



Centers for Medicare & Medicaid Services
Center for Consumer Information and
Insurance Oversight (CCIIO)

EDGE Server Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning

Version 1.0
December 20, 2019

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense. The information provided in this presentation is only intended to be a general informal summary of technical legal standards. It is not intended to take the place of the regulations that it is based on. We encourage audience members to refer to the applicable regulations for complete and current information about the requirements that apply to them.

Table of Contents

Section 1 - Introduction	7
1.1 Conventions	8
1.2 Additional Resources	9
1.3 Technical Assistance.....	11
Section 2 - System Overview.....	13
2.1 Functional System Overview	13
2.1.1 Issuer Responsibilities and Infrastructure Overview	14
2.1.2 Architecture.....	16
2.1.3 System Software Specifications.....	18
2.1.4 Application Users	18
2.1.5 Application Directories	18
2.1.6 Application Binary Files.....	19
2.2 Data Model & Dictionary.....	22
Section 3 - Provisioning & Set Up.....	24
3.1 EDGE Server Options	24
3.2 EDGE Server Management Console.....	24
3.3 Server Set-Up - On-Premise	25
3.3.1 Server Setup.....	25
3.4 Server Set-Up - AWS	30
3.4.1 AWS Account Setup	30
3.4.2 Request an AWS EDGE Server Instance	35
3.5 HIOS ESM Roles.....	42
3.5.1 Assigning an EDGE Server Role to HIOS User	44
3.6 Accessing the ESM Website	53
3.7 EDGE Server Contacts	57
3.8 EDGE Server Registration Overview.....	58
3.8.1 Issuer EDGE Registration Request Submitter (aka: Issuer Submitters)	59
3.8.2 Issuer EDGE Registration Request Approver	71
3.8.3 TPA EDGE Registration Submitter	74
3.8.4 EDGE Server Management Console - Server Status Tracking.....	81
3.8.5 On-Premise EDGE Server Provisioning.....	82
3.8.6 AWS EDGE Server Provisioning	103
3.9 Migration.....	120

List of Figures

Figure 1-1: REGTAP	9
Figure 2-1: AWS EDGE Server Data Flow	17
Figure 2-2: On-Premise EDGE Data Flow	17
Figure 3-1: OP Server Set Up.....	25
Figure 3-2: Oracle Java Download Page	27
Figure 3-3: AWS Setup Flow	30
Figure 3-4: Amazon Web Services	31
Figure 3-5: AWS Create Account Screen	31
Figure 3-6: Create a New AWS Account	32
Figure 3-7: Enter in Contact Information.....	32
Figure 3-8: Enter in Payment Information	33
Figure 3-9: Provide a Telephone Number.....	33
Figure 3-10: Identity Verification PIN	34
Figure 3-11: Click Continue to Complete Identity Verification.....	34
Figure 3-12: Select your AWS Support Plan.....	34
Figure 3-13: AWS Account Set-Up Complete.....	35
Figure 3-14: AWS My Account	36
Figure 3-15: Account Settings	36
Figure 3-16: AWS Homepage with Services Dropdown	36
Figure 3-17: Select Roles	37
Figure 3-18: Create New Role Button.....	37
Figure 3-19: Configure Role Window.....	37
Figure 3-20: Select Role Type	38
Figure 3-21: Enter Account IDs	38
Figure 3-22: Set Permissions - Custom Policy	39
Figure 3-23: EdgeInstallerPolicy- Custom Permissions.....	39
Figure 3-24: Final Review Page	40
Figure 3-25: Services Dropdown with All AWS Services Selected	41
Figure 3-26: EC2 Dashboard Options	41
Figure 3-27: Create Key Pair	41
Figure 3-28: Create Key Pair Name	42
Figure 3-29: CMS Enterprise Portal Homepage, Login, and Terms and Conditions.....	44
Figure 3-30: MFA Security Code	45
Figure 3-31: HIOS Button	45
Figure 3-32: HIOS Button (Expanded Menu).....	45
Figure 3-33: Access Plan Management & Market Wide Functions Link	46
Figure 3-34: Terms of Use	46
Figure 3-35: Manage Role Tab	46
Figure 3-36: Request Role Tab	47
Figure 3-37: EDGE Server Management (ESM).....	47
Figure 3-38: Issuer EDGE Registration Request Approver Role	48
Figure 3-39: Enter Issuer ID	48
Figure 3-40: Review/Continue Button.....	49
Figure 3-41: Submit Request.....	49

Figure 3-42: Confirmation Page.....	49
Figure 3-43: View Roles	50
Figure 3-44: Request a Role.....	51
Figure 3-45: Enter Issuer ID	51
Figure 3-46: Submit Request.....	52
Figure 3-47: Confirmation Page.....	52
Figure 3-48: View Roles	53
Figure 3-49: CMS Enterprise Portal Homepage, Login, and Terms and Conditions.....	54
Figure 3-50: MFA Security Code	54
Figure 3-51: HIOS Button	55
Figure 3-52: HIOS Button (Expanded Menu).....	55
Figure 3-53: Access Plan Management & Market Wide Functions Link	55
Figure 3-54: Terms of Use	56
Figure 3-55: EDGE Server Management.....	56
Figure 3-56: Launch This Module on ESM	56
Figure 3-57: Access the EDGE Server Management Application	57
Figure 3-58: EDGE Server Home	57
Figure 3-59: Create EDGE Server Request Button	59
Figure 3-60: EDGE Server Request POC Page	60
Figure 3-61: TPA Information	60
Figure 3-62: Select Server Type.....	61
Figure 3-63: EDGE Server Name	61
Figure 3-64: On-Premise Server Details.....	61
Figure 3-65: AWS Server Details.....	62
Figure 3-66: Download Attestation Agreement Template	63
Figure 3-67: Save Request.....	63
Figure 3-68: Upload Attestation Agreement.....	63
Figure 3-69: Attach and Upload Attestation Agreement	64
Figure 3-70: Successfully Uploaded the File Message.....	64
Figure 3-71: Submit Request.....	64
Figure 3-72: Homepage.....	65
Figure 3-73: Create EDGE Server Request Button	65
Figure 3-74: EDGE Server Request POC Page	66
Figure 3-75: Select TPA	66
Figure 3-76: EDGE Server Details.....	67
Figure 3-77: Download Attestation Agreement Template	67
Figure 3-78: Save Request.....	68
Figure 3-79: Upload Attestation Agreement.....	68
Figure 3-80: Attach and Upload Attestation Agreement	68
Figure 3-81: Successfully Uploaded the File Message.....	69
Figure 3-82: Submit Request.....	69
Figure 3-83: Rejected Requests in Issuer EDGE Registration Request Submitter's Inbox.....	70
Figure 3-84: Open Request	70
Figure 3-85: Issuer EDGE Registration Request Approver Homepage	72
Figure 3-86: Open Request	72
Figure 3-87: Request Approval.....	73
Figure 3-88: Reject Request.....	73

Figure 3-89: Approve Request.....	74
Figure 3-90: TPA EDGE Registration Submitter Homepage	75
Figure 3-91: Download TPA Attestation Agreement Template	75
Figure 3-92: Upload Signed TPA Attestation Agreement	76
Figure 3-93: Upload Attestation Agreement.....	76
Figure 3-94: Uploaded Attestations Agreement.....	76
Figure 3-95 Select to View Request	77
Figure 3-96: TPA EDGE Registration Submitters Request.....	77
Figure 3-97: Select Server Type.....	77
Figure 3-98: EDGE Server Name	78
Figure 3-99: AWS Server Details.....	78
Figure 3-100: AWS Details	78
Figure 3-100: Submit Button.....	79
Figure 3-101: Rejected Requests in Submitter's Inbox.....	79
Figure 3-102: Open Request	80
Figure 3-103: Search Requests Button	81
Figure 3-104: EDGE Server Request Search Screen.....	81
Figure 3-105: Pending Provisioning.....	82
Figure 3-106: Search Requests Button	82
Figure 3-107: Search Request Screen	83
Figure 3-108: Provisioning in Progress.....	83
Figure 3-109: Download Provisioning Installation Scripts	84
Figure 3-110: WinSCP Home Page.....	85
Figure 3-111: News Tab	85
Figure 3-112: Go to Download Page Link.....	85
Figure 3-113: Download WinSCP.....	85
Figure 3-114: Download Installation Package	86
Figure 3-115: WinSCP Login Screen.....	86
Figure 3-116: WinSCP Login Information	87
Figure 3-117: WinSCP Files and Folders	87
Figure 3-118: PuTTY Home Page	88
Figure 3-119: PuTTY Download Page.....	88
Figure 3-119: PuTTY Configuration Window	89
Figure 3-120: PuTTY Configuration - Add IP Address.....	89
Figure 3-121: Enter Username for PuTTY	90
Figure 3-122: Enter Password for PuTTY.....	90
Figure 3-123: Create EDGE folder and Open Files	91
Figure 3-124 Open EDGE Folder	91
Figure 3-125: Unzip On-Premise Installation Information File	92
Figure 3-126 Open Config Folder	92
Figure 3-127: Open Deployment Script and Property File	93
Figure 3-128: Open Properties File in Editable Format	94
Figure 3-129: Enter New Password for Database	95
Figure 3-130: edgserver_size field	96
Figure 3-131: Add/Modify EDGE Properties	96
Figure 3-132: Save File and Exit	97
Figure 3-133: Open Install Folder	97

