

Collaboration Backups with Cygwin + OpenSSH on Windows

By: Anthony Holloway

Created on May 14, 2014

Last modified July 28, 2015

Contents

Summary	1
Information Gathering	1
Obtain Software	2
Server Software.....	2
Client Software (For Testing)	2
SFTP Server Installation.....	2
SFTP Server Configuration	12
Validation	15
Configure Backup Device in Disaster Recovery.....	17
Stopping and Starting the SSHd Service.....	19

Summary

Cisco officially supports the Cygwin + OpenSSH solution on Windows computers as the backup solution for its collaboration products. This is a free option, and with how quickly it sets up, you really cannot beat it.

Presently this guide only works for local accounts defined on the SFTP server. Domain account support is pending further testing and validation, but is possible to do.

Information Gathering

Spend a few minutes to gathering the following information which you will need during the setup and testing. Some example values have been supplied.

Key	Value	Notes
SFTP Server Cygwin Install Directory	C:\cygwin	Use this default directory
SFTP Server Cygwin Package Directory	C:\cygwin\packages	
SFTP Server Operating System	Windows Server 2008 R2	
SFTP Server Hostname	SFTPSERVER01	
SFTP Server IP Address	10.10.10.10	
SFTP Server Backup Folder Location	D:\backups	Mind the storage space!

SFTP User Username	cisco	
SFTP User Password	Cisco123	
SFTP System User SSHD Username	sshd	System account
SFTP System User SSHD Password	Cisco123	
SFTP System User CYGWIN Username	cyg_server	System account
SFTP System User CYGWIN Password	Cisco123	
Frequency of Backups	Daily	Per product
Number of Backups to Store	3	Per product
Backup CDR?	No	CUCM Only
Back Greetings, Names, Messages?	Yes	CUC Only

Obtain Software

The only software you need to download is the server software, which is Cygwin. However, to test the SFTP solution from a client machine, you will also want to download an SFTP client.

Server Software

Download the Windows 32/64-bit binary file from:

<http://www.cygwin.com/>

The file is called setup-x86.exe for 32-bit systems and setup-x86_64.exe for 64-bit systems.

This file goes anywhere on your SFTP server. The desktop or downloads folders are both good choices.

Client Software (For Testing)

Download the Windows 32-bit binary file from:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

The file is called psftp.exe.

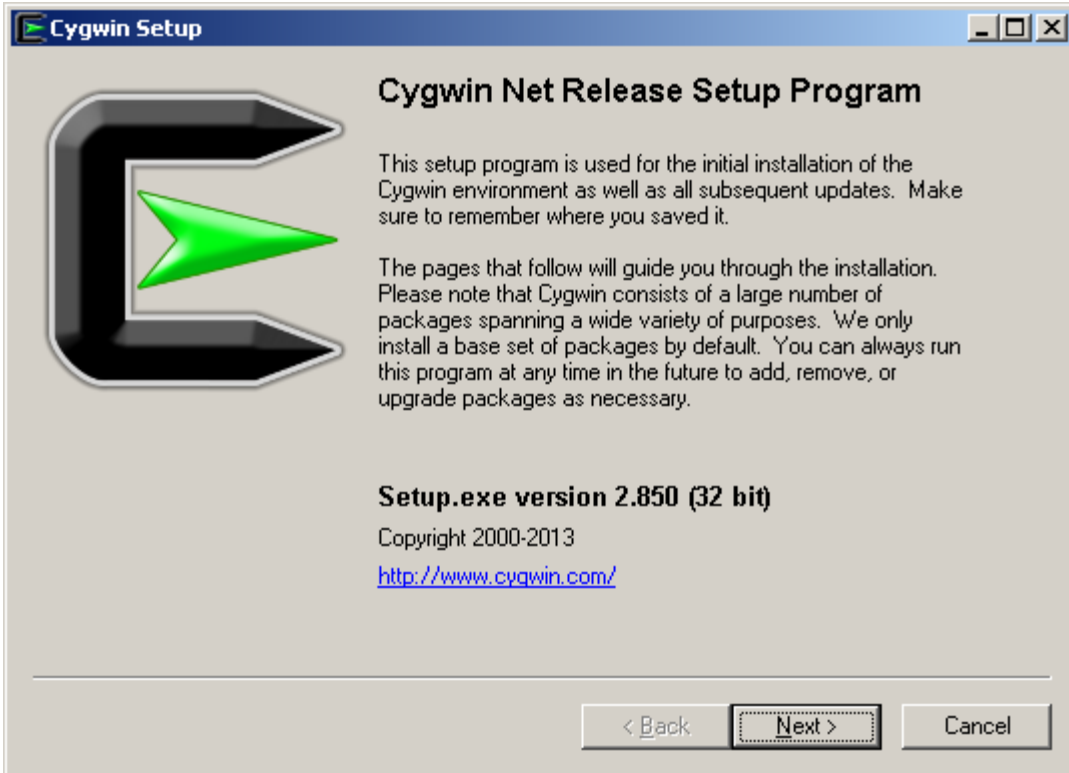
This file goes anywhere on your client computer. The desktop or downloads folders are both good choices.

