GE
Grid Solutions

Enterprise File Synchronization from G500 Sync Manager

Configuration Guide

SWM0104

Version 1.00 Revision 0

Associated Software Release: Version 1.00

GE Proprietary Information - Class II (Internal)

COPYRIGHT NOTICE

© 2018, General Electric Company. All rights reserved.

The Software Product described in this documentation may only be used in accordance with the applicable License Agreement. The Software Product and Associated Material are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and are delivered with Restricted Rights. Such restricted rights are those identified in the License Agreement, and as set forth in the "Restricted Rights Notice" contained in paragraph (g) (3) (Alternate III) of FAR 52.227-14, Rights in Data-General, including Alternate III (June 1987).

If applicable, any use, modification, reproduction release, performance, display or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is the exclusive property of General Electric Company, except as otherwise indicated. You may view, copy and print documents and graphics incorporated in this online publication (the "Documents") subject to the following: (1) the Documents may be used solely for personal, informational, non-commercial purposes; (2) the Documents may not be modified or altered in any way; and (3) General Electric Company withholds permission for making the Documents or any portion thereof accessible via the internet. Except as expressly provided herein, you may not use, copy, print, display, reproduce, publish, license, post, transmit or distribute the Documents in whole or in part without the prior written permission of General Electric Company. If applicable, any use, modification, reproduction, release, performance, display, or disclosure of the Software Product and Associated Material by the U.S. Government shall be governed solely by the terms of the License Agreement and shall be prohibited except to the extent expressly permitted by the terms of the License Agreement.

The information contained in this online publication is subject to change without notice. The software described in this online publication is supplied under license and may be used or copied only in accordance with the terms of such license.

TRADEMARK NOTICES

GE and are trademarks and service marks of General Electric Company.

* Trademarks of General Electric Company.

Other company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

Contents

About this Document 6

Purpose 6
Intended Audience 6
Additional Documentation 6

1. Overview 7

1.1 G500 Sync Manager 7
1.2 Copssh software 7
1.3 cwRsyncServer software 7
1.4 Installation Steps 7

2. Installation of copssh and cwRsyncServer 8

2.1 Software 8
2.2 Installation 8

3. Configuring G500 Sync Manager 25

3.1 Enable Sync Manager 25
3.2 Configure Sync Sets 25

4. Setting up Public Key Authentication 27

4.1 Update Permissions to SyncMgr Folder 27
4.2 Copy key from G500 to the Windows computer 27

A. Uninstalling cwRsyncServer and Copssh 29

B. Diagnostics 30

B.1 G500 Diagnostic Logs 30
B.2 Copssh Event Log on Enterprise Server 30

C. List of Acronyms 31

Figures

No table of figures entries found.

Tables

Table 1 Configure Sync Sets - Settings 25
Table 2 List of Acronyms 31

About this Document

Purpose

This document describes how to setup an enterprise server on a Windows-based computer to synchronize files from G500 device(s) that use the Sync Manager application (RSYNC/SSH protocol). This document outlines and details the procedures regarding:

- Installation and setup of CopSSH and cwRsyncServer tools on the computer. These are 3rd party software applications that have been tested with the G500 Sync Manager.
- Configuration of G500 Sync Manager Application to synchronize files to the enterprise server. The example is for ARRM files, but other user related files / folders may be synchronized too (e.g. Logs).

Once the data is present in the Windows Enterprise computer, the sharing of folders and files from this computer to Enterprise users is outside of scope of this document and can be achieved using any IT / Windows standard sharing methods.

Intended Audience

This document serves as a reference for systems integrators who wish to setup enterprise server on Windows-based computer to synchronize files from G500 Sync Manager device(s).

Additional Documentation

For further information about the Enterprise File Synchronization from G500 Sync Manager, refer to the following documents:

- G500 Substation Gateway, Software Configuration Guide, SWM0101
- G500 Substation Gateway, HMI Online Help

1. Overview

1.1 G500 Sync Manager

The Sync Manager is a G500 application that can be used to securely and automatically copy files from a location on your G500 device to a specified directory on a remote device. The application monitors the specified local directory for changed or added files. To reduce bandwidth demands on your network, only files found to have been changed or created since the last synchronization will be transferred. This utility employs the *rsync* protocol to perform this function, secured by an SSH layer.

Multiple file sets can be configured for synchronization in the G500, to send data to one or multiple target remote devices, using one or multiple user authentications.

1.2 Copssh software

Copssh is a 3rd party Windows-based software that enables SSH server on Windows-based computer.

1.3 cwRsyncServer software

cwRsyncServer is a 3rd party Windows-based software that enables rsync utility on Windows-based computer.

1.4 Installation Steps

1. Install cwRsyncServer and Copssh softwares on Windows-based computer acting as Enterprise Server (Refer chapter 2. Installation of copssh and cwRsyncServer)
2. Configure G500 Sync Manager Application (Refer to chapter 3. Configuring G500 Sync Manager)
3. Setup public key authentication between G500 (client) and enterprise server (Refer to chapter 4. Setting up Public Key Authentication).

2. Installation of copssh and cwRsyncServer

This chapter describes how to install Copssh and cwRsyncServer software on Windows-based Enterprise Server.

2.1 Software

- Obtain the commercial version of cwRsyncServer software from: https://www.itefix.net/cwrsync

  Note: obtain the server version of cwRsync, i.e., cwRsyncServer.

- Obtain the commercial version of Copssh software from: https://www.itefix.net/copssh

  Note: GE DE GA has no commercial / reseller agreements in place with ITeF!x

2.2 Installation

cwRsyncServer software must be installed before Copssh.

Note: Before starting the installation, ensure that any previous installation of cwRsyncServer and Copssh is completely uninstalled.

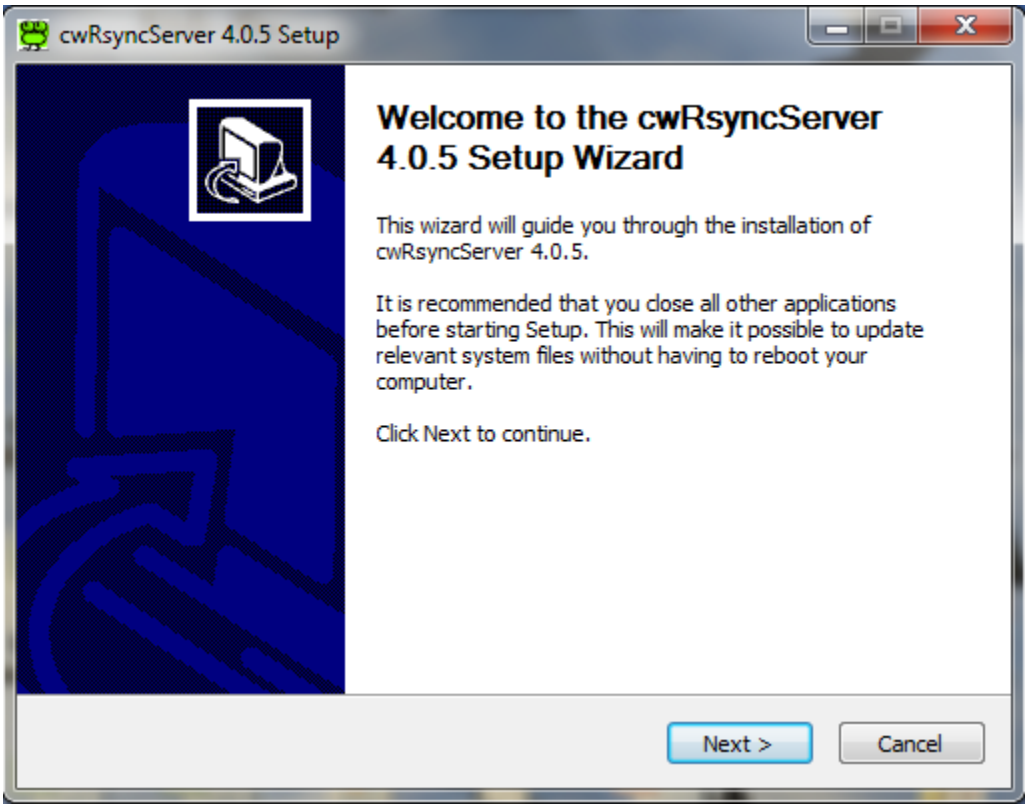
Follow Appendix A to completely uninstall cwRsyncServer and Copssh before proceeding with below steps.