Figure 3-134: Install EDGE Application	98
Figure 3-135: Confirm Successful Provisioning	98
Figure 3-136: MySQL Data Dump Commands	99
Figure 3-137: Create Databases	100
Figure 3-138: Create New Database User.....	100
Figure 3-139: Load Data to New Tables	101
Figure 3-140: Enter CRON Command.....	101
Figure 3-141: Configure Cron Timing	102
Figure 3-142: Save and Exit Cron	102
Figure 3-143: Confirm Provisioned Request.....	103
Figure 3-144: Pending Provisioning.....	104
Figure 3-145: Search Requests Button	104
Figure 3-146: Search Request Screen	105
Figure 3-147: Provisioning in Progress.....	105
Figure 3-148: Server Provisioned Status	106
Figure 3-149: Pending Provisioning.....	106
Figure 3-150: PuTTY Home Page	107
Figure 3-151: PuTTY Download Page.....	107
Figure 3-152: PuTTYgen Program Screen	108
Figure 3-153: PuTTYgen Notice	108
Figure 3-154: Save Private Key.....	109
Figure 3-155: Services and All AWS Services Dropdowns.....	110
Figure 3-156: EC2 Options	110
Figure 3-157: All Instances List	111
Figure 3-158: Public IP Address	111
Figure 3-159: PuTTY Configuration Window	112
Figure 3-160: PuTTY Configuration - Add IP Address.....	112
Figure 3-161: Category List on PuTTY Configuration Window	113
Figure 3-162: PuTTY Authentication Options	113
Figure 3-163: Browsing for PuTTY Private Key	114
Figure 3-164: Save Session	114
Figure 3-165: Completing PuTTY Configuration.....	115
Figure 3-166: PuTTY Security Alert.....	115
Figure 3-167: Enter Password	116
Figure 3-168: Enter NEW Password.....	116
Figure 3-169: EDGE Version Command.....	117
Figure 3-170: Select Change Termination Protection	117
Figure 3-171: Enable Termination Protection	118
Figure 3-172: Terminate Instances Message	118
Figure 3-173: Select EC2	119
Figure 3-174: Stop Server Instance.....	119
Figure 3-175: Confirm Stop Instance.....	120

List of Tables

Table 1-1: Conventions Table.....	8
Table 1-2: Key Documents	9
Table 1-3: Technical Assistance Table	11
Table 2-1: EDGE Server Schemas	16
Table 2-2: Software Stack Components	18
Table 2-3: EDGE Server Application Users	18
Table 2-4: Application Directories	18
Table 2-5: Binary Files.....	20
Table 2-6: Data Model & Dictionary	22
Table 3-1: AWS & OP Considerations	24
Table 3-2: Server Configuration Based on INTEL CPUs	26
Table 3-3: AWS S3 Endpoints	28
Table 3-4: Self-Hosted Path	70
Table 3-5: TPA-Hosted Path.....	71
Table 3-6: TPA-Hosted Path.....	80

Section 1 - Introduction

As part of the Patient Protection and Affordable Care Act (PPACA), the Risk Adjustment (RA) program mitigates the impact of adverse selection of plans and provides stability for issuers. Included in the RA program is the High Cost Risk Pool (HCRP), which was implemented starting BY2018 to mitigate incentives for risk selection to avoid high-cost enrollees. States have the option to operate the RA program (including HCRP) themselves or have the Department of Health and Human Services (HHS) operate the programs on their behalf.

- Section 1343 of the PPACA created the RA program to better spread the financial risk borne by health insurance issuers, to stabilize premiums and enable issuers to offer a variety of plans to meet the needs of a diverse population. Under the RA program, payments are transferred from issuers with relatively lower-risk populations to issuers with relatively higher-risk populations. Non-grandfathered Individual and Small Group Market plans, irrespective of whether they are a part of the Exchange, submit RA data (claims and enrollment data) that is used to determine individual-level risk scores and plan average actuarial risk and associated payments and charges.
- Beginning BY2018, the HCRP partially reimburses issuers for enrollees' aggregated issuer plan paid claim amounts that are above a certain threshold attachment point (AP), at a certain coinsurance rate. HCRP applies to all issuers who offer PPACA health insurance coverage in the small group and/or individual market (including catastrophic and merged), both on and off the Exchange. HCRP payments are funded by a national percent of premium charge on all issuers by market, and all payments and charges are in addition to any RA transfers. [Note: HCRP information can be found in the [2018 Payment Notice](#) (FR 81 94080-94082)].
- Section 1341 of the PPACA established the Reinsurance (RI) program as a temporary three (3)-year program which was applicable for BY2014 through 2016 with External Data Gathering Environment (EDGE) operations ceasing in 2017. RI provided funds to issuers that incur high costs for claims in the Individual Market. In accordance with [45 CFR § 153.230](#), RI payments are based on a coinsurance rate or proportion of an issuer's claims costs that are above an AP and below a RI cap for the applicable benefit year. The AP is the threshold dollar amount after which the issuer is eligible for RI payments. The RI cap is the dollar limit at which point an issuer is no longer eligible for RI payments. The AP, coinsurance rate and RI cap are applied to an issuer's total costs for an individual enrollee in a given calendar year. Individual Market plans, irrespective of whether they are part of the Exchange, submitted RI data (claims and enrollment data) that was used to determine if an Individual Market plan issuer was eligible for RI.

Under regulation with the authority of the HHS, the Centers for Medicare & Medicaid Services (CMS) was delegated the authority to collect data from issuers when CMS is operating RA and/or HCRP on behalf of a State. In response to community feedback, CMS developed the distributed data collection (DDC) methodology based on the fact that 1) issuers needed a dedicated data environment that protects personally identifiable information (PII) and issuer proprietary data and 2) CMS needed access to install and update a common software in the

distributed data environment to check data integrity and perform calculations for program implementation.

The EDGE application is a component of Financial Management (FM) within the Federally-facilitated Marketplace (FFM). Issuers in states where HHS is operating an RA program are required to submit enrollment, pharmaceutical claims and medical claim information on enrollees from issuers' proprietary systems to an issuer's EDGE server. In addition, issuers may submit supplemental diagnosis codes identified in medical records and associated with claim services that were otherwise not included on the claim. All processing of enrollment claims and supplemental diagnosis data, as well as calculation of individual risk scores and RI amounts, occurs on the issuer owned EDGE server.

The purpose of the EDGE Server Operations and Maintenance Manual (O&MM) is to provide the information necessary to operate and maintain the EDGE application. CMS has also published two (2) Interface Control Documents (ICD), which provide the technical specifications to create inbound eXtensible Markup Language (XML) files and receive outbound XML files. In addition, the EDGE Server Business Rules (ESBR) explain the EDGE application processing logic and requirements from a business operations perspective.

1.1 Conventions

The following documentation conventions will be used:

Table 1-1: Conventions Table

Convention	Description
Black highlighted in Gray: Text	Black characters highlighted in Gray indicate a command that should be run at the Linux or MySQL command line.
Red highlighted in Gray: <Text>	Red characters highlighted in Gray indicate text that needs to be replaced with a value that is specific to the issuer.
Blue and underlined: <u>Text</u>	Blue characters underlined indicate text that are hyperlinked to external documents or websites.
	You must contact the indicated party, or perform the indicated steps, before proceeding.
	Indicates a critical step or warning. If this guidance is not followed, it will have an impact to current or future functionality.
	Indicates information an issuer should note. Although the information may not impact a command, EDGE application update, and/or EDGE reference data update.



Please do not copy commands to the command line directly from this document to avoid execution errors caused by Windows End of Line (EOL) Conversion. Issuers can either type the commands in the command line or copy commands from this document to NotePad or TextPad, then copy it to the command line.

- Copy the entire installApplication.sh command into a text editor (Ex. NotePad++).
- Ensure EOL is Unix and then copy it back to the Linux terminal.

Technical Assistance

Financial Management Coordination Center (FMCC) representatives are available to answer any questions or assist issuers with this process. To contact an FMCC representative, send an email to EDGE_Server_Data@cms.hhs.gov.

1.2 Additional Resources

There are several resources published in the [Registration for Technical Assistance Portal](http://www.regtap.info) (REGTAP). REGTAP is the primary source for policy communications and documentation regarding the EDGE server. This site provides information on common questions CMS has received from issuers, as well as additional information and announcements from CMS related to the EDGE server implementation. To access the REGTAP web site, log into [http://www.regtap.info/](http://www.regtap.info) and click “Register as a New User” using an email address.



Figure 1-1: REGTAP

Issuers can sign up for training events, such as the EDGE Server Webinar Series, to receive updates about the EDGE server and ask questions to CMS representatives. In addition, issuers can access the Program Area page and review the DDC for RA, Including High Cost Risk Pool (HCRP), and EDGE server documents including, but not limited to, the following key documents:

Table 1-2: Key Documents

Document	Summary
EDGE Server Updates and Data Submission	Provides new information for EDGE functionality, operations and background information regarding deadlines. Note: this document has been retired and previous versions are located in the REGTAP Library, as well as the DDC Retired Resources Page located here, (https://www.regtap.info/ddcrr.php).

Document	Summary
EDGE Server Maintenance Release Notes	Provides EDGE server version numbers, date and time of releases and updates to the functionality of the new EDGE server versions.
EDGE Server Timeline	Provides important deadlines for maintenance releases, command deployments, submission, etc.
EDGE Server Storage Calculator	Template to calculate how much storage is needed for the EDGE server
Interface Control Document (ICD)	Tracks the necessary information required to effectively define the CMS-EDGE server system interface, as well as any rules for communicating with the EDGE servers, which provides guidance on the architecture of the system to be developed. Specifically, the ICD includes the detailed XML file layouts and XSDs for the four (4) input XML files (medical, pharmacy, enrollment and supplemental) and the related summary and detail output files generated during file processing. Also, the ICD helps ensure compatibility between system segments and components.
Risk Adjustment and Reinsurance (RARI) Interface Control Document (ICD) Addendum	An addendum to the ICD that provides file layouts and data element definitions/formats for the RA, RADV, HCRP, and analytic XML reports generated by the EDGE server. The RARI ICD Addendum includes five (5) documents: RA Addendum, RADV Addendum, RI Addendum, HCRP Addendum, and Issuer Frequency Report Addendum.
Financial Management (FM) Community WinAuth Download and Installation User Guide	Provides the steps for initial access to the FM Community, which includes the process for downloading the two-factor authentication application, WinAuth
EDGE Server Business Rules (ESBR)	Supplements the EDGE Server ICD by providing the EDGE server file processing business rules issuers are required to follow when submitting enrollment, pharmacy claims, medical claims and supplemental diagnosis code files.
High Cost Risk Pool (HCRP) Reference Guide	Provides issuers with an overview of the HCRP calculations and associated EDGE reporting. Beginning in BY2018, the RA Program will include the HCRP program, which helps to stabilize premiums by partially reimbursing issuers for enrollees with high claims costs above a certain threshold AP, at a certain coinsurance rate.
EDGE Server Migration Job Aids	Provides steps to complete a server migration for AWS and OP servers.