SFTP Server Installation

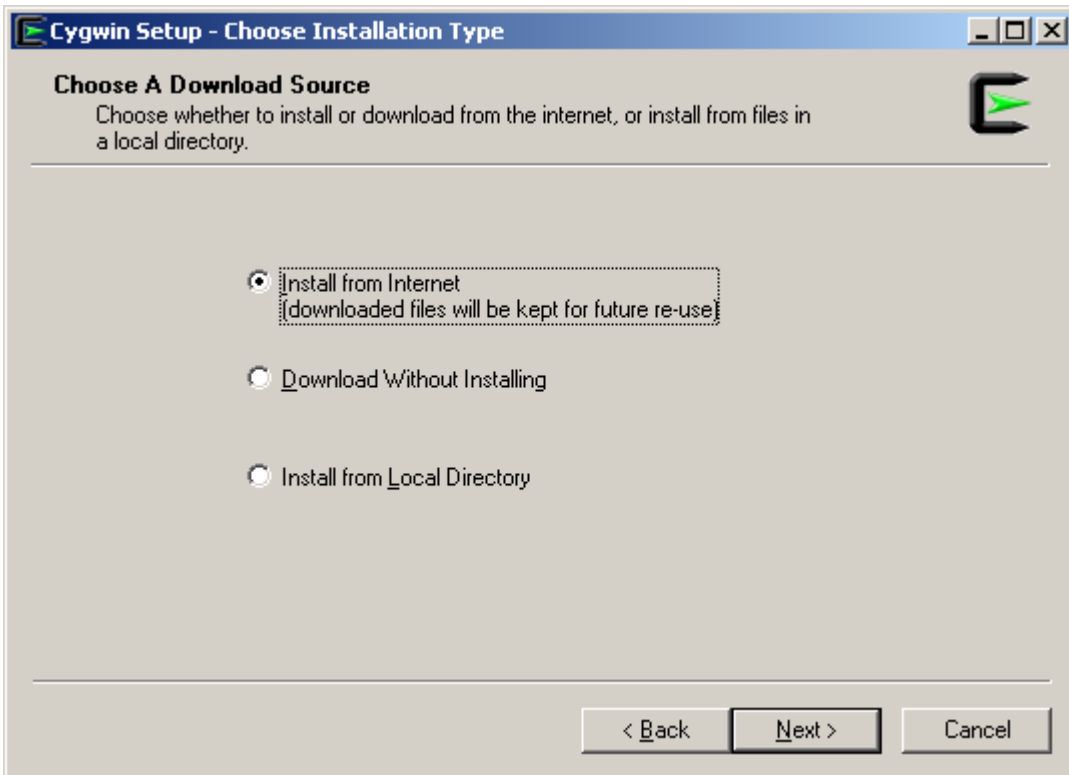
1. Run the setup file by double clicking it.



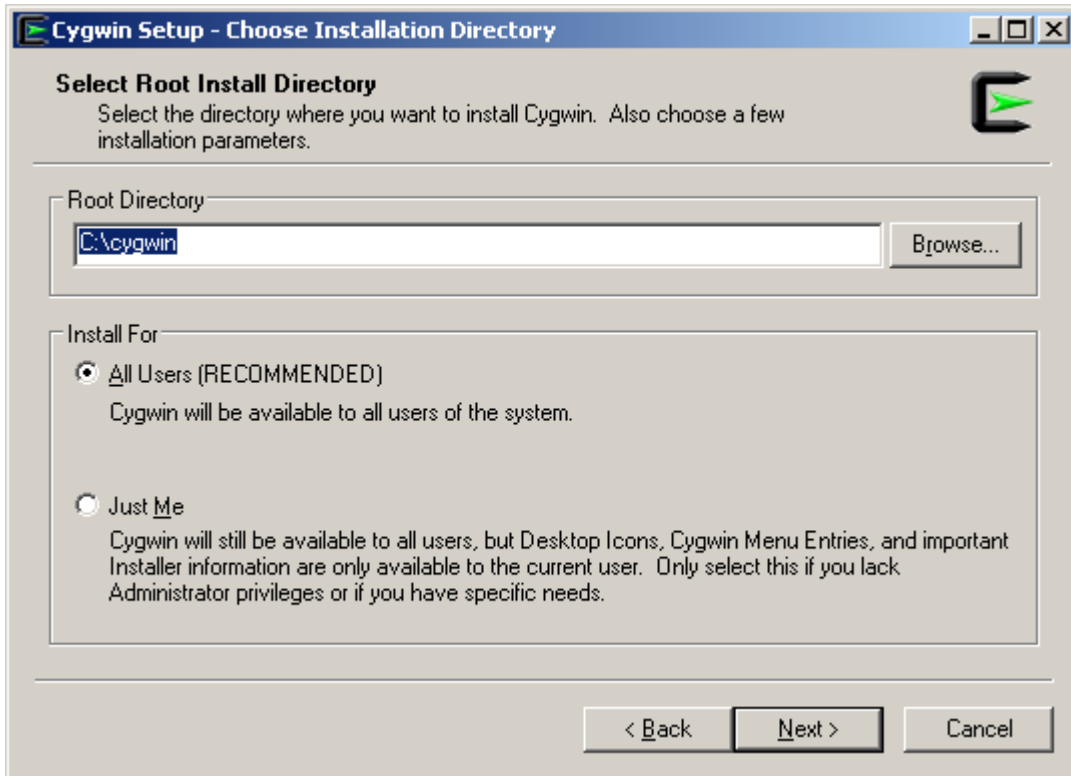
2. Click Next to begin setup.



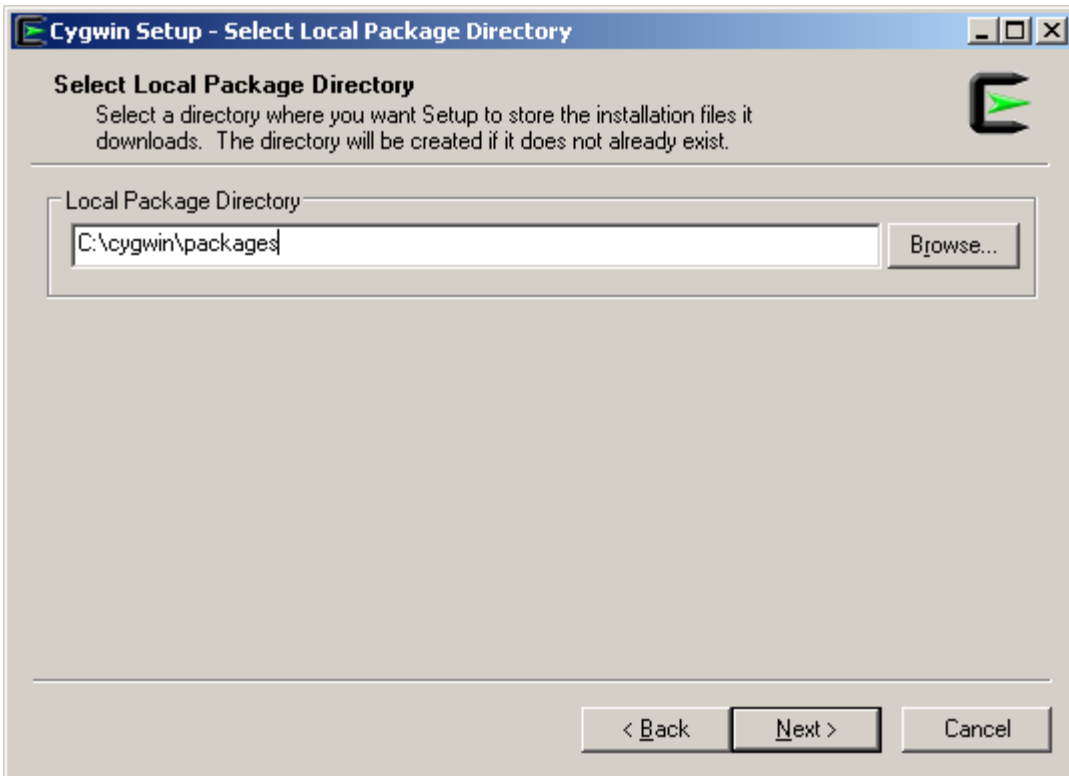
3. Select 'Install from Internet' and click Next.



