Centers for Medicare & Medicaid Services

# EDGE Server Job Aid
# Amazon EDGE Server Provisioning

**Version 2.0**
**10/30/2014**

**Step 4**

# Contents


**1. Introduction ..... 1**

**2. Pre-Requisites to Provisioning ..... 1**

**3. Amazon EDGE Server Provisioning ..... 1**

**3.1.** Provisioning Successful ..... 2
**3.2.** Manage EDGE Server ..... 4
**3.3.** Provisioning Failed ..... 7

**4. Confirming Successful Amazon EDGE Server Provisioning and Connect to the Server 9**

**4.1.** Download PuTTY ..... 9
**4.2.** Puttygen.exe ..... 10
**4.3.** Putty.exe ..... 12
**4.4.** Connect to EDGE Instance and confirm functionality ..... 18
**4.5.** Enable Termination Protection ..... 19
**4.6.** Reminder: Stop Server Instance ..... 21

# 1. Introduction

This document provides an overview of the steps issuers must follow in order to successfully provision an Amazon External Data Gathering Environment (EDGE) server, confirm successful provisioning, and connect to their server instance. It will also provide guidance on what to do in the event that provisioning fails.

The figures captured in this job aid are from Firefox web browser. Images displayed will vary depending on the web browser that is used.

The following process map provides an overview of the order of steps you need to complete in order to provision your Amazon EDGE server. The blue step reflect the current step you're executing, the grey steps reflect the subsequent steps that you need to execute thereafter. Each step below has corresponding training materials (job aids and video demos as applicable) available in the Registration for Technical Assistance Portal (REGTAP) Library; you can follow the link to access. Please make sure to reference all the available materials and confirm that you have completed all of these steps for each phase before moving onto the next step.

**Amazon EDGE Server**




**For EDGE server support, please send all questions to the Centers for Medicare & Medicaid Services (CMS) Help Desk email:** CMS_FEPS@cms.hhs.gov or call 1-855-CMS-1515.

# 2. Pre-Requisites to Provisioning

Amazon EDGE issuers should have completed the steps listed in the **EDGE Server Registration Job Aid** before executing the steps found in this job aid. This job aid will walk issuers through the provisioning of their server once the request for the server has been approved by CMS.

# 3. Amazon EDGE Server Provisioning

Once an Amazon EDGE server request has been approved by CMS, the EDGE server is automatically provisioned in the Amazon Web Services (AWS) cloud using the details provided by the issuer or Third Party Administrator (TPA) during registration. The provisioning process

itself is triggered by CMS approving the registration request through the EDGE Registration Site and requires no further action from the issuer. Once provisioning is completed, the request status is updated in the registration site and the user is able to log in to AWS and begin processing files.

The below steps will provide issuers an overview of the Amazon EDGE server request status updates that designate that provisioning has occurred and is successful.

## 3.1. Provisioning Successful

Once an EDGE server request has been approved by CMS, the request will return to the Issuer Submitter's inbox) with a status of **Pending Provisioning.** This indicates the request is ready for provisioning.

1. From the homepage, the Issuer Submitter will see the request in their inbox with a status of **Pending Provisioning.**
2. The Issuer Approver and TPA Requester can also track the provisioning status of approved EDGE server requests on the Search Requests page.

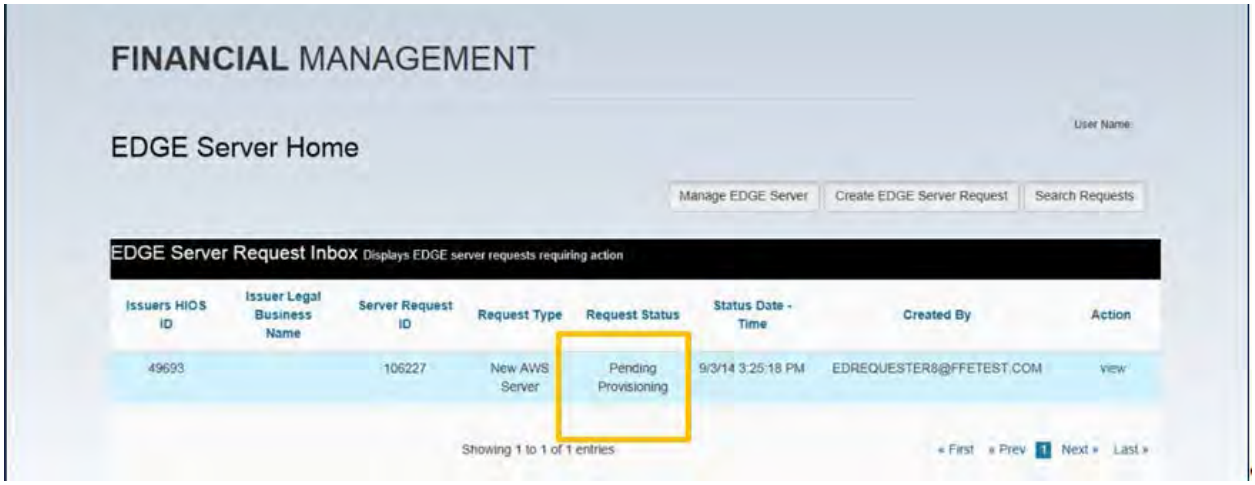



**Figure 1 – Pending Provisioning**

3. The information provided during the registration request is then automatically passed as parameters to the EDGE provisioning script. The script is executed to create the EDGE server with no further action required. At this point, the request status will be updated to **Provisioning in Progress.** Once this occurs, the request will clear from the Issuer Submitter's inbox. The Issuer Submitter will need to search for the request at this point to see the status of Provisioning in Progress. First, click the **Search Requests** button at the top right.




**Figure 2 – Search Requests Button**

4. In the Search Requests screen, select **Issuer HIOS ID** from the **Search Field** dropdown menu and enter your Health Insurance Oversight System (HIOS) Issuer ID in the **Search Value** Field. When finished, click the **Search** button to display the results. Any active requests associated with your Issuer HIOS ID will display.

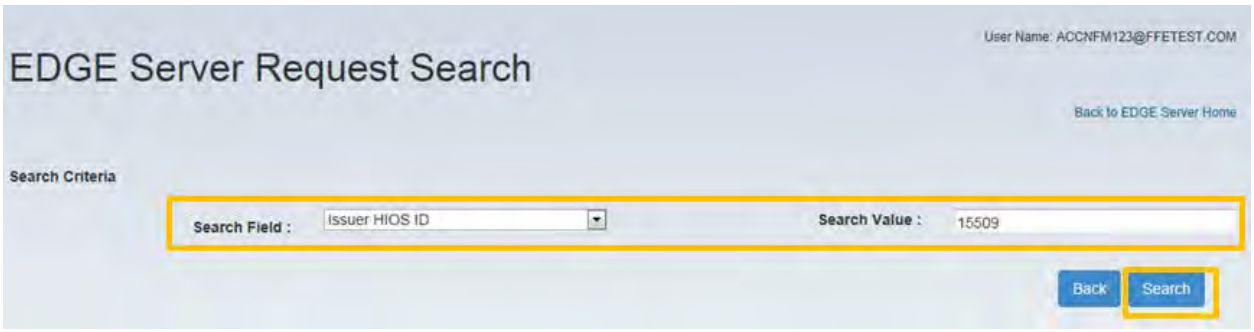



**Figure 3 – Search Request Screen**

5. The request will display with a status of **Provisioning in Progress**. At this point, you can refresh the page periodically to track the status as it updates. When provisioning has completed, it will update to **Provisioned.**

