Configure multiple SSH identities for TortoiseHg

If you are using TortoiseHg on Windows, you need the following programs to use SSH:

Program	Description
PuTTYgen	An RSA and DSA key generation utility. This is a part of the free PuTTY telnet/SSH Client. You can install this package separately from TortoiseHg. You can also install just `PuTTYgen.exe` into the same directory as TortoiseHg.
Pageant	An SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink. This is installed for you with TortoiseHg.

TortoiseHG connects with Plink and uses Pageant to identify which keys are available. To configure TortoiseHg so that you can access multiple Bitbucket Cloud accounts through SSH, do the following:

- Generate a key pair for a new identity
- Add your private keys to Pageant
- Add your SSH public key to Bitbucket
- Configure Mercurial Compression
- Clone a repository as you normally would
- Switching existing repositories from HTTPS to SSH (optional)

If you have a single identity and that is all you need, you can configure a single, global identity instead.

Generate a key pair for a new identity

PuTTYgen creates an identity for both public and private use. You save the private key in a **.ppk** file. You can also save the public key to a file but that isn't strictly necessary. These instructions assume you are only saving the private key file.

1. Locate the `puttygen.exe` executaible in your system and double click the icon to start it.
   The system opens the **PuTTY Key Generator** dialog.
2. Press **Generate**.
   Following the instructions to generate some randomness. When the generation completes, the system displays the public key and a number of other fields:

3. Edit the **Key comment**.
   The comment appears in the key list on Bitbucket. Using this comment is a great way to distinguish your keys.
4. Enter and confirm a key passphrase.
5. Press **Save private key**.
   The system prompts you for a location to save the file and a file name. By convention, store your key files in a folder called `C:\User`
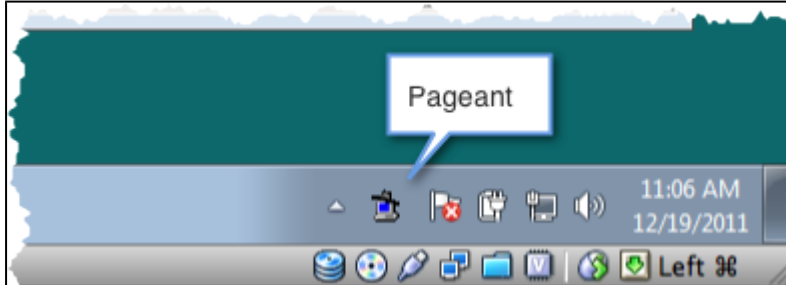
s*yourname*\\.ssh. and give it a .ppk extension.
6. Close the key generator.

Add your private keys to Pageant

1. Start Pageant by double clicking its icon.
   By default, TortoiseHG installs the Pageant in the C:\Program Files\TortoiseHG folder. When it is running, Pageant appears in your system tray:
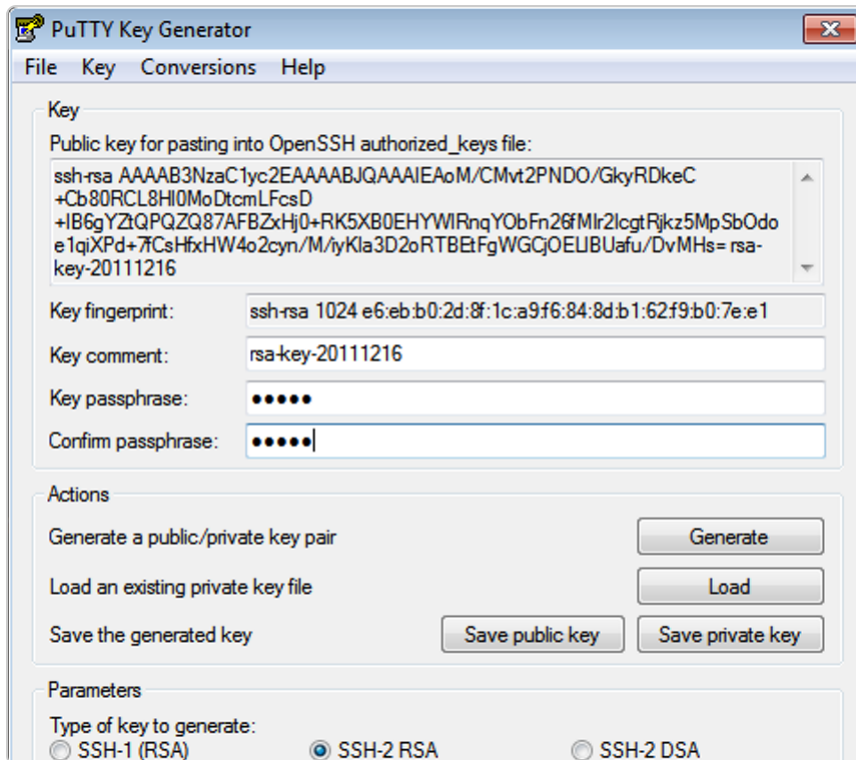

