

Download and set up PuTTY to connect using SSH in Amazon Lightsail

Last updated: August 16, 2018

You can use an SSH client like PuTTY to connect to your Lightsail instance. PuTTY requires a copy of your private SSH key. You might already have a key, or you might want to use the key pair that Lightsail creates. Either way, we've got you covered. For more information about SSH, see [SSH and connecting to your Lightsail instance](#).

This topic walks you through the steps to download a key pair and set up PuTTY to connect to your instance. You can also connect to your instance from within the Lightsail console without installing or configuring any software. For more information about connecting to your instance using the Lightsail console, see [Connecting to your Linux or Unix instance in Amazon Lightsail](#).

Prerequisites

- You need a running instance in Lightsail. For more information, see [Create an instance in Amazon Lightsail](#).
- We recommend that you create a static IP address and attach it to your instance so you won't have to reconfigure PuTTY if your public IP address changes later. For more information, see [Create a static IP and attach it to an instance in Amazon Lightsail](#).

Step 1: Download and install PuTTY

PuTTY is a free implementation of SSH for Windows. You can learn all about PuTTY on [this page](#), including restrictions related to countries where encryption isn't allowed. If you already have PuTTY, you can skip to **Step 2**.

1. Download the PuTTY installer or executable file from the following link: [Download PuTTY](#).

If you need help deciding which download to choose, see the [PuTTY documentation](#). We recommend using the latest version.

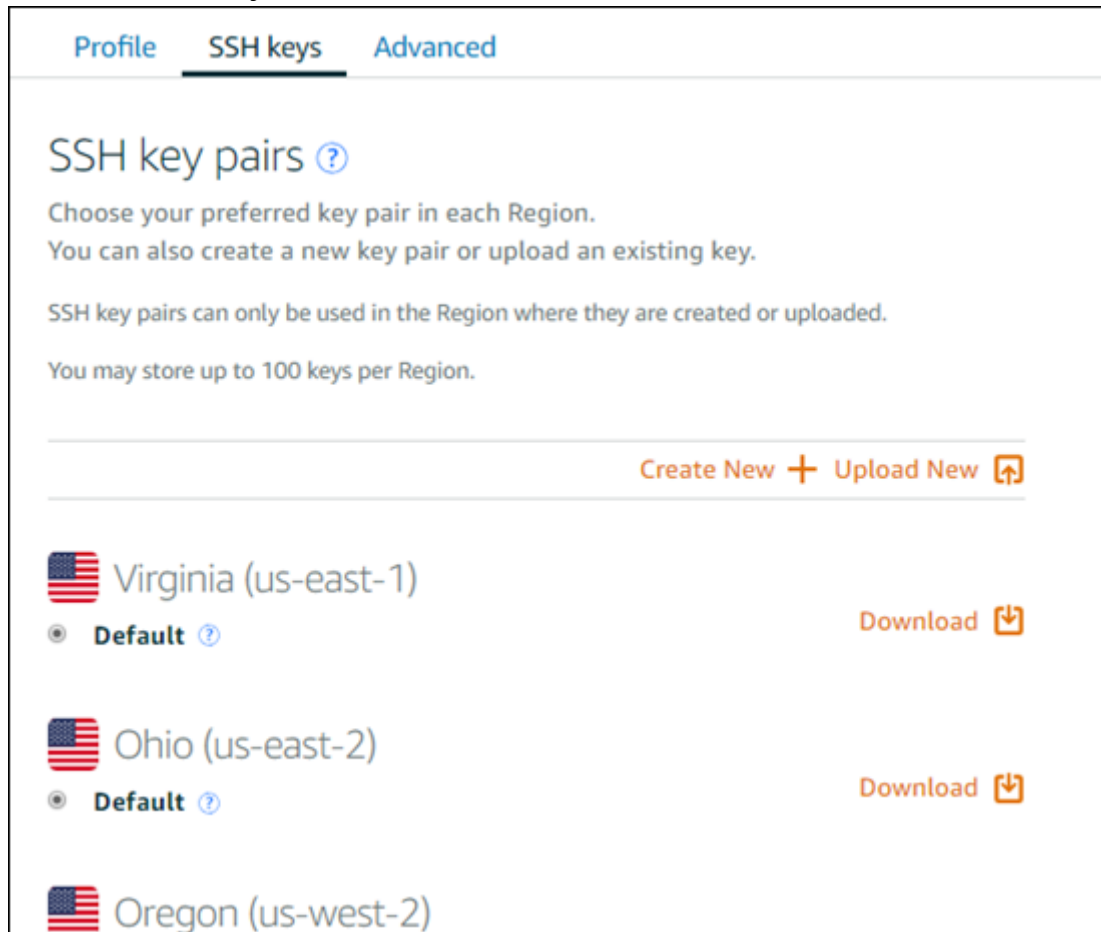
2. Go on to **Step 2** to get your private key before you configure PuTTY.