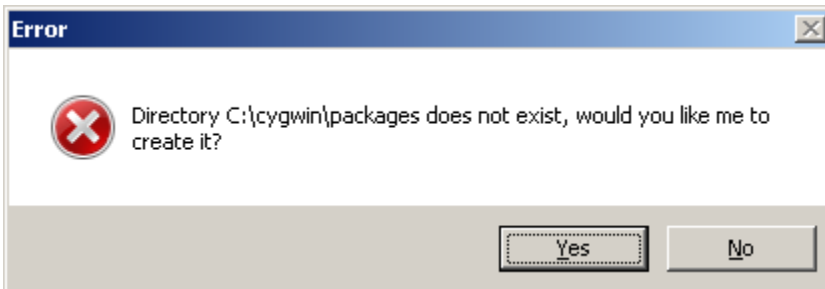
4. Enter your SFTP Server Cygwin Install Directory, Select All Users, Click Next



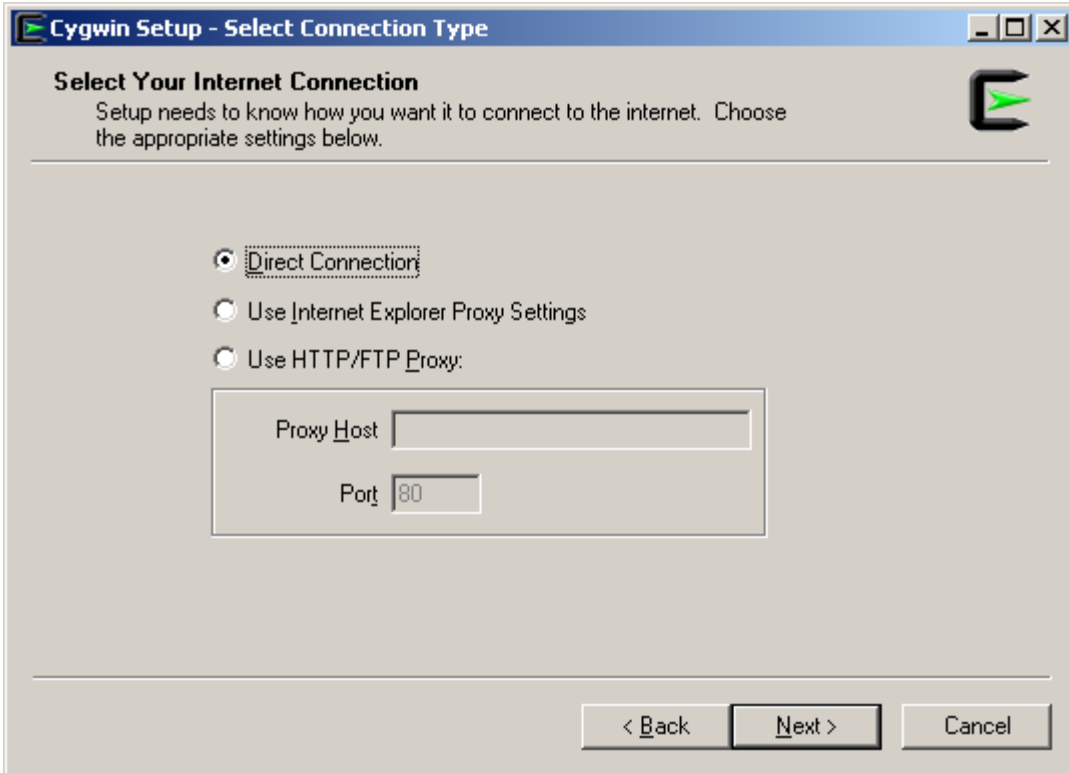
5. Enter your SFTP Server Cygwin Packages Directory, Click Next



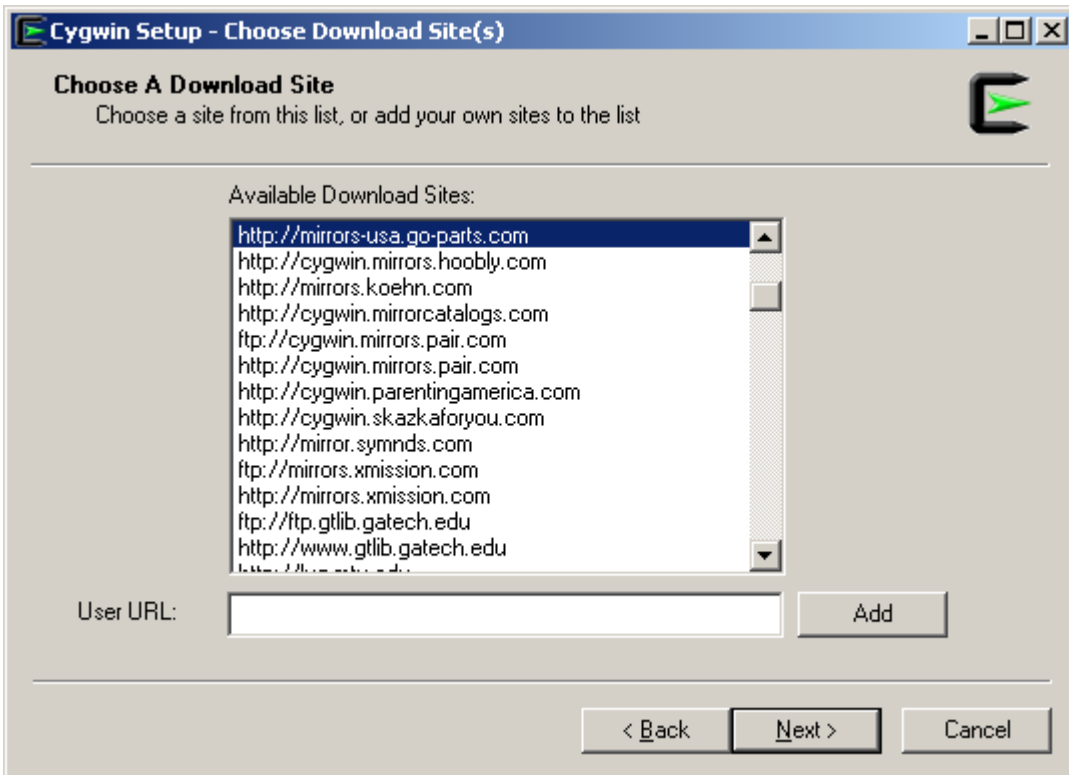
6. Select Yes to have the Packages directory created.