Document	Summary
EDGE Server Operations and Maintenance Manual (O&MM) – File Processing & Commands	Provides instruction for issuers to execute the EDGE operational activities including file processing, local and remote command execution, configuration management, and application errors.
EDGE Server Operations and Maintenance Manual (O&MM) – Configuration, Validation & Application Errors	Provides issuers with the requirements for proper EDGE application configuration in order to maximize functionality.
EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures	Provides issuers with an overview of the operational support and backup procedures for both AWS and OP EDGE servers which is part of the disaster recovery process.
EDGE Server Operations and Maintenance Manual (O&MM) – Reference Data	Provides issuers with an overview of Global Reference Data and Plan reference Data.

In addition, the REGTAP portal allows issuers to access a list of Frequently Asked Questions (FAQs) and review upcoming deadlines.

1.3 Technical Assistance

FMCC representatives are available to answer any questions or assist issuers with questions related to the technical operation of the EDGE server or software functionality including the file ingest and program calculations. To contact an FMCC representative, send an email to EDGE_Server_Data@cms.hhs.gov. For other inquiries, please see additional CMS contacts below:

Table 1-3: Technical Assistance Table

Reason	Email Address or Website
Technical assistance for EDGE server data submission/processing, EDGE reports, EDGE calculations	EDGE_Server_Data@cms.hhs.gov
Financial Management (FM) Community* for webforms and notifications including: Truncation, Baseline, Quantity/Quality Outliers, EDGE Server Status Update, Attestation and Discrepancy, RA Reconsiderations, Archive, and EDGE Server Contacts update, including Chief Executive Officer (CEO) Designation.	ccrms-rari.force.com/financialmanagement
Policy, baseline, EDGE data quantity notifications, payments/charges, exempt filing, general information	RARIPaymentOperations@cms.hhs.gov
EDGE data quality notifications	EDGEdatareply@cms.hhs.gov

Reason	Email Address or Website
EDGE Server Data Truncation	RARIPaymentOperations@cms.hhs.gov
RA Do-It-Yourself (DIY), SAS software model questions	hhshccraops@cms.hhs.gov
Risk Adjustment Data Validation (RADV)	CCIIOACARADatavalidation@cms.hhs.gov

*In September 2019, CMS introduced the FM Community to streamline issuer reporting to support EDGE server data submission for the RA program. Accessing the FM Community requires the use of a multi-factor authentication (MFA) application. Up to four (4) contacts from each participating company will have access to the FM Community, with the CEO Designate as the primary user. The CEO Designates responsibilities include maintaining contact information for EDGE contacts; completing or overseeing the completion of all webforms; and receiving EDGE related notifications.

The FM Community is only available to authorized contacts approved by the company.

Section 2 - System Overview

This section provides an overview of the EDGE application, the types of files submitted and output files generated, as well as the two (2) server options available for issuers. Each section is then further detailed later in the O&MM. In addition, this section details the system software specifications, types of users, directories and binary files used.

2.1 Functional System Overview

This section provides an overview of the EDGE application and functionality addressed in the O&MM. The EDGE application supports two (2) technical solutions, the first of which is the automated provisioning of the issuer EDGE server in Amazon Web Services (AWS). The second solution is an On-Premise (OP) issuer EDGE server that is set up and provisioned by the issuer in accordance with CMS requirements. The EDGE application includes the following functionality:

File Ingest Jobs

The file ingest job processes four (4) different types of files provided by the issuer. The files are:

- Enrollment File
- Medical Claims File
- Pharmacy Claims File
- Supplemental Diagnosis Code File

Each file is validated according to the field level technical validation rules outlined in the file ingest ICD (See [Interface Control Document \(ICD\)](#)) and the business validation rules outlined in the ESBP document (See [EDGE Server Business Rules \(ESBR\)](#)). Only successfully validated and accepted records are loaded to the EDGE database during processing.

Commands and Output Reports

CMS will deploy commands to issuer servers that produce RA, HCRP and analytic XML reports. Issuers will receive detail and summary reports; CMS will receive only summary reports. The summary reports generated from successful file processing are used to evaluate and perform RA and HCRP calculations for issuers and other stakeholders. Issuers may also execute commands locally. For additional details and a complete list of EDGE server input files, output files and their formats refer to the Appendices in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands Document](#).

Application Version Maintenance

CMS will periodically need to perform maintenance activities on issuer servers and will communicate the functionality being modified and a deployment schedule. Once a maintenance release occurs, issuer EDGE servers must be updated and be running on the most recent version of the EDGE application.

In order for any ingest file to be processed or any local or remote command to be executed on the EDGE server, the server must be on the latest application version released by CMS. Each time an EDGE job, which could be a command, EDGE application update and/or EDGE reference data update, is executed by an issuer, the server will first confirm if any EDGE application updates are available and apply them as needed. If the server fails to update to the

latest version, the server will stop processing until the error is addressed. The following updates may be applied by CMS in future EDGE maintenance release versions:

- EDGE server application updates including ingest functionality, outbound file structure or RA, HCRP, and/or RI calculation updates
- Reference table updates
- Operating system (OS) updates
- SQL database updates

The EDGE application and reference data updates must be on the latest version in order to have accurate claims processing. Operating system and database updates will be configured to require the database administrator to manually run the update command as new updates are made available. If desired, these updates can be configured to be applied automatically by enabling a CRON job, which is detailed in Section 3.1.4: Automated Job Scheduling in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – Configuration, Validation & Application Errors](#). For each update processed, the update type (OS, DB, application, reference data), date, completion status (successful/error), and issuer for which the update was made will be logged on the EDGE Server Management console database, which is further explained in [Section 3.2 EDGE Server Management Console](#).

The next section provides information related to individual components of the functional system.

2.1.1 Issuer Responsibilities and Infrastructure Overview

This section provides an overview of issuer responsibilities and the infrastructure of the AWS and OP EDGE Server application.

As mentioned earlier, the issuer EDGE Server solution supports two (2) scenarios. The first scenario is the issuer EDGE server hosted in an AWS environment which may be hosted by the issuer or a Third-Party Administrator (TPA).

The second scenario is the OP EDGE server. This server can be physical or virtual and may be managed and provisioned by an issuer or by a TPA on the issuer's behalf. More details about the differences between the two (2) options will be described in [Section 3.1 EDGE Server Options](#).

Issuer Roles and Responsibilities

Issuers are responsible for the following:

- Procuring dedicated server and Red Hat enterprise evaluation license
- Providing physical security and installation and maintenance of anti-virus and anti-intrusion software
- Developing the extract, transform and load (ETL) to extract data from issuer processing system and submit to the EDGE server
- Loading claim, enrollment and supplemental diagnosis code information to the dedicated server
- Masking enrollee identities on claims and enrollment files
- Reviewing and resolving processing errors identified on outbound files
- Evaluating accuracy of program calculations as provided on outbound reports
- Contacting CMS to report problems



Note: Issuers who chose to use a TPA to manage the EDGE server remain fully responsible for complete and accurate data submission, meeting all data and baseline submission deadlines, reviewing program reports for accuracy, and responding to CMS inquiries related to quantity and quality outliers.

File Processing Zones

Each EDGE server application supports the following three (3) separate file processing zones. When loading an ingest file for processing, issuers must indicate the intended file processing zone in the file name.

- **Production Zone**
 - Used by issuers to load production files for processing.
 - Enrollment, medical claims, pharmacy claims, and supplemental diagnosis data will be submitted, verified and stored for RA, HCRP, and RI processes.
 - A minimum number of data elements associated with rejected records will be stored for issuer reference and use.
 - Only data submitted to the production zone is used by CMS for RA and HCRP payments and charges and RI payments.
- **Test Zone**
 - Uses the same application version and file processing validation rules as the production zone.
 - Uses the same reference data as the production zone.
 - Issuers use the test zone to ingest files prior to loading into production. CMS encourages issuers to submit their files to the test zone and evaluate the results of the detail reports to limit the amount of rework necessary once data is submitted to production.
 - Issuers may submit enrollment for prior years, cross-year claims where the statement coverage end date is in the new benefit year and supplemental records are associated with claims for the new benefit year.
 - Available for issuers to test files any time with one (1) exception:
 - Once the production blackout is in effect, issuers cannot submit claim data to the test zone for a benefit year that has closed or is in the process of being finalized.
- **Validation Zone**
 - Uses a different application version and file processing validation rules as the production zone.
 - Uses a different set of reference data as the production and test zones.
 - The validation zone is intended for issuers to utilize, upon the direction of CMS, to test upcoming releases prior to deployment to the test and production zone which only house the current software version and table structures.
 - Issuers and CMS use the validation zone as a pre-prod environment to test EDGE application releases with pre-selected issuers or “beta” testers, using their existing EDGE servers, prior to releasing the application to production. Once the beta

testers have confirmed the accuracy of the release, all issuers will be permitted to utilize the validation zone for testing.

Server Schemas

In order to support the three (3) different file processing zones, the EDGE server is comprised of the following five (5) database schemas identified in the table below.

