

Content



How to connect to the server through SSH?

Connecting through a browser

Connecting through a browser from Bitnami Launchpad

Connecting through a browser from the Google Cloud Launcher

Obtaining your SSH credentials for your client

Obtaining your SSH credentials from the Bitnami Launchpad

Obtaining your SSH credentials from the Google Cloud Launcher

Connecting with an SSH client

Connecting with an SSH client on Windows

Connecting with an SSH client on Linux and Mac OS X

Forwarding your key using SSH Agent

[Bitnami Documentation Pages](#) > [Google Cloud Platform](#) > [Frequently Asked Questions](#)

Frequently Asked Questions For Google Cloud Platform

How To Connect To The Server Through SSH?

You can either [connect through a browser](#) or with an [SSH client](#).

Connecting Through A Browser

Connecting through a browser from Bitnami Launchpad

If you are using the Bitnami Launchpad, follow these steps:

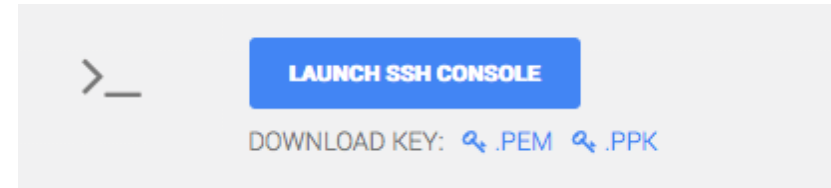
- Browse to the [Bitnami Launchpad for Google Cloud Platform](#) and sign in if required using your Bitnami account.
- Select the "Virtual Machines" menu item.
- Select your cloud server from the resulting list.
- Click the "Launch SSH Console" button.

Forwarding your key using SSH
Agent on Windows

Forwarding your key using SSH
Agent on Linux and Mac OS X

How to access a server using an SSH
tunnel?

[Accessing a server using an SSH tunnel](#)



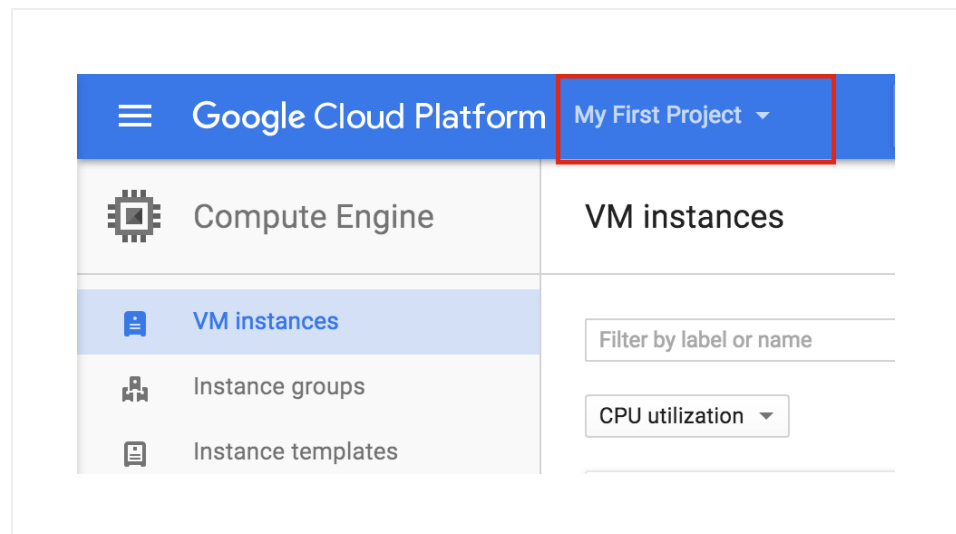
This will automatically transfer the necessary keys and connect you to your machine console in a new browser window.

NOTE: This is only supported in certain browsers, for more information, look at the [Google documentation](#).

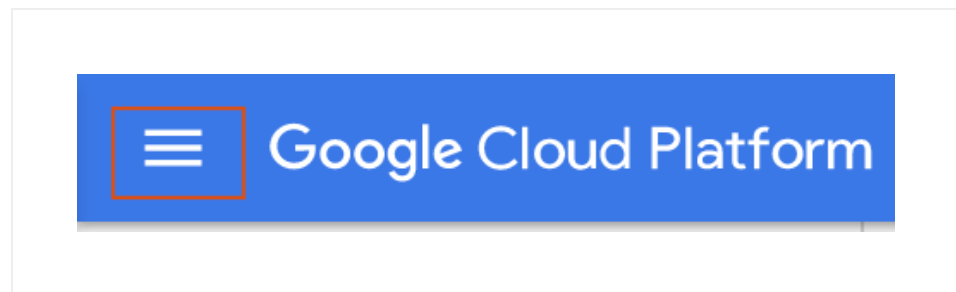
Connecting through a browser from the Google Cloud Launcher

You can also connect to your server using the [Google Cloud Platform console](#). Follow these steps:

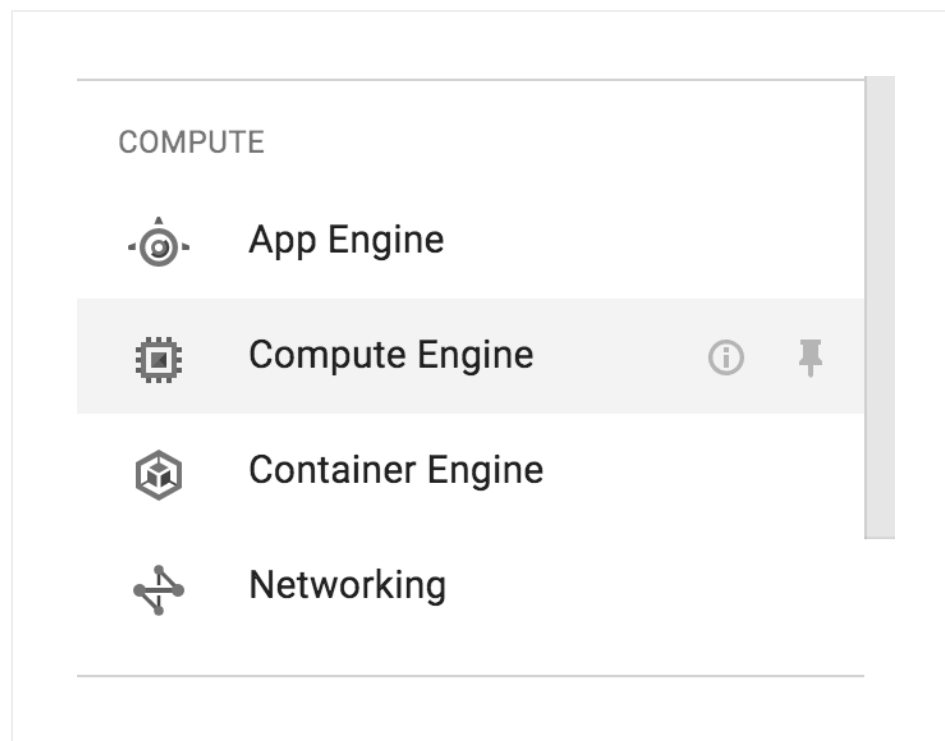
- Browse to the [Google Cloud Platform console](#) and sign in if required using your Google account.
- Find and select your project in the project list.



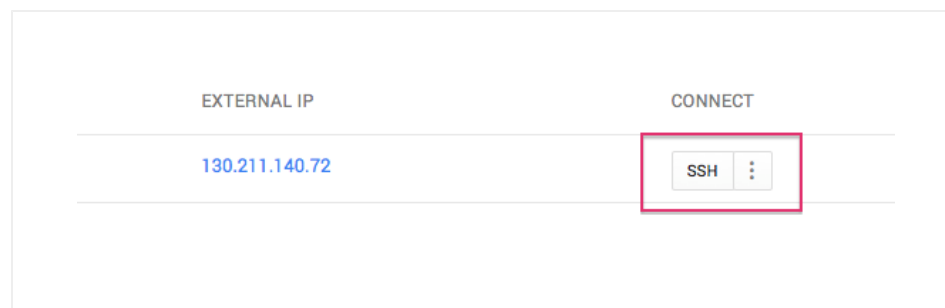
- Click the "Hamburger" button on the left side of the top navigation bar:



- Select the "Compute -> Compute Engine" menu item.



- Locate your server instance and select the SSH button.



This will automatically transfer the necessary keys and connect you to your machine console in a new browser window.

NOTE: Bitnami documentation usually assumes that server console

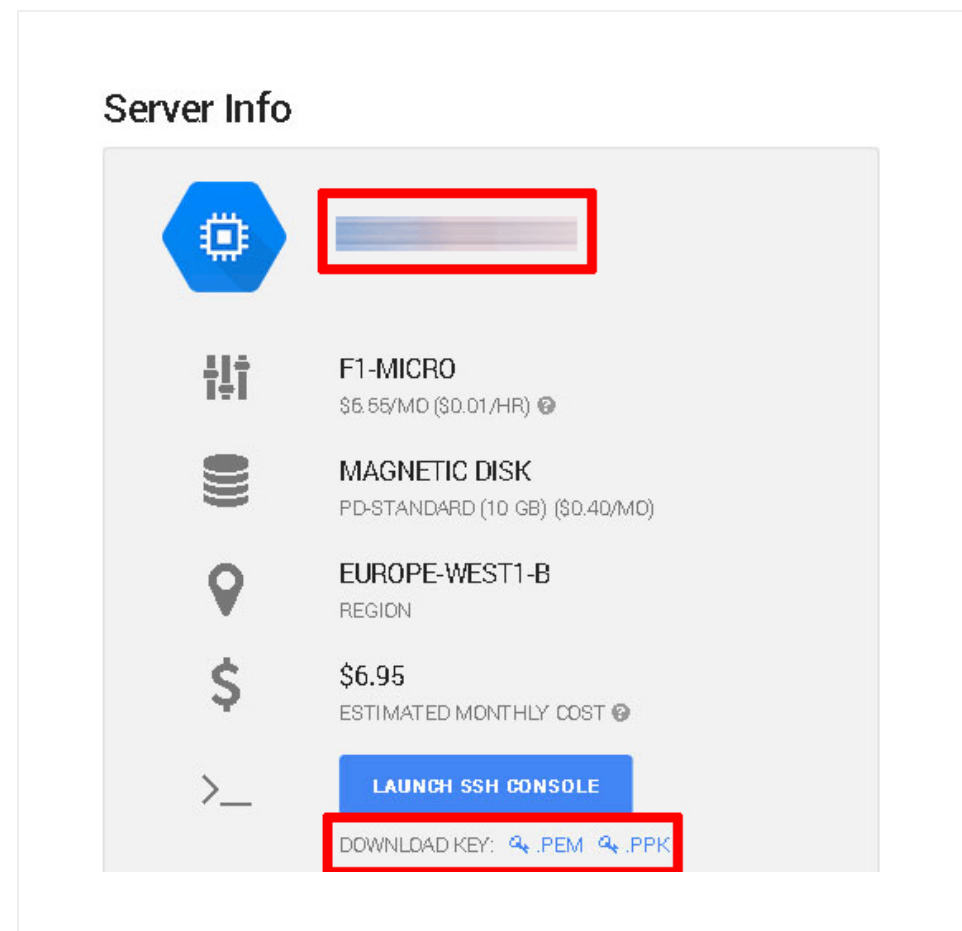
commands are executed under the bitnami user account. However, when connecting through a browser SSH console as described above, you may be logged in under a different user account. To switch to the bitnami user account, use the command `sudo su - bitnami`.

Obtaining Your SSH Credentials For Your Client

Obtaining your SSH credentials from the Bitnami Launchpad

The [Bitnami Launchpad for Google Cloud Platform](#) automatically injects an auto-generated public SSH key for the bitnami user and allows the user to download the private SSH key. To do so, follow these steps:

- Browse to the [Bitnami Launchpad for Google Cloud Platform](#) and sign in if required using your Bitnami account.
- Select the "Virtual Machines" menu item.
- Select your cloud server from the resulting list.
- Download the SSH key for your server (.pem for Linux and Mac OS X, .ppk for Windows). Note the server IP address on the same page.

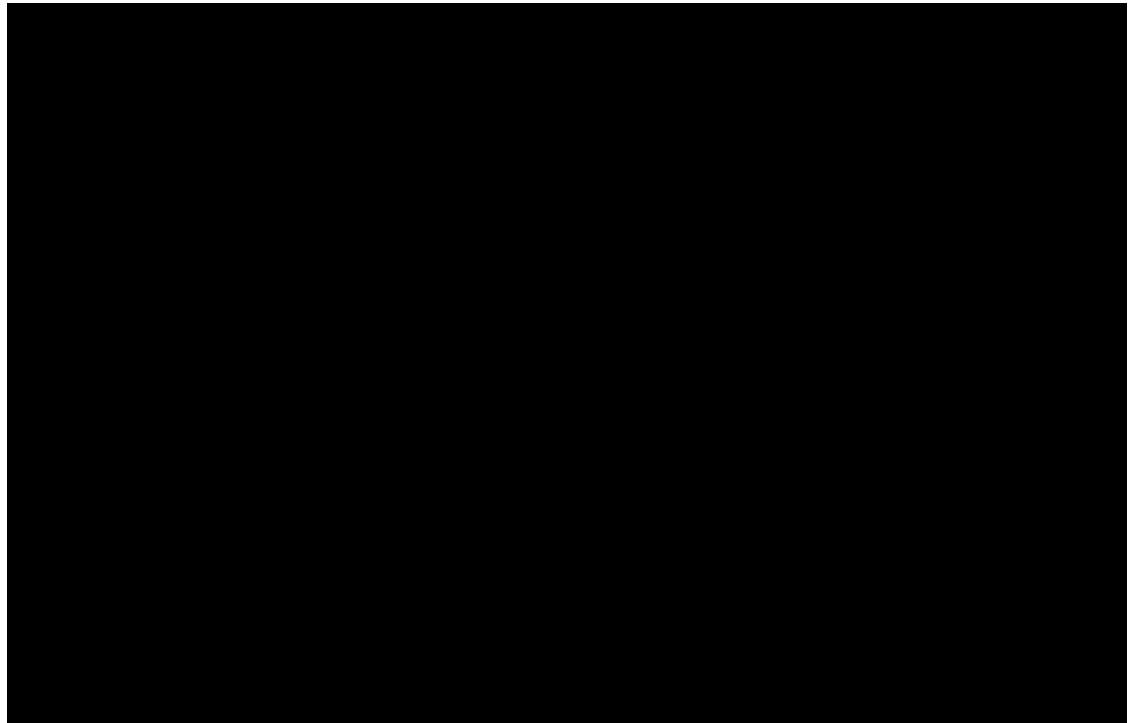


Obtaining your SSH credentials from the Google Cloud Launcher

The [Google Cloud Launcher](#) requires the user to manually add a public SSH key using the server administration page. It then uses the user@hostname comment at the end of the public SSH key to decide which user account on the server should be associated with the key.

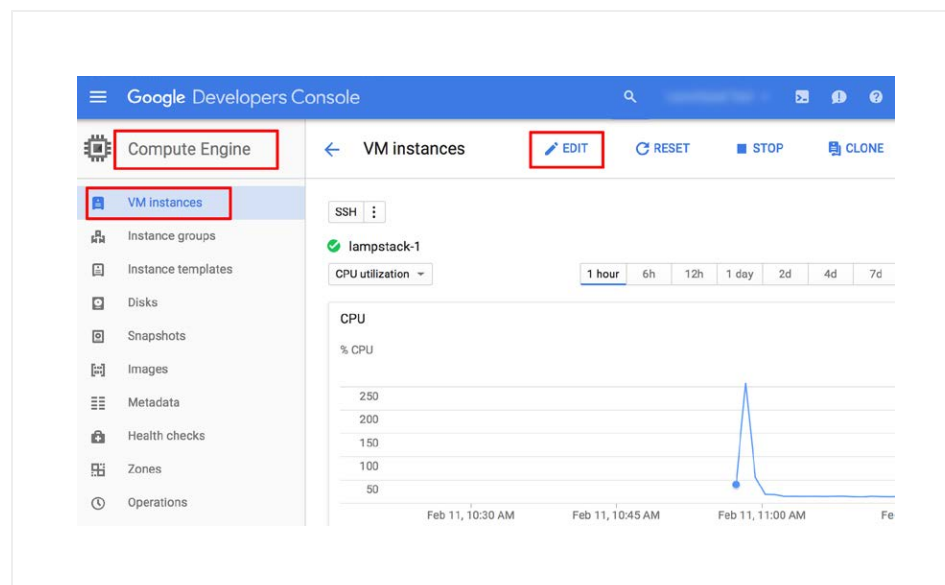
Watch the following video to learn how to add your SSH credentials to your

server through the Google Cloud Console:

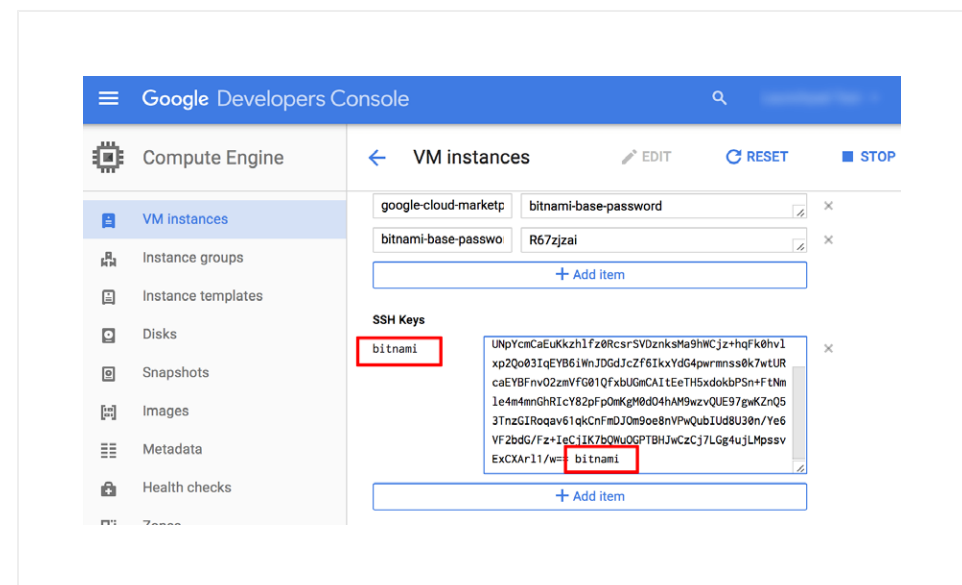


Follow the steps below in order to add your public SSH key:

- Prepare an SSH key pair for use.
- Log in to the [Google Cloud Console](#) and select your project.
- Navigate to the "Compute Engine -> VM Instances" page and select the server you wish to connect to.
- Click the "Edit" link in the top control bar.