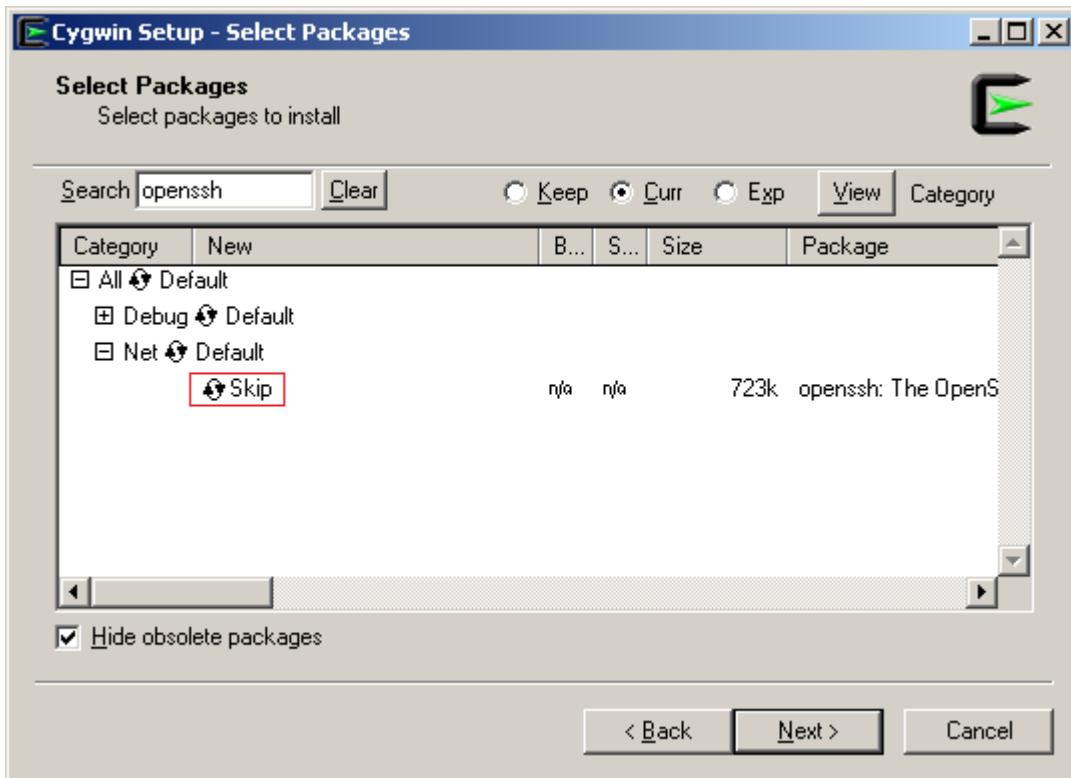
7. Select 'Direct Connection' and click Next.



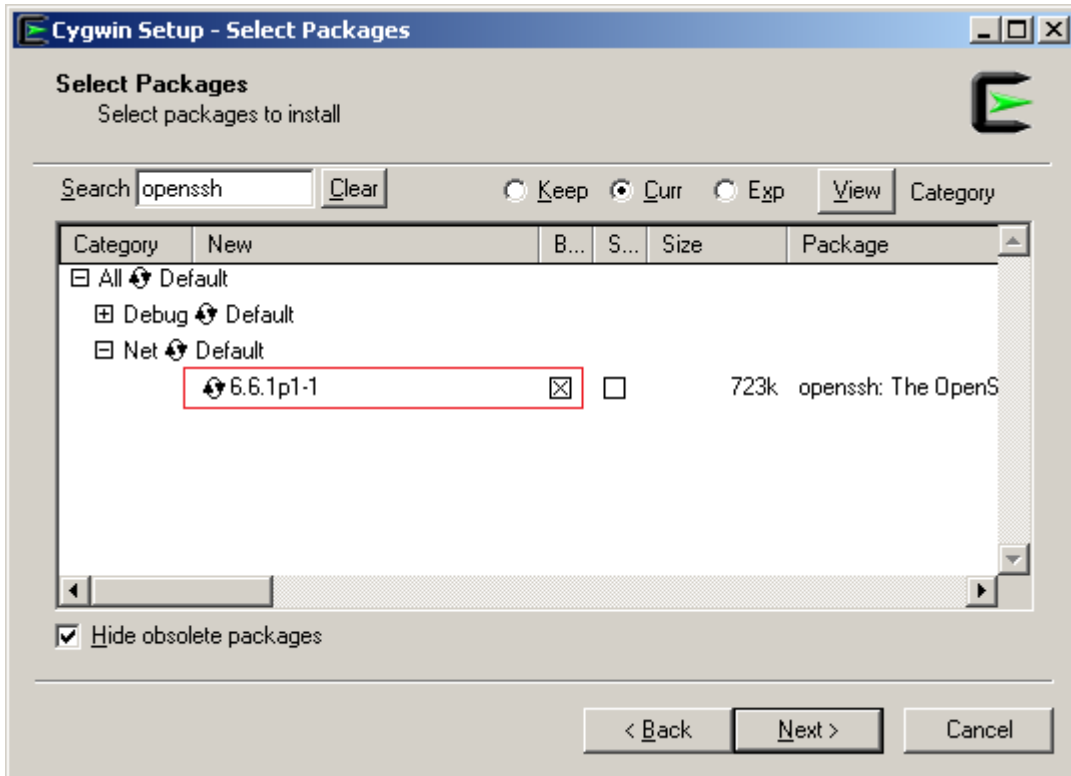
8. Select any download site from the list and click Next.