Table 2-1: EDGE Server Schemas

Schema Name	Description	EDGE Schema Name
EDGE Server Common Schema	Contains reference data used in both the production and test zones.	EDGE_SRVR_COMMON
EDGE Server Production Schema	Contains claim, enrollment and supplemental diagnosis code transactional data loaded in the production zone.	EDGE_SRVR_PROD
EDGE Server Test Schema	Contains claim, enrollment and supplemental diagnosis code transactional data loaded in the test zone.	EDGE_SRVR_TEST
EDGE Server Validation Schema	Contains claim, enrollment and supplemental diagnosis code transactional data loaded in the validation zone.	EDGE_SRVR_VALIDATION
EDGE Server Common Validation Schema	Contains reference data used in the validation zone.	EDGE_SRVR_COMMON_V

2.1.2 Architecture

Although the EDGE server solution supports an AWS and an OP scenario, the code base used in both solutions are the same. The configurations are slightly different to accommodate the implementation of the EDGE server in AWS or OP.

The figure below displays the logical flow of the EDGE server components in AWS after the issuer EDGE server has been deployed. The file ingestion flow starts when the issuer securely uploads their XML data files to the EDGE server. The following actions will occur:

- Validation and processing of the input data file
- Creation of summarized and detailed XML reports for review by the issuers
- Summarized XML reports are securely sent to the AWS Data Simple Storage Service (S3) bucket, where they are retrieved by the CMS EDGE File Sweep batch for CMS use.

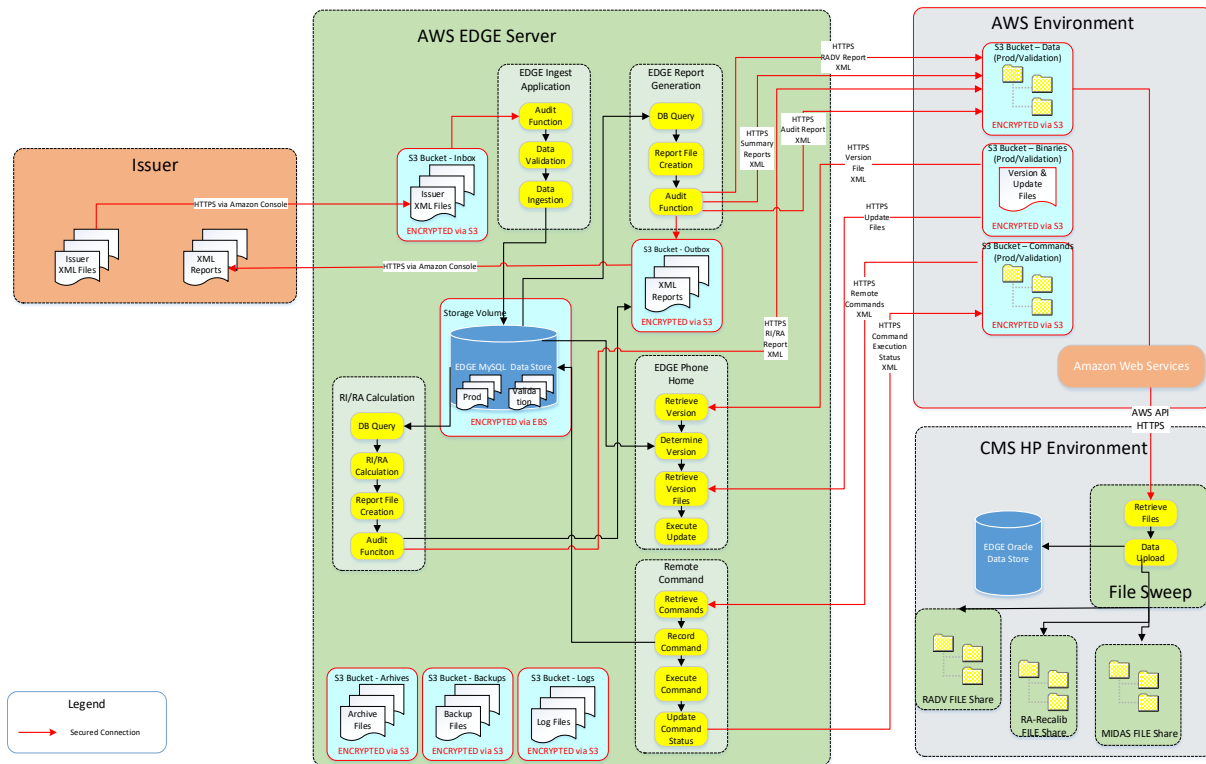


Figure 2-1: AWS EDGE Server Data Flow

The figure below displays the logical flow of the EDGE server components in the OP scenario after the issuer's EDGE server has been deployed. It is nearly identical to the EDGE solution in AWS except the EDGE server is in an issuer controlled environment and that the OP Server directories are located locally.

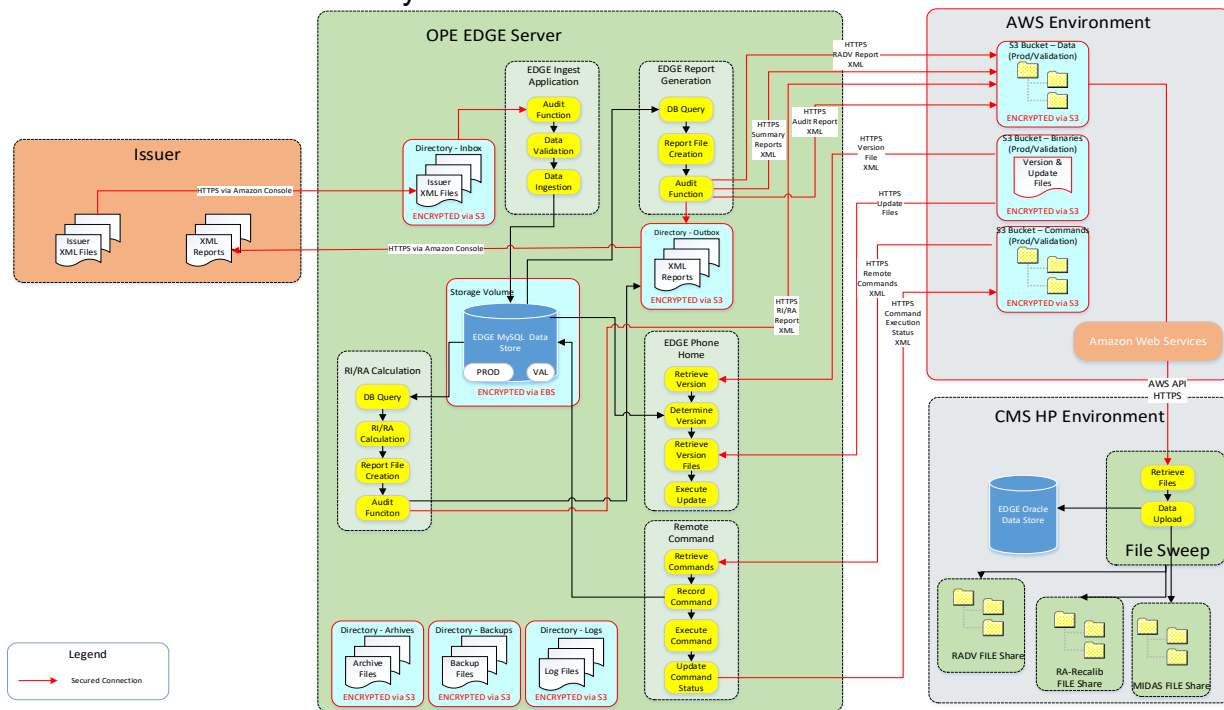


Figure 2-2: On-Premise EDGE Data Flow

2.1.3 System Software Specifications

The EDGE server application is deployed to either an AWS or OP server. The EDGE solution is a custom-built application that combines open-source software with custom objects. Table 2-2 below provides an overview of the EDGE server software components:

Table 2-2: Software Stack Components

Area	Vendor	Product
Common Services (afpj-common is used for exception handling)	CAN	afpj-common.jar
Batch	SpringSource	Spring Batch
Dependency Injection	SpringSource	Spring Framework
Security	SpringSource	Spring Security
Java	Oracle	JRE/JDK
Persistence	SpringSource	Spring JDBC
Database	MySQL	MySQL (EDGE)
Web Server	Apache	Tomcat
MVC	SpringSource	MVC
Amazon Cloud API	Amazon	AWS Java API
EDGE Operating System	Red Hat	Red Hat Enterprise

2.1.4 Application Users

The table below describes the user the EDGE server application utilizes.

Table 2-3: EDGE Server Application Users

Application ID	Scenario	Description
edgedbuser	AWS & OP	EDGE Server MySQL DB user
Ec2-user	AWS	EDGE Server Application ID User

2.1.5 Application Directories

The following directories are used by the EDGE server application.

Table 2-4: Application Directories

Directory	Description
/opt/edge	Parent EDGE server application directory
/opt/edge/bin	Contains the EDGE server binaries

Directory	Description
/opt/edge/config	Contains the EDGE server application configuration files
/opt/edge/ingest	Parent directory for the ingest application
/opt/edge/ingest/appdata	Contains EDGE server application data
/opt/edge/ingest/archives	Contains EDGE server archival files
/opt/edge/ingest/archives/accepted	Contains the issuer data files that have been processed
/opt/edge/ingest/archives/rejected	Contains the issuer data files that have been rejected due to data issues
/opt/edge/ingest/inbox	Directory that issuers post their Enrollment, Medical, Pharmacy, and Supplemental data files
/opt/edge/ingest/logs	Contains the EDGE server application log files
/opt/edge/ingest/outbox/cms	Contains summary report files that will be sent to CMS
/opt/edge/ingest/outbox/issuer	Contains the detailed and summary report files for the issuers
/opt/edge/update	Parent directory for EDGE server application update files
/opt/edge/update/app	Contains the EDGE server application update files
/opt/edge/update/config	Contains the EDGE server configuration files
/opt/edge/update/db	Contains the EDGE server database update files
/opt/edge/update/db/common	Contains the EDGE server database common SQL statements for performing the DB updates
/opt/edge/update/db/issuer	Contains the EDGE server issuer specific database SQL statements
/opt/edge/update/lib	Contains updated library files used by the EDGE server application
/opt/edge/update/scripts	Contains EDGE server scripts
/opt/edge/update/sql	Contains EDGE server SQL scripts
/opt/edge/lib	Contains library files used by the EDGE server application

2.1.6 Application Binary Files

The table below lists and describes the binary files used by the EDGE server. The list also includes the location of the binary files. These files are installed during the deployment of an AWS EDGE server or are manually installed for an OP EDGE server during provisioning.