- On the resulting page, copy and paste your public SSH key into the "SSH Keys" field.
- Update the user@hostname comment at the end of the SSH key content to bitnami. This will associate the SSH key with the bitnami user account that is already present on the server. The "Username" next to the form field will update accordingly.



- Add more keys as needed by clicking the "Add Item" button. Once done, save the changes by clicking the "Save" button.

Connecting With An SSH Client

Connecting with an SSH client on Windows

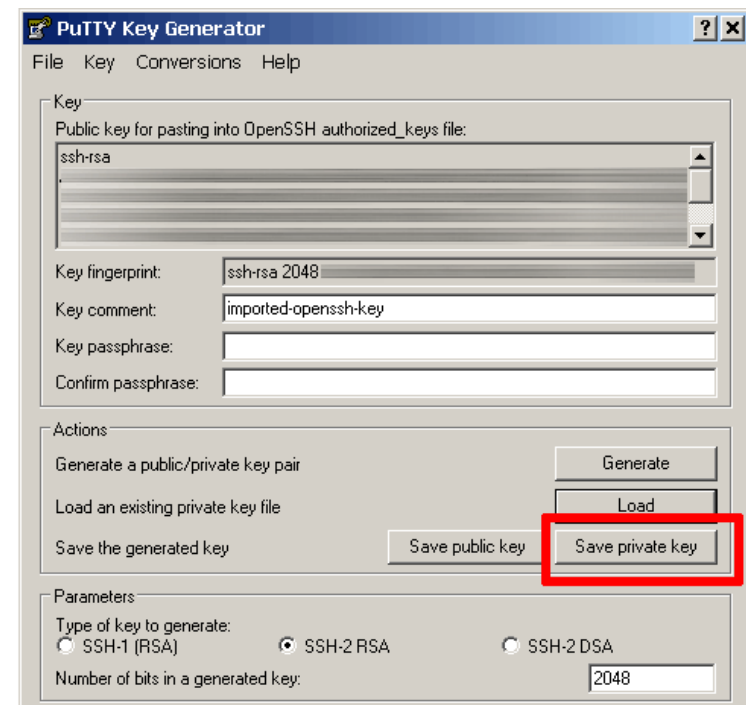
In order to access your server via SSH tunnel you need an SSH client. In the instructions below we have selected [PuTTY](#), a free SSH client for Windows and UNIX platforms. To access the server via SSH tunnel using PuTTY on a specific port using an SSH tunnel, you need to have it configured in order to allow connections to your server.

- Step 1: Obtain PuTTY
 - Download the PuTTY ZIP archive from [its website](#).
 - Extract the contents to a folder on your desktop.
- Step 2: Convert your PEM private key to PPK format (optional)

If your private key is in .pem format, it is necessary to convert it to PuTTY's own .ppk format before you can use it with PuTTY. If your private key is already in .ppk format, you may skip this step.

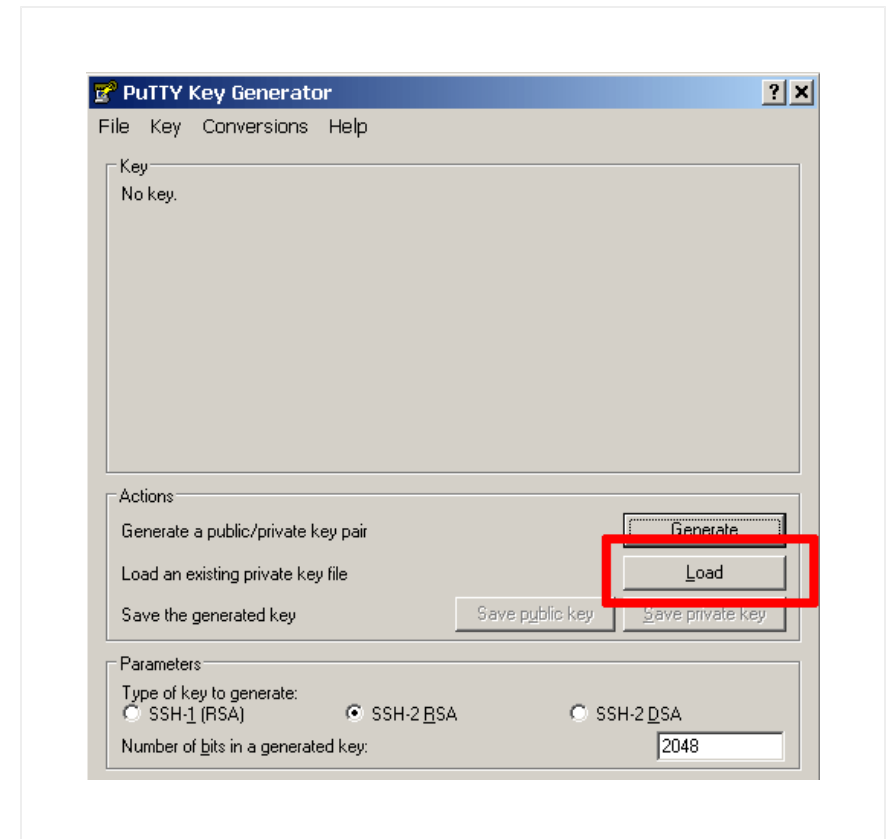
Follow the steps below to convert your .pem private key to .ppk format:

- Launch the PuTTY Key Generator by double-clicking the puttygen.exe file in the PuTTY installation directory.
- Click the "Load" button and select the private key file in .pem format.

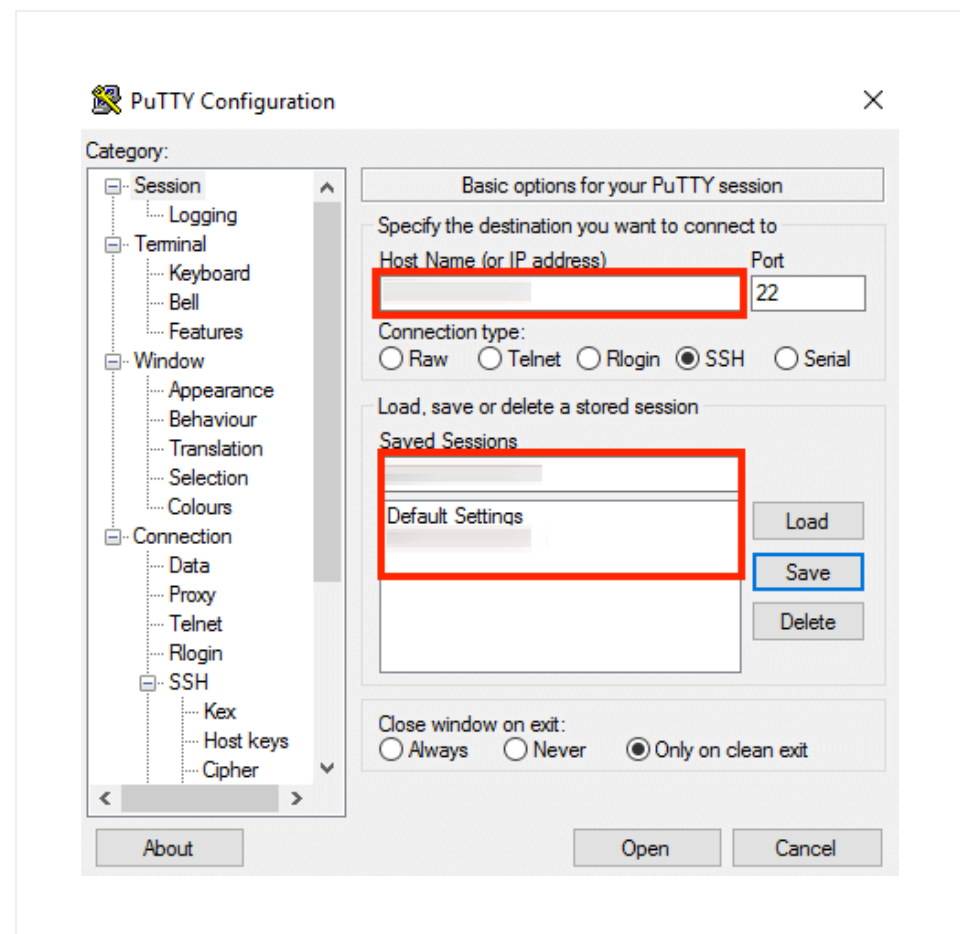


- Once the private key has been imported, click the "Save private

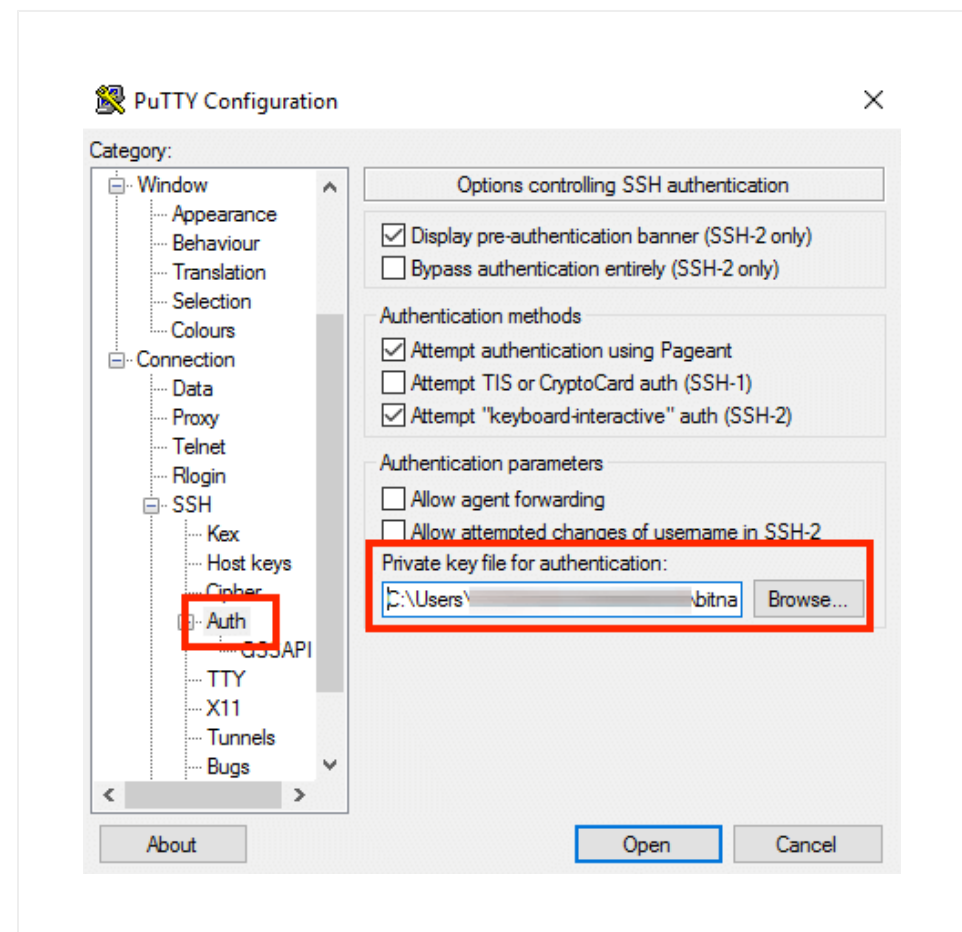
key" button to convert and save the key in PuTTY's .ppk key file format.



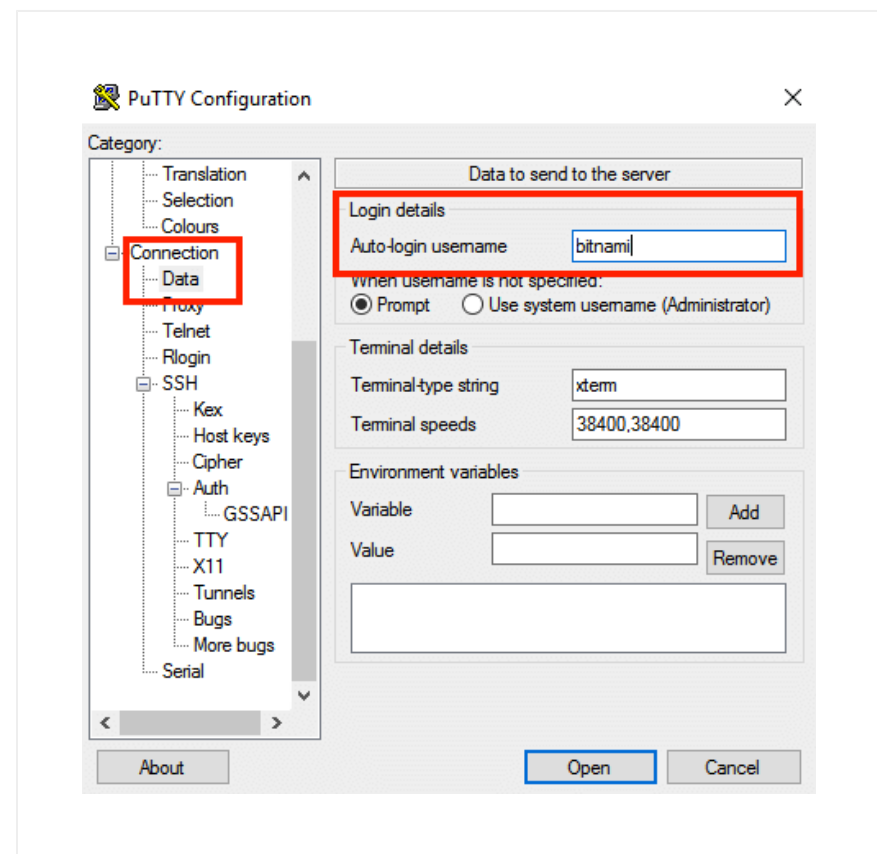
- Step 3: Configure PuTTY
 - Double-click the putty.exe file to bring up the PuTTY configuration window.
 - In the PuTTY configuration window, enter the host name or public IP address of your server into the "Host Name (or IP address)" field, as well as into the "Saved Sessions" field. Then, click "Save" to save the new session so you can reuse it later.



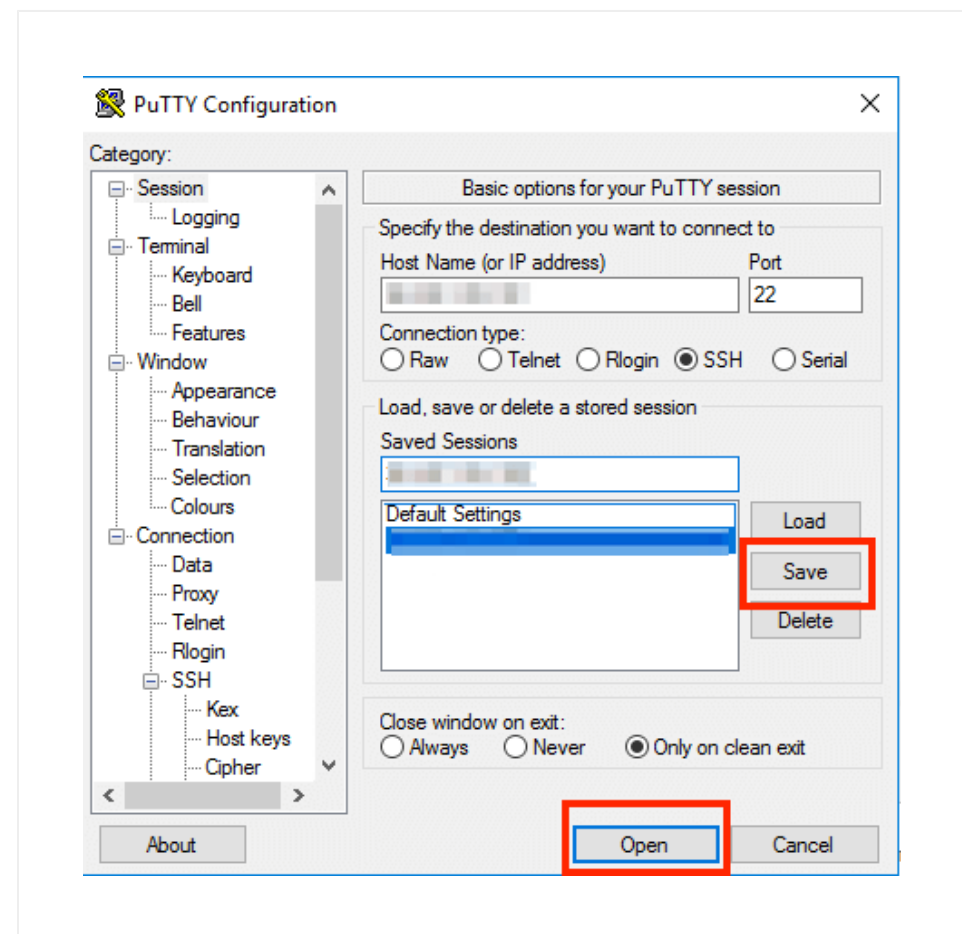
- Obtain your SSH credentials in order to allow the authentication against the server. Refer to the [FAQ](#) to learn how to obtain your SSH credentials for your client.
- In the "Connection -> SSH -> Auth" section, browse to the private key file (.ppk) you've previously obtained in the step above.



