Upload SSH Public Keys

Modified on: Sun, Oct 31, 2021 at 5:52 PM

SSH keys provide a cryptographically secure and convenient method to provide ssh terminal access to remote servers. In this process, users generate a private/public key pair that will be used to access the Colosseum SSH Gateway. The private key is maintained on the user's local machine and the public key is uploaded to the Colosseum. When the user logs on to the SSH gateway, the server authenticates the client by using the public key to verify that the client has the correct corresponding private key.

Users should take care to avoid disclosure of the private key generated in this process. If a user's private key is ever compromised, simply repeat the steps here to generate a new key pair and upload the new public key.

The steps discussed here are for unix-based systems, such as Linux or Mac OSX. Windows users should consult the users manual of their SSH client. A popular Windows SSH client is PuTTY:

- PuTTY Homepage: http://www.putty.org/ **(http://www.putty.org/)**
- Key generation for PuTTY: https://winscp.net/eng/docs/ui_puttygen **(https://winscp.net/eng/docs/ui_puttygen)**
    - PuTTYgen is a component of the WinSCP package, available at: https://winscp.net/ **(https://winscp.net/)**

Note: Colosseum helpdesk team does not provide support for the issues related to the users' ssh client. Windows users should consult the users manual of their ssh client.

Generate a New SSH Key (Linux/Mac)

To generate a new SSH key, copy and paste the text below, making sure to substitute the email address associated with your Colosseum user account.
By default the keys will be created in the ~/.ssh (or /home/<user>/.ssh) directory. The default settings are preferred, so when you're prompted to "Enter a file in which to save the key", just press **Enter** to continue for the default location.

```
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

Next, you'll be asked to enter a passphrase (and then confirm the password). This password will control access to the local private key when it is used. It is recommended that you choose a strong password.

Note: To reassure that the permissions for the SSH keys are set properly, users can change the permissions for the SSH keys by using the following commands:

```
chmod 600 ~/.ssh/id_rsa
chmod 644 ~/.ssh/id_rsa.pub
```

Generic

Users may also need to add the private key to the SSH agent by the following command:

```
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_rsa
```

Generic

Copying the SSH Public Key (Linux/Mac)

Copy the SSH public key to your clipboard. Keep in mind that your key may also be named id_dsa.pub, id_ecdsa.pub or id_ed25519.pub.

```
cat ~/.ssh/id_rsa.pub
```

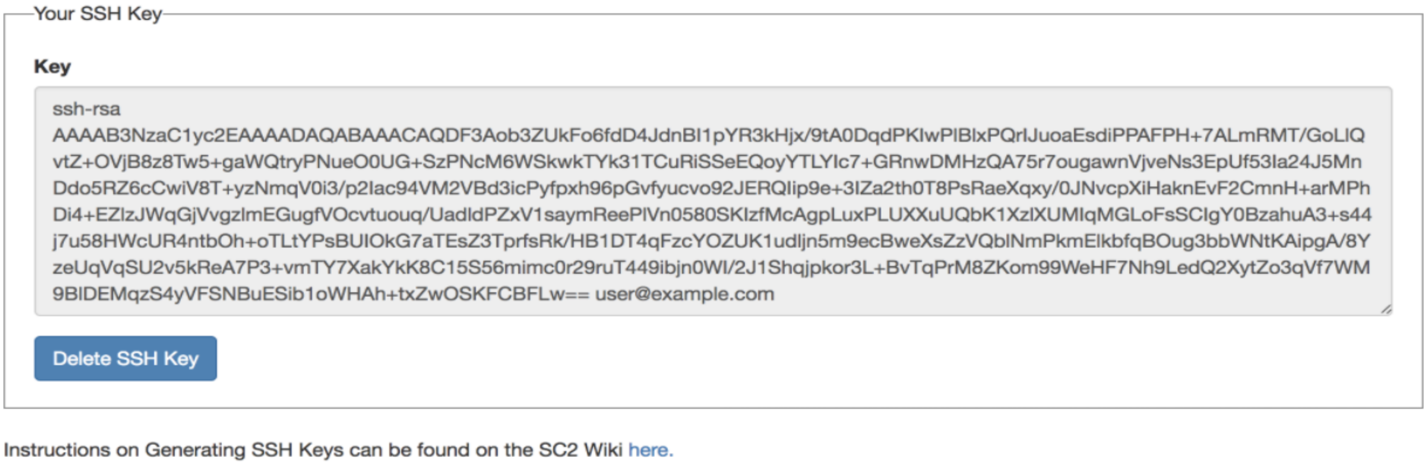
Copy the entire resulting string of the id_rsa.pub file to your clipboard. Alternatively, using your favorite text editor, you can open the public key file and copy the contents of the file manually.

Add SSH Public Key to Account (Linux/Mac/Windows)

Now that you have the key copied, it's time to add it to the Colosseum Website:

1. In the top menu, click "your username" -> "SSH Key".
2. Paste your key into the "Key" field.
3. Click **Add key**.

A properly-formatted SSH RSA public key entered on the website should be similar to this.



```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQDF3Aob3ZUkFo6fdD4JdnBI1pYR3kHjx/9tA0DqdPKIwPIBIxPQrIJuoaEsdiPPAFPH+7ALmRMT/GoLIQ
vtZ+OVjB8z8Tw5+gaWQtryPNueO0UG+SzPNcM6WSkwkTYk31TCuRiSSeEQoyYTLYIc7+GRnwDMHzQA75r7ougawnVjveNs3EpUf53Ia24J5Mn
Ddo5RZ6cCwiV8T+yzNmqV0i3/p2Iac94VM2VBd3icPyfpxh96pGvfyucvo92JERQIip9e+3IZa2th0T8PsRaeXqxy/0JNvcpXiHaknEvF2CmnH+arMPh
Di4+EZIzJWqGjVvgzImEGugfVOcvtuouq/UadIdPZxV1saymReePIVn0580SKIzfMcAgpLuxPLUXXuUQbK1XzIXUMIqMGLoFsSCIgY0BzahuA3+s44
j7u58HWcUR4ntbOh+oTLtYPsBUIOkG7aTEsZ3TprfsRk/HB1DT4qFzcYOZUK1udljn5m9ecBweXsZzVQbINmPkmElkbfqBOug3bbWNtKAipgA/8Y
zeUqVqSU2v5kReA7P3+vmTY7XakYkK8C15S56mimc0r29ruT449ibjn0WI/2J1Shqjpkor3L+BvTqPrM8ZKom99WeHF7Nh9LedQ2XytZo3qVf7WM
9BIDEMqzS4yVFSNBuESib1oWHAh+txZwOSKFCBFLw== user@example.com
```

Instructions on Generating SSH Keys can be found on the SC2 Wiki here.

Next Steps

Users should next follow the instructions for **[SSH Proxy Setup](https://colosseumneu.freshdesk.com/support/solutions/articles/61000253369-ssh-proxy-setup) (https://colosseumneu.freshdesk.com/support/solutions/articles/61000253369-ssh-proxy-setup)**. The private key can then be associated with connections that are made to the SSH gateway by modifying the ssh config file. Note the path to your private key that you generated in this process. The default path is: `/home/<user>/.ssh/id_rsa`

References

See the man page for ssh-keygen for more information.

Preview