2.2.1 cwRsyncServer

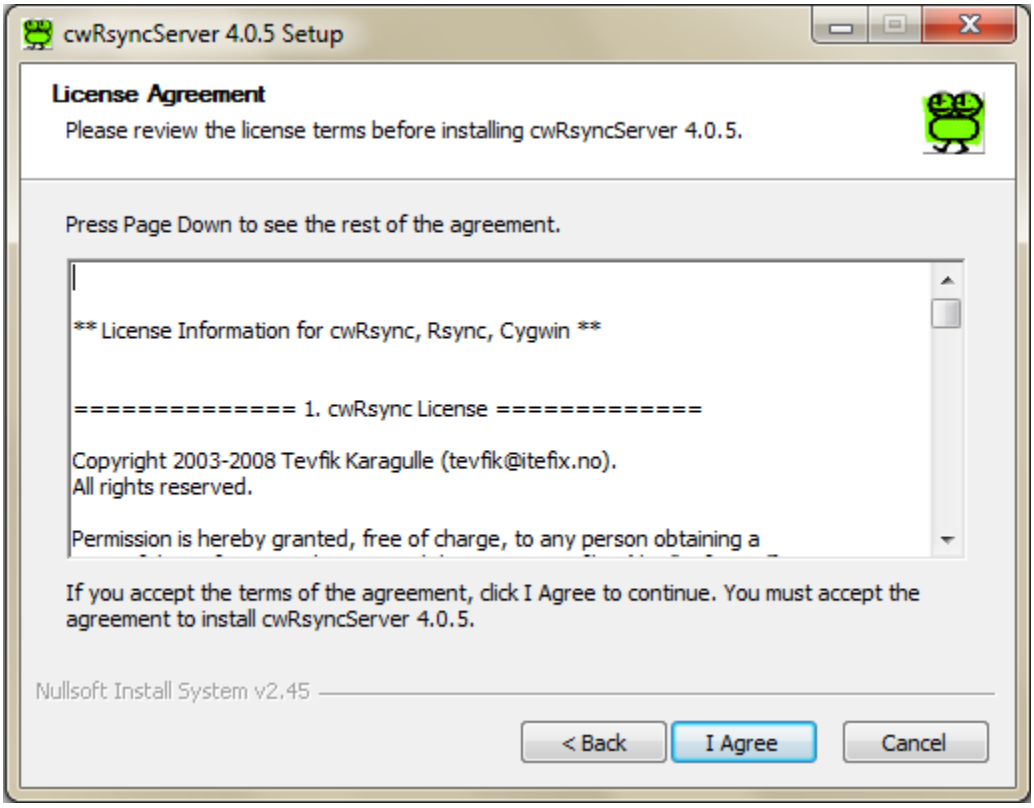
1. Start installation of cwRsyncServer by running its setup program. Follow the steps below to complete the installation.

   Note: The cwRsyncServer setup program must be run as administrator by Right click on the program, and selecting "Run as administrator" (Windows 7).

2. cwRsyncServer Setup dialog appears. Click “Next”.

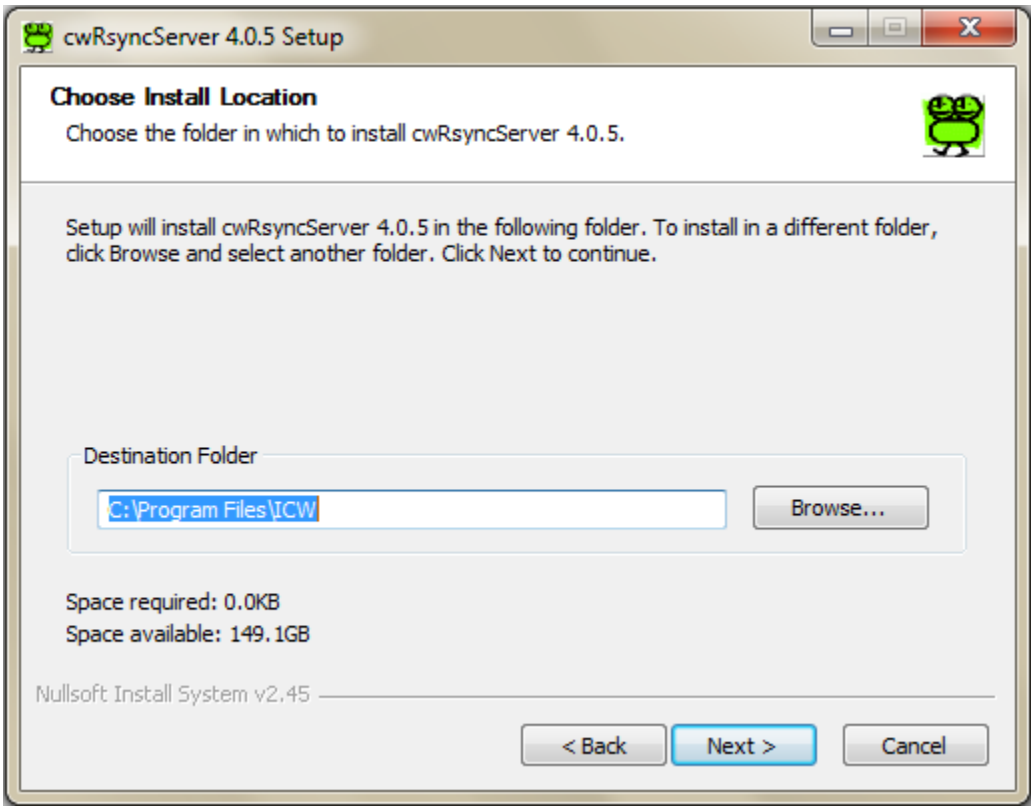


3. Click “I Agree” on the “License Agreement” window.

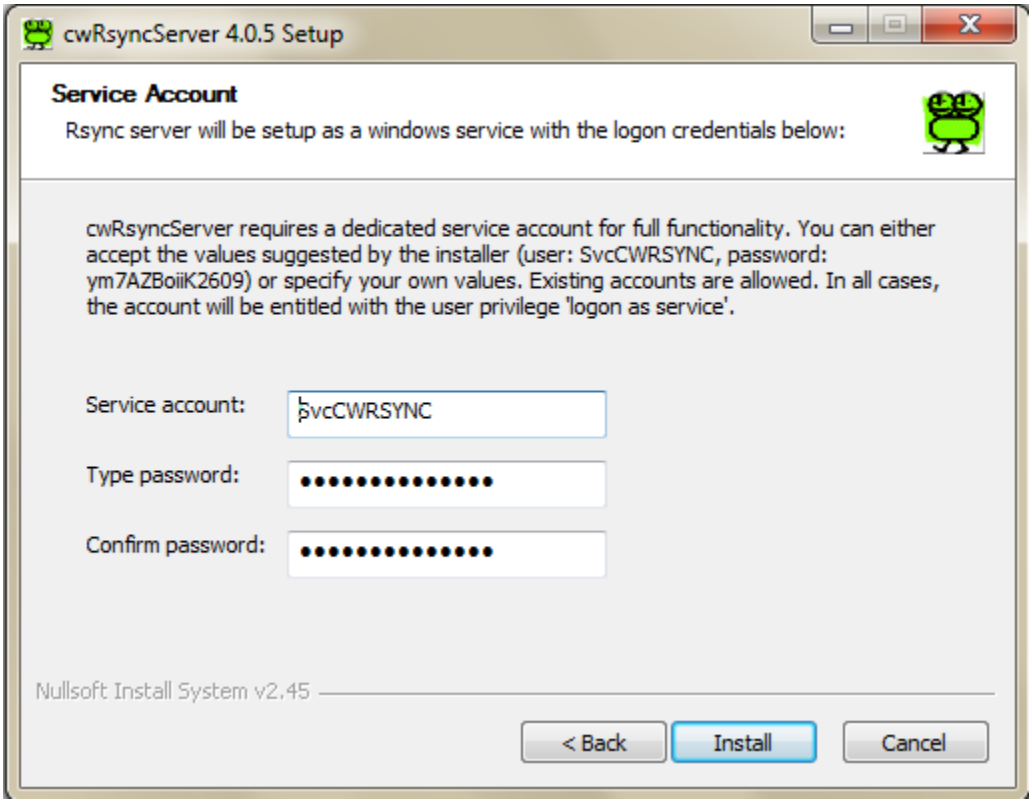


4. On the "Choose Install Location" window, click "Next" to select the default location.

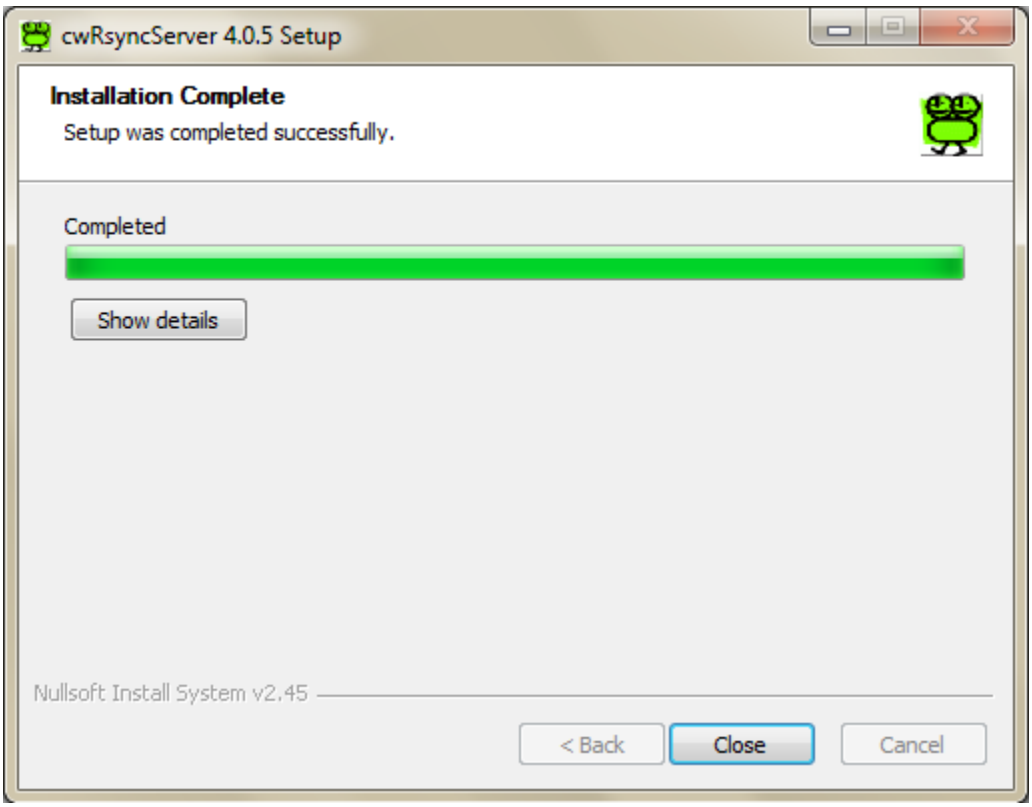
   Note: Ensure that destination folder is "**C:\Program Files\ICW**" on a 32-bit operating system or "**C:\Program Files (x86)\ICW**" on a 64-bit operating system. If not, manually update the installation location.