2. Double-click the Pageant icon to launch the **Pagent Key List** dialog.
3. Click the **Add Key** button.
   The system displays the **Select Private Key File** dialog.
4. Navigate to and open the public key file.
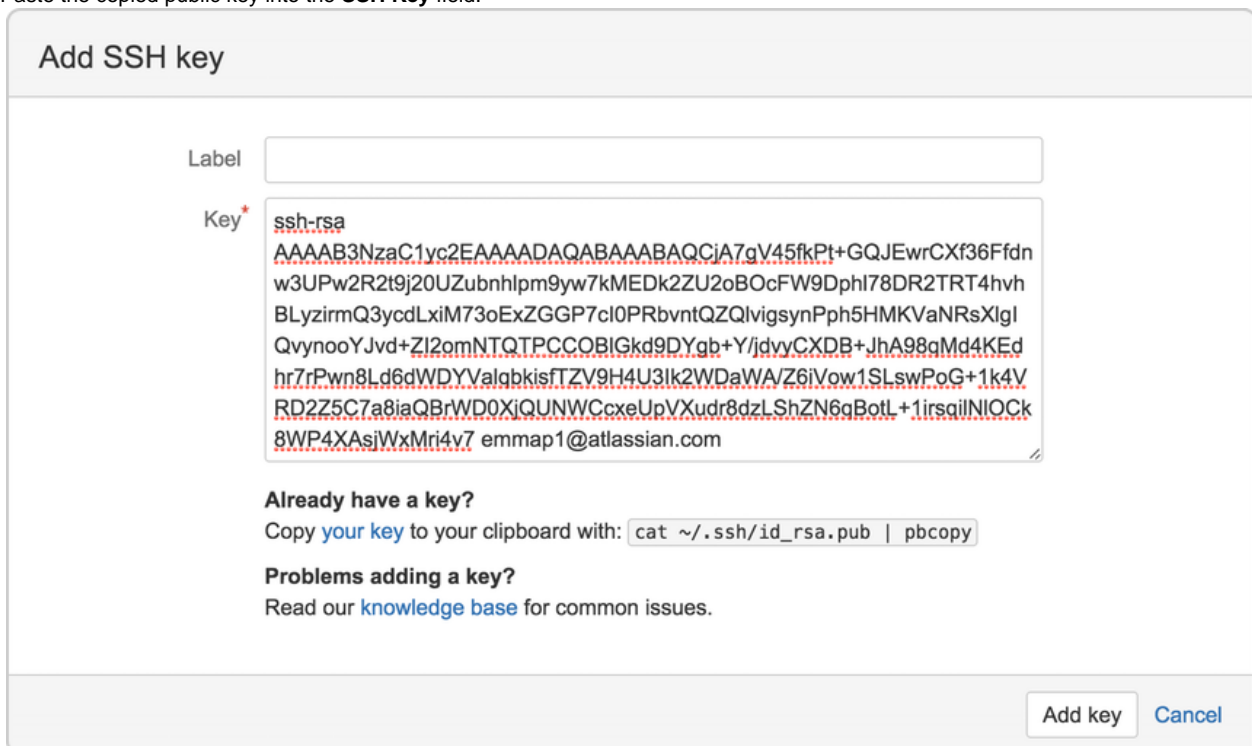5. Enter the passphrase when prompted:
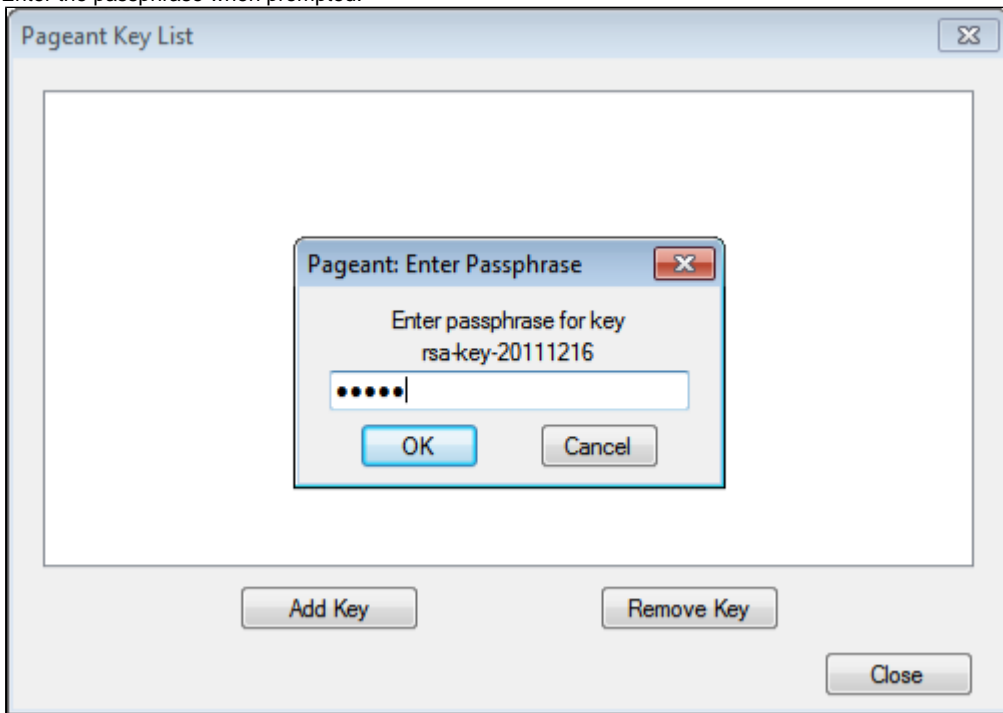
6. Press **OK**.
   Pageant shows your key in the running list.
7. Add any additional keys.
8. Press **Close** to close the dialog.
   Pageant continues to run on your system.