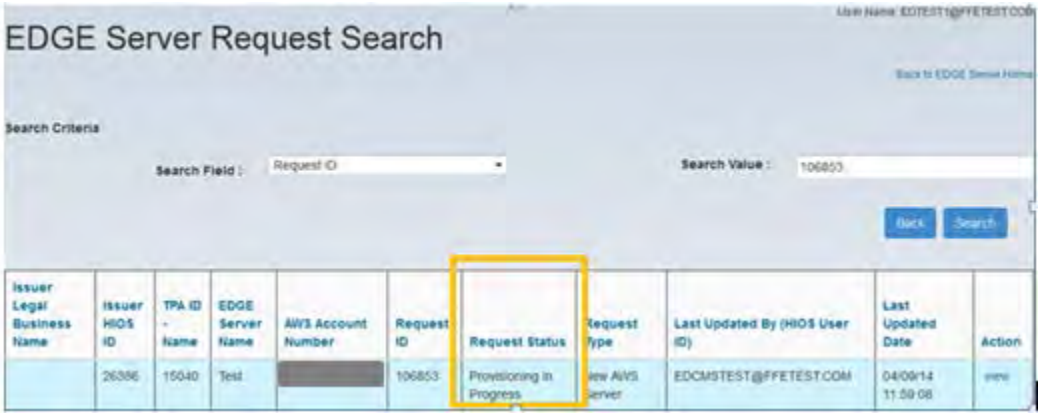



**Figure 4 – Provisioning in Progress**

6. Once the Amazon EDGE server has been successfully provisioned, the request status will be updated to **Provisioned.** This indicates that the Amazon EDGE server has connected with the Phone Home service for the first time.

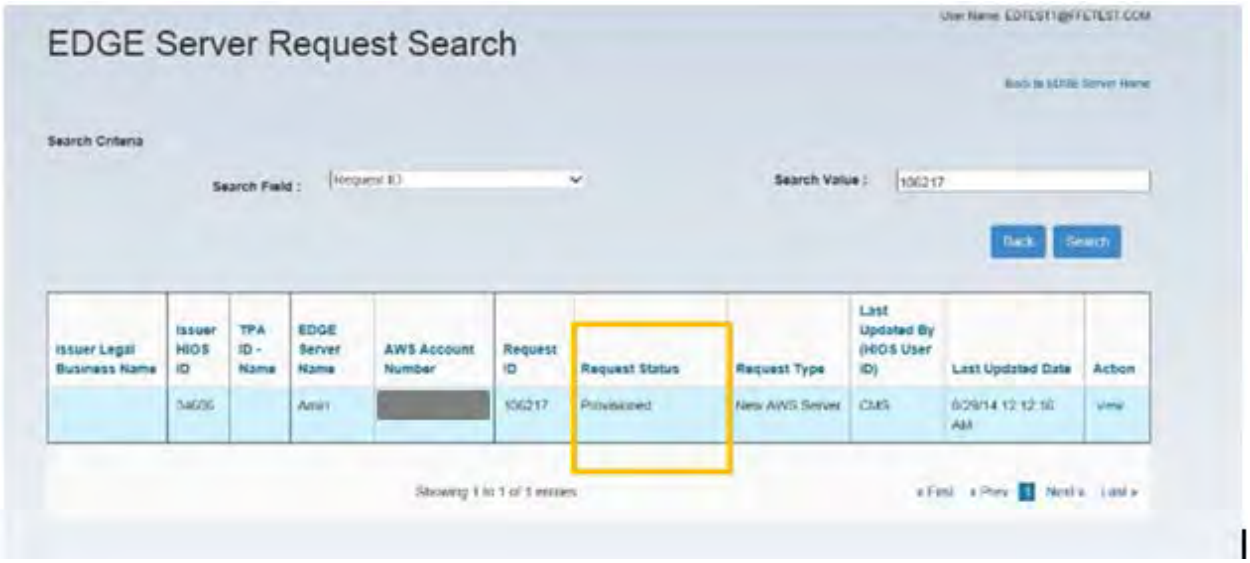



**Figure 5 – Server Provisioned Status**

**The process described above typically takes about 60 minutes to complete. Issuers will be able to access their AWS accounts and confirm successful provisioning by following the steps outlined in Section 4 below.**

## 3.2. Manage EDGE Server

Following successful provisioning, Issuer Submitters may need to update point of contact information (all requests) or update TPA information (TPA-hosted ONLY) on their EDGE server request. The following steps provide guidance on how Issuer Submitters can access their **Provisioned** server request and update information.

1. From the homepage, click the **Manage EDGE Server** button at the top right.




**Figure 6 – Manage EDGE Server Button**

On the Manage EDGE Server screen, the Provisioned request associated with your Issuer HIOS ID will display. To update information on this request, click the **View** button from the **Action** column on the right.