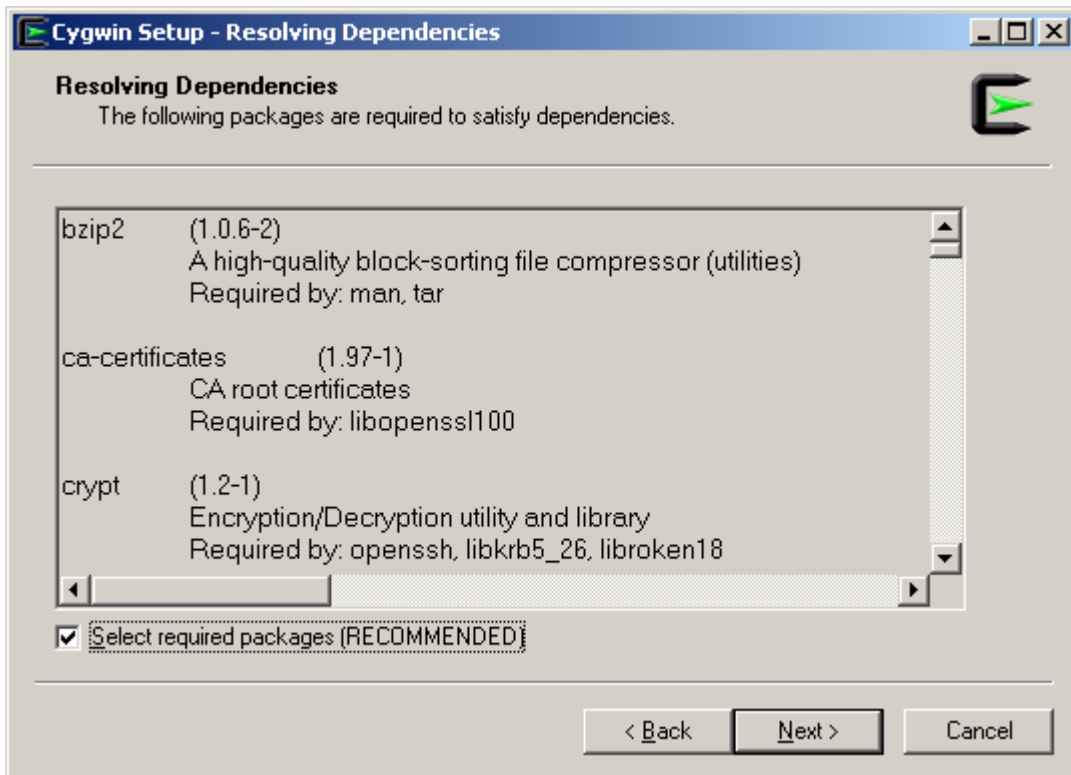
9. Enter 'OpenSSH' into the search field, expand 'Net', and click on Skip one time.



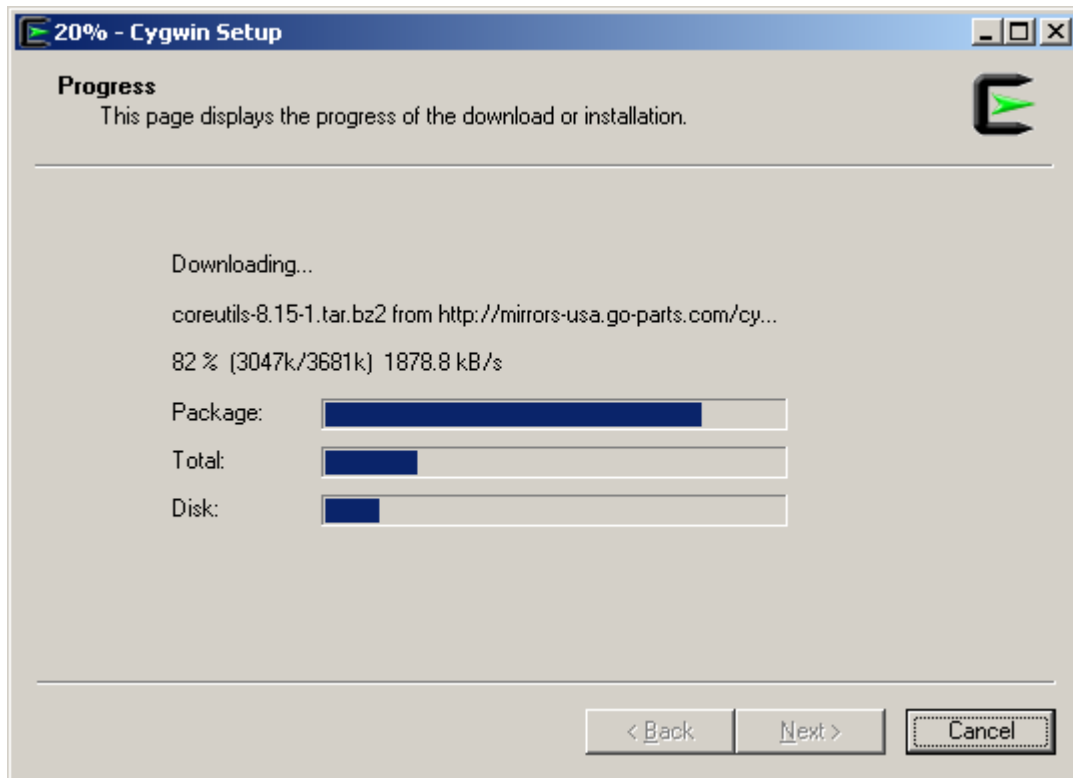
10. Confirm that the package will be installed by verifying a version number and the 'X' in the Binary column, then click Next.