Note: The location information in the table below is for the AWS EDGE server. The location of the OP EDGE server scenario will be different. Issuers should consult with their local Information Technology (IT) team who performed the OP EDGE server installation for the binary file location.

Table 2-5: Binary Files

Binary Name	Description
afpj-common-6.5.0.jar	Accenture federal framework
annox-0.5.0.jar	Java extension contains annotations from XML
aopalliance-1.0.jar	Aspect orient programing (AOP) open sources library
aws-java-sdk-1.7.11.jar	Amazon java library to access amazon web service resources
bsh-2.0b4.jar	BeanShell library for dynamic execution of java syntax
cglib-nodep-2.2.2.jar	AOP Support library
classmate-1.0.0.jar	Generic type declarations
commons-beanutils-1.9.1.jar	Java common bean utils
commons-codec-1.3.jar	Java based encode and decode library
commons-collections-3.2.1.jar	Java collection library contains iterators, maps, list and array collections
commons-configuration-1.7.jar	Java common configuration handling components
commons-dbcp-1.4.jar	Java common database components
commons-digester-1.8.1.jar	Java common XML digester classes
commons-io-2.4.jar	Java common file IO classes
commons-lang-2.3.jar	Java common objects classes
commons-logging-1.1.1.jar	Java common logging framework
commons-pool-1.5.4.jar	Java common connection pool classes
edge-server-application.jar	Edge application binaries, contains edge batch processes
gson-2.2.4.jar	Google library to parse JSON objects
guava-17.0.jar	Guava library contain google collection, caching and concurrency. Used by gson library.
hamcrest-core-1.3.jar	Library of match objects used by other frameworks
hibernate-validator-5.1.0.Final.jar	Hibernate validator library
hibernate-validator-cdi-5.1.0.Final.jar	Hibernate validator library
hsqldb-1.8.0.7.jar	Hyper SQL library, used for execute queries against relational database
httpclient-4.2.jar	Java HTTP client library
httpcore-4.2.jar	Java HTTP core library
jackson-annotations-2.1.1.jar	Jackson library for XML parsing
jackson-core-2.1.1.jar	Jackson library for XML parsing
jackson-databind-2.1.1.jar	Jackson XML library, to build XML to java objects
javassist-3.18.1-GA.jar	Java assist provides basic java class objects

Binary Name	Description
javax.el-2.2.4.jar	Java extension for Expression Language, supports for JSP and JSF
javax.el-api-2.2.4.jar	Java extension for Expression Language, supports for JSP and JSF
jaxb2-basics-0.6.3.jar	XML Schema compiler
jaxb2-basics-annotate-0.6.3.jar	XML Schema compiler using annotations
jaxb2-basics-runtime-0.6.3.jar	XML Schema compiler runtime
jaxb2-basics-tools-0.6.3.jar	XML Schema compiler tools
jboss-logging-3.1.3.GA.jar	Jboss logging framework
jcommander-1.27.jar	Command line parameter parser framework
jettison-1.1.jar	Java API for DOM and STaX parsing
joda-time-2.4.jar	Joda time a replacement for native java date time object
junit-4.11.jar	Junit framework for unit testing
liquibase-core-3.2.2.jar	Liquibase used for database change log and database schema maintenance
log4j-1.2.12.jar	Log4j library for logging
log4j-over-slf4j-1.7.7.jar	Log4j library for logging
logback-classic-1.1.2.jar	Logback logging framework
logback-core-1.1.2.jar	Logback logging framework
mysql-connector-java-5.1.30.jar	MySQL connection/driver classes
objenesis-1.3.jar	Objenesis framework to invoke methods using reflection
slf4j-api-1.7.6.jar	Simple logging façade used for logging
slf4j-simple-1.7.6.jar	Simple logging façade used for logging
snakeyaml-1.13.jar	YAML parser
spring-aop-4.0.3.RELEASE.jar	Spring aspect-oriented programming framework components
spring-batch-core-2.2.5.RELEASE.jar	Spring batch framework components
spring-batch-infrastructure-2.2.5.RELEASE.jar	Spring batch framework components
spring-beans-4.0.3.RELEASE.jar	Spring framework for bean definition
spring-context-4.0.3.RELEASE.jar	Spring framework context management objects
spring-context-support-4.0.3.RELEASE.jar	Spring framework context management objects
spring-core-4.0.3.RELEASE.jar	Spring framework core components

Binary Name	Description
spring-expression-4.0.3.RELEASE.jar	Spring framework expression components
spring-jdbc-4.0.3.RELEASE.jar	Spring framework JDBC objects for database operations
spring-oxm-4.0.3.RELEASE.jar	Spring framework XML to object mapping classes
spring-retry-1.0.2.RELEASE.jar	Spring framework batch component
spring-test-4.0.3.RELEASE.jar	Spring testing framework
spring-tx-4.0.3.RELEASE.jar	Spring framework transaction management classes
testng-6.8.7.jar	Testing framework for unit testing
tomcat-jdbc-7.0.53.jar	Tomcat framework for jdbc operations
tomcat-juli-7.0.53.jar	Tomcat framework objects
validation-api-1.1.0.Final.jar	Validation framework for XML
xpp3_min-1.1.4c.jar	XML publish library
xstream-1.3.jar	XML streaming library

2.2 Data Model & Dictionary

The EDGE server data submission process is identical in both the AWS and OP EDGE server scenarios. Issuers' data will be submitted to the EDGE servers by placing one (1) or more of the following file types in the Inbox S3 bucket or directory depending on the EDGE server scenario:

- Enrollment File
- Medical Claims File
- Pharmacy Claims File
- Supplemental Diagnosis Code File

CMS owns the data schemas, tables and software that exist on the EDGE server. The EDGE Server Data Models and EDGE Server Data Dictionaries detail and describe individual elements in the issuer's server environments and allows issuers to troubleshoot data issues. The EDGE Server Data Model illustrates all the data tables in the EDGE server and how they relate to each other. The EDGE Server Data Dictionary specifies what is collected in the table outlined in the corresponding data model.

Table 2-6: Data Model & Dictionary

Schema Name	Description	Data Model Link	Data Dictionary Link
EDGE Server Common Schema	The common schema contains reference data required by the EDGE application and is applicable to both the test and production zones.	EDGE Server Common Schema Data Model	EDGE Server Common Schema Data Dictionary

Schema Name	Description	Data Model Link	Data Dictionary Link
EDGE Server Production Schema	The production schema is used by the issuer to process production files.	EDGE Server Production Schema Data Model	EDGE Server Production Schema Data Dictionary
EDGE Server Test Schema	The test schema can be used to test and validate inbound XML files.	EDGE Server Test Schema Data Model	EDGE Server Test Schema Data Dictionary
EDGE Server Validation Schema	The validation zone serves as a pre-production environment for CMS to test EDGE application releases with issuers, using their existing EDGE servers, prior to releasing the application to production. The validation schema can be used to test and validate inbound XML files.	EDGE Server Validation Schema Data Model	EDGE Server Validation Schema Data Dictionary
EDGE Server Common Validation Schema	The common validation schema contains the reference data required by the validation zone to test EDGE application releases with issuers.	EDGE Server Common Validation Schema Data Model	EDGE Server Common Validation Schema Data Dictionary

EDGE Server File Reports

The EDGE server generates several outbound reports to inform both CMS and the issuer on various aspects of data submissions. With the exception of ad hoc query reports, which are in TXT format, all EDGE server outbound reports are generated in XML format and deposited in either the Outbox directory (OP server) or AWS S3 bucket (AWS server). There are two (2) categories of outbound reports:

- Summary and detail reports are generated each time an ingest file is processed.
- RA, HCRP, RI and analytic reports are generated by remote commands sent out by CMS and run by issuers.
 - Issuers can generate select RA, HCRP, RI and analytic reports through local commands. Please see Appendix G: EDGE Server Reports and Local Commands in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands](#) for a complete list.

XSD and Example XML Files

The input and output files will be transmitted using XML with predefined XSDs as described in the ICD. There are two (2) kinds of primary transactions across the EDGE server interface - inbound data submission files and outbound data files that contain both detail and summary reporting data. The [EDGE Server XML XSD Zip File Contents Job Aid](#) provides the breakdown of the list of XML/XSD for inbound and outbound reports. The following zip files contain example files for [XML/XSD Outbound Files](#) and [XML/XSD Inbound Files](#) that provide the structure and layout of the files.

Section 3 - Provisioning & Set Up

This section provides an overview of the EDGE server options and the EDGE Server Management (ESM) console used to create server requests, provision a server, and view reports, among other basic EDGE actions. In addition, this section provides steps on how to set up an AWS or OP server, as well as how to migrate servers after provisioning.

3.1 EDGE Server Options

Issuers have the flexibility to select either an AWS or OP server. The below key points of consideration are provided to help guide an organization in choosing the best EDGE server option based on its needs.