Add your SSH public key to Bitbucket

1. From your avatar in the bottom left, click **Bitbucket settings**.
   Bitbucket displays the **Account settings** page.
2. Click **SSH keys**.
   The **SSH Keys** page displays. It shows a list of any existing keys. Then, below that, a dialog for labeling and entering a new key.
3. Switch to your local desktop and start the PuTTYgen program.
4. Press **Load**.
5. Navigate to and open your default private key.
6. Enter your passphrase when prompted and press OK.
   The system displays your public key.

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAoM/CMvt2PNDO/GkyRDkeC
+Cb80RCL8HI0MoDtcmLFcsD
+IB6gYZtQPQZQ87AFBZxHj0+RK5XB0EHYWlRnqYObFn26fMlr2lcgtRjkz5MpSbOdo
e1qiXPd+7fCsHfxHW4o2cyn/M/iyKla3D2oRTBEtFgWGCjOELlBUafu/DvMHs= rsa-
key-20111216

Key fingerprint: ssh-rsa 1024 e6:eb:b0:2d:8f:1c:a9:f6:84:8d:b1:62:f9:b0:7e:e1
Key comment: rsa-key-20111216
Key passphrase: •••••
Confirm passphrase: •••••

Actions

Generate a public/private key pair   Generate
Load an existing private key file   Load
Save the generated key   Save public key   Save private key

Parameters

Type of key to generate:
○ SSH-1 (RSA)   ● SSH-2 RSA   ○ SSH-2 DSA

7. Select and copy the contents of the **Public key for pasting into OpenSSH authorized_keys file** field.
8. Back in your browser, enter a **Label** for your new key, for example, `Default public key`.
9. Paste the copied public key into the **SSH Key** field:

Add SSH key

Label   [   ]

Key*   ssh-rsa
         AAAAB3NzaC1yc2EAAAADAQABAAAABAQCjA7gV45fkPt+GQJEwrCXf36Ffdn
         w3UPw2R2t9j20UZubnhlpm9yw7kMEDk2ZU2oBOcFW9DphI78DR2TRT4hvh
         BLyzirmQ3ycdLxiM73oExZGGP7cl0PRbvntQZQlvigsynPph5HMKVaNRsXlgl
         QvynooYJvd+Zl2omNTQTPCCOBIGkd9DYgb+Y/jdvyCXDB+JhA98qMd4KEd
         hr7rPwn8Ld6dWDYValqbkisfTZV9H4U3lk2WDaWA/Z6iVow1SLswPoG+1k4V
         RD2Z5C7a8iaQBrWD0XjQUNWCcxeUpVXudr8dzLShZN6qBotL+1irsqilNlOCk
         8WP4XAsjWxMri4v7 emmap1@atlassian.com

         Already have a key?
         Copy your key to your clipboard with: `cat ~/.ssh/id_rsa.pub | pbcopy`

         Problems adding a key?
         Read our knowledge base for common issues.

                                              Add key   Cancel

10. Press **Add key**.
    The system adds the key and it appears in the **SSH Keys** listing.
11. Close PuTTYgen.

Configure Mercurial Compression

When sending or retrieving data using SSH, Git does compression for you. Mercurial does not automatically do compression. If you are using Mercurial, you should enable SSH compression as it can speed up things drastically, *in some cases*. To enable compression for Mercurial, do the following:

1. Start the TortoiseHg Workbench.
2. Select **File > Settings**.
3. Make sure you have the global settings tab selected.

4. Press **Edit File**.
5. Add the following line to the UI section:

```
ssh = "TortoisePlink.exe" -ssh -2 -batch -C
```

When you are done the file should look similar to the following:

```
[ui]
# Name data to appear in commits
username = Emma Paris <emmap1@atlassian.com>
ssh = "C:\Program Files\TortoiseHg\TortoisePlink.exe" -ssh -2
-batch -C
```