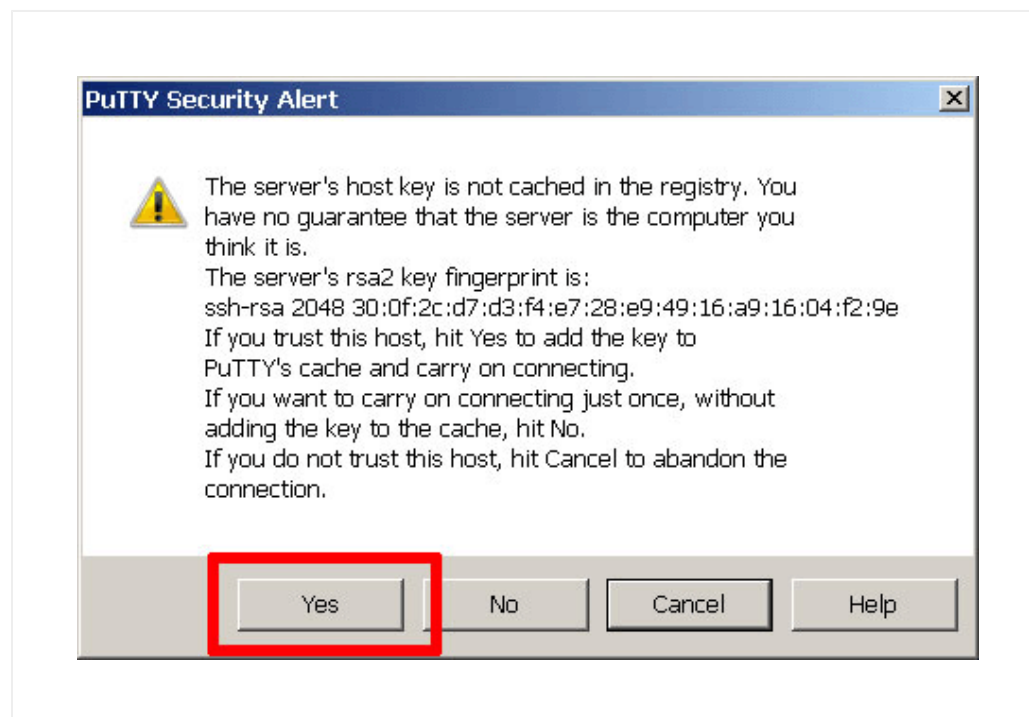
- In the "Connection -> Data" section, enter the username bitnami into the "Auto-login username" field, under the "Login details" section.



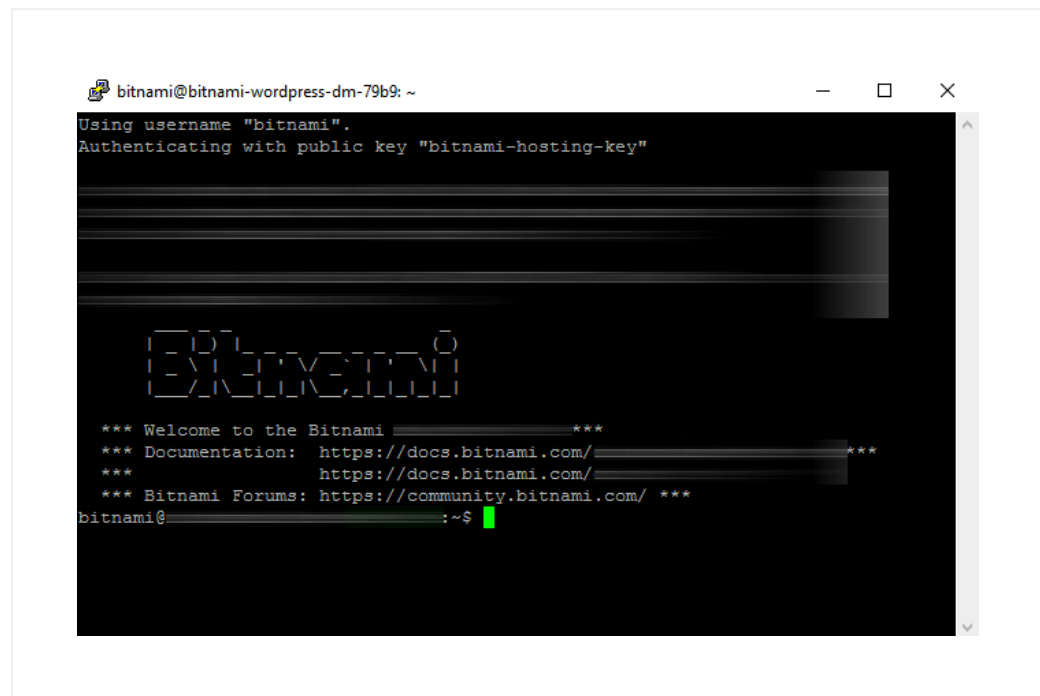
- In the "Session" section, click on the "Save" button to save the current configuration.
- Select the session you want to start (in case that you have saved more than one session) and click the "Open" button to open an SSH session to the server.



PuTTY will first ask you to confirm the server's host key and add it to the cache. Go ahead and click "Yes" to this request ([learn more](#)).



You should now be logged in to your server. Here is an example of what you'll see:



Connecting with an SSH client on Linux and Mac OS X

Linux and Mac OS X come bundled with SSH clients by default. In order to log in to your server, follow the steps below:

- Open a new terminal window on your local system (for example, using "Finder -> Applications -> Utilities -> Terminal" in Mac OS X or the Dash in Ubuntu).
- Set the permissions for your private key file (*.pem) to 600 using a command like the one below. Refer to the [FAQ](#) to learn how to obtain your SSH credentials.

```
$ chmod 600 KEYFILE
```

- Connect to the server using the following command:

```
$ ssh -i KEYFILE bitnami@SERVER-IP
```

Remember to replace KEYFILE in the previous commands with the path to your private key file (.pem), and SERVER-IP with the public IP address or hostname of your server.

- Your SSH client might ask you to confirm the server's host key and add it to the cache before connecting. Accept this request by typing or selecting "Yes" ([learn more](#)).

You should now be logged in to your server. Here is an example of what you'll see:



Forwarding Your Key Using SSH Agent

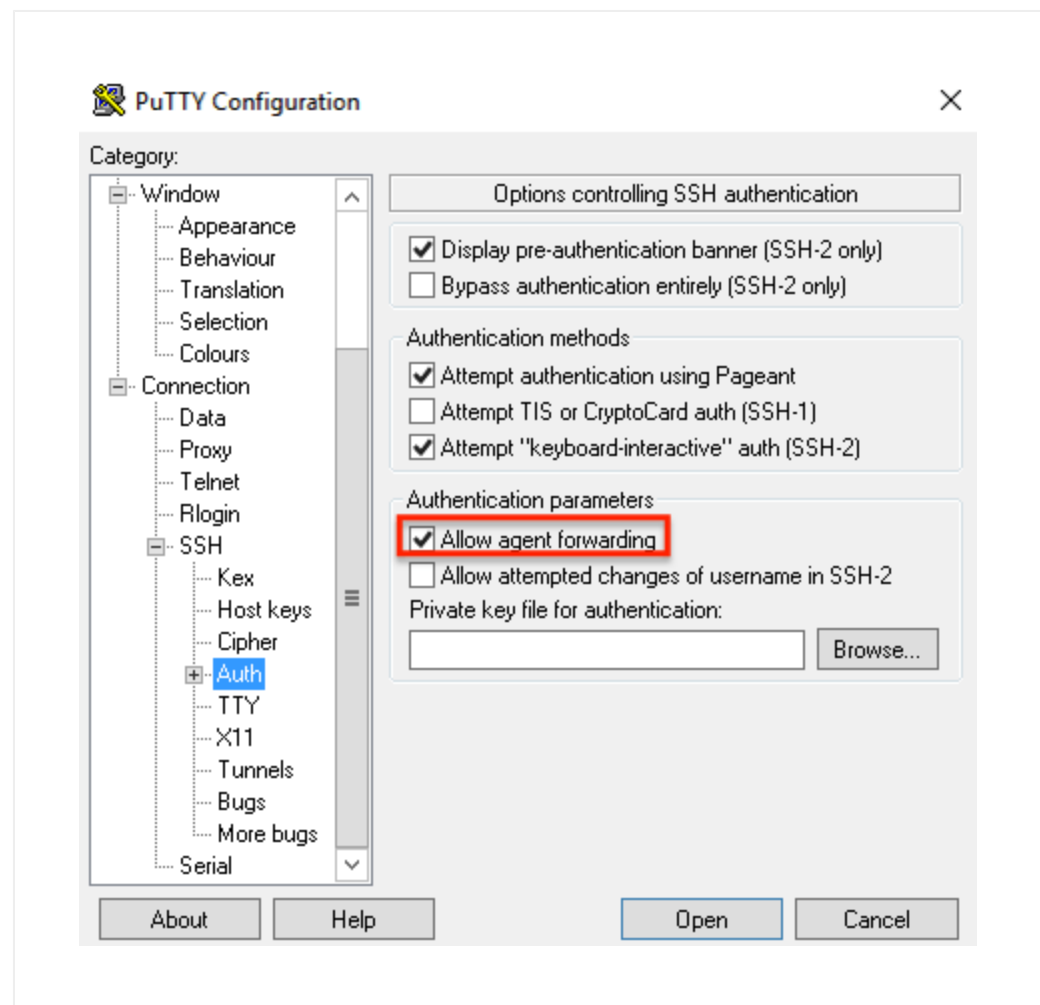
Forward your key it is an easy way to connect to a host (host A) with your SSH key, and from there, to connect to another host (host B) using the same key.

Forwarding your key using SSH Agent on Windows

To access the server via SSH forwarding your key using PuTTY you must have it configured. Please, check the [how to connect to the server through SSH using an SSH client on Windows](#) section for more information on this.

Once you have your SSH client correctly configured, you need to enable the SSH Agent forwarding. For doing so, follow these steps:

- In the "Connection -> SSH -> Auth" section, activate the "Allow agent forwarding" checkbox.



- In the "Session" section, save your changes by clicking the "Save" button.
- Click the "Open" button to open an SSH session to the server. The SSH session will now forward your key, you can check it by running the following:

```
$ ssh-add -L
```

Forwarding your key using SSH Agent on Linux and Mac

OS X

To access the server forwarding SSH keys, follow the steps below.

- Open a new terminal window on your local system (for example, using "Finder -> Applications -> Utilities -> Terminal" in Mac OS X or the Dash in Ubuntu).
- To access the server forwarding your key, you need to have the following information:
 - Server's IP address.
 - [SSH key \(.pem key file\)](#) in hand.

- Run the following command to add the SSH key to the agent. Remember to replace KEYFILE with the path to your private key:

```
$ ssh-add KEYFILE
```

- Connect to the server using -A option, remember to replace SERVER-IP with the public IP address or hostname of your server:

```
$ ssh -A bitnami@SERVER-IP
```

- The SSH session will now forward your key, you can check it by running the following:

```
$ ssh-add -L
```

How To Access A Server Using An SSH

Tunnel?

Bitnami strongly discourages you from opening server ports apart from those defined by default. In case you need to access a server on a specific port remotely, Bitnami recommends creating an SSH tunnel instead of opening the port in the server firewall.

Depending on your operating system, follow these instructions to create an SSH tunnel and ensure secure access to the application.

IMPORTANT: Before following the steps below, ensure that your application server is running.

Accessing A Server Using An SSH Tunnel On Windows

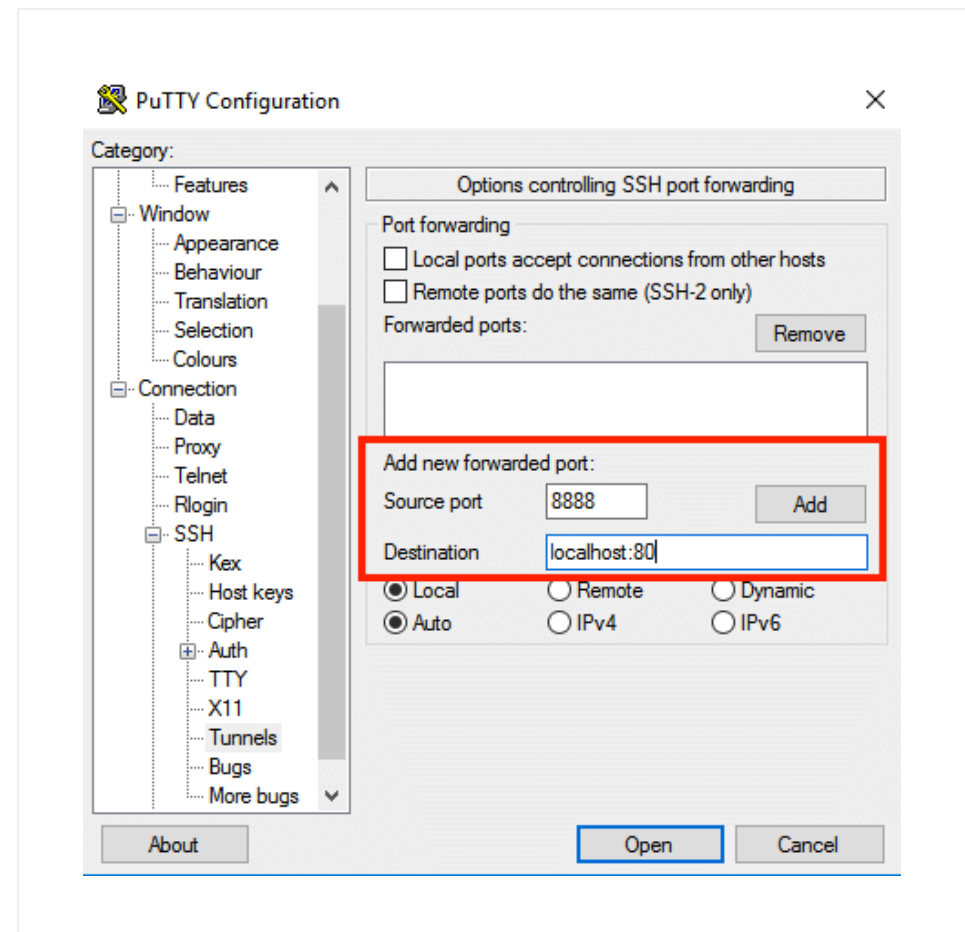
In order to access your server via SSH tunnel you need an SSH client. In the instructions below we have selected [PuTTY](#), a free SSH client for Windows and UNIX platforms.

- To access the server via SSH tunnel using PuTTY on a specific port you must have it configured. Please, check how to configure PuTTY in the section [how to connect to the server through SSH using an SSH client on Windows](#).

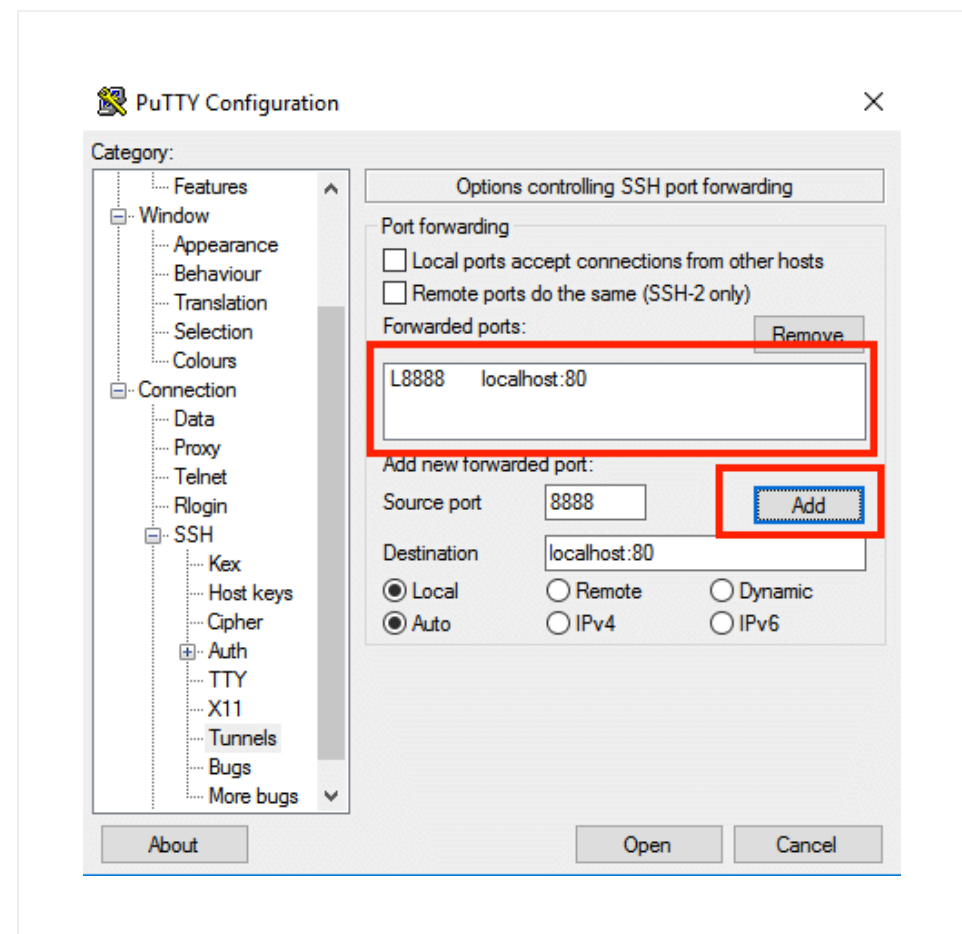
Once you have your SSH client correctly configured and you tested that you can successfully access to your instance via SSH, you need to create an SSH tunnel. For doing so, follow these steps:

- In the "Connection -> SSH -> Tunnels" section, create a secure tunnel by forwarding a port (the "destination port") on the remote server to a

port (the "source port") on the local host (127.0.0.1 or localhost). An example of configuring an SSH tunnel between remote port 80 and local port 8888 is displayed below.



