Using the non-default key with Windows-based Lightsail instances

Last updated: October 16, 2017

When you create a Windows Server-based Lightsail instance, we use the default password for the AWS Region where we create the instance. This makes it easier to connect using the browser-based remote desktop (RDP) client, as well as a client such as Remote Desktop Connection.

Important
We strongly encourage you to let Lightsail generate the password for your instance. Since we don't store your custom password, you can risk losing access to your Lightsail instance if you change the Administrator password.

Changing your Administrator password using Windows Server

You can change your Administrator password using the Windows Server **Change Password** tool. Type `Ctrl` + `Alt` + `Del` on your Windows Server-based Lightsail instance, and then choose **Change a password**.

Decrypt your key

If you change your password on your Windows Server-based Lightsail instance, you can use the AWS Command Line Interface (AWS CLI) to get information that helps you decrypt your password.

Get your ciphertext using the AWS CLI

1. If you haven't done so already, install and configure the AWS CLI.

   For more information, see Configuring the AWS Command Line Interface to work with Amazon Lightsail.

2. Open a command prompt or a terminal.

3. Type the following command.

   ```
   aws lightsail get-instance-access-details --instance-name my-instance
   ```

   Where *my-instance* is the name of the instance you want to get information about.

   You'll see output similar to the following.

   ```
   {
       "accessDetails": {
           "username": "Administrator",
           "protocol": "rdp",
           "ipAddress": "12.345.678.910",
           "passwordData": {
   ```

```
            "ciphertext": "cipher",
            "keyPairName": "my-ohio-key"
        },
        "password": "",
        "instanceName": "2016-ohio-windows"
    }
}
```

4. You can use the ciphertext with any available application to decrypt your password.