**Figure 7 – Manage EDGE Server Screen**

2. From the EDGE Request screen, you can update any POC or TPA-related information as applicable to your EDGE server.

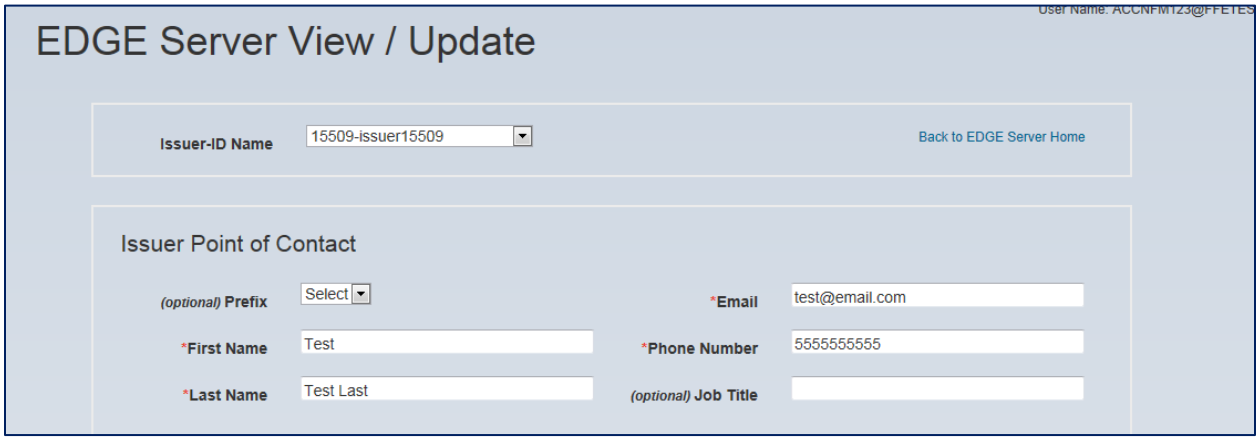



**Figure 8 – EDGE View/Update Screen**

3. When finished making updates, scroll to the bottom of the screen and click the **Submit** button.

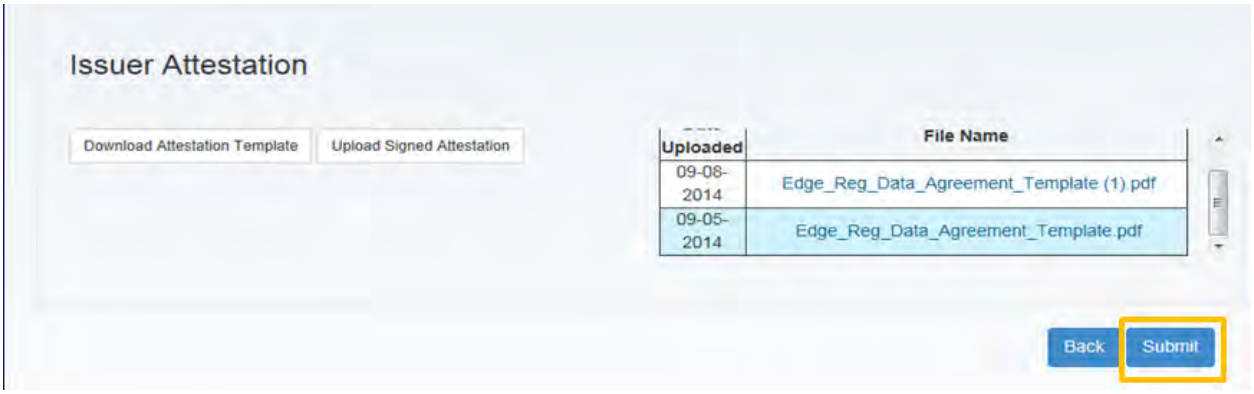



**Figure 9 – Submit Update**

4. Upon clicking **Submit,** a window will display asking you to **SUBMIT REQUEST** to save the updates and initiate the approval process or **CANCEL** to return to the previous page without saving. Click the **Submit Request** button.




**Figure 10 – Submit Request Button**

**NOTE:** Issuer Submitters will be taken back to their homepage after submitting the updates. The request will go back through the approval process. No further action is required by the Issuer.

The request will follow one of the following approval processes depending on the update made:

- POC Update ONLY: If only POC information was updated, the request will only require Issuer Approval (Org Approval).
- Migration/Host Change: If TPA information was updated or if the request was changed from self-hosted to TPA-hosted or vice-versa, the request will require both Issuer Approval and CMS Approval.

## 3.3. Provisioning Failed

The EDGE Registration Site monitors the completion of the AWS provisioning script. If the provisioning script does not complete successfully, this indicates that the AWS details provided by the issuer/TPA were incorrect. The status of the request will be updated to **Provisioning Failed** and the request will be sent back to the Issuer Submitter's inbox to update and re-submit.

A request that has failed provisioning will return to the Issuer Submitter's inbox. At this point, the Issuer Submitter will need to contact the **CMS Helpdesk** to determine the reason provisioning failed. The TPA Requester and Issuer Requester can also view the provisioning status by going to the Search Request page.

1. From the homepage, the Issuer Submitter will initially see the request in their inbox with a status of **Pending Provisioning.**

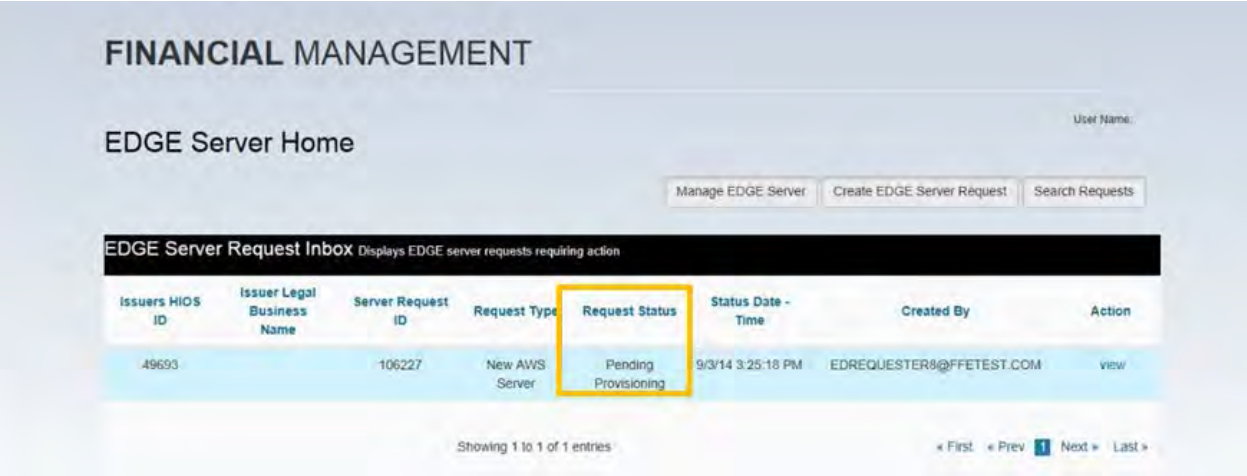



**Figure 11 – Pending Provisioning**

2. Once the request fails the provisioning process, the request status will update to **Provisioning Failed.** This will indicate that the provisioning process has stopped and was unsuccessful.




**Figure 12 – Provisioning Failed**

3. When provisioning has failed, the Issuer Submitter will need to contact the **CMS Helpdesk** to determine the cause of the failure. The CMS Helpdesk will provide more details on the cause of the failure and the resolution process.

**CMS Help Desk email:** CMS_FEPS@cms.hhs.gov
**CMS Help Desk phone:** 1-855-CMS-1515

4. Once the cause of the failure has been determined, the Issuer Submitter will need to update the request and re-submit the request. When the updated request is approved by CMS, the request will enter the provisioning process again and return to a status of **Pending Provisioning.**

# 4. Confirming Successful Amazon EDGE Server Provisioning and Connect to the Server

## 4.1. Download PuTTY

The first step for Issuers following successful provisioning is to download PuTTY in order to connect to their provisioned server. However, issuers may use their SSH Client of choice. PuTTY is a commonly used application for this purpose, and the steps for downloading and configuring PuTTY are described below. Issuers will need to adapt these instructions if they choose to use a different SSH client.