5. On the "Service Account" window, click "Install" to select default service account name and password.



6. On the "Installation Complete" window, click "Close" to complete the installation.



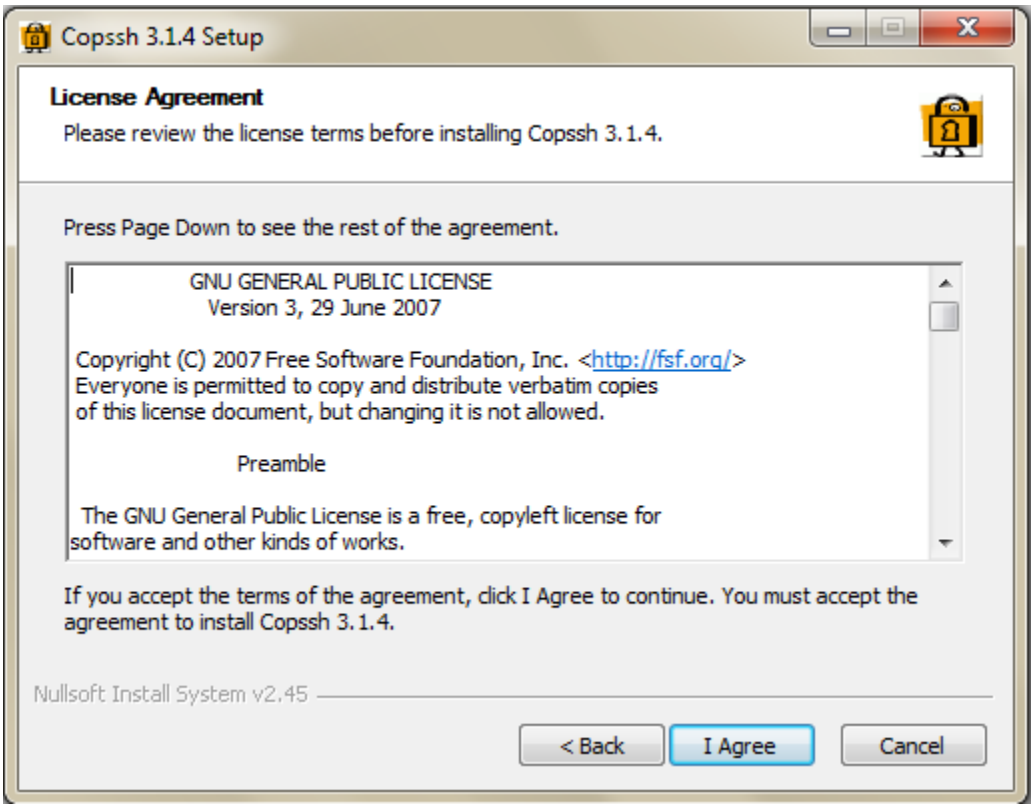
2.2.2 Copssh

1. Start installation of Copssh by running its setup program. Follow the steps below to complete the installation.

   Note: The Copssh setup program must be run as administrator by Right click on the program, and selecting "Run as administrator".

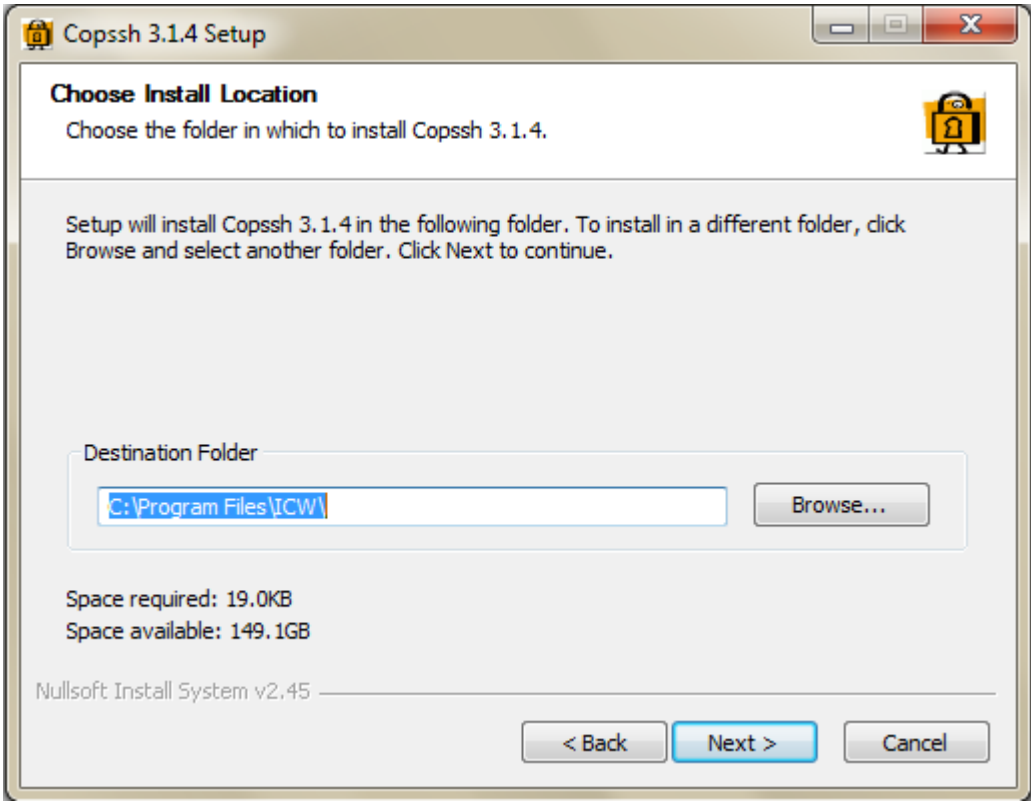
2. On the "Copssh Setup" window, select "Next".