- Click the "Add" button to add the secure tunnel configuration to the session. (You'll see the added port in the list of "Forwarded ports"). An example of configuring an SSH tunnel between remote port 80 and local port 8888 is displayed below.



- In the "Session" section, save your changes by clicking the "Save" button.
- Click the "Open" button to open an SSH session to the server. The SSH session will now include a secure SSH tunnel between the two specified ports.

While the tunnel is active, you should be able to access the application through the secure SSH tunnel you created, by browsing to `http://127.0.0.1:SOURCE-PORT/` or `http://localhost:SOURCE-PORT/`. Remember to replace SOURCE-PORT with the source port number specified.

Accessing A Server Using An SSH Tunnel On Linux And Mac OS X

To access the server on a specific port using an SSH tunnel, follow the steps below.

- Open a new terminal window on your local system (for example, using "Finder -> Applications -> Utilities -> Terminal" in Mac OS X or the Dash in Ubuntu).
- To access the server on a specific port using an SSH tunnel, you need to have the following information:
 - Server's IP address
 - [SSH key \(.pem key file\)](#) in hand.
- Run the following command to configure the SSH tunnel. Remember to replace SOURCE-PORT with the source port, DESTINATION-PORT with the destination port, KEYFILE with the path to your private key, and SERVER-IP with the public IP address or hostname of your server:

```
$ ssh -N -L SOURCE-PORT:127.0.0.1:DESTINATION-PORT -i  
KEYFILE bitnami@SERVER-IP
```

NOTE: If successful, the above command will create an SSH tunnel but will not display any output on the server console.

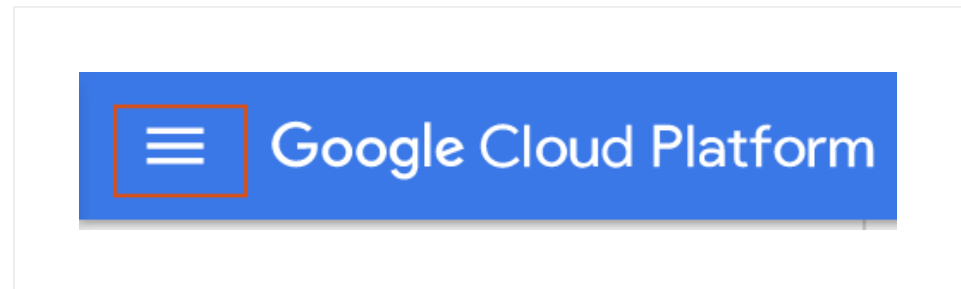
While the tunnel is active, you should be able to access the application through the secure SSH tunnel you created, by browsing to `http://127.0.0.1:SOURCE-PORT/` or `http://localhost:SOURCE-PORT/`. Remember to replace SOURCE-PORT with the source port number specified.

How To Find Application Credentials?

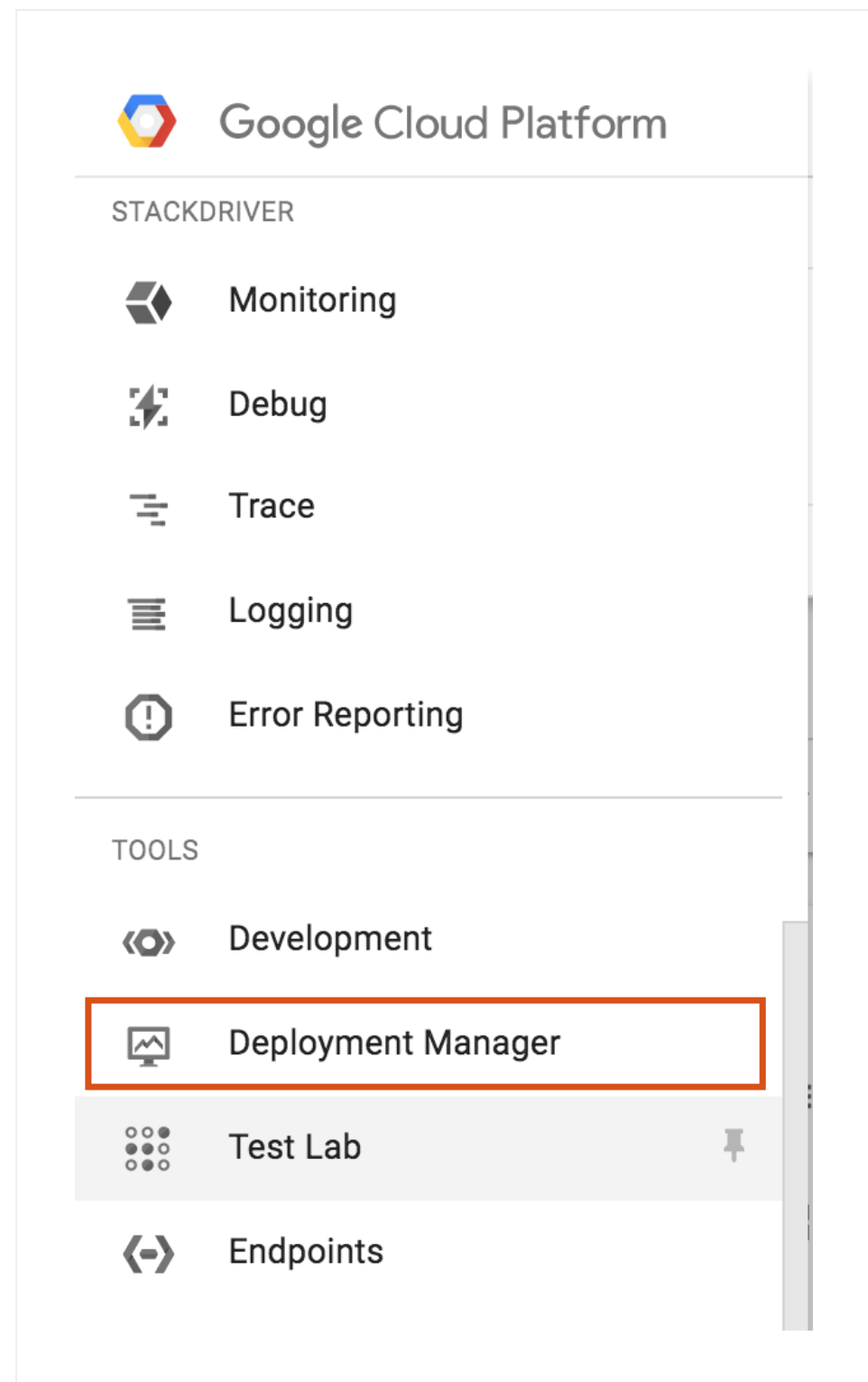
Servers Deployed Using The Google Cloud Launcher

Your default credentials become available once you create a cloud server. To find them, follow these steps:

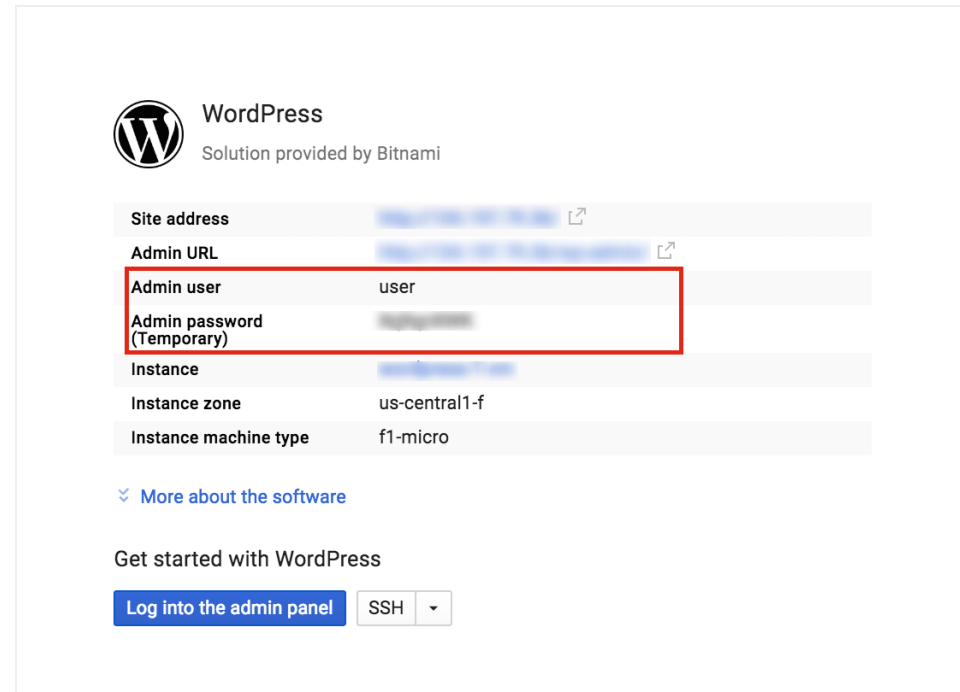
- Browse to the [Google Cloud Platform console](#) and sign in if required using your Google account.
- Click the "Hamburger" button on the left side of the top navigation bar:



- Select the "Deployment manager" menu item.



- Select your cloud server from the resulting list.
- In the right panel, the username and password are specified in the "Admin User" and "Admin Password (Temporary)" fields respectively.



WordPress
Solution provided by Bitnami

Site address	<input type="text" value="http://127.0.0.1"/>
Admin URL	<input type="text" value="http://127.0.0.1"/>
Admin user	user
Admin password (Temporary)	<input type="password" value="12345678"/>
Instance	<input type="text" value="wordpress-12345"/>
Instance zone	us-central1-f
Instance machine type	f1-micro

[More about the software](#)

Get started with WordPress

[Log into the admin panel](#) SSH ▾

You can also obtain the application username from [the application page in our documentation](#).

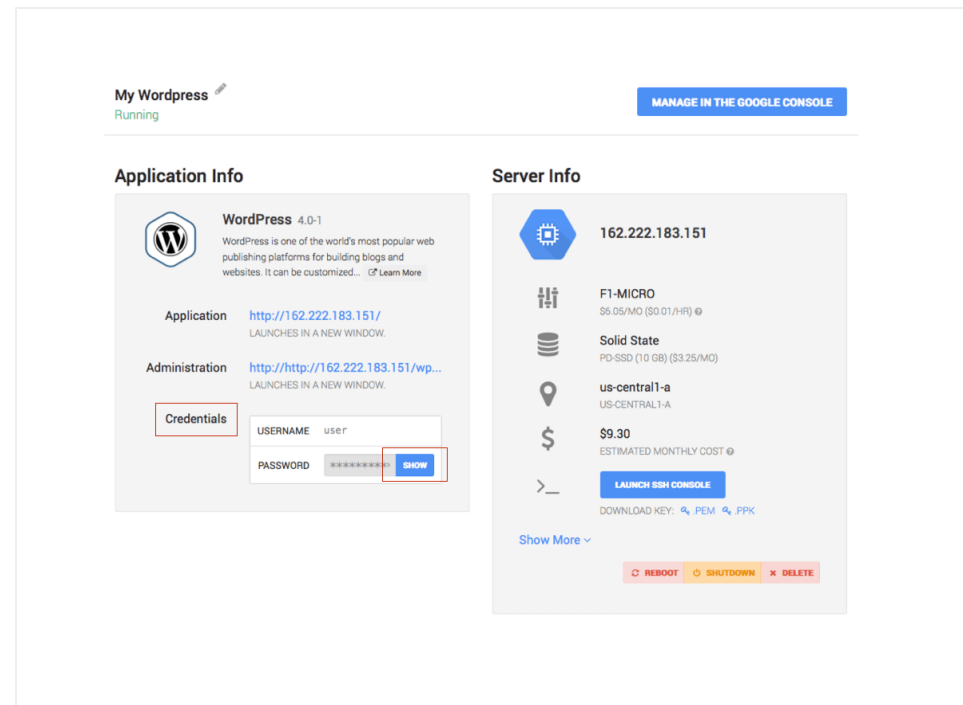
- To access your database, the database password is the value next to "Admin Password (Temporary)" as well.

NOTE: You should change the passwords after your first login.

Servers Deployed Using The Bitnami Launchpad

Your default credentials become available once you create a cloud server. To find them, follow these steps:

- Browse to the [Bitnami Launchpad for Google Cloud Platform](#) and sign in if required using your Bitnami account.
- Select the "Virtual Machines" menu item.
- Select your cloud server from the resulting list.
- The "Application Info" section in the left panel contains the credentials for your instance. The password is hidden by default but will be displayed in plain text when the "Show" button, adjacent to the password input, is clicked.



What Is A Bitnami Image?

A Bitnami image includes everything you need to run your Bitnami-packaged application of choice. The installation and configuration of all of the software included in the stack is completely automated, making it easy for everyone, including those who are not very technical, to get them up and running.

All Bitnami images are completely self-contained and run independently of the rest of the software or libraries installed on your system. This means that you don't have to worry about installing any other software on your system to make the new application work. They also won't interfere with any software already installed on the system, so everything will continue to work normally.

How To Start Or Stop The Services?

Each Bitnami stack includes a control script that lets you easily stop, start and restart services. The script is located at `/opt/bitnami/ctlscript.sh`. Call it without any service name arguments to start all services:

```
$ sudo /opt/bitnami/ctlscript.sh start
```

Or use it to restart a single service, such as Apache only, by passing the service name as argument:

```
$ sudo /opt/bitnami/ctlscript.sh restart apache
```

Use this script to stop all services:

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

Restart the services by running the script without any arguments:

```
$ sudo /opt/bitnami/ctlscript.sh restart
```

Obtain a list of available services and operations by running the script without any arguments:

```
$ sudo /opt/bitnami/ctlscript.sh
```

What Is The Directory Structure?

The installation process will create several sub-directories under the /opt/bitnami directory:

- Servers and related tools: apache2/, mysql/, postgresql/, apache-tomcat/, etc.
- Languages: php/, python/, ruby/, tcl/, etc.
- Application files: apps/phpMyAdmin/, apps/drupal/, apps/joomla/, apps/redmine/, etc.
- Common libraries: common/
- Licenses of the components included in the stack: licenses/

Application files are stored in the /opt/bitnami/apps/APPNAME/htdocs directory. The configuration file for the Apache Web server is stored in the

/opt/bitnami/apps/APPNAME/conf/ directory.

How To Open The Server Ports For Remote Access?

IMPORTANT: Making this application's network ports public is a significant security risk. You are strongly advised to only allow access to those ports from trusted networks. If, for development purposes, you need to access from outside of a trusted network, please do not allow access to those ports via a public IP address. Instead, use a secure channel such as a VPN or an SSH tunnel. Follow these instructions to [remotely connect safely and reliably](#).

By default, Google cloud servers have some or all of their ports closed to secure them against external attacks. In some cases, ports needed for specific applications to operate properly are also left open by default.

If you need to access your server remotely, you must first open the necessary port(s) using the [Google Console](#).

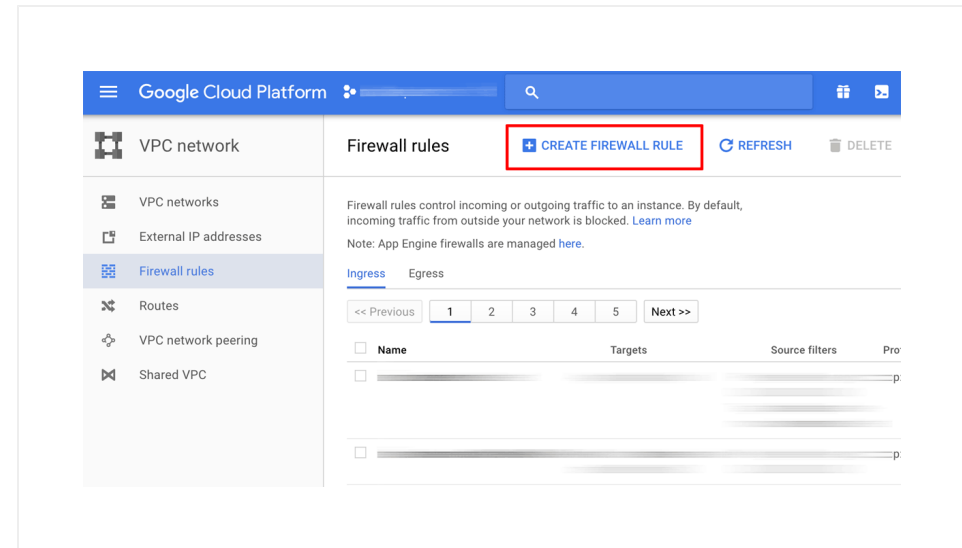
NOTE: For servers launched through the [Bitnami Launchpad for Google Cloud Platform](#), select the cloud server you wish to modify in the Bitnami Launchpad and click the "Manage in the Google Console" button to access the Google management console.

Follow the steps below:

- Log in to the [Google Cloud Console](#) using the Google Account

associated with your project.

- Select the "Networking -> VPC network -> Firewall rules" menu.
- On the resulting page, create a new firewall rule for your network by clicking the "Create firewall rule" button.



- Enter details for the new firewall rule using the guidelines below:
 - Name: Use a human-readable name that makes it easy to identify the rule
 - Description: Enter a description for the firewall rule (optional)
 - Network: Select the network used by your server
 - Direction of traffic: Select the "Ingress" option
 - Action on match: Select the "Allow" option
 - Source filter: Select the "IP ranges" option
 - Source IP ranges: Use 0.0.0.0/0 to allow access from anywhere, or specify an IP address range
 - Specified protocols or ports: Enter the port numbers prefixed by either tcp: or udp:. Use commas to separate multiple port

numbers and semi-colons between protocol blocks. For example: tcp:80, 443; udp:8001

The image below sets up a firewall rule for Apache Cassandra on TCP ports 9042 and 7000 as an example.

