter].

2.3.1. Find Workgroup Name

1. Press Windows key (⊞) and search "System".
2. Scroll down and press "About".



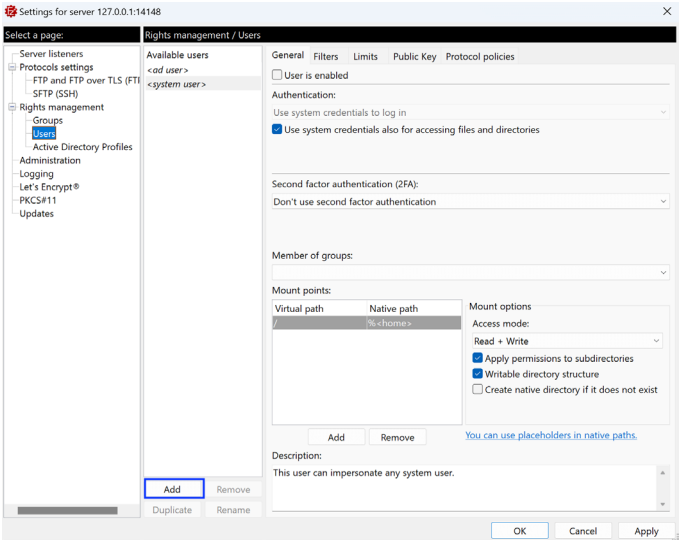




3. FTP / FTPS SERVER SETUP (FILEZILLA)

This section contains instructions for configuring a FTP server using FileZilla Server v1.12.5 with secure FTPS (FTP over TLS).

Follow the installation process after opening the FileZilla installer. The user will be prompted to create an administrator password to log into the FileZilla Server after installation.



Note: *Please consult local IT department for secure installation.*

The FTP installations consists of two primary functional components:

- FileZilla Server, runs in the background and handles network traffic (serving or receiving files). The server must be started using `"Start FileZilla Server"` shortcut installed.
- Administer FileZilla Server, the graphical configuration app, used to manage the server.

Note: *Stop the FileZilla Server service before changing configuration. Restart service after changes.*

3.1. FILEZILLA SERVER OPTIONS

1. Open **Administer FileZilla** Server.
2. Press [Server] and enter adminstrator credentials.
3. Press [Configure].
4. Add **Users.**
   - 4.1. Select [Users] then click [Add].
   - 4.2. Enter a username.
   - 4.3. Set a secure password.

   Note: these will be the credentials used in FTP Setup on HI932.

5. Assign **Directory.**
   5.1. Go to [Mount Points] and click on [Add].
   5.2. Select a folder (e.g. C:\FTP) as the user's home directory.
   The folder path must be typed under Native path.
6. Assign required **Permissions** (read, write, delete, append).
7. **Load Certificate Files,** required files: **server.key** (private key) + **server.crt** (certificate file).
   7.1. Under protocol settings, go to [FTP] and [FTPS over TLS (FTPS)], then [TLS Credentials] section.
   7.2. From drop-down menu, select: `"Provide a X.509 certificate and private key"`.
   7.3. Enter the **Certificate** path to file: [path]\server.crt
   7.4. Enter the **Private key** path to file: [path]\server.key
   7.5. Enter the private key password when prompted.
   7.6. Save the configuration.

Notes: *The certificate and private key must match; the private key must be protected. Incorrect files will prevent TLS from working. Please consult local IT department on how to obtain server certificates and keys.*

3.2. SERVER LISTENERS

1. Open Administer FileZilla Server → go to [Server Listeners].
2. [Explicit FTPS]
   - Port [21]
   - Configuration: enable FTP protocol, select Explicit FTP over TLS, select insecure (plain) FTP
   - Description: starts as FTP and upgrades to TLS
   - Usage: recommended for broad configuration and supports secure and legacy clients
3. [Implicit FTPS]
   - Port [990]
   - Configuration: enable TLS immediately
   - Description: fully encrypted from connection start
   - Usage: used for compatibility with specific systems, no upgrade required
4. [Multiple Listeners]
   Configuration
   - Port [21] (Explicit FTPS)
   - Port [990] (Implicit FTPS)

3.3. PASSIVE MODE CONFIGURATION

1. Configure **passive mode ports** to [50000-51000].
2. **External Address**
   Enter the server's public IP address or hostname.
   Note: *Required for most client connections, or when behind firewalls or NAT.*

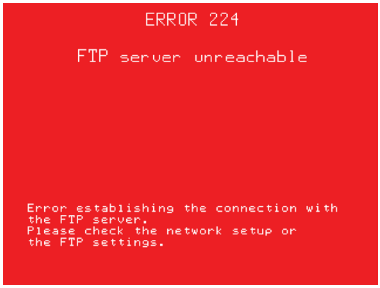
3.4. WINDOWS FIREWALL CONFIGURATION

This section explains how to configure Windows Defender Firewall for FileZilla Server.

1. Open **Windows Defender Firewall**.
   1.1. Open the Start Menu.
   1.2. Search for `"Windows Defender Firewall with Advanced Security"`.
   1.3. Open the application.
2. **Port 21** (Explicit FTPS)
   2.1. Click [Inbound Rules] then [New Rule].
   2.2. Select [Port], then [Next].
   Select [TCP] and enter [21].
   2.3. Select [Allow the connection] followed by [Apply to all profiles].
   2.4. Name the rule `"FileZilla Server - Port 21"` and click [Finish].
3. **Port 990** (Implicit FTPS)
   3.1. Follow steps listed above but change target port from TCP port 21 to TCP port [990].
   3.2. Name the rule `"FileZilla Server - Port 990"` and click [Finish].
4. **Passive Ports**
   4.1. Click [New Rule] then select [Port]. Next, select [TCP] and enter [50000-51000].
   4.2. Select [Allow the connection] followed by [Apply to all profiles].
   4.3. Name the rule `"FileZilla Server - Passive Ports"` and click [Finish].

3.5. TROUBLESHOOTING

1. Connection issues
   1.1. Server must be running.
   Note: *Restart the FileZilla Server service after configuration changes.*
   1.2. Ensure rules are [Enabled], ports are listed, and TCP is selected.
   » [Explicit FTPS]
   Port [21], [Explicit FTP over TLS] encryption
   » [Implicit FTPS]
   Port: [990], [Immediate TLS] encryption
   1.3. Check passive mode.
   1.4. Check firewall and passive ports configuration.



2. Login errors
   2.1. Check login credentials (username / password).
   2.2. Verify user configuration.
3. TLS errors
   3.1. Check if the certificates load correctly.
   3.2. Check private key and password.
4. Transfer issues
   4.1. Check connection to FTP server.
   4.2. Check shared folder permissions.