3. Click “I Agree” on the “License Agreement” window.

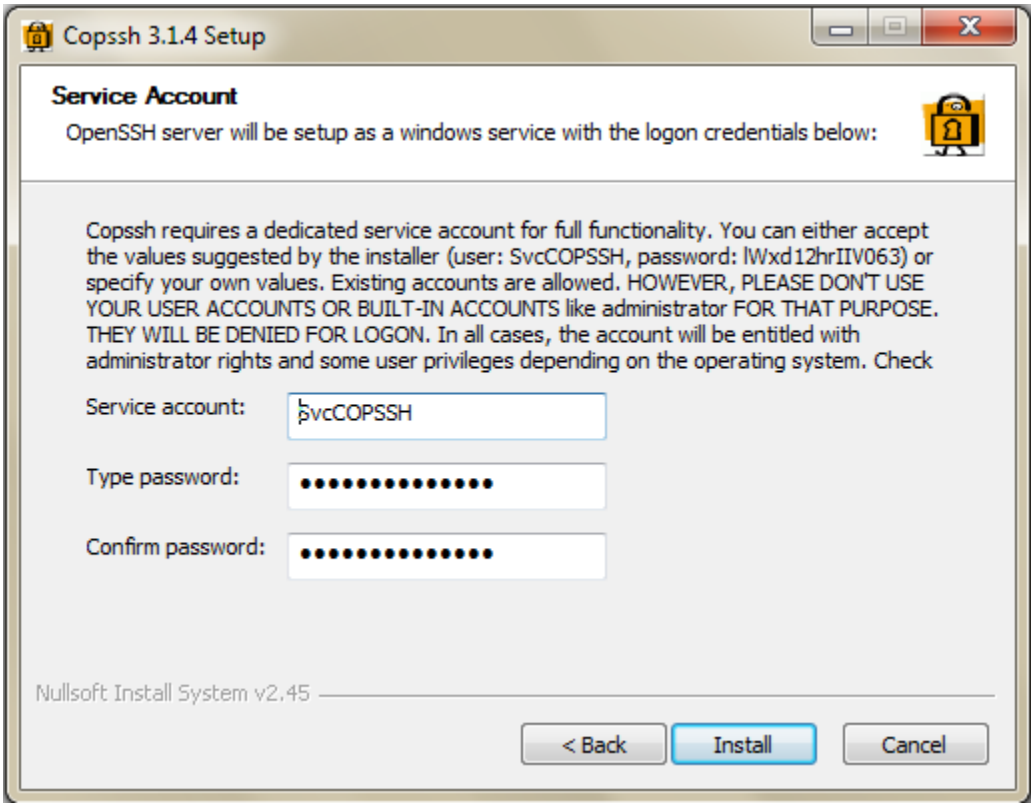


4. On the "Choose Install Location" window, click "Next" to select the default location.

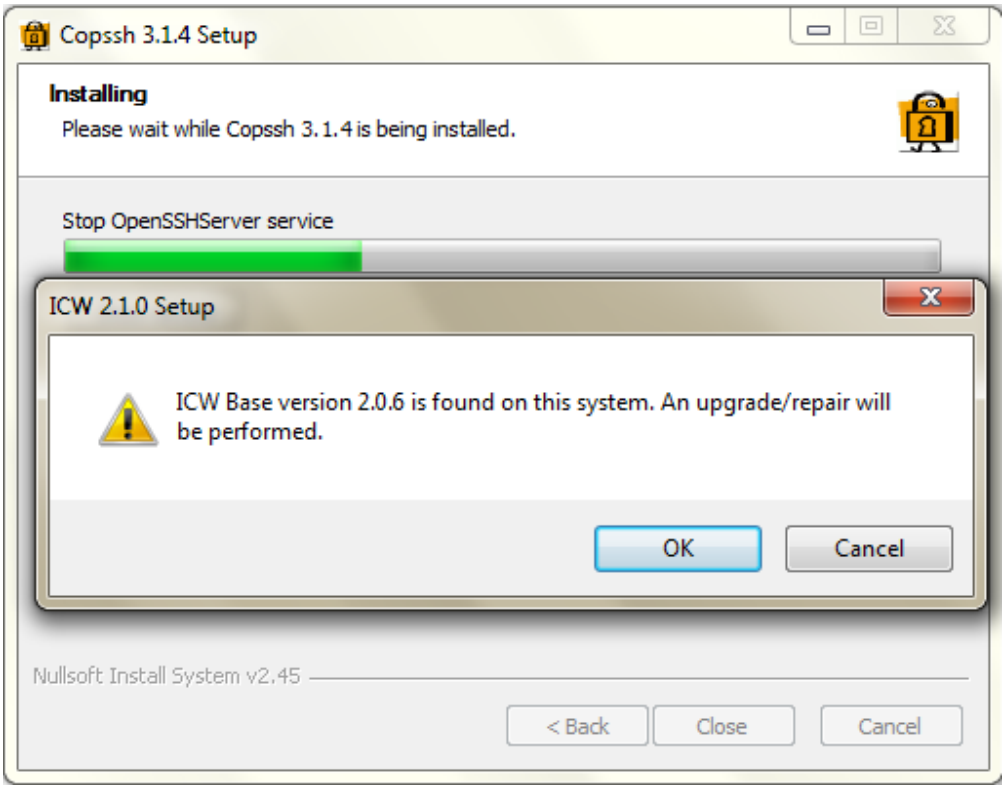
   Note: Ensure that destination folder is "**C:\Program Files\ICW**" on a 32-bit operating system or "**C:\Program Files (x86)\ICW**" on a 64-bit operating system. If not, manually update the installation location to match the installation location of the cwRsyncServer installation folder.



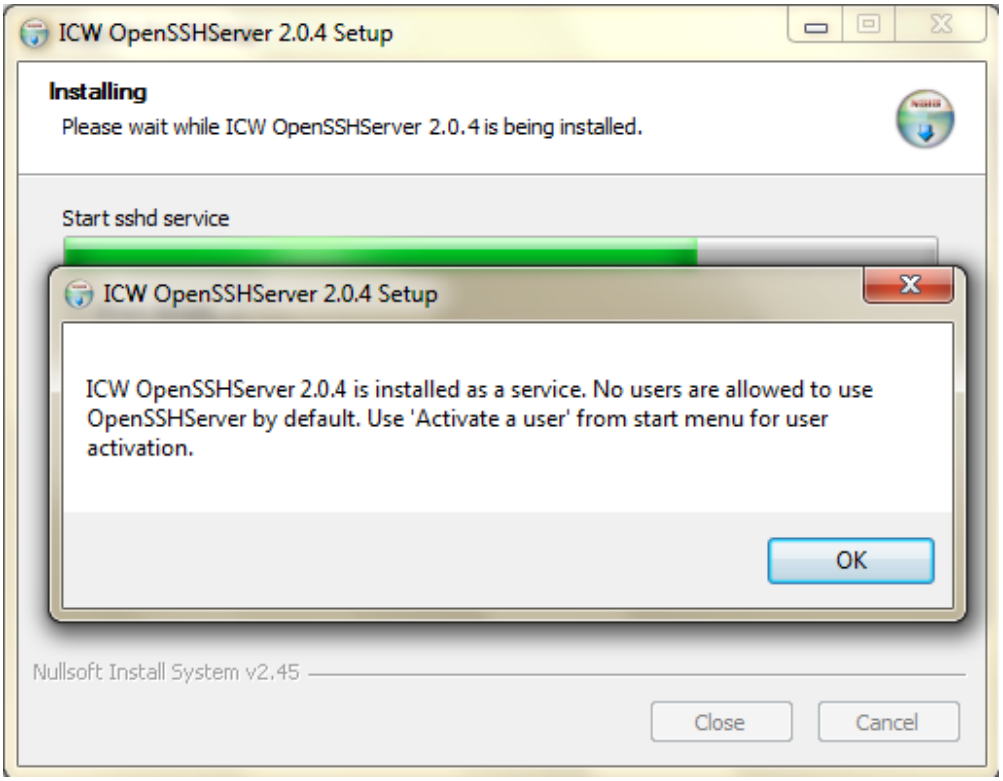
5. On the “Service Account” window, click “Install” to select default service account name and password.



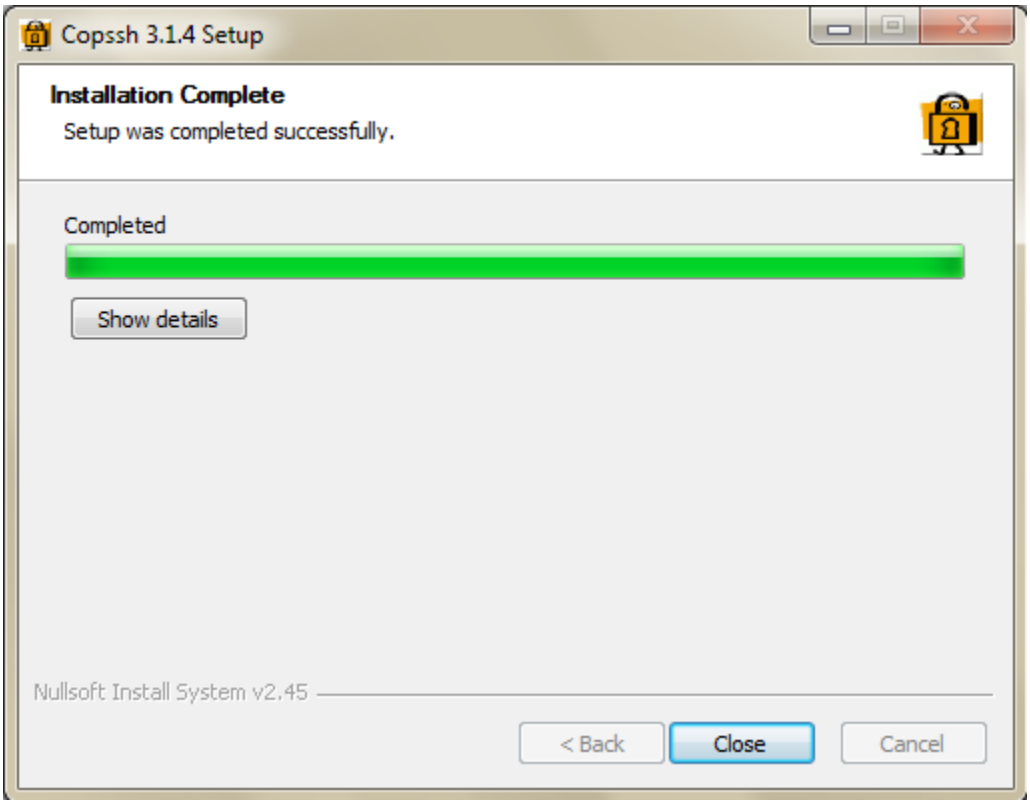
6. Since cwRsyncServer is already installed, installer will warn that ICW Base is already installed, and upgrade/repair will be performed. Click “OK”.



7. At the end of installation, Setup program will notify to activate user(s) that are allowed to use OpenSSH server. Click “OK” to complete the installation.