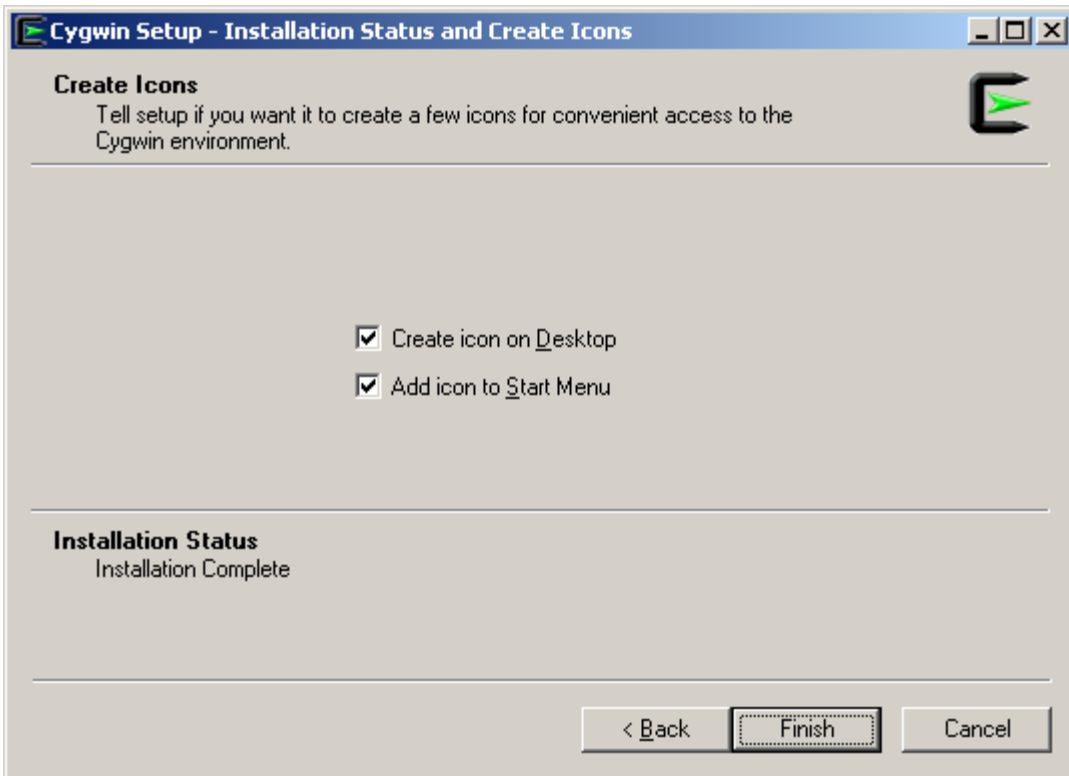
11. Select 'Select required packages (RECOMMENDED)' and click Next



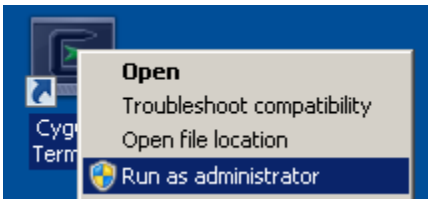
12. Wait while packages are downloaded and installed.



13. Click Finish.



14. Right click the Cygwin icon on your desktop and select 'Run As Administrator'.



15. In the Cygwin terminal, enter the command: `ssh-host-config`, and follow the prompts as in the example below. Leave this window open, we'll come back to it.

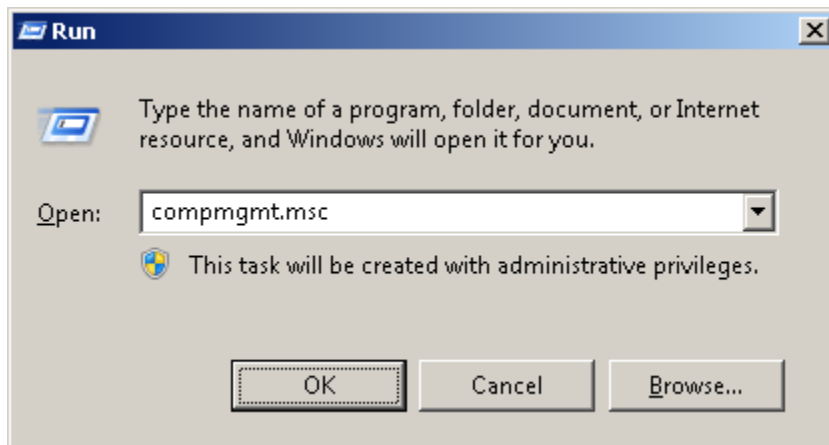
SFTP Server Configuration

Now you will create your backup folder, user account and then set its home directory to the backup folder directory.

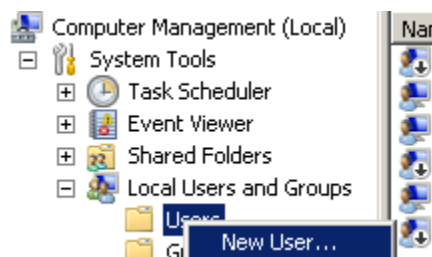
1. Use Windows Explorer to create your backup folder.



2. Use Start > Run and enter compmgmt.msc to launch the Computer Management console.



3. Expand System Tools > Local Users and Groups and Right click on Users, selecting New User...



4. Fill in the appropriate fields using the below illustration as a guide, then click Create followed by Close. Close the Computer Management window, we're done with it.

