Remote Data Upload System Guide

Table of contents

Requirements

Hardware	<Suggestions>	Software
Server	• 2GHz processor • 2GB RAM	• Ubuntu Linux Server 18.04 (Other Linux/Unix distributions can be used if the user knows how to adapt the instructions in this document to the particular distribution)
Desktop	• O/S 64 bits • Windows, Linux or Mac	• Plain Text Editor[1] • EMpower • Rsync or SFTP client to retrieve the time series from the server
Receiver	• Supported receiver, for example an ***MTU-5C receiver***	• Firmware v1.35.x or above

[1] Use plain text mode in TextEdit on Mac (Format -> Make Plain Text)

Server Setup

1. ***Install Ubuntu Server 18.04***
   - During the installation process, you will be asked a few questions. Most of them you will have to answer according to your hardware and local language
   - You need to create a user account to administer the server, this guide assumes the admin username is **`phoenix`**
   - When the installer asks if you want to install ***OpenSSH***, answer *yes*
   - Do not install any special packages
   - After the installation is complete, reboot the system
2. ***Configure system for network upload***
   - Login to the server as **`phoenix (command)`**
   - System software upgrade

     ```
     $  sudo apt update; sudo apt upgrade -y
     ```
   - Enable public key server login

     ```
     $  sudo sed -i s/#PubkeyAuth/PubkeyAuth/g /etc/ssh/sshd_config
     $  sudo systemctl restart ssh.service
     ```
3. ***Create a user account for uploading files to the server***
   - *For instance, if you want to create a user named **`username`**:*

     ```
     $  sudo adduser username
     ```
4. ***Create an SSH key for secure data transfer***

   ```
   $  sudo su - username
   $  ssh-keygen \
              -b 4096 \
              -C "Key for secure MTU-5C file transfer"
   ```

   Use the default filename (~/.ssh/id_rsa)

   ****** IMPORTANT: Do not use a passphrase *** (press enter)***
5. ***Enable public key user login***

   ```
   $  cat ~/.ssh/id_rsa.pub > ~/.ssh/authorized_keys
   $  chmod 600 ~/.ssh/authorized_keys
   ```
6. ***Save SSH Private key***

   ```
   $  cat ~/.ssh/id_rsa
   ```
   - Copy and Paste the key file into the text editor ***on Desktop***: (*<documents>/**username**_key.txt*) and save
7. ***Logout of server***

Network setup

You will need to provide a network connection between the receiver and the server. This connection can be local or it can go through the Internet.

The receiver can work with an IP address and other network parameters provided automatically through a DHCP server, or manually with a static IP configuration.

Consult your network/system administrator for help in determining the network details and to set up the required connections.

Configuring a receiver for network upload

1. ***Open EMpower v1.35.x or later***
    - Click ***Prepare*** in the main window
2. ***Select the receiver type***
    - At the top of the window that appears, select the type of receiver that you are configuring (example ***MTU-5C***), and then click the ***MT*** button inside of the ***Recording*** box
3. ***Configure networking***
    - Click the ***Channel*** selector at the top right part of the window, and then select ***NET***
    - Select the Network Mode
        - Select ***Auto (DHCP)*** for automatic configuration (*most common*)
        - Select ***Static*** if you need to configure manually (*Consult your network/system administrator for the required information)*
            - IP Address
            - Network Mask
            - Default Gateway
            - Nameservers
4. ***Configure File Transfer***
    - Select the ***File Transfer Method***
        - For this guide, use ***RSync*** which is much faster than ***SFTP***
    - Enter the ***Server URL***, *examples:*

      servername.com:/home/**username**
      192.168.1.77:/home/**username**
    - Enter the ***User Name*** of the user you created above, example:

      `username`
    - Paste the content of the ***SSH Key*** you generated above:

      *(<documents>/**username**_key.text)*
5. ***Configure normal recording details (gains, filters, setc)***
6. ***Save the configuration file to SD card***

Notes

The installation is very basic, and much more can be done to improve the server and its security. We recommend that you use the “authoriozed_keys” file to limit the capabilities of the login via the key generated, to prevent login for instance.

Also note that in the first release, files will be deleted from the receiver when they have been confirmed to be uploaded to the server to avoid getting permanent stations stopped due to lack of SD card space.