Table 3-1: AWS & OP Considerations

Considerations	AWS	OP
Server Set-up	Automated	Manual
Hardware Requirements	None	Server
Software Requirements	Operating System included in Amazon server purchase	Issuer purchases Operating System license, see Section 3.3.1: Server Setup for more details
Security	Shared Responsibility between Amazon and issuers	Issuer-Owned
Infrastructure	Leverages Amazon's existing infrastructure	Issuer provided based on CMS specifications
Scalability	Additional capacity available	Dependent on issuer capability
Health Insurance Portability and Accountability Act (HIPAA)	Amazon offers HIPAA compliance programs	Issuer is responsible for complying with HIPAA requirements
Costs	Vary based on size of server	Vary based on needs of issuer. Issuers also need to purchase necessary operating system and other software.

3.2 EDGE Server Management Console

ESM is a website that issuers can access through the Health Insurance Oversight System (HIOS). Issuers can use ESM to complete the below activities:

- Register and create a request to provision an EDGE server
- Provision OP and AWS EDGE servers
- View the status of pending or provisioned EDGE server(s) and associated details
- Perform basic EDGE server actions such as acquiring security keys and updating TPA host information
- View annual RA and RI payment reports
- Initiate the Prod to Test and Prod to Validation Copy Feature

- Refresh Plan Data

3.3 Server Set-Up - On-Premise

The following process flow guide provides the order of steps that issuers need to complete in order to provision an OP EDGE server.



Figure 3-1: OP Server Set Up

3.3.1 Server Setup

This section provides an overview of the technical guidance and specifications for pre-configuration of your OP EDGE server. The OP EDGE server can be set-up on physical hardware, on a virtual server farm or in another cloud provider's space. Issuers have the option of choosing between a physical or virtual server (a virtual cloud provider, other than Amazon, may be used for OP deployment).



Note: Issuers are required to set-up one (1) server per HIOS Issuer ID. Issuers are not permitted to configure the deployment properties file to allow multiple HIOS Issuer IDs on a single server instance. Attempting to deploy property files to multiple servers will result in significant risks related to maintenance updates and program calculations. Issuers will be responsible for such risks and any consequences that may result in a failure to meeting submission deadlines or inaccurate calculations. Issuers have the option to use a hypervisor to create multiple virtual instances on a single physical server (e.g. VMWare, Xen, and Microsoft). This section focuses on configuration of a physical server, but Issuers electing to use virtual servers should follow the same set-up procedures.



Note: Please do not copy commands to the command line directly from this document to avoid execution errors caused by Windows End of Line Conversion. Issuers can either type the commands in the command line or copy commands from this document to NotePad or TextPad, then copy it to the command line.

- Copy the entire installApplication.sh command into a text editor (Ex. NotePad++).

Ensure EOL is Unix and then copy it back to the Linux terminal.

The following table provides examples of hardware server configuration specifications based on organization size:

Table 3-2: Server Configuration Based on INTEL CPUs

Metric	Small	Medium	Large
Number of Enrollees	1,000,000	5,000,000	20,000,000
Claims Processing Throughput per hour	500,000	1,000,000	2,000,000
Processor	2 x 4-Core	2 x 8-Core	4 x 8-Core
Memory	8 GB	16 GB	64 GB
Recommended Storage	1.4 TB RAID 5 (OS and Data)	200 GB RAID 0 or 1 (OS) 6 TB RAID 5 (Data)	200 GB RAID 0 or 1 (OS) 10 TB RAID 5 (Data)

Refer to the table above for recommended volume storage allocation. Depending on the server size, it is recommended to have 100 gigabyte (GB) allocated for the root mount. The remaining storage can be allocated to the EDGE home directory (/opt/edge) and MySQL data storage (/var/lib/mysql).

Issuers can also use the [EDGE Server Storage Calculator](#) to approximate the size of the server needed to establish an EDGE server. The estimates produced in this spreadsheet give a rough order of magnitude set of assumptions that may guide issuers in their purchase of a server of adequate processing power and storage capacity to support ongoing operations. An issuer may adjust the volume assumptions based on knowledge of claims and/or enrollee patterns.

Ultimately, it is up to the issuer's organization to comply with their internal enterprise policies regarding data storage.

OP EDGE Environment Setup & Configuration

1. Issuers must install and configure their OP EDGE server with the following software:



Note: OP issuers are responsible for downloading and installing this software on their own. OP issuers are also responsible for preparing their internal system administrators and IT staff for setting up and maintaining the above systems and databases.

- Red Hat Enterprise Linux (RHEL) version 7.3 (64 bit)
 - A RHEL subscription is not version specific. Once a subscription has been purchased, customers have access to currently supported versions based on the RHEL Life Cycle. The RHEL Life Cycle is available [here](#).
 - Subscription available for purchase [here](#).
 - Issuers may choose to procure RHEL through their own software vendors.
 - While RHEL 7.3 is the currently supported version, issuers do not need to request approval from CMS to apply Linux 7.3 patches to EDGE servers. These patches will not impact EDGE server functionality. Example patches include kernel patches, security fixes, tools, etc.

Refer to Section 3.5: EDGE Server Application and Software Stack Version Updates in the [EDGE Server Operations & Maintenance Manual \(O&MM\) – Backup & Maintenance Procedures](#) for additional information

- MySQL version 5.7.16
 - Available for download [here](#).
 - Issuers have the option of purchasing MySQL server support.
 - Issuers may opt for the free or paid version of MySQL.
- Oracle Java version 1.8
 - Available for download [here](#).

Note: If you see the screen in the below figure, you will need to perform the following actions:

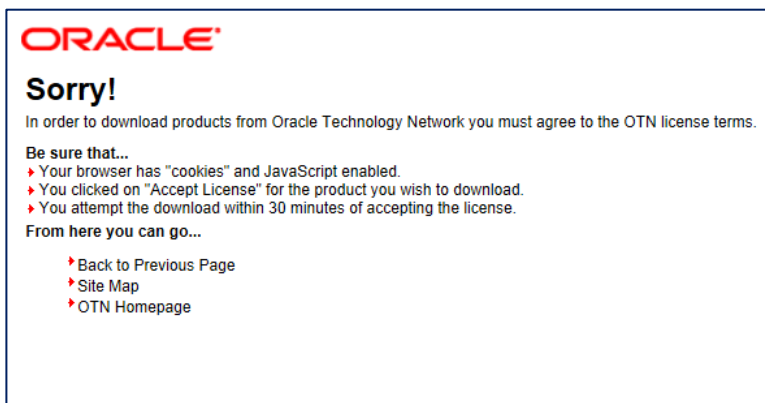


Figure 3-2: Oracle Java Download Page

1. Log into your server using PuTTY. You may download PuTTY [here](#).
2. Open PuTTY and login using your server's Internet Protocol (IP) address.
3. Enter the following command:

```
a. wget --no-cookies --no-check-certificate --header "Cookie:
    gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie"
```

Oracle Java should download after executing this command.

4. Issuers may choose to install additional software (monitoring, antivirus, IDS/IPS, etc.) as required by your company's policies.
5. The environment variable, JAVA_HOME, should be configured to point to the directory where Java is installed.
6. Configure users
 - a. Login as **root** and create user "**edgeadm**".
 - b. Login as system admin and run command:
 - `useradd edgeadm`
 - c. Enter username **edgeadm**
 - d. Enter command

```
• passwd edgeadm
```

- e. Then enter a password
- f. Ensure the “**edgeadm**” user have read/write/execute access for “**/opt/edge**”. The next steps will configure user “**edgeadm**” to have sudo access.
- g. Connect to EDGE server as user who has sudo access or as root
- h. Run the following command to open up **/etc/sudoer** file, which contains the user ID and groups that have sudo access
 - `sudo visudo`
- i. Navigate to the end of the file
- j. Insert line
 - `"edgeadm ALL=(ALL) ALL"`
- k. Save and exit out of vi by pressing the ESC key then the command
 - `:wq`
- l. For more information, please access the [Red Hat Customer Portal](#).

OP EDGE Server Connectivity

Enable AWS Connectivity

The issuer network team must enable connectivity to AWS S3 services. The table below provides the AWS S3 endpoint for connectivity.

Table 3-3: AWS S3 Endpoints

AWS Service	URL	Protocol	Required
S3	s3.amazonaws.com	HTTPS	All servers

OP EDGE servers must be able to connect to CMS’ AWS S3 bucket as part of file processing once you have provisioned your server and verified it is running. As part of the initial setup of your OP EDGE server, there is a command that can be executed in PuTTY (or Secure Shell [SSH] client of your choice) to verify connectivity to CMS’ AWS S3 bucket.

Please execute the following command to test connectivity:

1. Log into PuTTY (or SSH client of your choice)
2. Run the following command:
 - a. `curl https://s3.amazonaws.com/connectivity.test/connectionSuccessful.txt`

If the connectivity test is successful, you will receive a status code = 200.

If the connectivity test fails, you will receive one (1) of the following error codes:

- **403 - Access Denied:** this could happen if the proxy server has missing credentials.

Resolution: Provide proxy credentials as the URL parameter (refer to curl documentation for proxy parameters: `curl -x PROXY-SERVER:PORT -U USER:PASS URL`)

- **404 - URL not found:** this could happen if your Dominion Name System (DNS) server is unable to resolve the host name to IP address for AWS services.

Resolution: Work with your DNS administrator or service provider to resolve.

Verify MySQL Connectivity

Issuers must enable connectivity to MySQL from the server where the EDGE application will be installed. The EDGE installation program creates the user and the schemas that are required by the EDGE application to operate.

In order for the EDGE installation to work, the Database Administrator (DBA) requires access to the MySQL server.

The required DBA access can be configured using the following steps:

For MySQL located on *same* server as the EDGE application

1. Connect to server as “**edgeadm**”
2. Run the following command to verify if root account has connectivity to MySQL without a password.

```
a. sudo mysql
```

If you are unable to connect to MySQL without a password, this indicates you have a separate MySQL DBA account that is required. The DBA account may be the root account with a different password.