New User [?] [X]

User name:

Full name:

Description:

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

5. Back in the Cygwin terminal window, enter the following command: `mkgroup --local > /etc/group`

```
IEUser@IE9Win7 ~  
$ mkgroup --local > /etc/group
```

6. Now enter the command: `mkpasswd -l > /etc/passwd`

```
IEUser@IE9Win7 ~  
$ mkpasswd -l > /etc/passwd
```

7. You can now close the terminal window.
8. Open the following file in notepad: `C:\cygwin\etc\passwd`, and locate your SFTP user's home directory.

```

SYSTEM: *:18:544:,S-1-5-18::
LocalService: *:19:544:U-NT A
NetworkService: *:20:544:U-NT
Administrators: *:544:544:,S-
TrustedInstaller: *:4294967295-3418522649-1831038044:
Administrator: unused:500:513:Administrator: /home/Administrator: /bin/bash
cisco: unused:1009:513:cisco: /home/cisco:/bin/bash
CiscoHistRprtUsr: unused:1001:513:3664321-2923530833-354
cyg_server: unused:1008:513:3530833-3546627382-100:
Guest: unused:501:513:U-IE9W1 /Guest:/bin/bash
IEUser: unused:1000:513:U-IE9 /home/IEUser:/bin/bash
sshd: unused:1007:513:sshd pr 32-1007:/var/empty:/bin,

```

truncated

9. Modify the `/home/cisco` path to your SFTP Server Backup Directory path, using the special Cygwin syntax. Save and close the file.

```

SYSTEM: *:18:544:,S-1-5-18::
LocalService: *:19:544:U-NT A
NetworkService: *:20:544:U-NT
Administrators: *:544:544:,S-
TrustedInstaller: *:4294967295-3418522649-1831038044-18532926:
Administrator: unused:500:513:Administrator: /home/Administrator: /bin/bash
cisco: unused:1009:513:cisco: /home/cydrive/d/backups:/bin/bash
CiscoHistRprtUsr: unused:1001:513:3664321-2923530833-3546627382-100:
cyg_server: unused:1008:513:3530833-3546627382-1008:/var/empty:
Guest: unused:501:513:U-IE9W1 /Guest:/bin/bash
IEUser: unused:1000:513:U-IE9 /home/IEUser:/bin/bash
sshd: unused:1007:513:sshd pr 32-1007:/var/empty:/bin/bash

```

truncated

10. Open the following file in notepad: `C:\cygwin\etc\sshd_config`, and paste the below two lines at the end of the file. Save and close the file.

```

Ciphers 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,arcfour,arcfour128,arcfour256,blowfish-cbc,cast128-cbc,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com

```

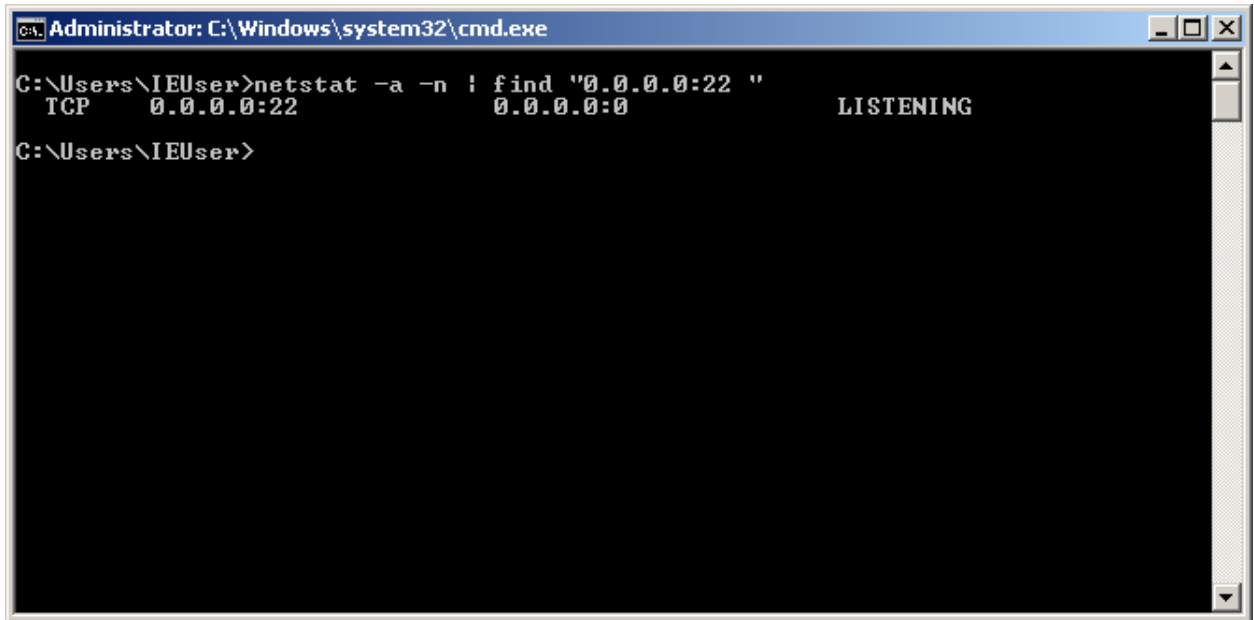
```

KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-

```

hellman-group14-sha1

11. Reboot the SFTP server and the sshd process should start automatically. Verify by opening a command prompt window and enter: `netstat -a -n | find "0.0.0.0:22 "`

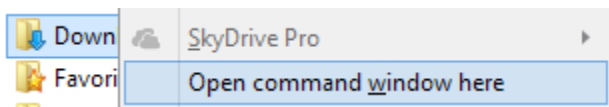


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\IEUser>netstat -a -n | find "0.0.0.0:22 "
TCP      0.0.0.0:22          0.0.0.0:0          LISTENING
C:\Users\IEUser>
```

Simple Validation

Now that you have your SFTP server setup and running automatically upon reboot, let's see if we can actually transfer files back and forth and delete from the remote machine.

1. On your client machine where you have psftp.exe saved, right click on its parent folder and select 'Open Command Window Here'



2. Enter the command: `psftp cisco@10.10.10.10`, substituting your actual values for username and IP Address, enter 'y' to accept the key, and then supply the password for your user account. Note the working directory is the same as your backup path.