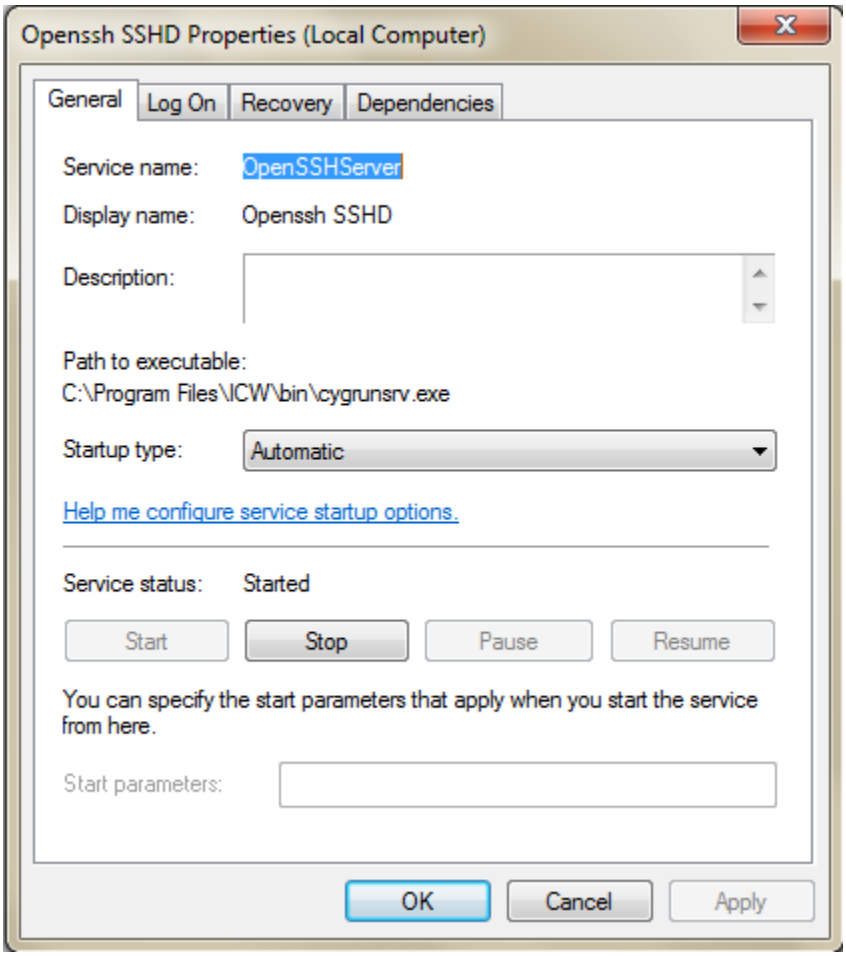
8. On the “Installation Complete” window, click “Close” to complete the installation.



9. Open Services Microsoft Management Console (MMC), from Control Panel → Administrative Tools → Services.

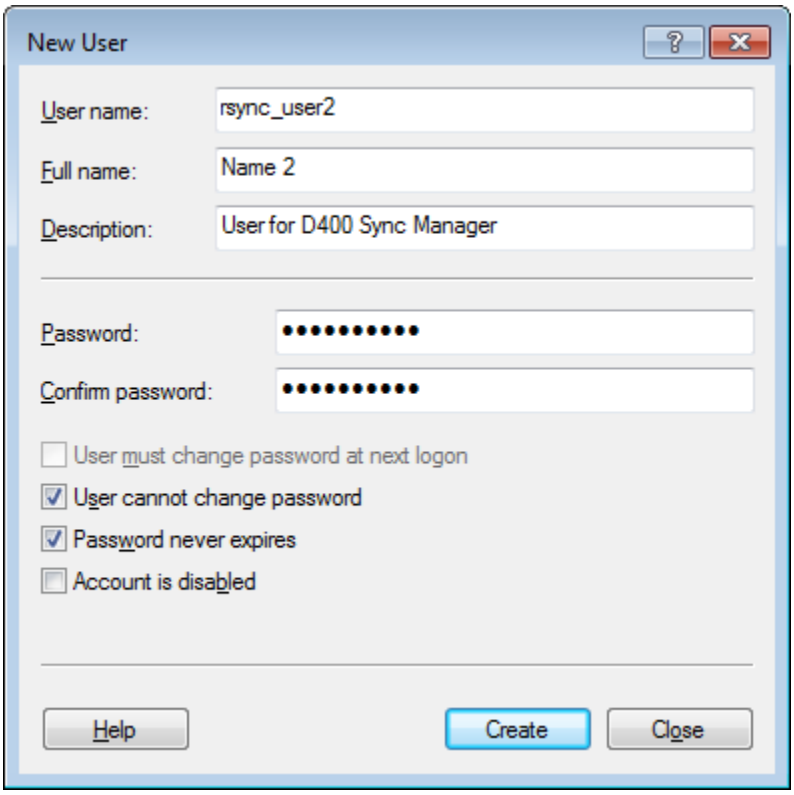
10. Double click on “Openssh SSHD” service to open its properties.

    Ensure that its Startup type is set to “Automatic”, and service is already in Started state.



2.2.3 Create Users in Windows computer

1. The users intended to be configured in G500 Sync Manager sync sets must exist in the Windows computer.
2. Use the Windows Control Panel / User management interface to add all users as needed. They should be “user” class, with password set to “user cannot change” and “no expire”. The password used here will not be used for G500 Sync Manager actions (Windows account only). These users have no need to login into the Windows computer account, and these credentials should be used only for the purpose of establishing sessions between the G500 and the Enterprise server.



2.2.4 Activate Users

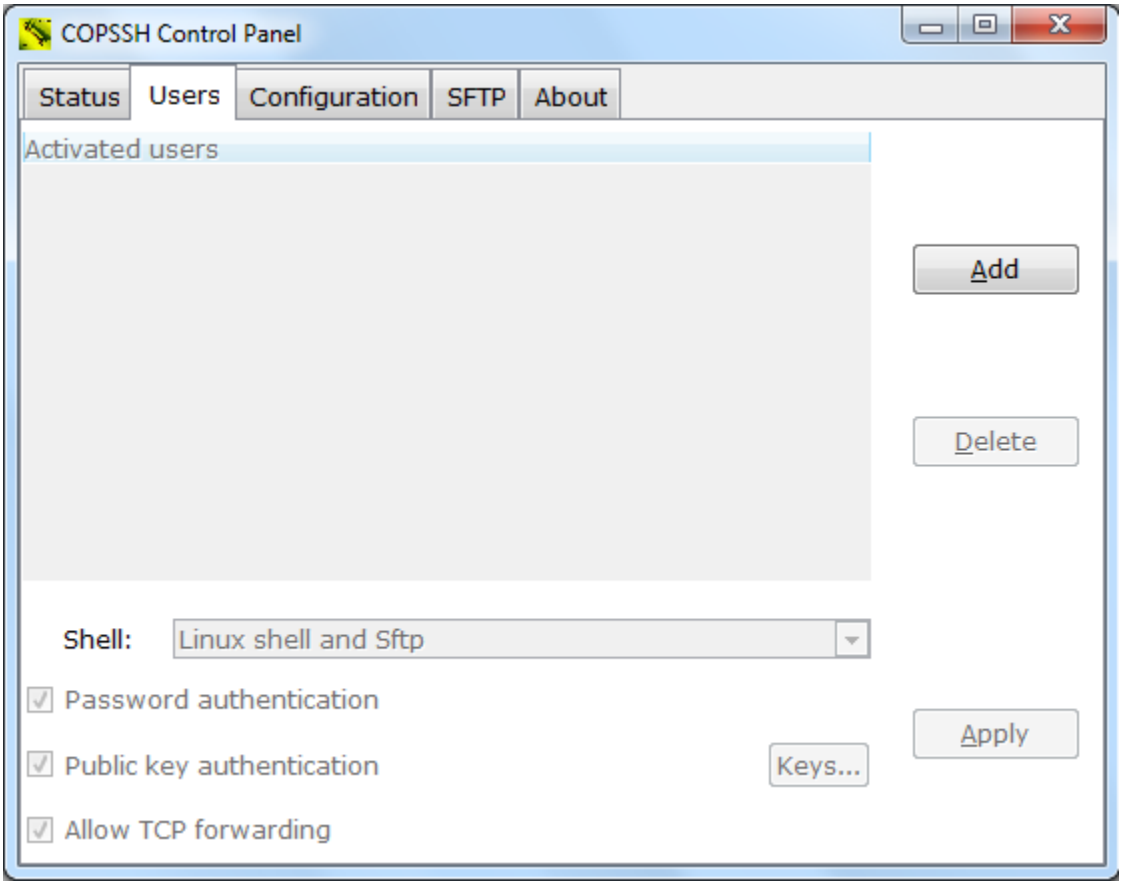
A Windows computer existing user must be activated before it can use OpenSSH service. This user will be used to sync files on this Windows-based computer from the G500 Rsync Manager. The user name must match the one configured in the G500 Sync Manager (each sync set has an option for a user name, they can be either common or distinct).

Depending on the software version, the dialog to activate users may be different.