3. Run command:

```
b. mysql --user=<DBA USER ID> -p
```

This will prompt the user to enter a password and log into MySQL to verify connectivity. These will be the credentials that will be used by the EDGE installation program.

For MySQL located on a *different* server from EDGE application

1. Connect to server as “**edgeadm**”
2. Run command:

```
c. mysql --host=<MySQL Server Name/IP Address> --port=<MySQL Server Port> --user=<DBA User ID> -p
```

This will prompt the user to enter a password and log into MySQL to verify connectivity. These will be the credentials that will be used by the EDGE installation program.

File Directories

The inbound and outbound directory will be defaulted to the following directories:

- /opt/edge/ingest/inbox
- /opt/edge/ingest/outbox
- /opt/edge/ingest/archive
- /opt/edge/ingest/logs

Issuers may update the directories to configure to point to the directory paths of their choosing.

Server Hardening

Issuers will need to harden their OP server according to their own organization's standards.



Note: The OP server installation script does NOT include a hardening script. OP server issuers should perform their hardening scripts after provisioning has been completed and confirmed.

3.4 Server Set-Up - AWS

The AWS EDGE server is a cloud server provisioned by Amazon Web Services. The following process flow provides the order of steps that issuers need to complete in order to provision an Amazon EDGE server.



Figure 3-3: AWS Setup Flow

3.4.1 AWS Account Setup

This section provides an overview of the steps Amazon EDGE server issuers must take to establish an AWS account.



Note: AWS updates the user interface for the website often. Although the below figures may change, the steps are accurate.

In addition to the instructions in this section, an Amazon developed YouTube video on “Creating an Amazon Web Services Account” is accessible via the following link:

<https://www.youtube.com/watch?v=WviHsoz8yHk>



Note: A new AWS account must be created for each issuer EDGE server to be provisioned.

In addition, in the event an issuer must transfer hosting to or from a TPA, ownership of the AWS account must be transferred as well. The steps to complete a server migration is provided in more detail in [Section 3.9: Migration](#).

1. Go to [AWS](#) and click the **Sign Up**.

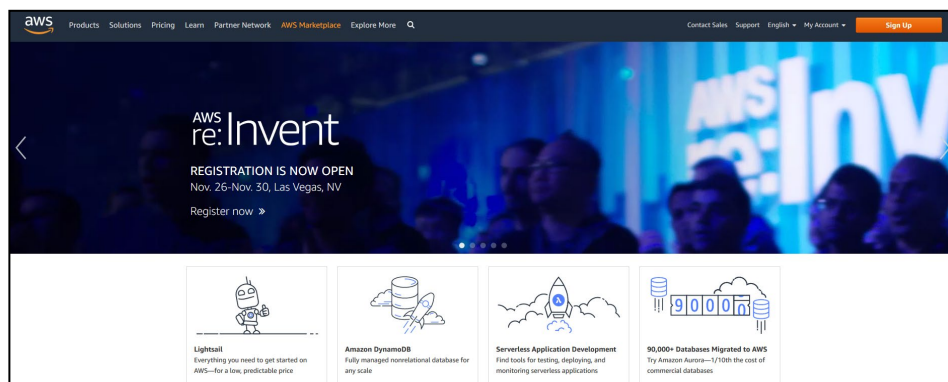


Figure 3-4: Amazon Web Services

2. On the next page, complete the following:
 - a. Enter an email address
 - b. Enter your password
 - c. Enter your password a second time
 - d. Enter your AWS account name and click **Continue**

The image shows the 'Create an AWS account' screen. On the left, it says 'AWS Accounts Include 12 Months of Free Tier Access' and lists services included: Amazon EC2, Amazon S3, and Amazon DynamoDB. It also mentions 'Visit aws.amazon.com/free for full offer terms'. On the right is a form with the following fields: 'Email address' (with 'test@email.com' entered), 'Password', 'Confirm password', and 'AWS account name' (with a help icon). Below the form is a yellow 'Continue' button. At the bottom of the form area is a link: 'Sign in to an existing AWS account'. At the very bottom of the screen is copyright information: '© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy' and 'Terms of Use'.

Figure 3-5: AWS Create Account Screen

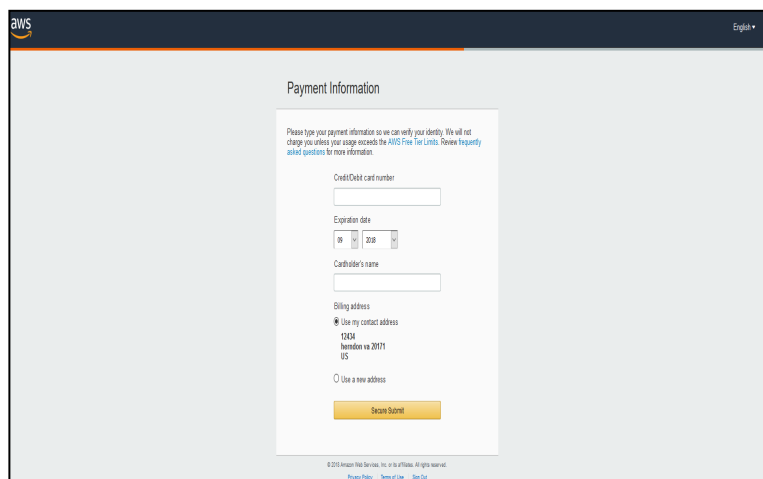
3. At the **Login Credentials** screen, click on **Create a new AWS account**.

Figure 3-6: Create a New AWS Account

4. The **Contact Information** page should appear. Enter your Contact Information, complete the Security Check, and read and agree to the terms of the Amazon Web Services Customer Agreement.

Figure 3-7: Enter in Contact Information

5. Enter payment information on the **Enter Your Payment Information** section of the screen and then **Enter Your Billing Address**.



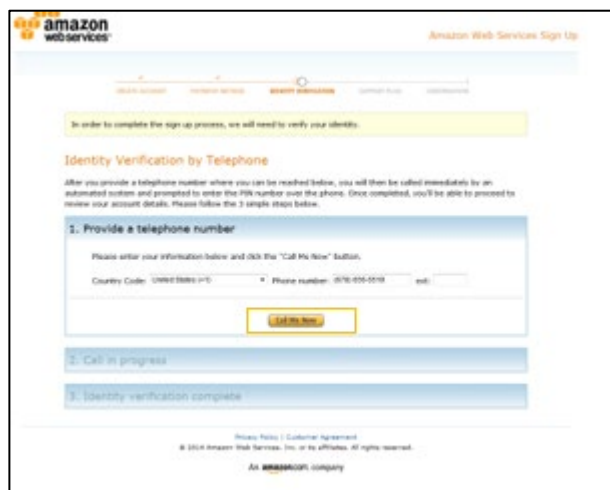
The screenshot shows the AWS 'Payment Information' form. At the top, it says 'Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the AWS Free Tier Limits. Review frequently asked questions for more information.' Below this, there are fields for 'Credit/debit card number', 'Expiration date' (with month and year dropdowns), and 'Cardholder's name'. Under 'Billing address', there are two radio buttons: 'Use my contact address' (which is selected) and 'Use a new address'. The 'Use my contact address' option shows '12345', 'helloworld@2017', and 'US'. A 'Secure Submit' button is at the bottom. The footer includes '© 2017 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy', 'Terms of Use', and 'Sign Out'.

Figure 3-8: Enter in Payment Information



Note: Issuers will not be billed at this point in time and will only be billed if they choose to purchase additional AWS support or functionality. Issuers may choose to work with AWS to convert their account to an invoicing method. Charges will begin when the Amazon EDGE server is on and operating. However, all AWS accounts are started with a credit card.

6. Enter the phone information and click **Call Me Now**.



The screenshot shows the 'Amazon Web Services Sign Up' page for 'Identity Verification by Telephone'. It includes a progress bar with steps: 'Create account', 'Verify identity', 'Select a payment method', 'Complete sign-up', and 'Account created'. The current step is 'Verify identity'. Below the progress bar, it says 'In order to complete the sign-up process, we will need to verify your identity.' The section 'Identity Verification by Telephone' explains that after providing a telephone number, the user will be called by an automated system to enter a PIN. It lists three steps: '1. Provide a telephone number', '2. Call in progress', and '3. Identity verification complete'. Step 1 includes a form with 'Country Code' (set to 'United States (+1)'), 'Phone number' (with a sample '576-555-0198'), and an 'Add this phone' button. The footer contains 'Privacy Policy | Customer Agreement', '© 2017 Amazon Web Services, Inc. or its affiliates. All rights reserved.', and 'An Amazon.com company'.

Figure 3-9: Provide a Telephone Number

A PIN will be displayed on the issuer's screen. AWS will call the number provided and ask for the PIN displayed. Enter the PIN when prompted.

Figure 3-10: Identity Verification PIN

7. Click **Continue** to complete identity verification.

Figure 3-11: Click Continue to Complete Identity Verification

8. Select a support plan and then click **Continue**.



Note: Issuers must select a support plan. AWS customers can change their level of support at any time should their support needs change.

Figure 3-12: Select your AWS Support Plan

9. You are now registered for an AWS Account!



Figure 3-13: AWS Account Set-Up Complete



Note: Issuers who require more than 20 servers must request a service limit increase from AWS so that their server can be provisioned by CMS at the desired size. Please see Section 3.1.3: Storage Requirements in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – Configuration, Validation & Application Errors](#) document for more information. Since it typically takes AWS 48 hours to process these requests, issuers will need to complete this step prior to requesting an AWS EDGE server. For issuers who need more than 20 EDGE servers, it is highly recommended that the service increase request be submitted to AWS when you are at 18 instances, in order to allow a few extra instances without hitting the 20 instances limit.