6. Press **Save** to store your settings and close the file.
7. Press **OK** to close the settings dialog.

Clone a repository as you normally would

1. Start TortoiseHG Workbench.
2. Select **File > Clone Repository**.
3. Enter the proper SSH syntax (you can copy this from Bitbucket's repository **Overview** page) in the **Source** field.
4. Enter a **Destination** for your repository.
   At this point the clone dialog looks similar to the following:
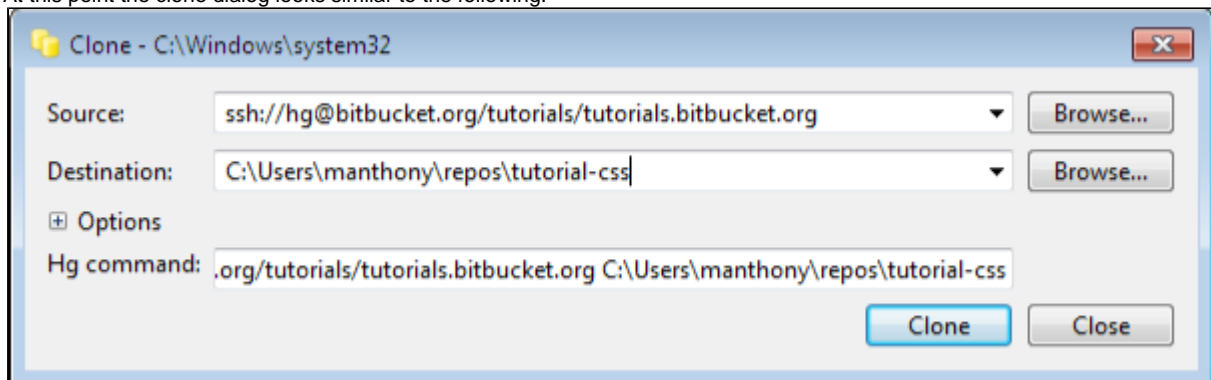
5. Press **Clone**.
   The system clones the repository and adds it to your repository registry in TortoiseHg.
6. Right click the new repository in the registry and choose **Settings**.
   The system displays the **TortoiseHG Settings** dialog with the *name* **repository settings** tab active.
7. Press **Edit File**.
8. View your current repository configuration.
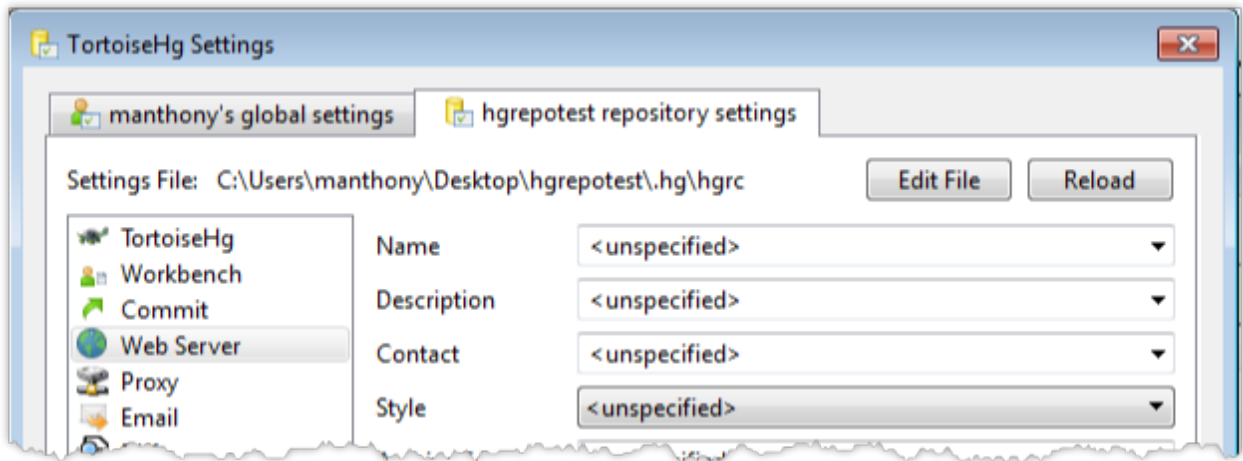   You should see something similar to the following:

```
[paths]
default = ssh://hg@bitbucket.org/newuserme/bb101repo
```

Go ahead and close the file and the settings dialog.

Switching existing repositories from HTTPS to SSH (optional)

You can change existing repository configurations to use a SSH configuration that makes use SSH. You'll only need to do this for repositories that you have already cloned with HTTPS.

1. Start TortoiseHG Workbench.
2. Right click a repository and choose **Settings**.
   The system displays the **TortoiseHG Settings** dialog with the *name* **repository settings** tab active.

3. Press **Edit File**.
4. View your current repository configuration.
   You should see something similar to the following:

```
[paths]
default = https://bitbucket.org/accountname/reponame
```

5. Change the `default` value to use the SSH format for that repository.
   When you are done you should see something similar to the following:

```
[paths]
default = ssh://hg@bitbucket.org/accountame/reponame
```

6. Press **Save** to close the editor.
7. Press **OK** to close the settings dialog.

Configure a single, global identity

If you only plan on ever using a single identity with your TortoiseHG installation, you can create a global configuration for yourself. To do this, start the TortoiseHG Workbench and do the following:

1. Choose **File > Settings**.
   The system opens the settings dialog.
2. Select the ***username* global settings** tab.
3. Press **Edit File**.
   The system opens an editor with the `C:\Users\`*username*`\mercurial.ini` file.
4. Edit the [ui] section and add an identity to the TortoisePlink call:

```
# Generated by TortoiseHg setting dialog
[ui]
username = yourusername <youremail@yourdomain.ext>
ssh = "C:\Program Files (x86)\TortoiseHg\TortoisePlink.exe" -ssh -2
-i C:\Users\yourusername\.ssh\keyname.ppk
```

5. Press **Save** to close the editor.
6. Press **OK** to close the dialog.

Plink has a number of command line options that TortoisePlink accepts. For more information, see the PuTTYgen documentation.