***For Help with PuTTY or PuTTY Gen, contact:*** CMS_FEPS@cms.hhs.gov

1. Issuers should first go to ***www.putty.org*.**

2. After going to the PuTTY home page, Issuers should click **you can download PuTTY here.**

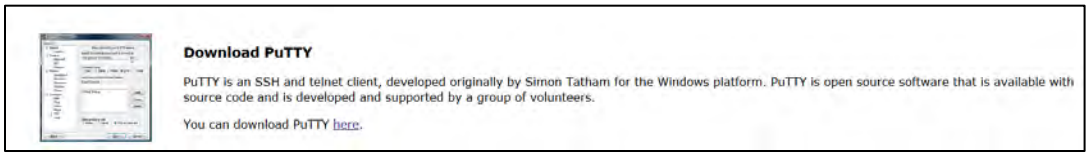



**Figure 13 – PuTTY Home Page**

3. The PuTTY download page will appear. Issuers should download both **putty.exe** and **puttygen.exe**.

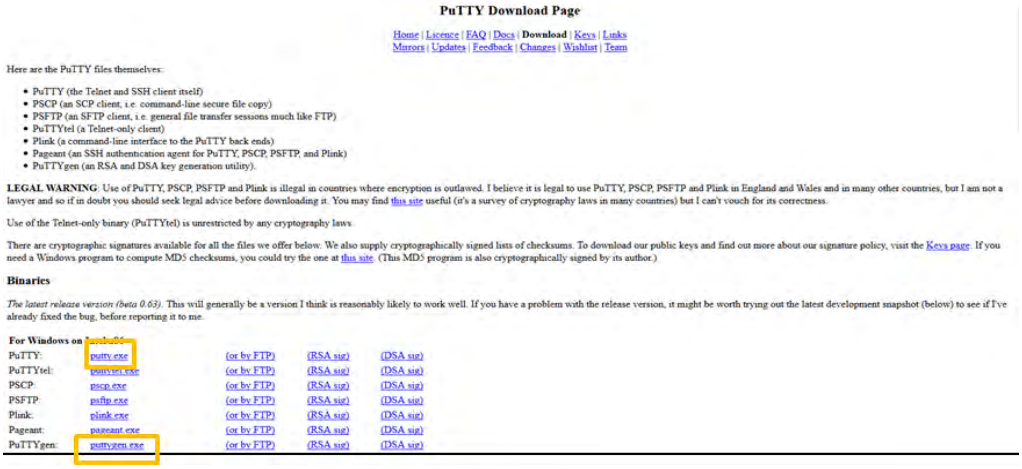



**Figure 14 – PuTTY Download Page**

## 4.2. Puttygen.exe

Issuers must first configure puttygen.exe.

1. Issuers should open and run the puttygen.exe file they downloaded.

2. After running puttygen.exe, the following window will appear. Issuers should click ***Load*** and then select the Key Pair file that was saved to their computer (.pem file). – saved in the **Request an AWS Instance Job Aid** (step 5)

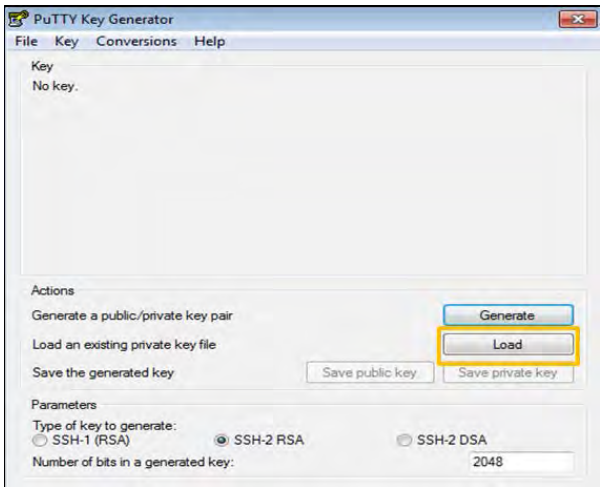



**Figure 15 – PuTTYgen Program Screen**

a. After loading the Key Pair file from your computer, the following pop-out window will display. Click **OK** to generate the file in .ppk format. This is the format you will need to utilize the Private key in later steps.

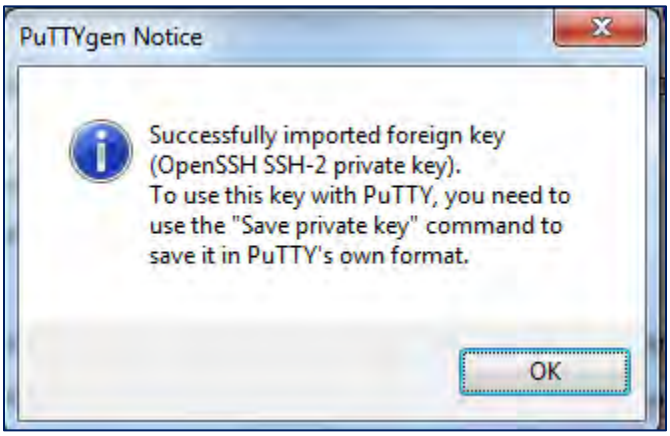



**Figure 16 – PuTTygen Notice**

3. After loading the Key Pair, in the next window, issuers will click **Save private key** button. In the **PuTTYgen Warning** window, click **Yes** to save the key without a passphrase. (You may save the key with a passphrase if desired).

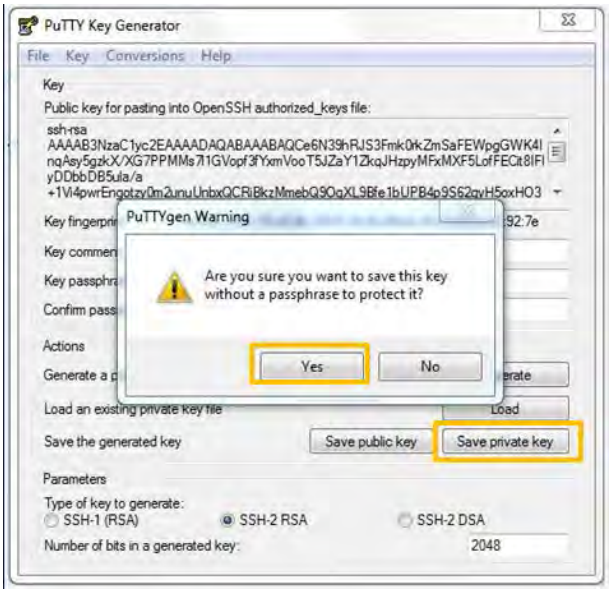



**Figure 17 – Save Private Key**

4. A window will display allowing you to save the Private Key to your local computer as a .ppk file. After saving, you can close the PuTTY Key Generate window.

**Important: Issuers should save the private key to a secure location and keep the key on their computer. You will need your Private Key for Step 10 later in this document as part of configuring PuTTY.exe.**

## 4.3. Putty.exe

The next step is to run and configure Putty.exe.

**NOTE:** Issuers will need to execute these steps again if their server is restarted for any reason. If this occurs, some of the information noted below (i.e., public IP address) will change and issuers will need to note the new information.