The screenshot displays the 'Create a firewall rule' page in the Google Cloud Platform console. The left sidebar shows the navigation menu with 'Firewall rules' selected. The main content area contains the following fields:

- Network:** A dropdown menu set to 'default'.
- Priority:** A text input field set to '1000'.
- Direction of traffic:** Radio buttons for 'Ingress' (selected) and 'Egress'.
- Action on match:** Radio buttons for 'Allow' (selected) and 'Deny'.
- Targets:** A dropdown menu set to 'Specified target tags'.
- Target tags:** An empty text input field.
- Source filter:** A dropdown menu set to 'IP ranges'.
- Source IP ranges:** A text input field containing '0.0.0.0/0'.
- Second source filter:** A dropdown menu set to 'None'.
- Protocols and ports:** Radio buttons for 'Allow all' and 'Specified protocols and ports' (selected). Below this, a text input field contains 'tcp:9042; tcp:7000'.

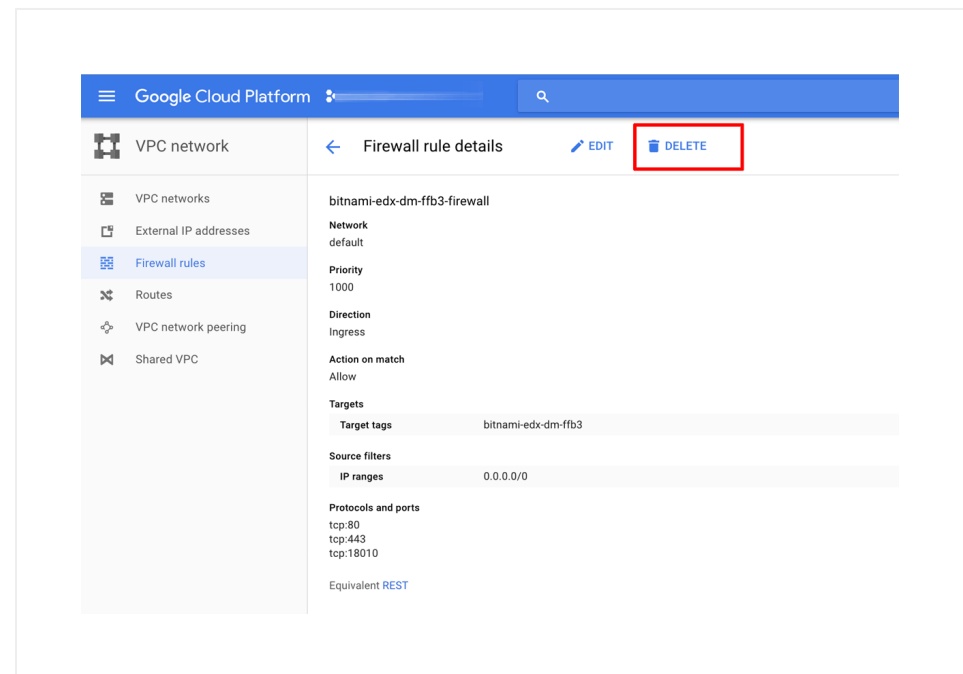
- Click "Create" to save the firewall rule. The new firewall rule will come into effect immediately.

How To Close The Server Ports And Deny Remote Access?

NOTE: For servers launched through the [Bitnami Launchpad for Google Cloud Platform](#), select the cloud server you wish to modify in the Bitnami Launchpad and click the "Manage in the Google Console" button to access the Google management console.

To close a server port and deny remote access on that port, follow these steps:

- Log in to the [Google Cloud Console](#) using the Google Account associated with your project.
- Select the "Networking -> VPC network -> Firewall rules" menu.
- Find the firewall rule(s) for the port(s) you wish to close. Select each rule and click the "Delete" button at the top of the page. The change will come into effect immediately.

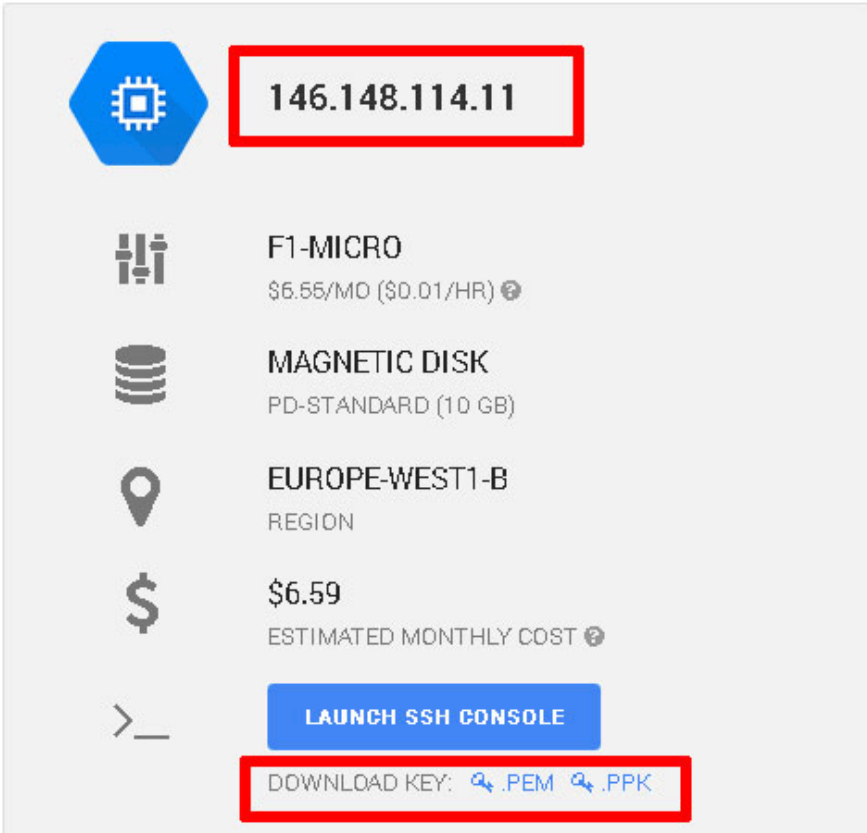








How To Upload Files To The Server With SFTP?

NOTE: Bitnami applications can be found in /opt/bitnami/apps.

- If you are using the [Bitnami Launchpad for Google Cloud Platform](#), obtain your server SSH key by following these steps:
 - Browse to the Bitnami Launchpad for Google Cloud Platform dashboard and sign in if required using your Bitnami account.
 - Select the "Virtual Machines" menu item.
 - Select your cloud server from the resulting list.
 - Download the SSH key for your server in PPK or PEM format. Note the server IP address on the same page.

Server Info



	146.148.114.11
	F1-MICRO \$6.55/MO (\$0.01/HR) ⓘ
	MAGNETIC DISK PD-STANDARD (10 GB)
	EUROPE-WEST1-B REGION
	\$6.59 ESTIMATED MONTHLY COST ⓘ
	LAUNCH SSH CONSOLE
	DOWNLOAD KEY: 🔗 .PEM 🔗 .PPK

- If you are using the [Google Cloud Launcher](#), you will need to [generate](#) and [add your SSH key manually using these instructions](#).
- Generate SSH key pair by executing the following commands:

NOTE: Replace USERNAME in the commands below with your Google Cloud platform username.

```
$ sudo su USERNAME
```

```
$ ssh-keygen -t rsa -f ~/.ssh/my-ssh-key -C USERNAME
```

- Enter the passphrase twice. The SSH key pair will be generated and saved in `/home/USERNAME/.ssh/my-ssh-key` and `/home/USERNAME/.ssh/my-ssh-key.pub`.

Although you can use any SFTP/SCP client to transfer files to your server, this guide documents [FileZilla](#) (Windows, Linux and Mac OS X), [WinSCP](#) (Windows) and [Cyberduck](#) (Mac OS X).

Using An SSH Key

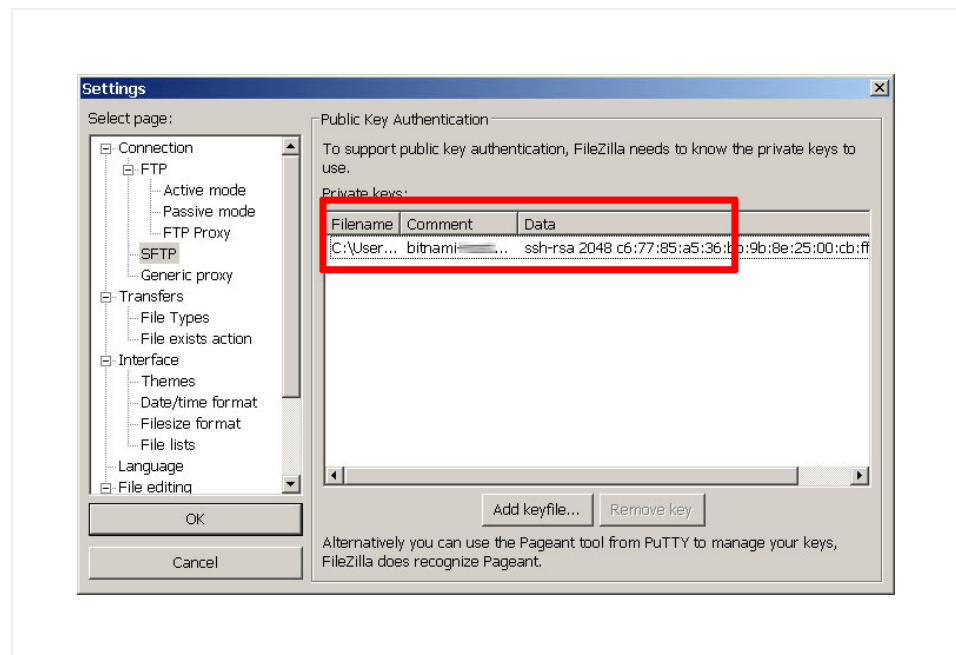
Once you have your server's SSH key, choose your preferred application and follow the steps below to connect to the server using SFTP.

FileZilla

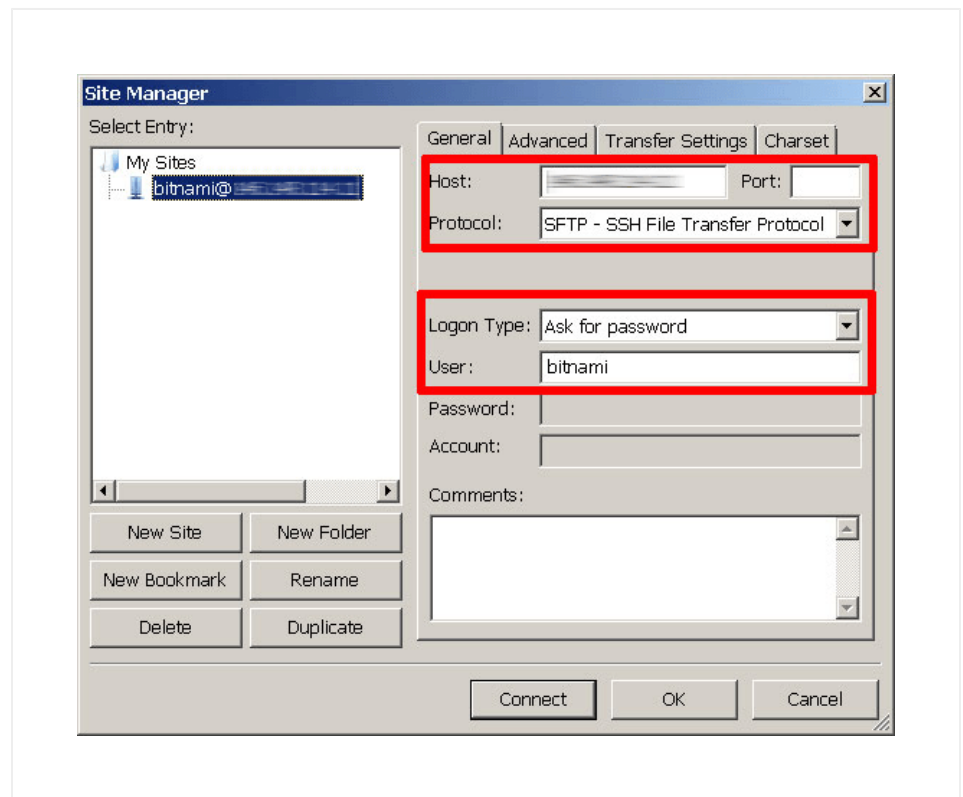
IMPORTANT: To use FileZilla, your server private key should be in PPK format.

Follow these steps:

- Download and install FileZilla.
- Launch FileZilla and use the "Edit -> Settings" command to bring up FileZilla's configuration settings.
- Within the "Connection -> SFTP" section, use the "Add keyfile" command to select the private key file for the server. FileZilla will use this private key to log in to the server.



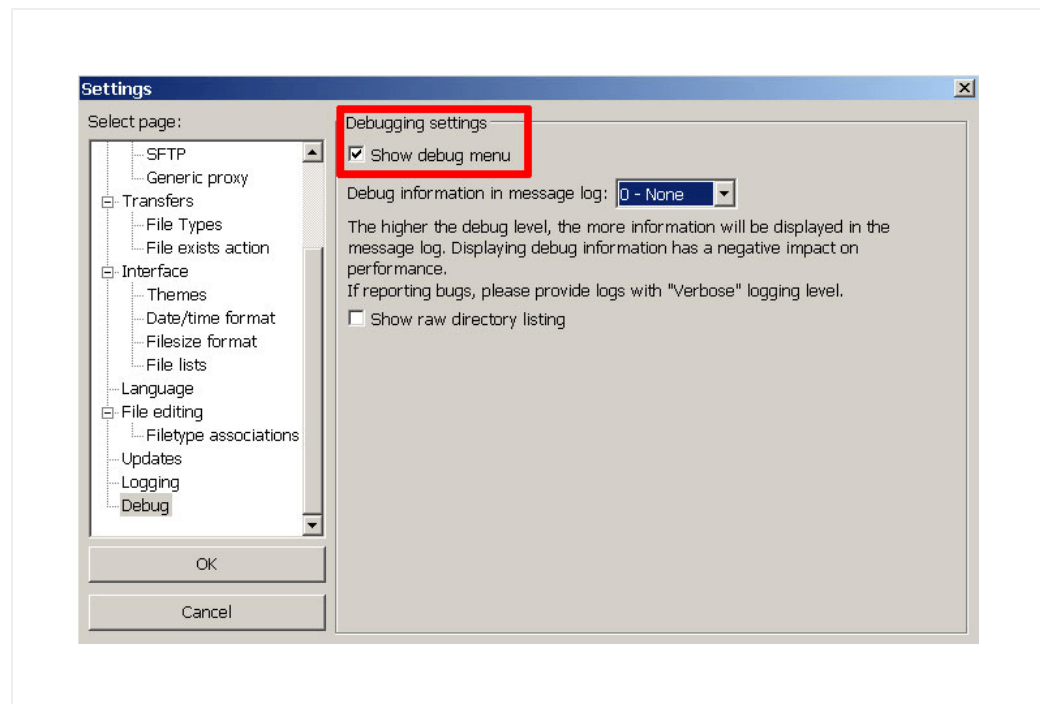
- Use the "File -> Site Manager -> New Site" command to bring up the FileZilla Site Manager, where you can set up a connection to your server.
- Enter your server host name and specify bitnami as the user name.
- Select "SFTP" as the protocol and "Ask for password" as the logon type.



- Use the "Connect" button to connect to the server and begin an SFTP session. You might need to accept the server key, by clicking "Yes" or "OK" to proceed.

You should now be logged into the /home/bitnami directory on the server. You can now transfer files by dragging and dropping them from the local server window to the remote server window.

If you have problems accessing your server, get extra information by use the "Edit -> Settings -> Debug" menu to activate FileZilla's debug log.