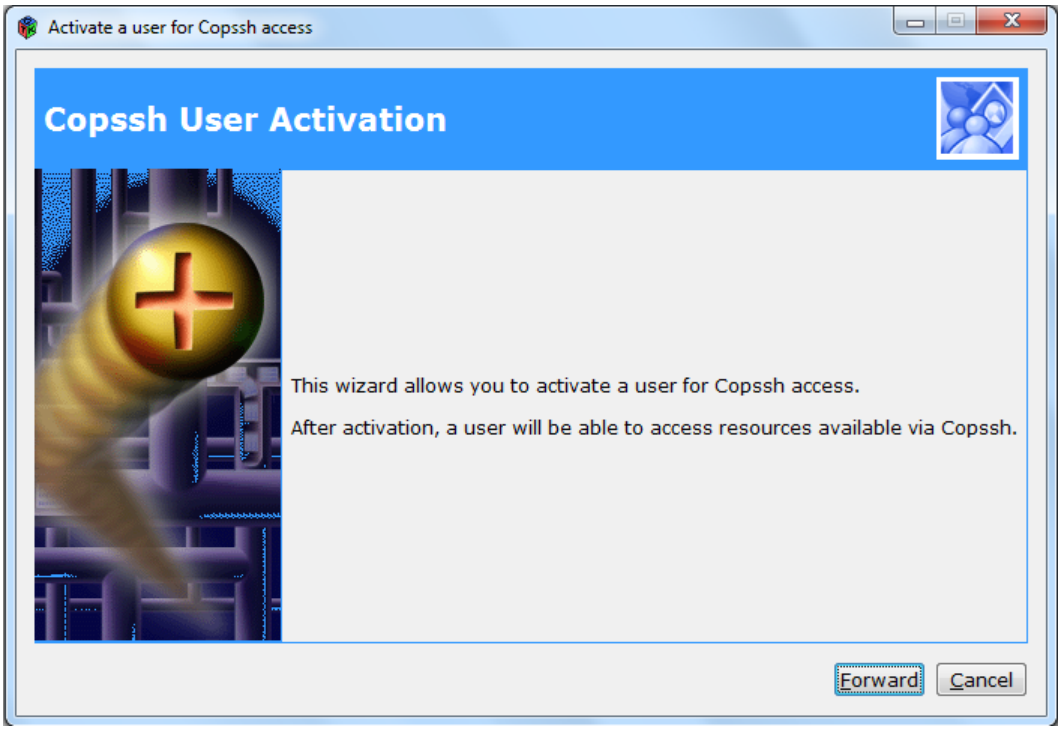
2.2.4.1 Method 1

1. Start “Copssh Control Panel” from Start Menu → All Programs → Copssh → Copssh Control Panel → Go to User tab.

   Note: The “Copssh Control Panel” program must be run as administrator.

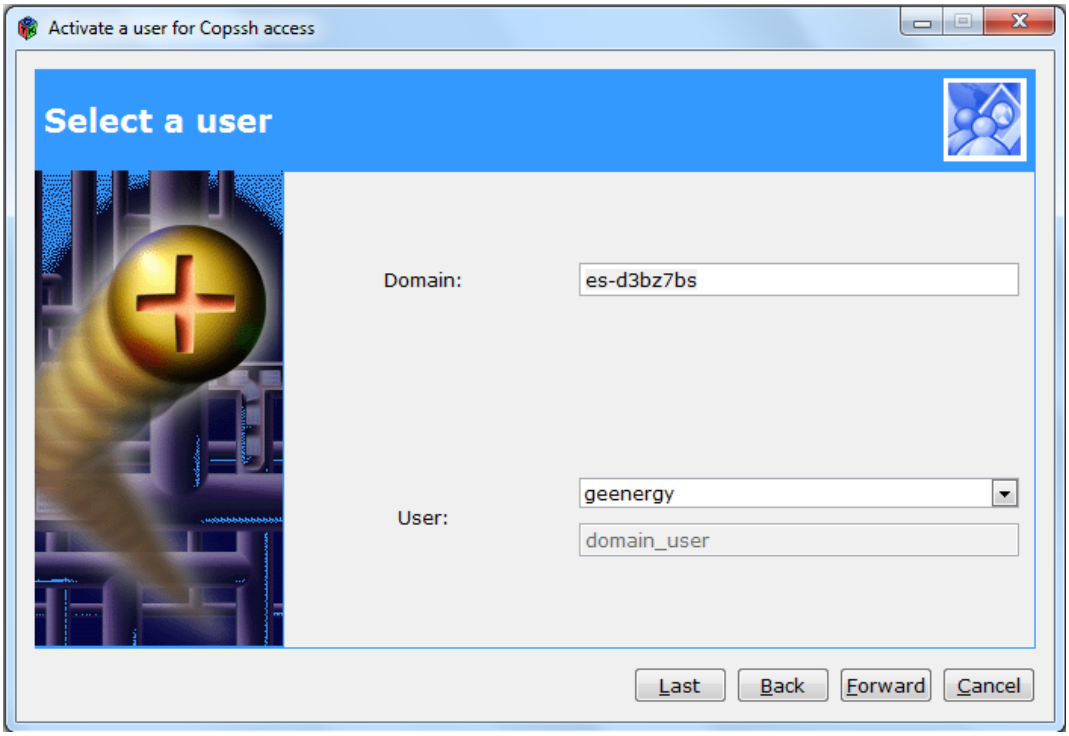


2. Click “Add” to activate a user: “Copssh User Activation” wizard opens.

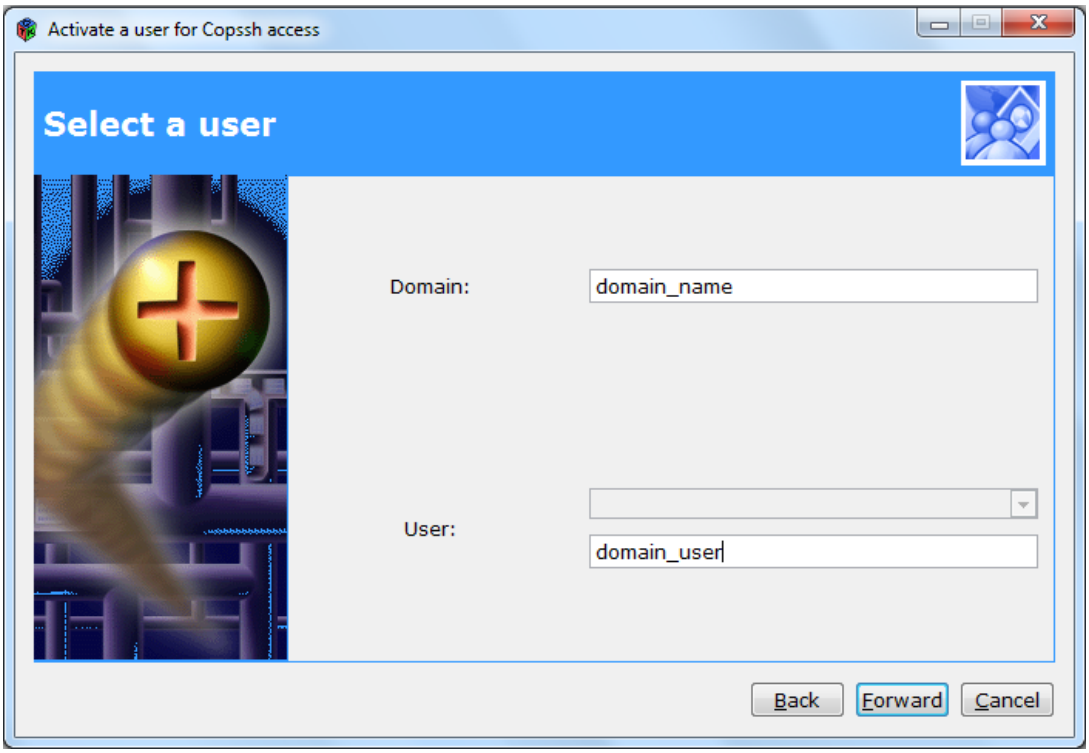


3. Click “Forward”: User selection interface opens. A local or domain user can be utilized on Windows-based computer for Copssh access.

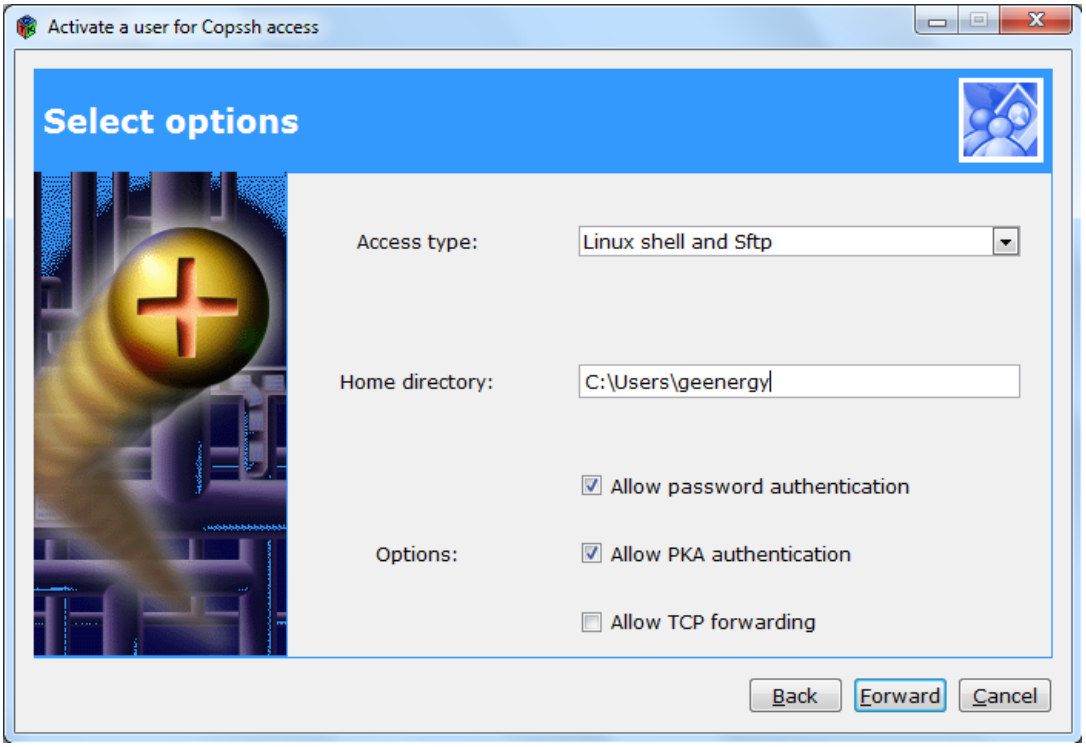
   Local User: Select a local user from the “User” drop down list.