```
psftp cisco@10.90.90.137

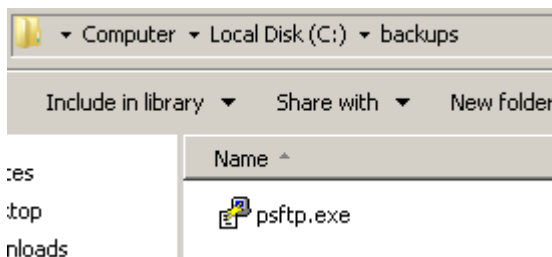
#psftp cisco@10.90.90.137
WARNING - POTENTIAL SECURITY BREACH!
The server's host key does not match the one PuTTY has
cached in the registry. This means that either the
server administrator has changed the host key, or you
have actually connected to another computer pretending
to be the server.
The new rsa2 key fingerprint is:
ssh-rsa 2048 80:1a:99:25:48:66:f7:49:d0:31:33:5d:47:94:c6:1b
If you were expecting this change and trust the new key,
enter "y" to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating
the cache, enter "n".
If you want to abandon the connection completely, press
Return to cancel. Pressing Return is the ONLY guaranteed
safe choice.
Update cached key? (y/n, Return cancels connection) y
Using username "cisco".
cisco@10.90.90.137's password:
Remote working directory is /cygdrive/c/backups
psftp>
```

3. Copy a file over to the server by entering the command: `put psftp.exe`

NOTE: I am copying the psftp.exe file by choice, you can copy any file you want.

```
psftp> put psftp.exe
local:psftp.exe => remote:/cygdrive/c/backups/psftp.exe
psftp>
```

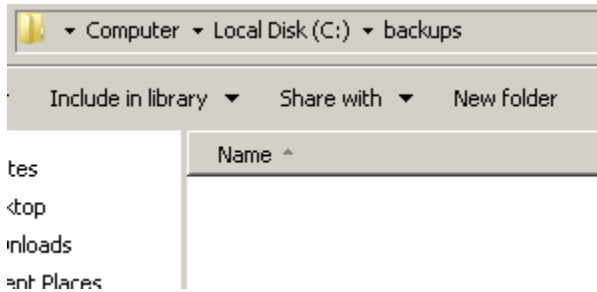
4. Validate that the file does in fact exist on the SFTP server.



5. Delete the file on the server by entering the command: `del psftp.exe`

```
psftp> del psftp.exe
rm /cygdrive/c/backups/psftp.exe: OK
psftp>
```

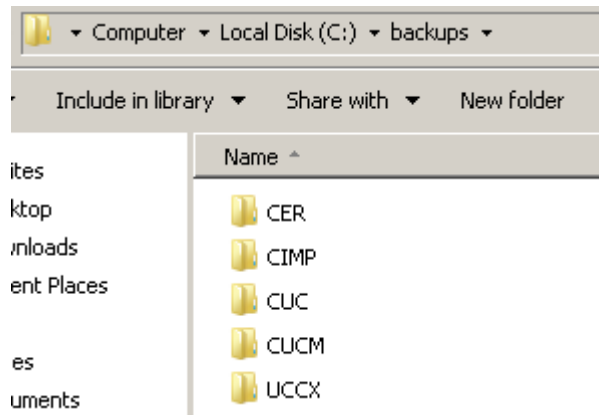
6. Validate that the file no longer exists on the SFTP server.



7. Disconnect from the server by entering the command: **bye**

Configure Backup Device in Disaster Recovery

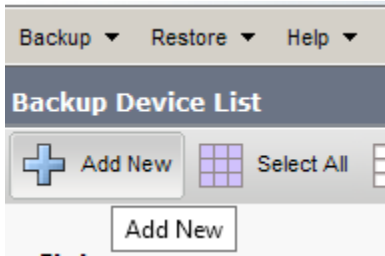
Before you begin the configuration within Disaster Recovery, you'll want to create a folder for each product inside of your backup folder. In the below example, I have create a folder for each of: CUCM, CUC, CER, CIMP, and UCCX.



Next, log into Disaster Recovery on each of your products to perform the following tasks.

1. Select Backup > Backup Device > Add New





- Enter a device name of your choosing, the IP Address of your SFTP server, the path for this product, the username/password to access SFTP, and the number of backups to keep. Click Save.

Backup Device

Save ← Back

Status

Status: Ready

Backup device name

Backup device name* CygwinOpenSSH

Select Destination*

Tape Device

Device Name -- Not Selected -- Tape drive is not supported on a virtual machine

Network Directory

Host name/IP address 10.90.90.137

Path name UCCX

User name cisco

Password ●●●●●●

Number of backups to store on Network Directory 3

The system will actually attempt a login, putting a file on the remote server, and then deleting it.

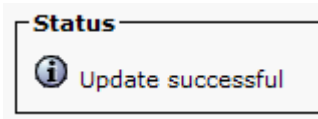
```

Administrator: C:\Windows\system32\cmd.exe
C:\backups\UCCX>dir
Volume in drive C has no label.
Volume Serial Number is E0CE-337D

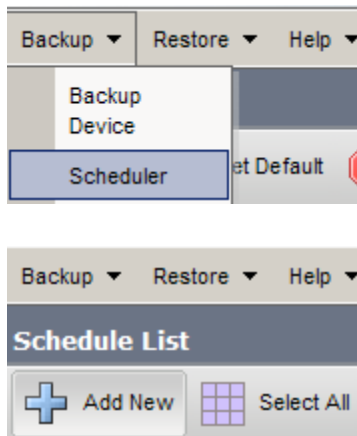
Directory of C:\backups\UCCX

05/14/2014  03:48 PM    <DIR>          .
05/14/2014  03:48 PM    <DIR>          ..
05/14/2014  03:48 PM                0 dUmmI_Drf
                1 File(s)      0 bytes
                2 Dir(s)  120,532,217,856 bytes free
  
```

If it can do that, then the Save will work. If not, it will fail. This is a very good validation test for connectivity, as it tests: Network connectivity, SSH Protocol, Ciphers, KeyExchange, and File permissions.



3. Select Backup > Scheduler and then click Add



4. Enter a scheduler name, such as Daily, select the backup device you just defined in the previous step, then select the components you want to backup, followed by setting a time of day to run the backups (consider staggering each product), and finally set the frequency of the schedule. Click Save.

No screenshot as each product page is slightly different.

Stopping and Starting the SSHd Service

To stop or start the sshd service use the following commands in a Cygwin terminal window.

- Stop

```
cygrunsrv --stop sshd
```

- Start

```
cygrunsrv --start sshd
```