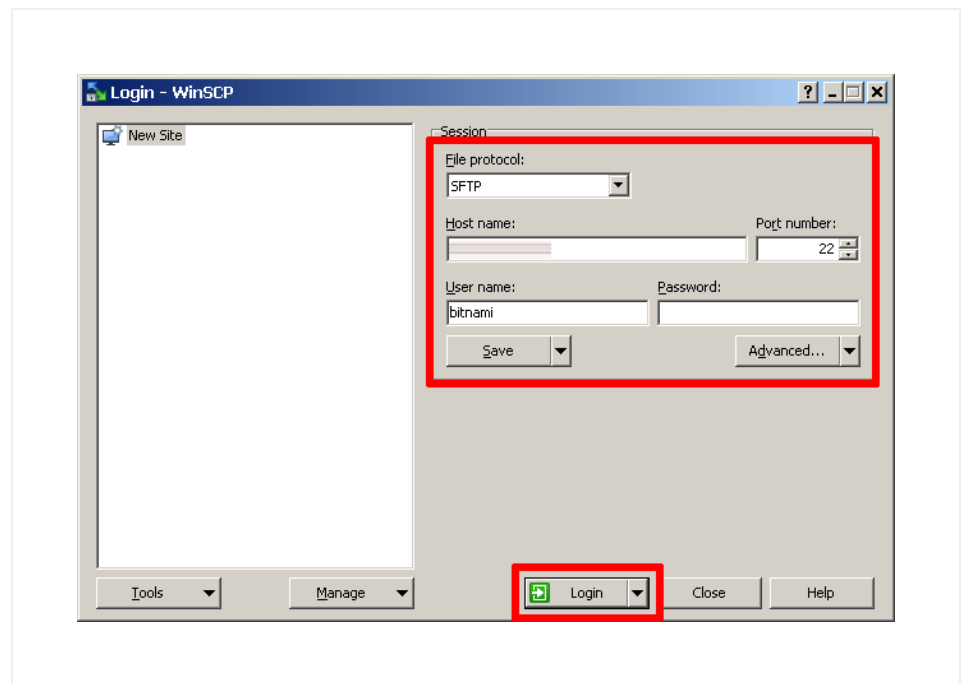


WinSCP

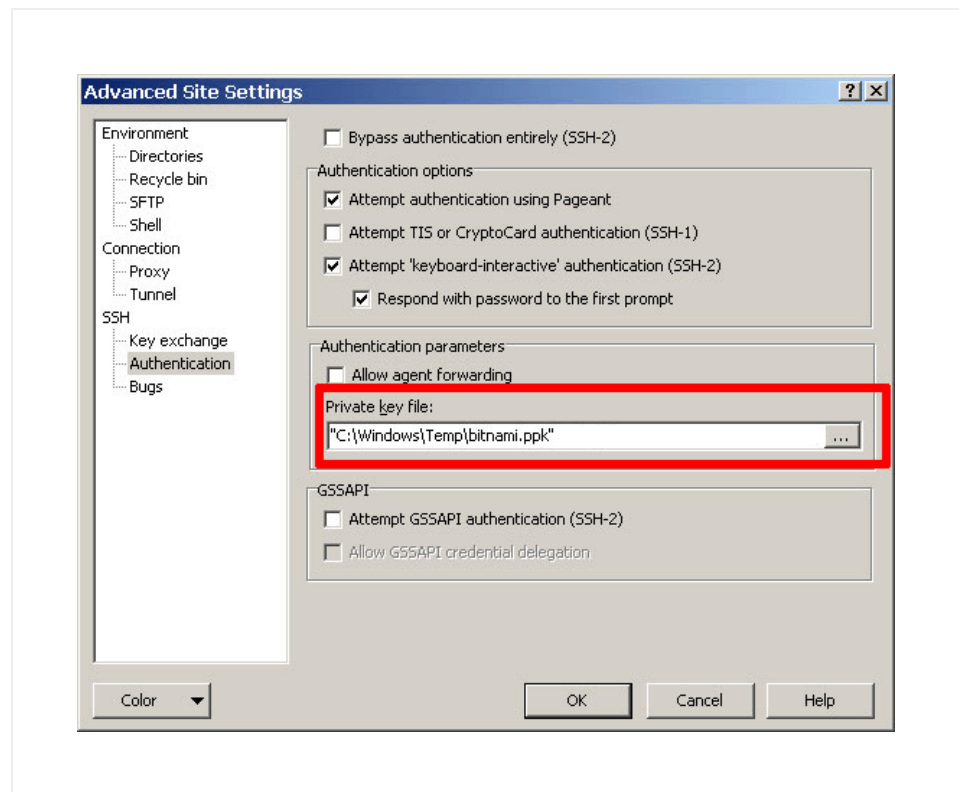
IMPORTANT: To use WinSCP, your server private key should be in PPK format.

Follow these steps:

- Download and install WinSCP.
- Launch WinSCP and in the "Session" panel, select "SFTP" as the file protocol.
- Enter your server host name and specify bitnami as the user name.



- Click the "Advanced..." button and within the "SSH -> Authentication -> Authentication parameters" section, select the private key file for the server. WinSCP will use this private key to log in to the server.

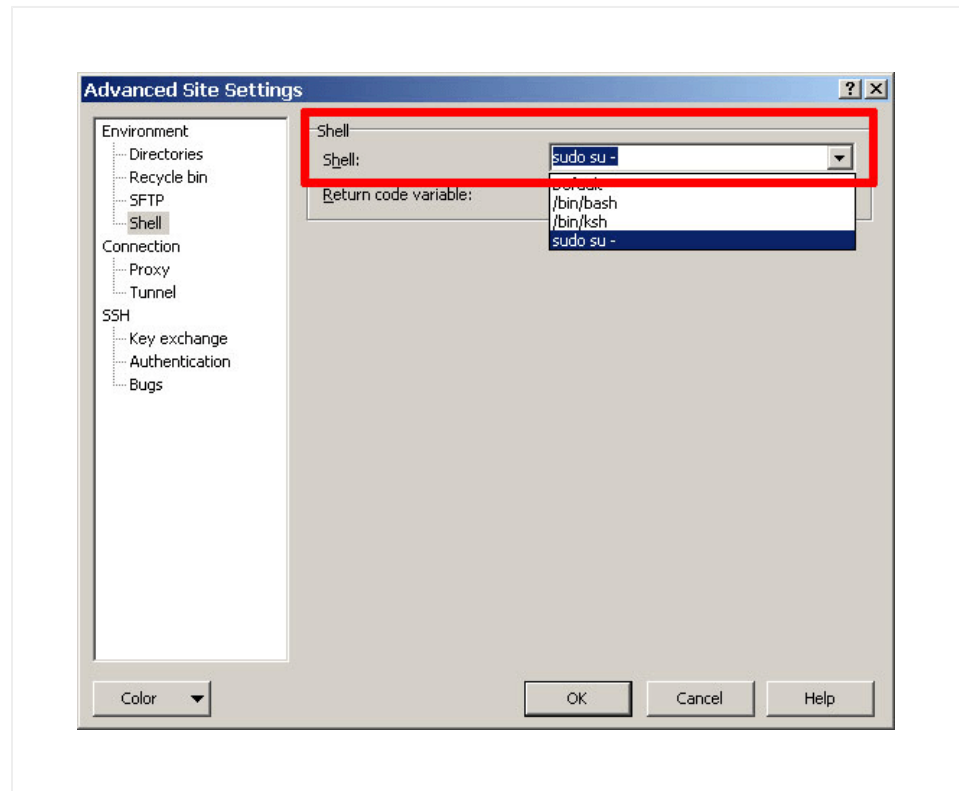


- From the "Session" panel, use the "Login" button to connect to the server and begin an SCP session.

You should now be logged into the /home/bitnami directory on the server. You can now transfer files by dragging and dropping them from the local server window to the remote server window.

If you need to upload files to a location where the bitnami user doesn't have write permissions, you have two options:

- Once you have configured WinSCP as described above, click the "Advanced..." button and within the "Environment -> Shell" panel, select `sudo su -` as your shell. This will allow you to upload files using the administrator account.



- Upload the files to the /home/bitnami directory as usual. Then, connect via SSH and move the files to the desired location with the sudo command, as shown below:

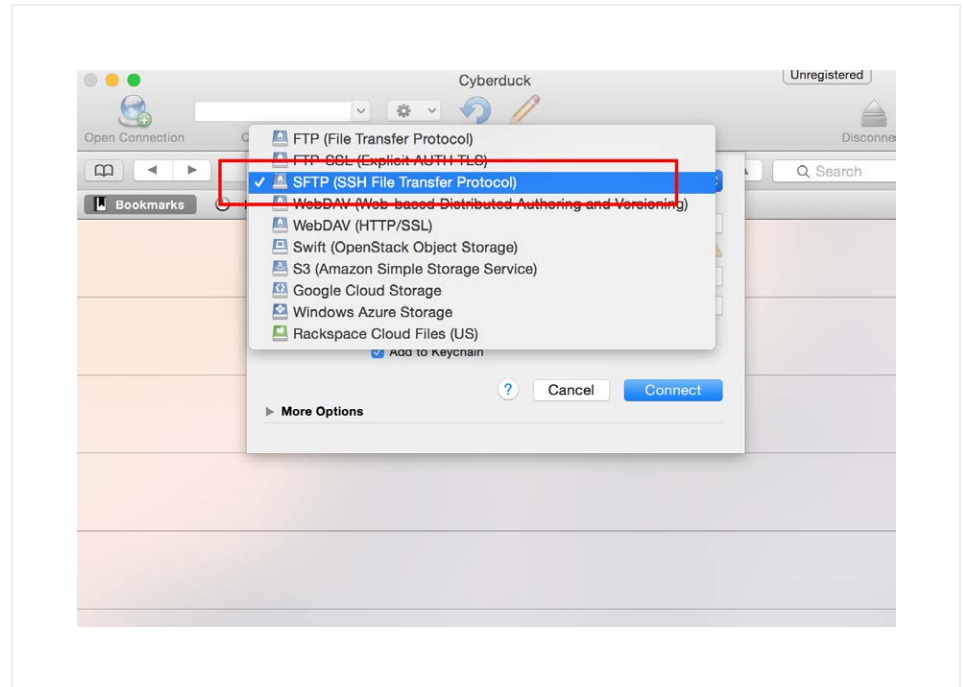
```
$ sudo mv /home/bitnami/uploaded-file /path/to/desired/location/
```

Cyberduck

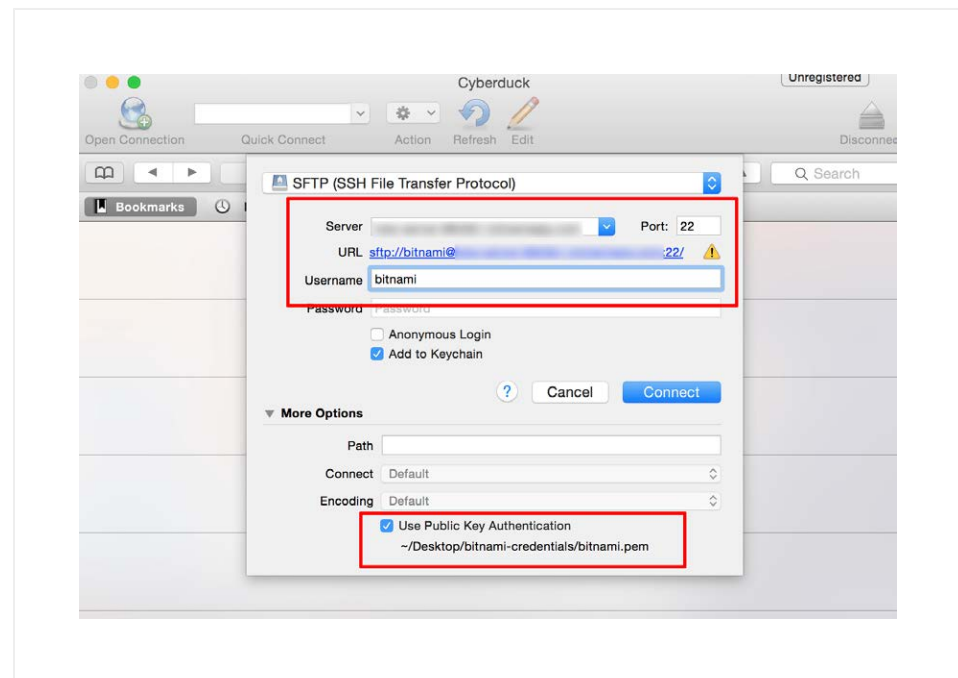
IMPORTANT: To use Cyberduck, your server private key should be in PEM format.

Follow these steps:

- Select the "Open Connection" command and specify "SFTP" as the connection protocol.



- In the connection details panel, under the "More Options" section, enable the "Use Public Key Authentication" option and specify the path to the private key file for the server.



- Use the "Connect" button to connect to the server and begin an SFTP session.

You should now be logged into the /home/bitnami directory on the server. You can now transfer files by dragging and dropping them from the local server window to the remote server window.

How To Connect Instances Hosted In Separate Virtual Networks Or VPCs?

The Google Cloud Platform makes it possible to connect instances hosted in separate Virtual Private Clouds (VPCs), even if those instances belong to different projects or are hosted in different regions. This feature, known as VPC Network Peering, can result in better security (as services do not need to be exposed on public IP addresses) and performance (due to use of private,

rather than public, networks and IP addresses).

[Learn more about VPC Network Peering.](#)

How To Block A Suspicious IP Address?

NOTE: The steps below should be performed on all instances that receive inbound Internet traffic.

If you have detected an IP address that is collapsing your server or just making suspicious requests, block it using iptables. To do this, run the following command:

```
$ sudo su
$ iptables -A INPUT -s 1.2.3.4 -j DROP
```

Remember to replace 1.2.3.4 with the IP address you want to block.

IMPORTANT: Use with caution. If you don't specify an IP address, you will block yourself.

This will block all requests from that IP address. To have your iptables rules active even after rebooting the server, follow these steps:

- Execute these commands:

```
$ sudo su
$ iptables-save > /opt/bitnami/iptables-rules
$ crontab -e
```

- Edit the above file with your favourite editor and include this line at the end of the file:

```
@reboot /sbin/iptables-restore < /opt/bitnami/iptables
-rules
```

- Save the file and exit.

Now, on every boot, the system will load and apply the iptables rules.

To delete a rule, run the following command:

```
$ sudo su
$ iptables -D INPUT -s 1.2.3.4 -j DROP
```

This will delete the rule. Remember to replace 1.2.3.4 with a valid IP address.

Rerun the iptables-save command shown previously to make the new rules active even after rebooting the server.

How To Configure A Custom Domain?

To use a custom domain with a server started through the Bitnami Launchpad, follow these steps:

Configure A Static IP Address For Your Cloud Server

[Follow these instructions.](#)

Configure The Domain In Your DNS Provider

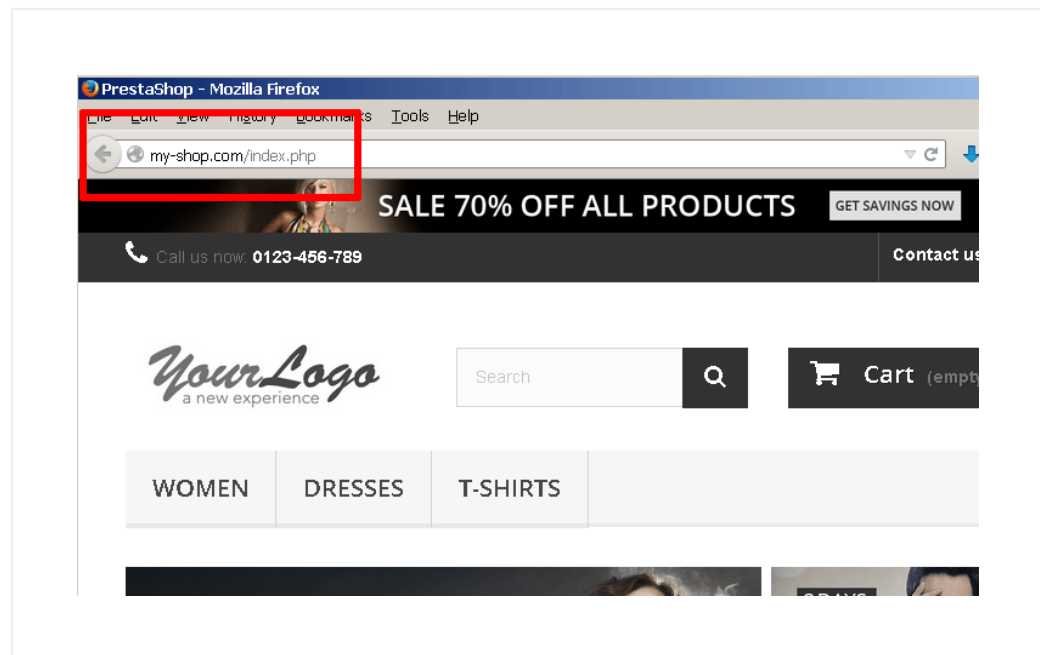
The next step is to update your domain's DNS settings, specifically by adding an A record that points to the static IP address of your cloud server.

This change can only be accomplished through your domain name provider; it cannot be made through the Bitnami Launchpad. You will therefore need to log in to your domain name provider's management console and make the necessary changes. Step-by-step instructions for some popular providers are listed below:

- [EasyDNS](#)
- [DNS Made Easy](#)
- [GoDaddy](#)
- [Namecheap](#)

Remember that once you make the necessary changes, it can take up to 48 hours for the change to propagate across other DNS servers. You can verify the new DNS record by using the [Global DNS Propagation Checker](#) and entering your domain name into the search field.

At the end of this step, entering your custom domain name into the browser address bar should take you to your Bitnami application on the cloud server, as shown below:



Update Application Configuration

For some applications, such as Prestashop, it is also necessary to perform additional configuration so that the application "knows" its domain and the domain name is correctly reflected in application URLs. This is easily accomplished with the command-line Bitnami Configuration tool, `bnconfig`, which will update the application configuration and database to use the new domain wherever needed.

To use this tool, follow these steps:

- Log in to your server console ([instructions](#)).
- Change to your application directory, usually located under `/opt/bitnami/apps/APP-NAME`.
- Execute the following command:

```
$ sudo ./bnconfig --machine_hostname DOMAIN-NAME
```

For example, to configure Prestashop to use the domain my-shop.com, use the commands below:

```
$ cd /opt/bitnami/apps/prestashop
$ sudo ./bnconfig --machine_hostname my-shop.com
```

Or, to configure your WordPress Multisite blog to use the primary domain my-blog.com, use the commands below:

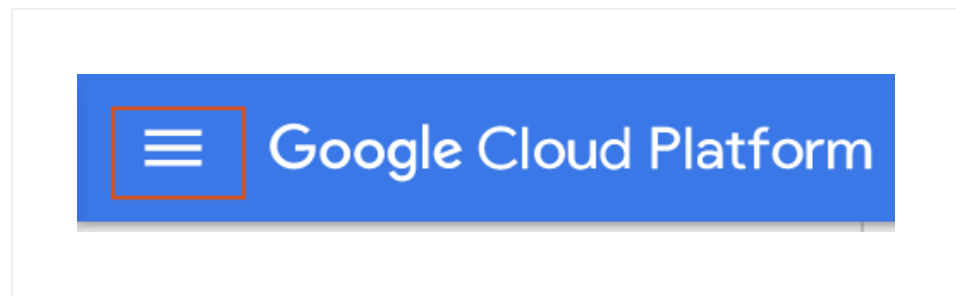
```
$ cd /opt/bitnami/apps/wordpress
$ sudo ./bnconfig --machine_hostname my-blog.com
```

How To Backup A Server?