Domain User: Enter domain name and user name in respective fields.



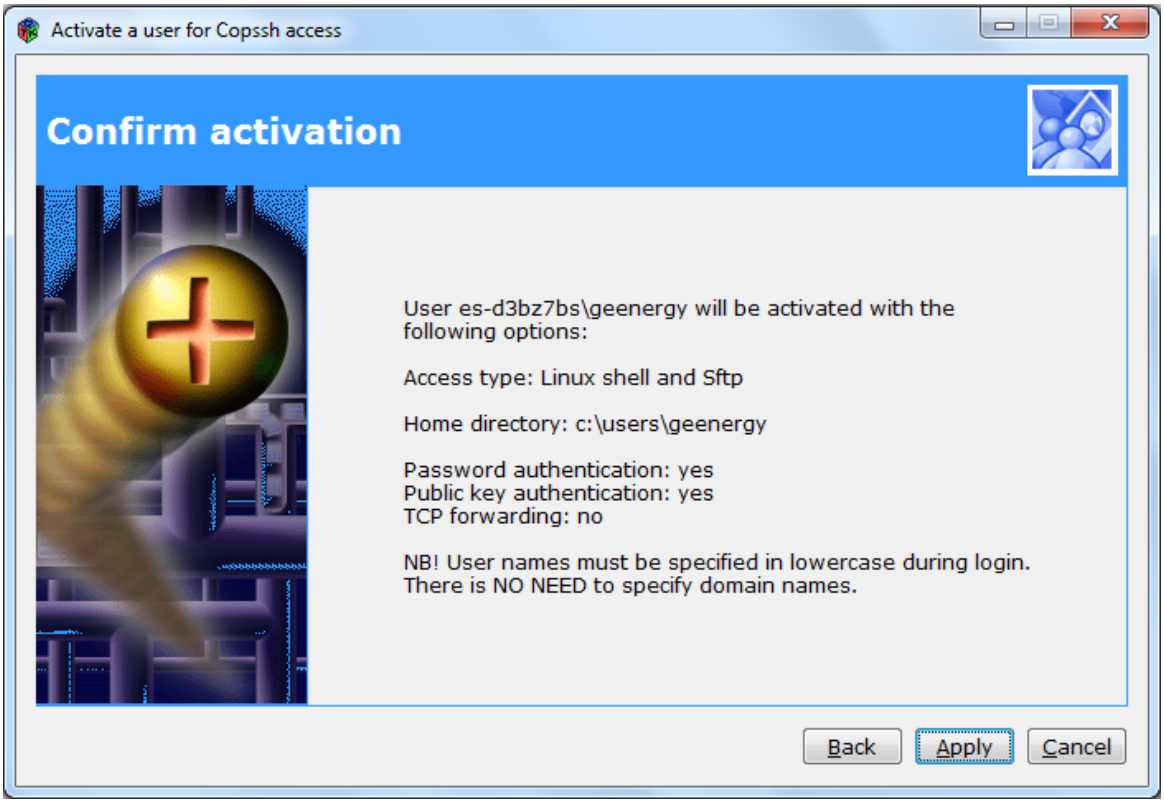
4. Click “Forward”: Select options interface opens.



5. Ensure that "Home directory" is set to "**C:\Users\<user_name>**", where user_name is user selected in previous step. If not, manually update the "Home directory" field.

   Note: This is typical home directory on Windows 7 computer.

6. Deselect "Allow TCP forwarding" option.
7. Click "Forward": Confirm activation interface appears.

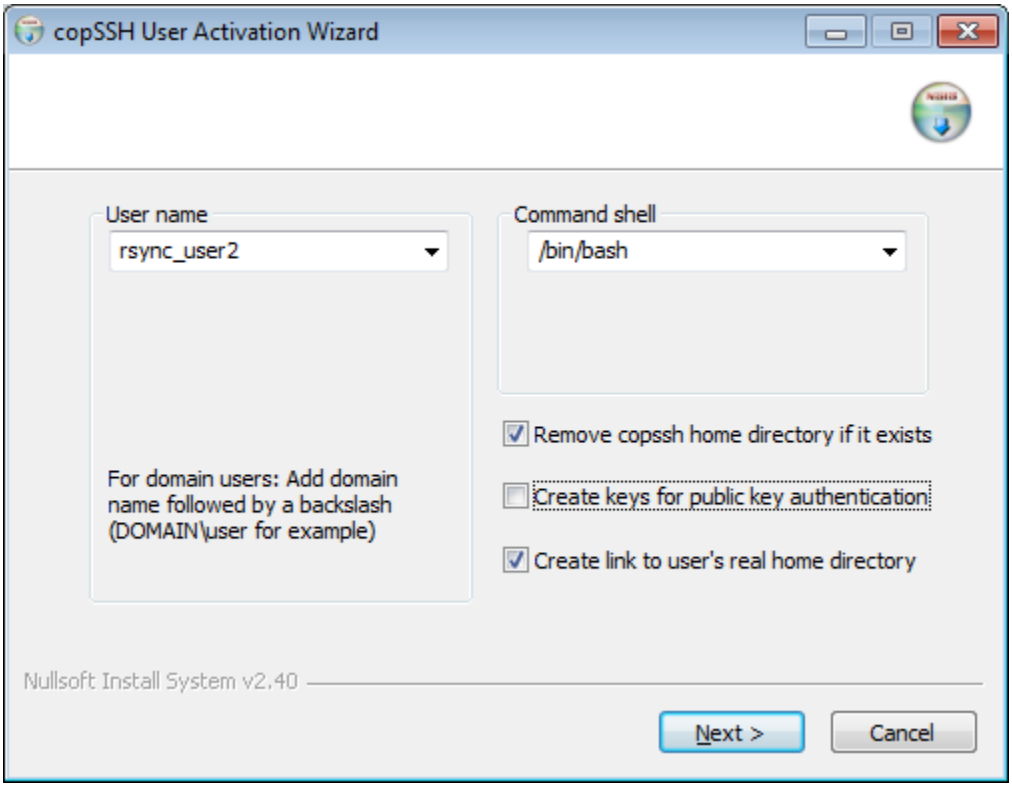


8. Verify details and click "Apply" to activate user.

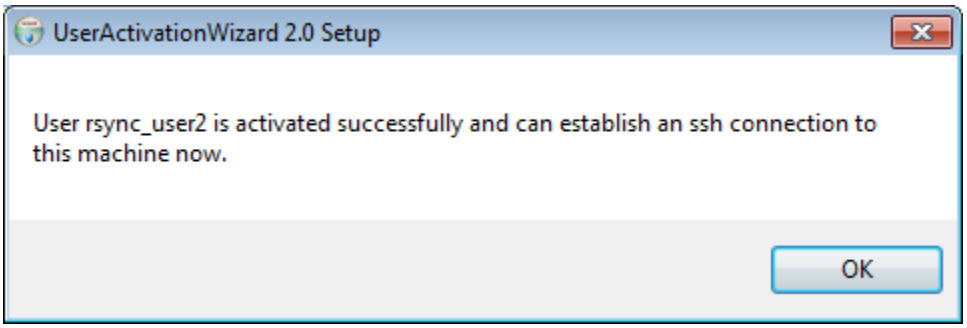
2.2.4.2 Method 2

1. Use the direct entry under Start Menu → All Programs → Copssh → Activate User.
2. Select the user name from the drop down list, and the other options as in the following figure.
3. Ensure you don't select the option to create keys; these will be created by the G500.

4. Click on Next.



A confirmation dialog will be presented, click on OK.



3. Configuring G500 Sync Manager

You can configure the settings of the G500 Sync Manager through the **Sync Manager** menu under G500 Config Tool (g500cfg). G500 applications must be restarted after changes to the configuration of Sync Manager.

3.1 Enable Sync Manager

Enable Sync Manager Application using option "Enable Sync Manager" under "Configure Sync Manager" menu, in the G500 Config Tool (g500cfg). When Sync Manager is enabled, a private/public key pair is generated.

Note: Files from the G500 are securely copied to the remote device over an SSH connection. To facilitate authentication on this link, a private/public key pair are used.

When a key set is generated, the files are stored in the G500 under **/mnt/datalog/SSHKeys/SyncMgr/**. You should copy the public key file (*id_rsa.pub*) from this location and store it in the appropriate location on the remote device. Refer to chapter 4. Setting up Public Key Authentication for details.