1. Issuers should first go to their AWS console, click **Services,** click **All AWS Services, and** then click **EC2.**

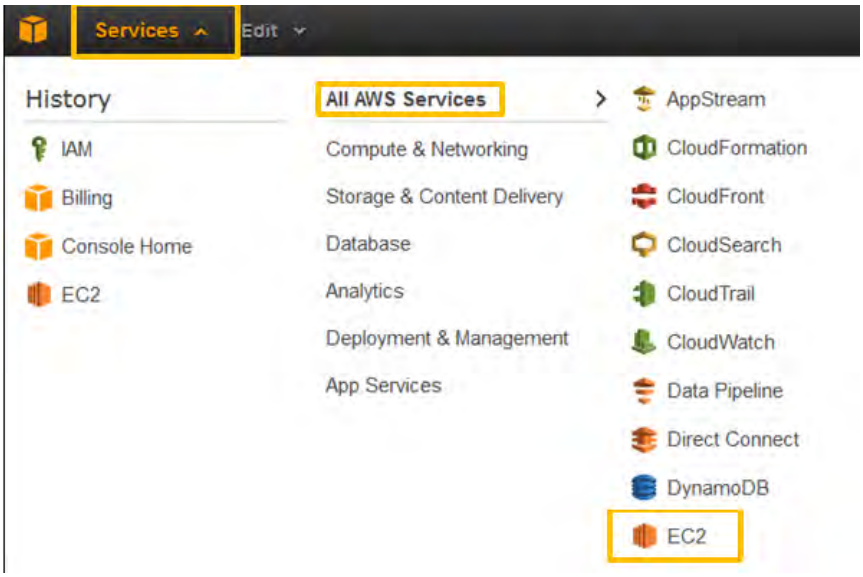



**Figure 18 - Services and All AWS Services Dropdowns**

*Issuers should click **Instances** on the upper left corner of the page.*

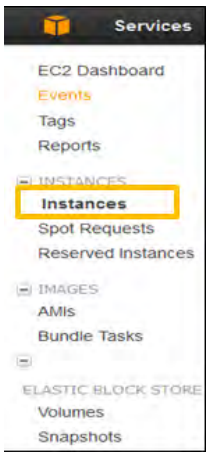



**Figure 19 – EC2 Options**

2. Issuers will find the available EDGE server instances listed in the menu. The correct server instance should have an **Instance State** set to **running.** Issuers can identify their correct server by finding their Issuer HIOS ID in the **Name** column on the right.

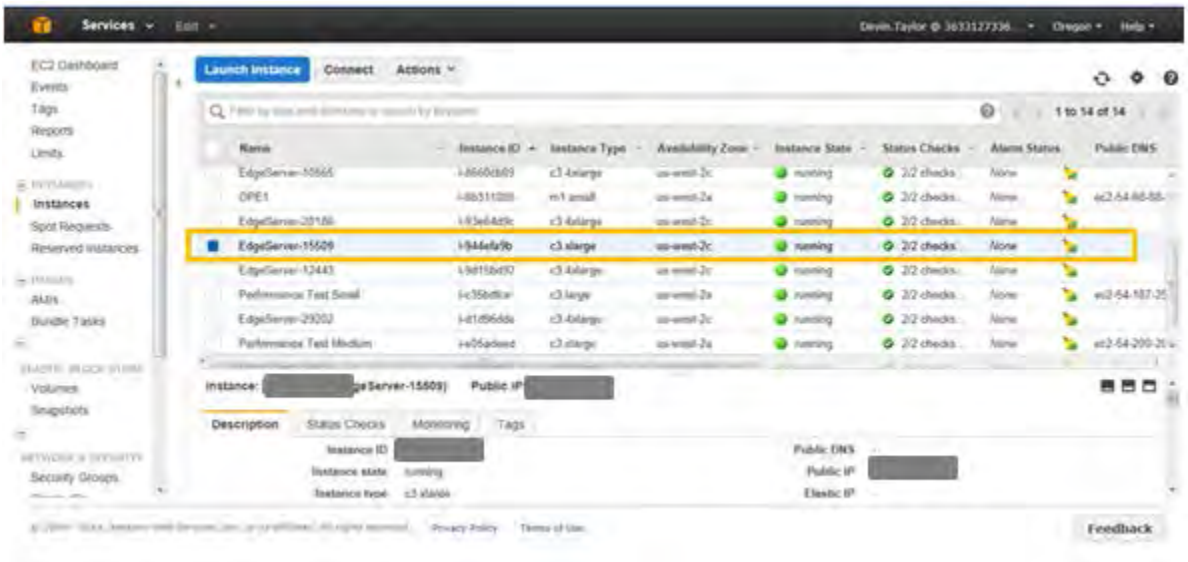



**Figure 20 – All Instances List**

3. After selecting the **EDGE Server Instance**, Issuers should find the public IP address in the bottom section of the page on the **Description tab.**

**NOTE:** Remember to save this IP address number. You will need this public IP address for configuring PuTTY in the steps below.

**IMPORTANT:** If the server ever crashes or is restarted for any reason, the public IP address will change to a new number. Issuers will need to remember to note this new IP address number when executing these steps again.




**Figure 21 - Public IP Address**

4. Issuers should now locate the PuTTY.exe file that they downloaded to their computer.

5. After running PuTTY.exe, Issuers will see the PuTTY configuration window.

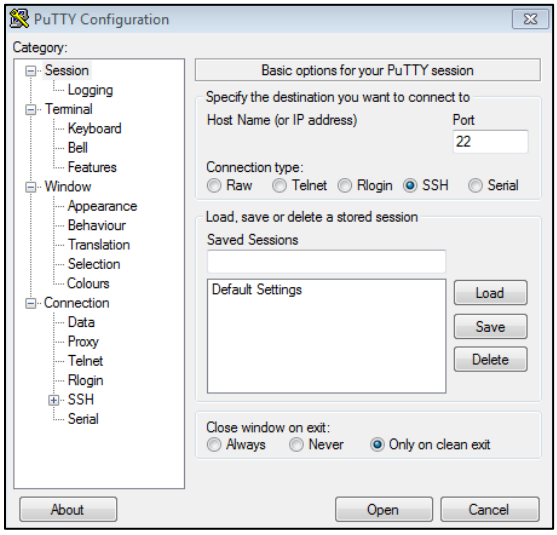



**Figure 22 – PuTTY Configuration Window**

6. Issuers should select the Connection type ***"SSH"*** and then enter ***"ec2-user@<IP address>"*** into ***"Host Name (or IP address)."(*****IP Address is found in Step4 of Section 4.3 above)**

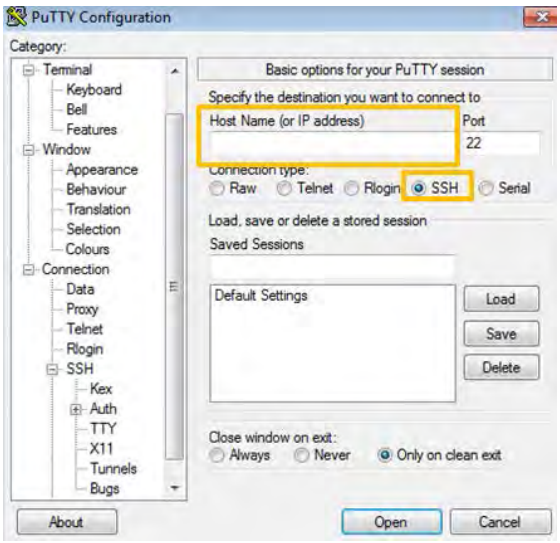



**Figure 23 - PuTTY Configuration – Add IP Address**

7. Issuers should now click the ***SSH dropdown*** from the Category list on the left side of the PuTTY Configuration window and should then select ***Auth.***