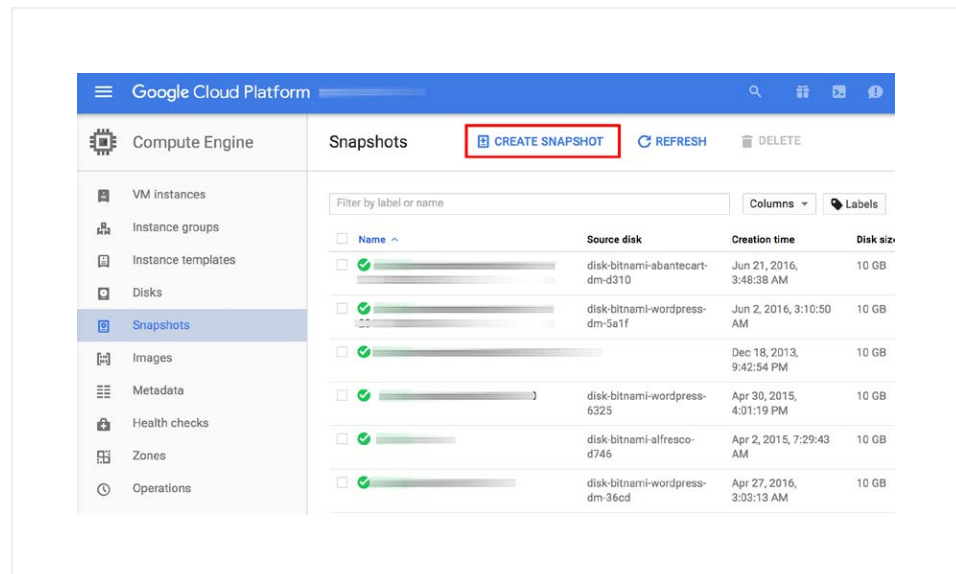
IMPORTANT: We strongly recommend creating a backup of your server prior to any major changes or upgrades.

To create a backup, you will use Google Cloud Platform's snapshot feature. This feature creates a new snapshot of the disk, which can later be used to restore the server to an earlier state. Follow the steps below:

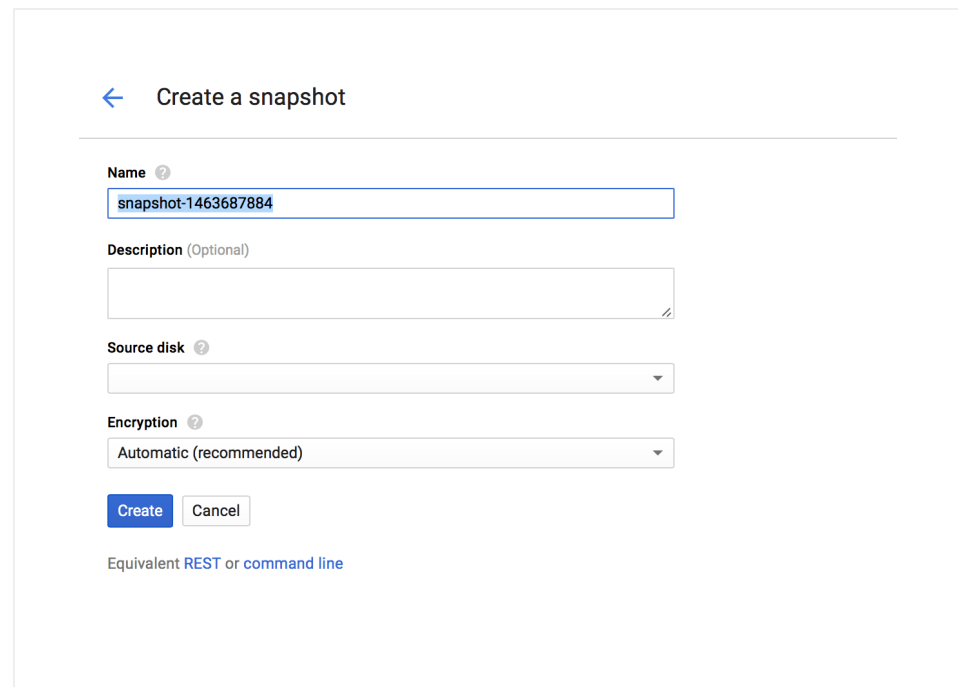
- Log in to the [Google Cloud Console](#) using the Google Account associated with your project.
- Select your project from the list of available projects.
- Click the "Hamburger" button on the left side of the top navigation bar:



- Navigate to the "Compute -> Compute Engine -> Snapshots" sub-menu.
- Select the "Create snapshot" button.



- Create a new snapshot of your instance disk by entering a name and description and then pressing the "Create" button



The screenshot shows the 'Create a snapshot' interface in Google Cloud Platform. At the top, there is a back arrow and the title 'Create a snapshot'. Below this is a form with the following fields:

- Name**: A text input field containing 'snapshot-1463687884'.
- Description (Optional)**: A text input field.
- Source disk**: A dropdown menu.
- Encryption**: A dropdown menu with 'Automatic (recommended)' selected.

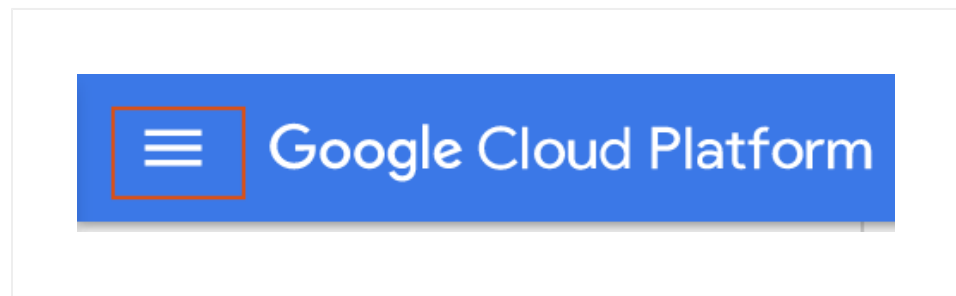
At the bottom of the form are two buttons: 'Create' (in blue) and 'Cancel' (in grey). Below the buttons, there is a link: 'Equivalent [REST](#) or [command line](#)'.

Your new snapshot will be created and will appear in the list of snapshots.

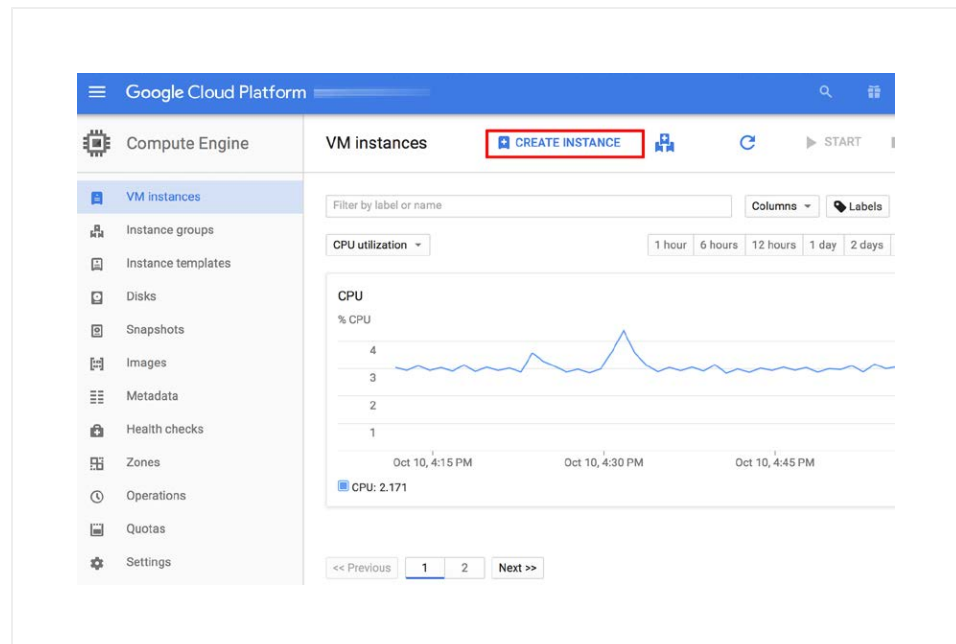
How To Restore A Backup Of A Server?

You can restore a server by initializing a new server from the corresponding snapshot. Follow these steps:

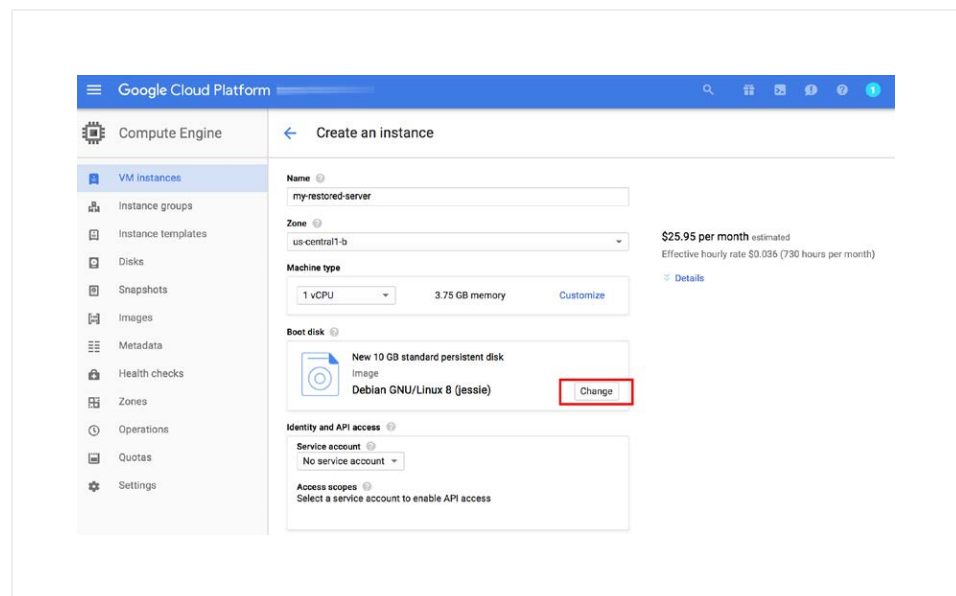
- Log in to the [Google Cloud Console](#) using the Google Account associated with your project.
- Select your project from the list of available projects.
- Click the "Hamburger" button on the left side of the top navigation bar:



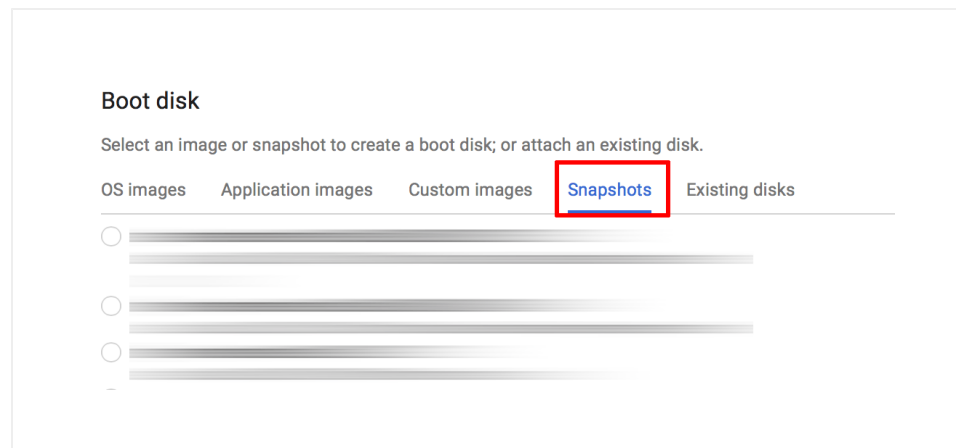
- Navigate to the "Compute -> Compute Engine -> VM Instances" sub-menu.
- Click the "Create instance" button.



- Configure the new instance by entering a name, selecting the instance type and allowing HTTP and HTTPS connections.
- In the "Boot disk" tab, click the "Change..." button.



- In the resulting dialog, select the "Snapshots" tab and select the snapshot you wish to restore. Click the "Select" button once done.



- Click the "Create" button to create a new server instance from the snapshot.

Your new server will now be created from the snapshot.

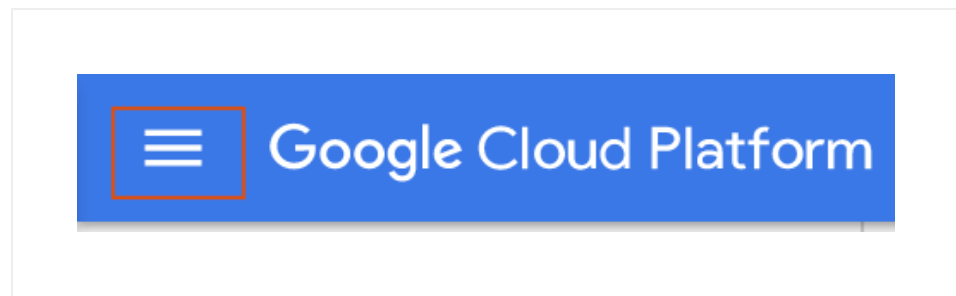
How To Change The Server Type Or Resize The Server?

The Bitnami Launchpad for Google Cloud Platform only supports server re-sizing during the server build. Since the server is accessible via the Google Compute Engine console, you can get a resized version of the server from there afterwards if needed.

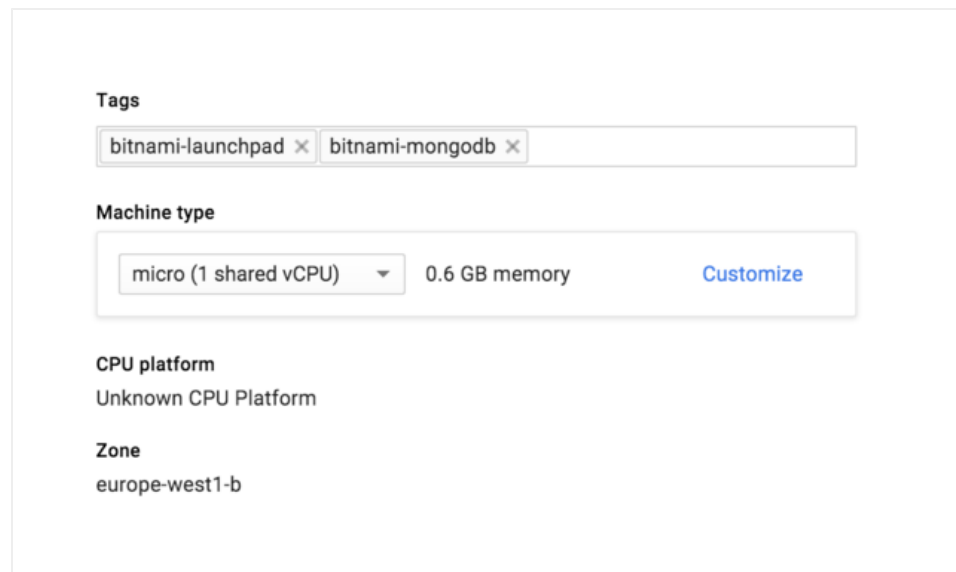
The procedure consists of creating a new server using the same disk as the server to be resized, and then deleting the old one following the steps below.

NOTE: For servers launched through the [Bitnami Launchpad for Google Cloud Platform](#), select the cloud server you wish to modify in the Bitnami Launchpad and click the "Manage in the Google Console" button to access the Google management console.

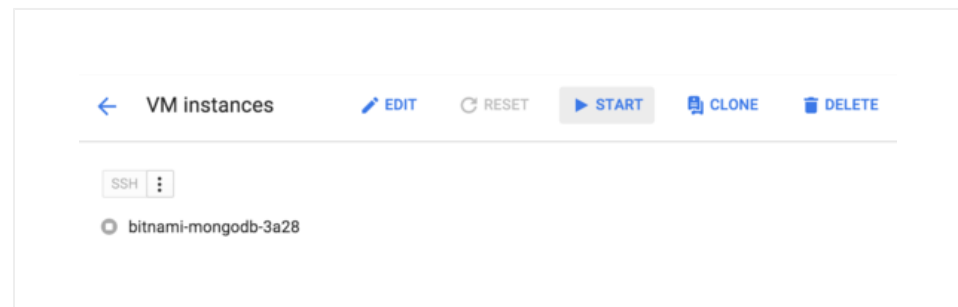
- Log in to the [Google Cloud Console](#) using the Google Account associated with your project.
- Select your project from the list of available projects.
- Click the "Hamburger" button on the left side of the top navigation bar:



- Select the "Compute -> Compute Engine -> VM Instances" menu item.
- Select the instance you wish to resize.
- Stop the instance by clicking the "Stop" button.
- Once stopped, click the "Edit" button.
- Change the instance type and click the "Save" button at the bottom of the page.



- Click the "Start" button and wait for the instance to start again.



The server should restart using the new type.

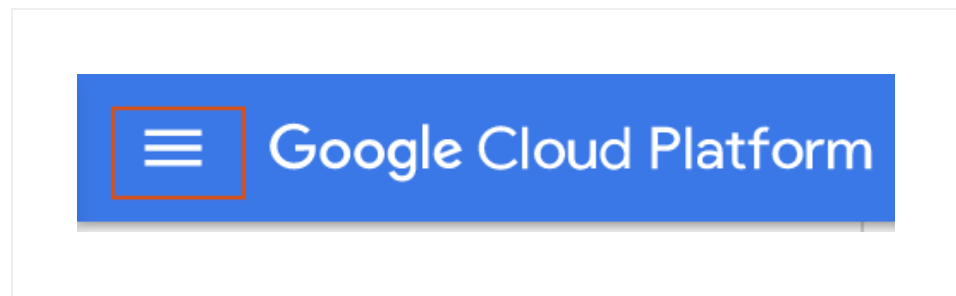
How To Configure A Static IP Address?