3.2 Configure Sync Sets

Up to 8 sync sets can be created at any time. The following settings can be configured for each set:

Table 1 Configure Sync Sets - Settings

Setting	Description	Range
Sync Set ID	A unique number used by the system to identify the sync set. Not editable; automatically assigned.	Auto-incremented from 1. Once a number has been assigned, it is never reused.
Destination IP Address	The IP address of the enterprise server where the files are to be copied.	Valid IPv4 address belonging to the Windows computer server
Destination User Name	The username used for SSH authentication on the enterprise server.	1 to 128 ASCII characters These are user names activated in section 2.2.3 Create Users in Windows computer
Source Path Name	The absolute directory pathname that will be synched to the remote device. **Note**: ARRM files are kept in **/mnt/datalog/arrm** folder in G500. You can specify this folder or a device specific sub-folder.	2 to 120 ASCII characters pointing to a valid location on the G500 file system
Destination Path Name	The absolute directory pathname that the files will be copied to. **Note**: If destination folder is C:\ARRM\G500_1\ on enterprise server, specify destination path name as **/cygdrive/c/ARRM/G500_1**	2 to 120 ASCII characters pointing to a valid location on the remote device's file system

Setting	Description	Range
Check and rsync Interval	The amount of time, in seconds, that the Sync Manager waits before checking the source path for changes. If changed or created files are detected, an rsync operation is triggered. Typical value: 60 seconds	60 to 86400 seconds
Forced rsync Interval	The amount of time, in seconds, that the Sync Manager waits before a forced rsync operation is triggered, regardless of detected changes. This will recreate files that have been deleted from the remote device as well as forcing the transfer of files whose changes may not have been detected due to MD5 collision, an extremely rare occurrence. Typical value: 300 seconds	60 to 86400 seconds

Notes:

- The Sync Manager will only copy files to the remote Windows-based computer. Files are not deleted from the remote system if these are deleted from the G500 after synchronization. If files are deleted from the remote system, it will be recreated during the next sync operation.
- A forced rsync will be performed upon each startup of your G500 device.
- The path equivalence between the Windows computer file system and the G500 destination path name is as following:

  Windows file system:

  <drive_letter>:\<path1>\<path2>

  G500 Sync Manager destination path:

  /cygdrive/<drive_letter>/<path1>/<path2>

  (the drive letter must be lower case, and path strings same case as seen in Windows file system)

  For e.g.:

  Windows path:

  C:\ARRM\Sub_01

  Corresponds to the following in G500 Sync Manager:

  /cygdrive/c/ARRM/Sub_01

4. Setting up Public Key Authentication

G500 uses public key authentication to authenticate itself to Enterprise Server. When Sync Manager application is enabled in G500, it creates a public key (**id_rsa.pub**). This public key is required to be transferred to Enterprise Server.

4.1 Update Permissions to SyncMgr Folder

When a key set is generated, the files are stored in `/mnt/datalog/SSHKeys/SyncMgr/`.

In order to copy the key from this folder to the computer, the permissions of this folder need to be updated after the Sync Manager is enabled (this must be performed every time a new set is generated or after G500 restarts or re-logins).

Upon exiting the G500 Config Tool (g500cfg), execute the following command at the G500 prompt:

sudo chmod ug+x /mnt/datalog/SSHKeys/SyncMgr

(if prompted for a password, enter the password associated with the root account).

4.2 Copy key from G500 to the Windows computer

1. On the G500 the Sync Manager's public key **id_rsa.pub** is available in **/mnt/datalog/SSHKeys/SyncMger/** folder.

   This key must be transferred to the Windows computer. Depending on the copSSH software version and Windows OS version, the target location of the key file may be different.

2. `<C:\Users\<user name>\.ssh>` folder **is** present

   - If an `\.ssh\` folder exists in the `C:\Users\<user name>` , the public key shall be transferred to that **\.ssh** folder on the Enterprise Server.

3. `<C:\Users\<user name>\.ssh>` folder is **NOT** present

   - If an `\.ssh\` folder does not exist in the `C:\Users\<user name>` , the public key shall be transferred to the installation path of the software, typically:

     "**C:\Program Files\ICW\home\<user name>\.ssh**" on a 32-bit operating system or

     "**C:\Program Files (x86)\ICW\home\<user name>\.ssh**" on a 64-bit operating system.

4. The public key file in the Windows **\.ssh** folder must have the name **authorized_keys**

   There can be only one such file per user.

   First time a G500 is added to a user, rename the copied **id_rsa.pub** to **authorized_keys**

   If configuring multiple G500 units to sync files to an Enterprise Server, using the same user name, the public key content (one text line) from the **id_rsa.pub** of each G500 shall be appended to the already existent **authorized_keys** file on Enterprise Server using a text editor. Each public key is a single line entry in **authorized_keys** file; ensure that it is not broken in multiple lines while copying and pasting.

5. Ensure the user permissions are updated as shown in 4.1

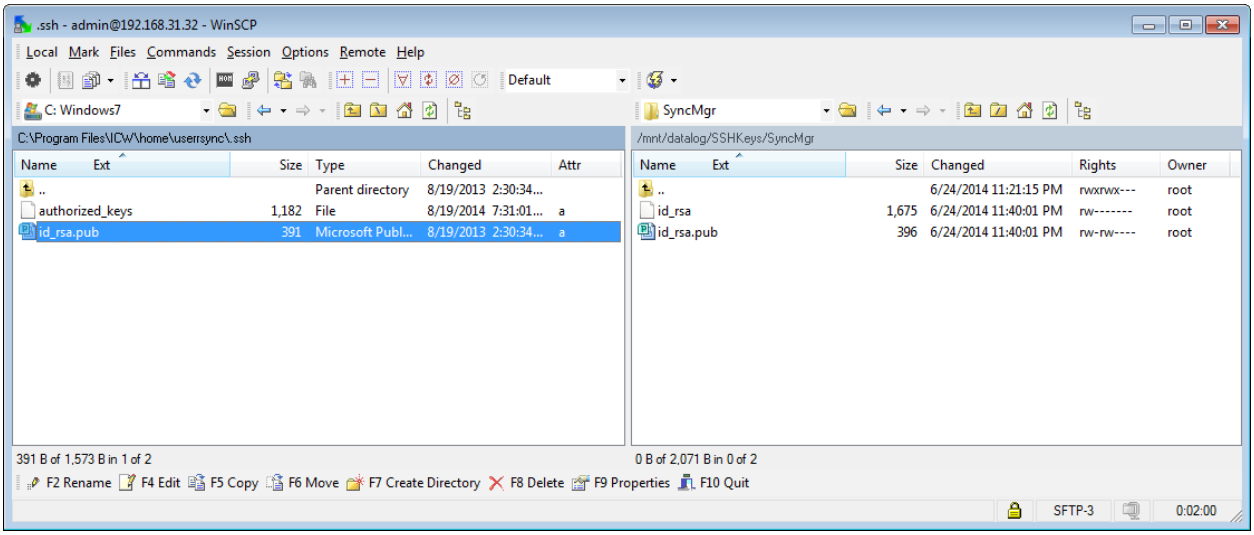
6. Transfer Sync Manager's public key to Enterprise Server using WinSCP program or USB pen drive.

   Note: The WinSCP program must be run as administrator by Right click on the program, and selecting "Run as administrator".

7. If this is the first G500-user, rename **id_rsa.pub** to **authorized_keys**

   (In the left-side window of WinSCP, right click on file → Rename), or use a text editor to append the new key to an existing file "authorized_keys".

8. Repeat this for every user and G500 station.



9. Reboot the G500 and the Windows computer.

   The system is now ready to operate.

A. Uninstalling cwRsyncServer and Copssh

This chapter describes how to uninstall cwRsyncServer and Copssh softwares.

1. All active users must be deactivated first. To deactivate a user, use “copSSH User Activation Wizard”. Start “copSSH User Activation Wizard” from Start Menu → All Programs → Copssh → Deactivate Users.
2. Open Services Microsoft Management Console (MMC), from Control Panel → Administrative Tools → Services. Right click on service “Openssh SSHD”, and select “Stop” to stop it.
3. Uninstall Copssh software from Start Menu → All Programs → Copssh → Uninstall COPSSH.
4. Uninstall cwRsyncServer software from Start Menu → All Programs → cwRsyncServer → Uninstall cwRsyncServer Server.
5. Delete Copssh service user from Control Panel → User Accounts → Manage User Accounts → Select SvcCOPSSH user → Click “Remove”.
6. Delete cwRsync service user from Control Panel → User Accounts → Manage User Accounts → Select SvcCWRSYNC user → Click “Remove”.

B. Diagnostics

B.1 G500 Diagnostic Logs

- Connect to G500 HMI
- Click on “System Logs” button on the power bar
- Select “Diagnostic Log” tab
- Filter Application field for “B048”
- Export logs to CSV file using “Export data” button
- If rsync command error is reported, check destination IP, user name, destination folder details mentioned in the message.
- If error message “Check destination server connectivity and SSH public key authentication with it” is reported, check:
    - IP connectivity to Enterprise Server
    - Correct installation of cwRwyncServer and Copssh softwares
    - Configuration of SSH keys in Enterprise Server

B.2 Copssh Event Log on Enterprise Server

Depending on the copSSH software application version, the following log may not be available.

- Start “Copssh Control Panel” from Start Menu → All Programs → Copssh → Copssh Control Panel → Go to Status tab.
- Check status of Copssh service
- Open “Copssh events” log; check whether access requests from G500 IP are reaching and successful to Enterprise Server.

C. List of Acronyms

Table 2 List of Acronyms

Abbreviation	Description
SSH	Secure Shell
ARRM	Automatic Record Retrieval Manager
DCA	Data Collection Application
DPA	Data Presentation Application
DTA	Data Translation Application
HMI	Human Machine Interface
IED	Intelligent Electronic Device
RTDB	Real Time Data Base
RTU	Remote Terminal Unit

MODIFICATION RECORD

VERSION	REV.	DATE	AUTHOR	CHANGE DESCRIPTION
1.00	0	29.Oct.2018		Document Draft Created.