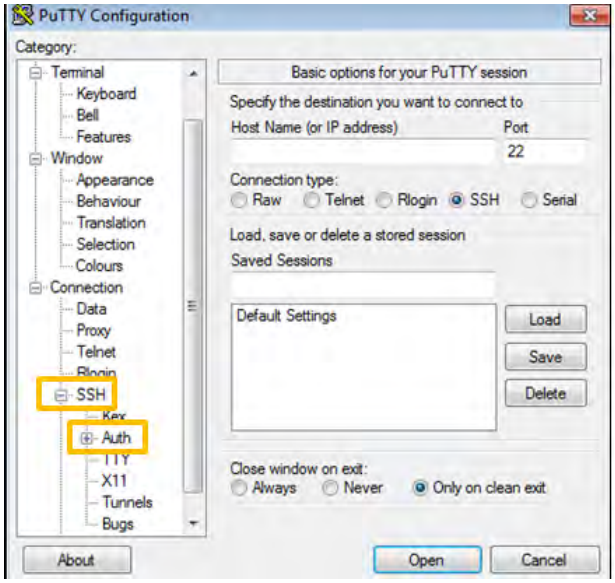



**Figure 24 - Category List on PuTTY Configuration Window**

8. Issuers should see Authentication Options and click ***Browse.***

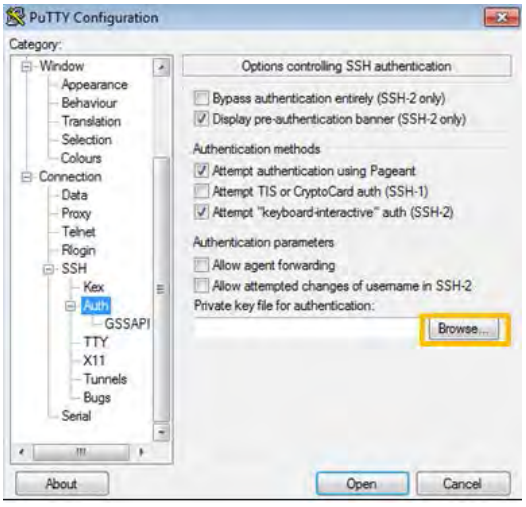



**Figure 25 - PuTTY Authentication Options**

9. Issuers should now find their PuTTY Private Key and click ***Open*****. The Private Key was created and saved in Step 3 of Section 4.2 above. This file should be in .ppk format.**

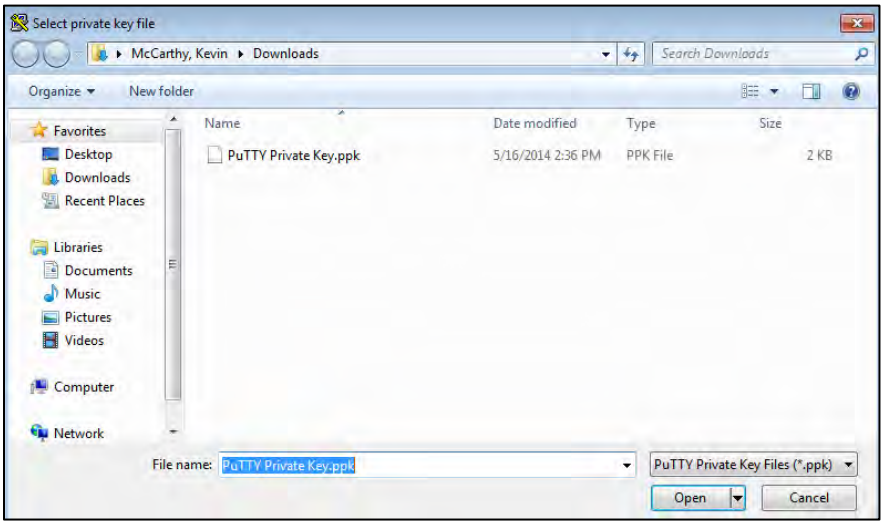



**Figure 26 – Browsing for PuTTY Private Key**

10. After loading the Private Key file, users should save their session prior to executing. When running PuTTY for the first time, a password reset is required that will close the program and require to execute the PuTTY configuration again. Saving the session will store the data you entered above. In the PuTTY configuration window, click the **Session** option at the top right. Make sure the Host Name filed is populated correctly with the name you entered. Enter a name for your session in the **Save Sessions** field and then click **Save.**

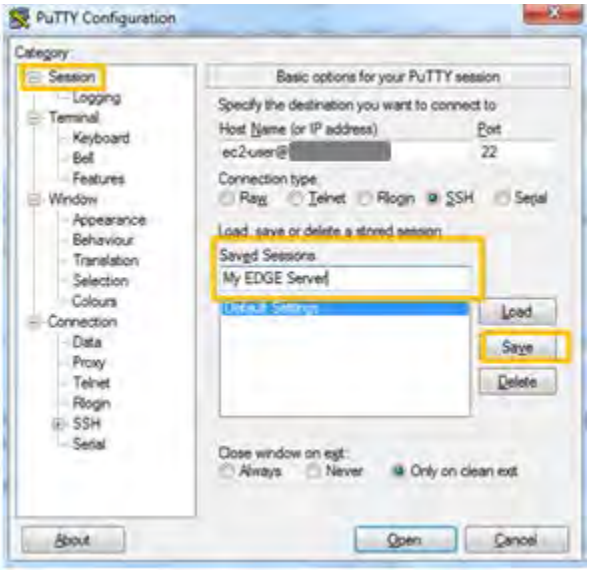



**Figure 27 - Save Session**

11. After saving, the session will appear in the list below. Issuers should now click **Open** in the PuTTY Configuration window to open the PuTTY program.

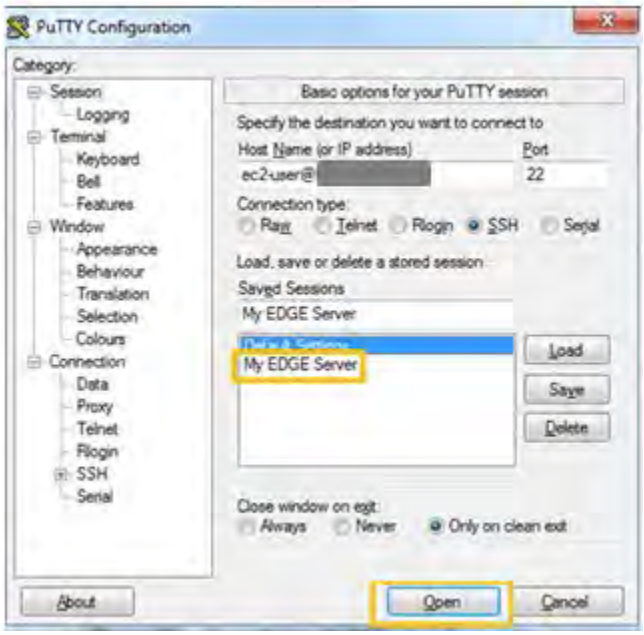



**Figure 28 - Completing PuTTY Configuration**

12. After clicking **Open**, the following security alert will appear verifying that you trust the host and that you want to add the key to PuTTY's cache and continue connecting. Click the **Yes** button to continue




**Figure 29 - PuTTY Security Alert**

## 4.4. Connect to EDGE Instance and confirm functionality

1. When logging into the server for the first time, you will need to enter the following password in the PuTTY window: **edgeserver (enter as one word with no spaces).** You will then need to enter a new password for your server for future logins. The cursor will not move when typing in password characters (passwords only). Remember to be precise when entering your password.