Google Cloud Platform instances are launched with a dynamic IP address by default, which means that the IP address changes every time the server is stopped and restarted. In many cases, this is not desired and so, users also have the option to assign the server a static IP address.

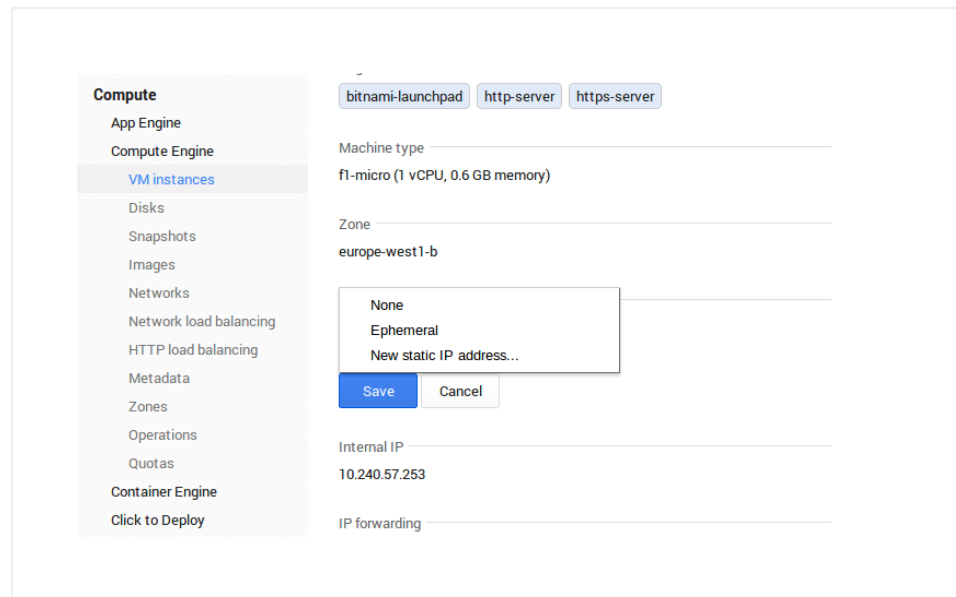
NOTE: For servers launched through the [Bitnami Launchpad for Google Cloud Platform](#), select the cloud server you wish to modify in the Bitnami Launchpad and click the "Manage in the Google Console" button to access the Google management console.

To configure a static IP address:

- Log in to the [Google Cloud Console](#) using the Google Account associated with your project.
- Select your project from the list of available projects.
- Click the "Hamburger" button on the left side of the top navigation bar:



- Select the "Compute -> Compute Engine -> VM Instances" menu item.
- The resulting page displays a list of VM instances. Select the instance which you wish to configure.
- In the "External IP" section, select "New static IP address"



- Save your changes.

What Is The Bitnami Vault?

The Bitnami Vault is a secure password storage area associated with your Bitnami account. It stores all your Launchpad passwords (needed to deploy or manage servers from the various Bitnami Launchpads).

To use it, log in to your Bitnami account once. Once logged in, you can gain access to one or more Launchpads simply by providing the corresponding Bitnami Vault password as needed.

How To Configure Your Application To Use A Third-Party SMTP Service For Outgoing Email?

Google Cloud Platform doesn't allow SMTP traffic through default ports: 25, 465, 587. Check [Google cloud documentation](#) to learn how to use a VPN to bypass these restrictions or use a different port for sending emails from your application.

Bitnami applications can be configured to use a third-party SMTP service for outgoing email. Examples of such third-party SMTP services are [SendGrid](#) and [Mandrill](#). Instructions for using both these are provided below.

SendGrid

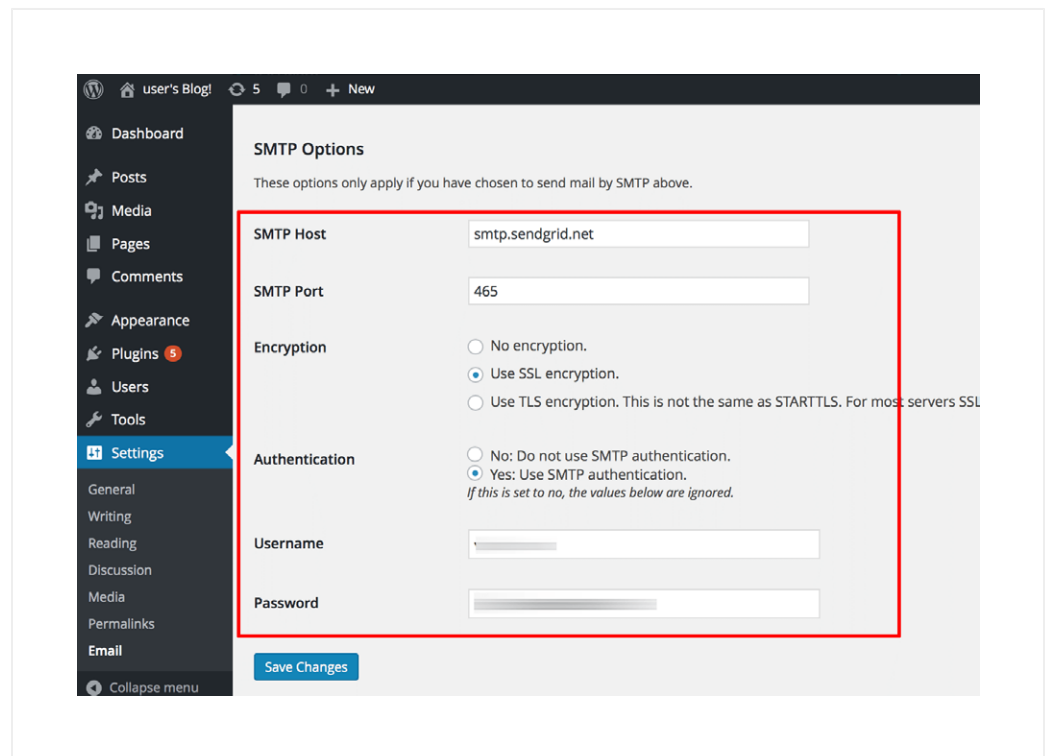
SendGrid's SMTP service can be accessed using your SendGrid account credentials. These credentials can be obtained by logging in to the SendGrid website and visiting the "Account Details" page.

The screenshot shows a 'Account Details' form. It has five input fields: 'NAME', 'EMAIL ADDRESS', 'PHONE NUMBER' (with the value '123456789'), 'USERNAME', and 'PASSWORD'. The 'USERNAME' and 'PASSWORD' fields are highlighted with a red rectangle. To the right of the 'NAME' and 'EMAIL ADDRESS' fields is a button labeled 'Change Contact Info'. To the right of the 'USERNAME' and 'PASSWORD' fields is a button labeled 'Change Username and Password'.

To configure your application to send email through SendGrid's SMTP service, use the settings below. Replace USERNAME with your SendGrid account username and PASSWORD with your SendGrid account password.

- SMTP host: smtp.sendgrid.net
- SMTP port: 2525
- SMTP username: USERNAME
- SMTP password: PASSWORD

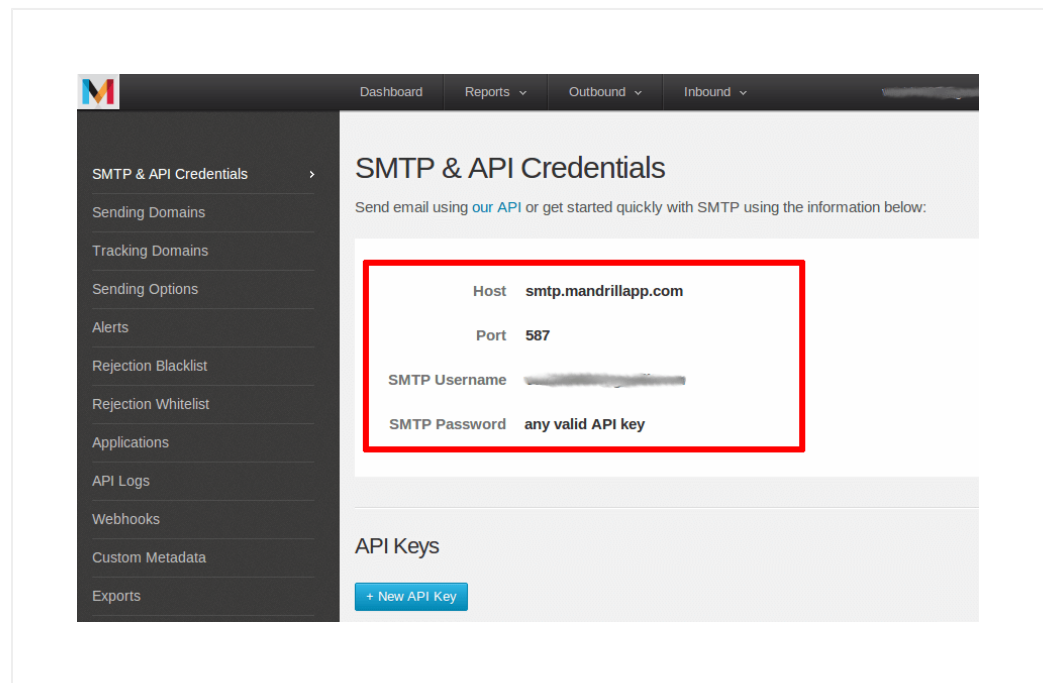
Here's an example of configuring WordPress to use SendGrid:



More information is available in [the SendGrid documentation](#).

Mandrill

Mandrill's SMTP service requires an API key for access. To obtain this key, log in to the Mandrill website, navigate to the "SMTP & API" section and create an API key. Note the SMTP server name, username and API key, as these serve as your credentials for accessing the Mandrill SMTP server.



To configure your application to send email through Mandrill's SMTP service, use the settings below. Replace USERNAME with your SMTP username and API-KEY with the generated API key.

- SMTP host: smtp.mandrillapp.com
- SMTP port: 2525
- SMTP username: USERNAME
- SMTP password: API-KEY

Here's an example of configuring WordPress to use Mandrill:

user's Blog! 5 0 + New

SMTP Options

These options only apply if you have chosen to send mail by SMTP above.

SMTP Host

SMTP Port

Encryption

- ☐ No encryption.
- ☒ Use SSL encryption.
- ☐ Use TLS encryption. This is not the same as STARTTLS. For most s recommended option.

Authentication

- ☐ No: Do not use SMTP authentication.
- ☒ Yes: Use SMTP authentication.
If this is set to no, the values below are ignored.

Username

Password

[Save Changes](#)

More information is available in [the Mandrill documentation](#).

Similar steps can be followed for other third-party SMTP services as well. Consult your service provider's documentation to obtain details on authentication credentials and available ports.

Does Bitnami Collect Any Data From Deployed Bitnami Stacks?

Yes. Bitnami cloud images and virtual machines include a small agent that starts on boot and collects a few pieces of information about the system. For users of Bitnami Virtual Machine Images, Cloud Templates, and Container Images we may also collect information from downloaded, pulled or deployed images or instances, such as the instance type, IP address and operating system version or the Bitnami account used to launch the image in order to improve our product offerings.

We encourage you to leave this tracking on, but if you would like to turn it off, you can comment out or delete the following line in the `/etc/crontab` file:

```
X * * * * bitnami cd /opt/bitnami/stats && ./agent.bin --run  
-D
```

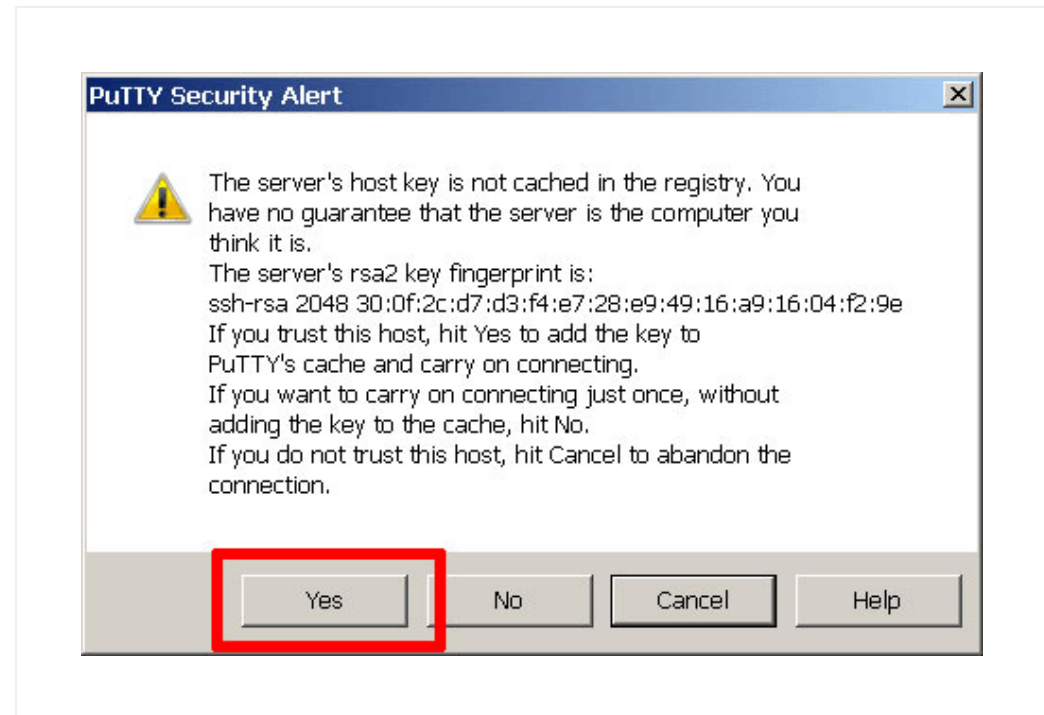
(where X is a random number for each instance generated at the boot time)

Our complete [privacy policy](#) is available online. If you have any questions, please feel free to contact us at hello@bitnami.com.

What Does The SSH Warning 'REMOTE HOST IDENTIFICATION HAS CHANGED' Mean?

This warning is normal when trying to connect to the same IP address but a different machine - for instance, when you assign the same static IP address to another server. You can fix the problem by removing the IP address that you are trying to connect to from your `~/.ssh/known_hosts` file.

If you use PuTTY, the SSH key mismatch warning looks like the image below:



In this case, click "Yes" if you know the reason for the key mismatch (IP address reassigned to another server, machine replaced, and so on).

How To Troubleshoot Server Performance Problems?

There are several possible reasons why your server might be under-performing. Use the list below to identify what could be affecting it.

- Check the server type and ensure that it has the necessary CPU and RAM resources to meet your application requirements and user load.
- Check if your application is using a cache. Consider enabling a cache if

one is not already present. For applications like WordPress, caching plugins like W3 Total Cache can produce a significant improvement in performance.

- Check if there are any cron jobs running on the server and consuming resources.
- Review the server dashboard or monitoring page and check the list of processes consuming CPU and memory. Alternatively, log in to the machine console via SSH and execute the following command to see a list of running processes:

```
$ ps -e -orss=,args= | sort -b -k1,1n | pr -TW$COLUMNS
$ ps -e -o pcpu,nice,state,cputime,args --sort -pcpu |
head -10
```

- In case of problems with the disk size, check the free disk space and which directories have a large number of files:

```
$ df -ih
$ df -h
$ cd /opt/bitnami
$ sudo find . -type f | cut -d "/" -f 2 | sort | uniq -
c | sort -n
$ du -h -d 1
```

- Try performing a complete reboot of the server.
- Check if your server is being accessed by suspicious IP addresses and block them if so. [Refer to the FAQ for detailed instructions.](#)

How To Improve Server Performance?

Consider the following tips to improve the performance of your server.

- Enable [the Apache PageSpeed module](#) or [the Varnish web application accelerator](#) if not already enabled.
- Consider [installing the APCu, XCache, memcached or eAccelerator modules](#) to cache and optimize your PHP applications.
- [Use the myslqtuner script](#) to check and optimize your MySQL or MariaDB database server configuration.
- If you are experiencing bot attacks that are affecting your server, use the Apache configuration file to [filter out and deny requests by specified IP address](#).

What Are The Bitnami Cloud Tools?

[Bitnami Cloud Tools](#) are a multi platform, self-contained and easy-to-use prepackaged software that allows you to manage and monitor your cloud deployments.

By downloading it, you will obtain a wide range of command line utilities and a pre-configured version of the major programming languages such as Python or Perl. These tools are really useful for those developers that want to use, in a more advanced way, the Cloud APIs offered by different cloud providers.

Select your cloud platform and download from the [Bitnami official web page](#) the package that corresponds to your operating system.

Bitnami Documentation

FAQs

How to find application credentials?

How to connect to the server through SSH?

How to upload files to the server with SFTP?

How to open the server ports for remote access?

How to configure your application to use a third-party SMTP service for outgoing email?

How to block a suspicious IP address?

Platform Documentation

Google Cloud Platform

AWS Cloud

Oracle Cloud Platform

Microsoft Azure

Bitnami Cloud Hosting

CenturyLink Cloud

1&1 Cloud Platform

Huawei Cloud

Open Telekom Cloud

Windows / Linux / MacOS

Virtual Machines

Containers

Kubernetes

General Documentation

[Bitnami Application Stacks](#)
[Bitnami Infrastructure Stacks](#)
[How-To Guides](#)
[Bitnami Components](#)
[Security Notices](#)

© Bitnami 2017



Apps

[Applications](#)
[Add-ons](#)
[Vote!](#)

What we do

[Cloud Hosting](#)
[Pricing](#)
[Enterprise](#)
[Cloud Partners](#)
[Software Partners](#)
[Customers](#)
[FAQs](#)

Who we are

[About](#)
[Contact](#)
[Careers](#)
[What's New?](#)

[Press](#)

[Blog](#)

[Legal](#)

Support

[Documentation](#)

[Forums](#)

[Helpdesk](#)

[Webinars](#)