Step 2: Get your private key ready

You have several options for getting your private key. You might want to use the default private key that Lightsail generates, you might want to have Lightsail create a new private key for you, or you might already have one from another service. The steps for each of these options is outlined in the following procedures:

1. Sign in to the [Lightsail console](#).
2. Choose **Account** on the top navigation bar, and then choose **Account** from the drop-down.

3. Choose the **SSH Keys** tab.



4. Choose one of the following options depending on which private key you prefer to use:

- **To use the default private key that Lightsail generates**, choose **Download** next to the default private key for the AWS Region where your instance is located.
- **To create a new key pair in Lightsail**, choose **Create New**. Choose the AWS Region where your instance is located, and choose **Create**. Enter a name, and choose **Generate key pair**. You will be given the option to download the private key. **Important**
You can only download the private key once. Save it in a secured location.
- **To use your own key pair**, choose **Upload New**. Choose the AWS Region where your instance is located, and choose **Upload**. Choose **Upload file**, and then locate the file in your local drive. Choose **Upload key** when you're ready to upload your public key file to Lightsail.

5. If you downloaded the private key, or you created a new private key in Lightsail, then make sure to save the **.pem** key file somewhere you can easily find it.

We also recommend that you set permissions for the file so that no one else can read it.

Step 3: Configure PuTTYgen with your Lightsail private key

Now that you have a copy of your **.pem** key file, you can set up PuTTY using the PuTTY Key Generator (PuTTYgen).

1. Start PuTTYgen (for example, from the **Start** menu, choose **All Programs, PuTTY, PuTTYgen**).
2. Choose **Load**.

By default, PuTTYgen displays only files with the **.ppk** extension. To locate your **.pem** file, select the option to display files of all types.

3. Choose **lightsailDefaultKey.pem**, and then press **Open**.

PuTTYgen confirms that you successfully imported the key, and then you can choose **OK**.

4. Choose **Save private key**, and then confirm you don't want to save it with a passphrase.

If you choose to create a passphrase as an extra measure of security, remember you will need to enter it every time you connect to your instance using PuTTY.

5. Specify a name and a location to save your private key, and then choose **Save**.

6. Close PuTTYgen.

Step 4: Finish configuring PuTTY with your private key and instance information

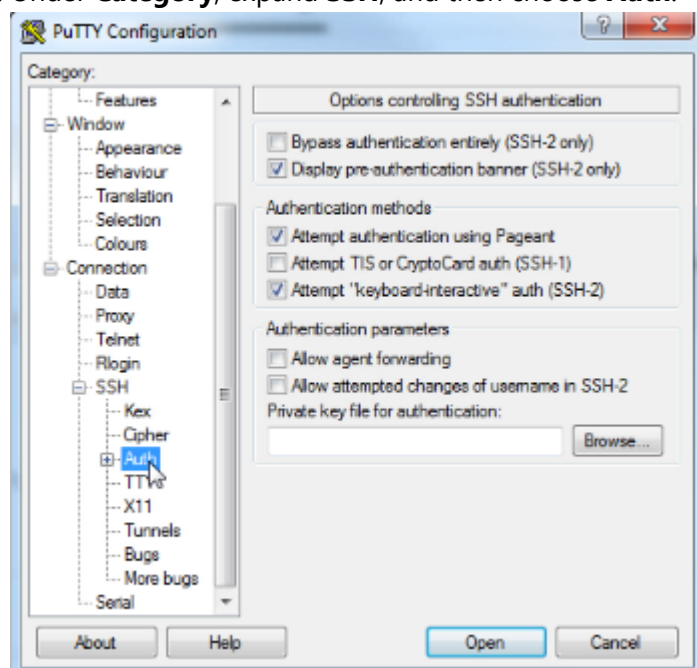
You're almost there! Hang on while we make one last change.

1. Open PuTTY.
2. From Lightsail, grab the public IP address (hopefully you're using a [static IP address](#)) from the instance management page.

You can get the public IP address from the Lightsail home page, or choose your instance to view more details about it.

3. Type (or paste) the public IP address into the **Host Name (or IP address)** field. **Note** Port 22 is already open for SSH on your Lightsail instance, so accept the default port.

4. Under **Category**, expand **SSH**, and then choose **Auth**.



5. Choose **Browse** to navigate to the **.ppk** file that you created in the previous step, and then choose **Open**.

6. Choose **Open** again, and then choose **Yes** to trust this connection in the future.
7. Log in using one of the following default user names depending on your instance operating system:
 - Amazon Linux, openSUSE, and FreeBSD: `ec2-user`
 - Debian: `admin`
 - Ubuntu: `ubuntu`
 - Powered by Bitnami instances: `bitnami`
 - Plesk instances: `ubuntu`

For more information about instance operating systems, see [Choosing an image in Lightsail](#).

8. Be sure to save your connection for future use.

Next steps

If you need to connect again, see [Connect to your Lightsail instance using PuTTY](#).