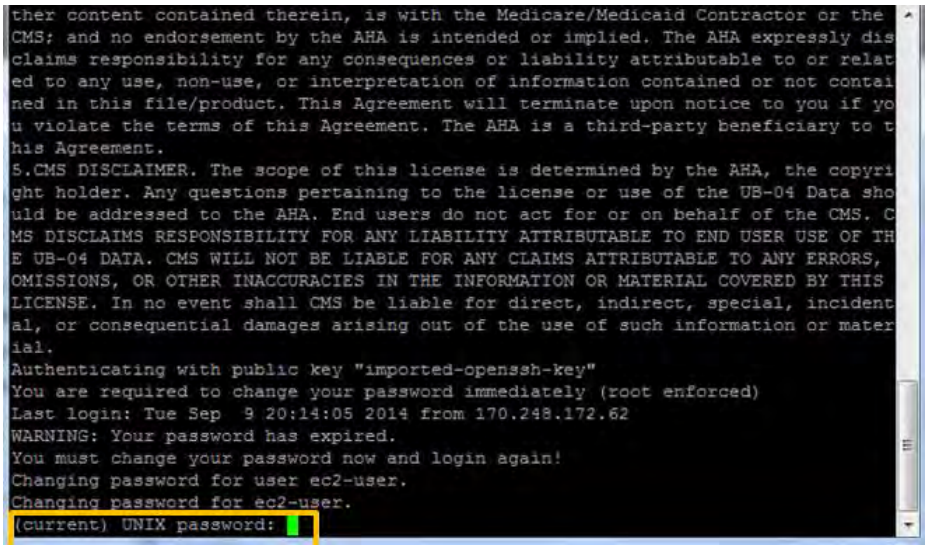



**Figure 30 - Enter Password**

You will then need to enter and then re-type a new password for your server for future logins.

When creating your new password, please follow the criteria below in order to ensure you create a valid password:

**EDGE server password MUST:**

- Have at least 14 characters
- NOT be a dictionary word
- Contain at least one (1) lowercase alpha character
- Contain at least one (1) uppercase alpha character
- Contain at least one (1) number
- Contain at least one (1) special character

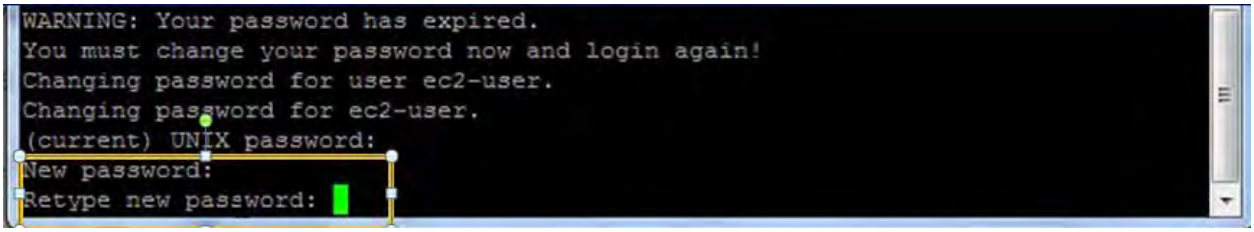



**Figure 31 - Enter NEW Password**

**NOTE:** After entering your new password, the PuTTY session will close automatically. Issuers will need to log back into PuTTY and enter their new password to access their server.

2. Users will now see the PuTTY program, and should enter **edge version (space between words)** into the Command Line and press enter.

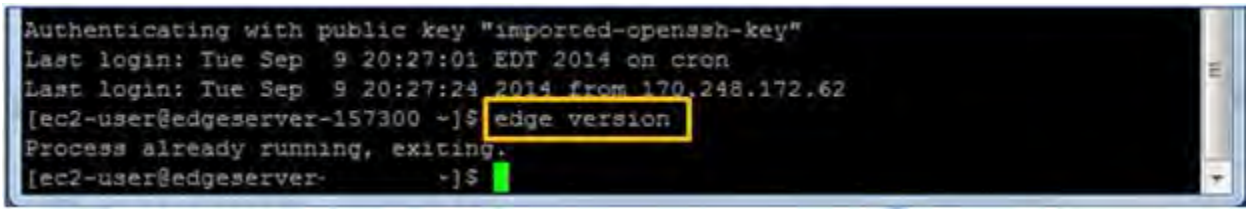



**Figure 32 – EDGE Version Command**

3. The EDGE version command will check if the system is running on a regular version and will generate database and application updates automatically when an application update is available and the issuers access the EDGE Server.

## 4.5. Enable Termination Protection

By default, your server instance does not have termination protection enabled. Selecting **Terminate** will shut down the instance and you will no longer be able to connect to or restart the instance after you've terminated it. The root device volume will be deleted and the EIP is disassociated from the instance. **This will effectively destroy your server instance permanently.**

In order to prevent your server instance from accidently being terminated, Issuers should enable termination protection on their server instance.

1. To enable termination protection on a server instance, Issuers should click **Instances** on the left hand side of the screen, then click **Actions,** then scroll down and click **Change Termination Protection.**

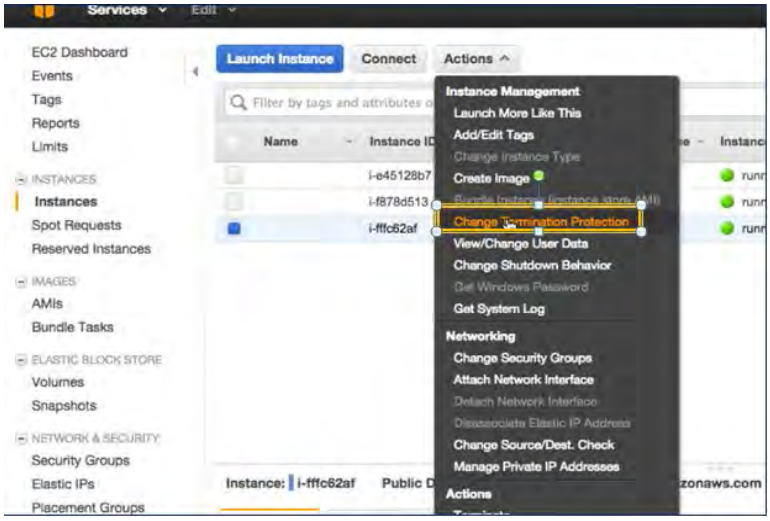



**Figure 33 - Select Change Termination Protection**

2. Issuers will receive a notification message asking them to confirm. Issuers should click ***Yes, Enable*** in the window.




**Figure 34 – Enable Termination Protection**

7. Once Termination Protection is enabled, selecting Terminate will produce the following dialog telling the Issuer that the instance has ***Termination Protection and will not be terminated.***

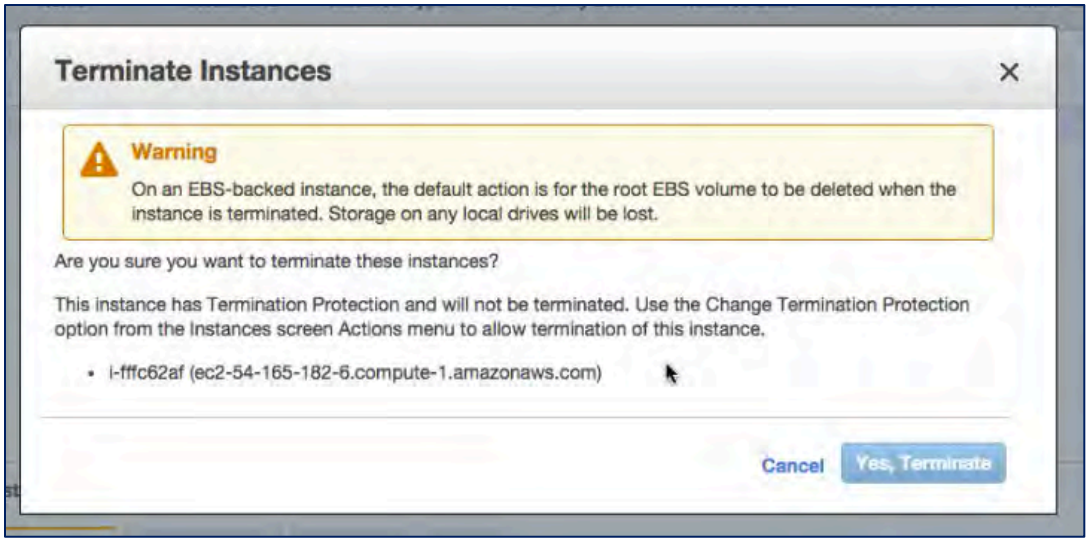



**Figure 35 – Terminate Instances Message**

## 4.6. Reminder: Stop Server Instance

In order to avoid continuous usage charges for a server instance, Issuers should remember to turn off their server instance when not in use.

1. To stop a server instance, Issuers should click **Instances** on the left hand side of the screen, then click **Actions,** then scroll down and click **Stop.**

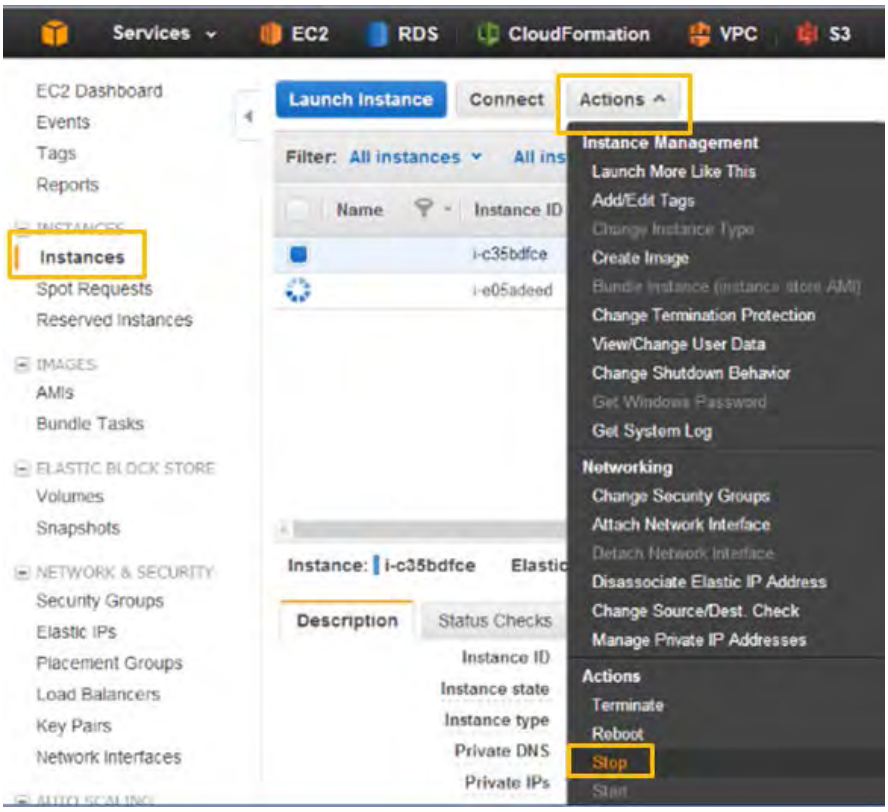



**Figure 36 - Stop Server Instance**

Issuers will receive a notification message asking them to confirm. Issuers should click Yes, Stop in the window.

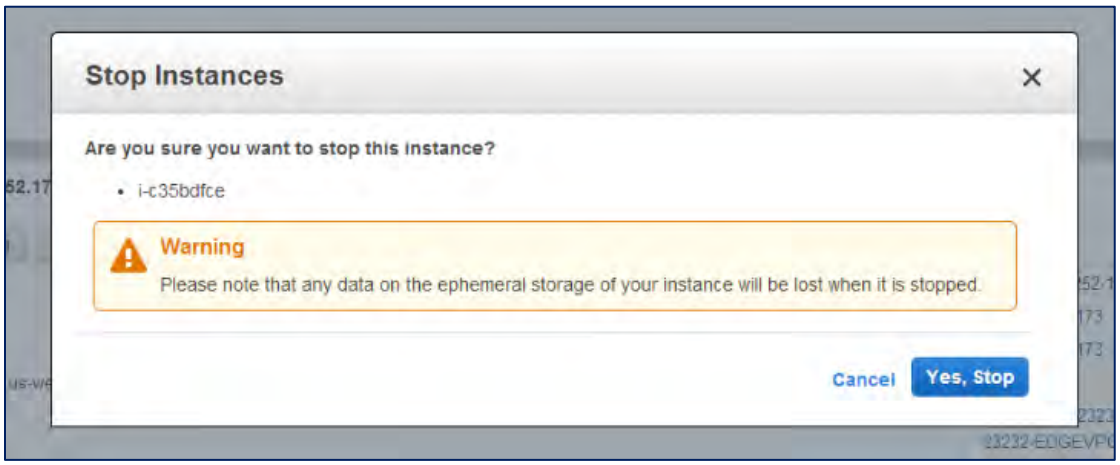



**Figure 37 – Stop Instance**

**This completes the Amazon EDGE Server Provisioning Job Aid. Issuers can now begin file processing. Please refer to the Amazon EDGE Server File Processing Job Aid for guidance.**