3.4.2 Request an AWS EDGE Server Instance

This section provides the steps issuers who wish to provision an Amazon EDGE server must take prior to registering their Amazon EDGE server with CMS through the EDGE Registration site. The steps provided should be performed after setting up an AWS account.

Locate Account Number

1. Log into the AWS Account previously created.
2. Click on the **User Name Dropdown** in the upper right corner of the screen and choose **My Account**.

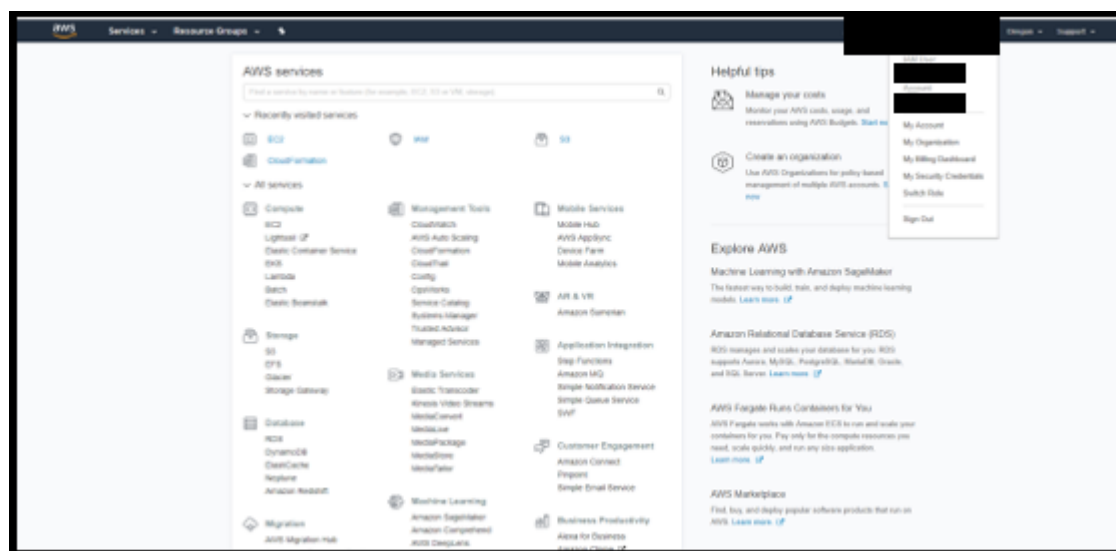


Figure 3-14: AWS My Account

3. Make a note of the Account ID under the Account Settings section at the top of the screen.

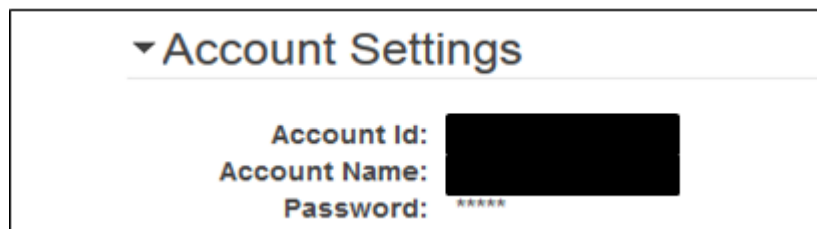


Figure 3-15: Account Settings

Create EDGE Installer Role

4. Click on **Services** in the upper left corner of the screen, click on **All AWS Services** and then click on **IAM**.

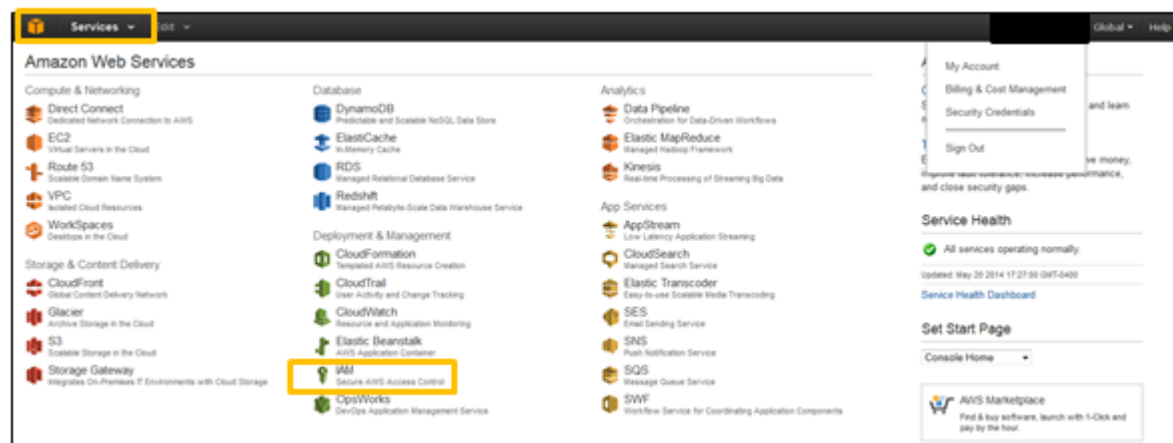


Figure 3-16: AWS Homepage with Services Dropdown

5. Select **Roles** from left navigation bar



Figure 3-17: Select Roles

6. Click on **Create New Role** at the top.



Figure 3-18: Create New Role Button

7. Enter “**EdgeInstaller**” in the text box and select **Continue** button.

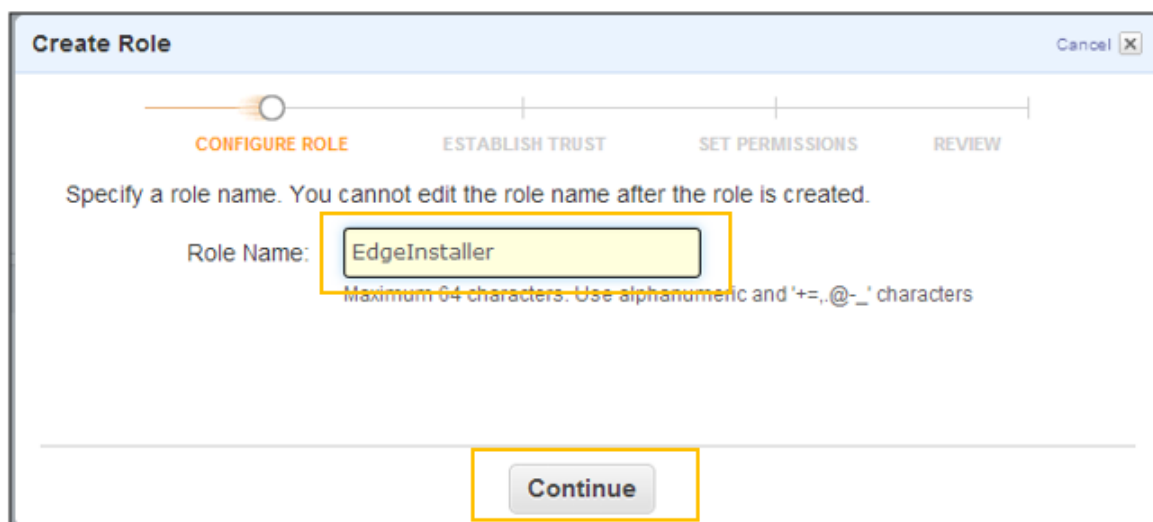
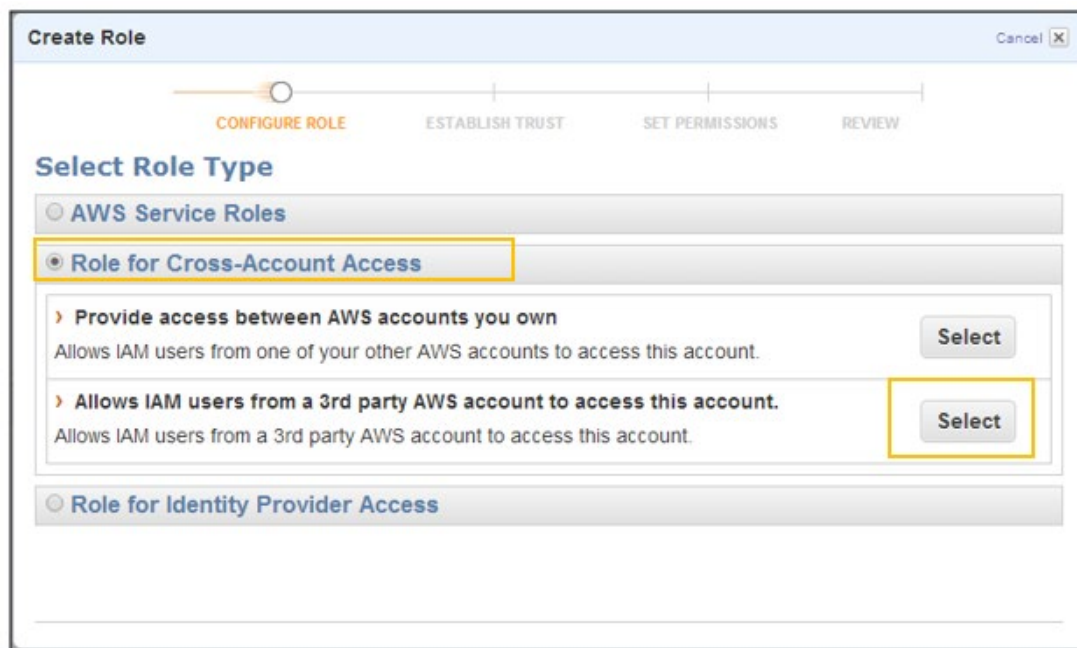


Figure 3-19: Configure Role Window

8. In the next window select, **Role for Cross-Account Access** option.
9. Click the **Select** button for the option: **Allows IAM users from a 3rd party**

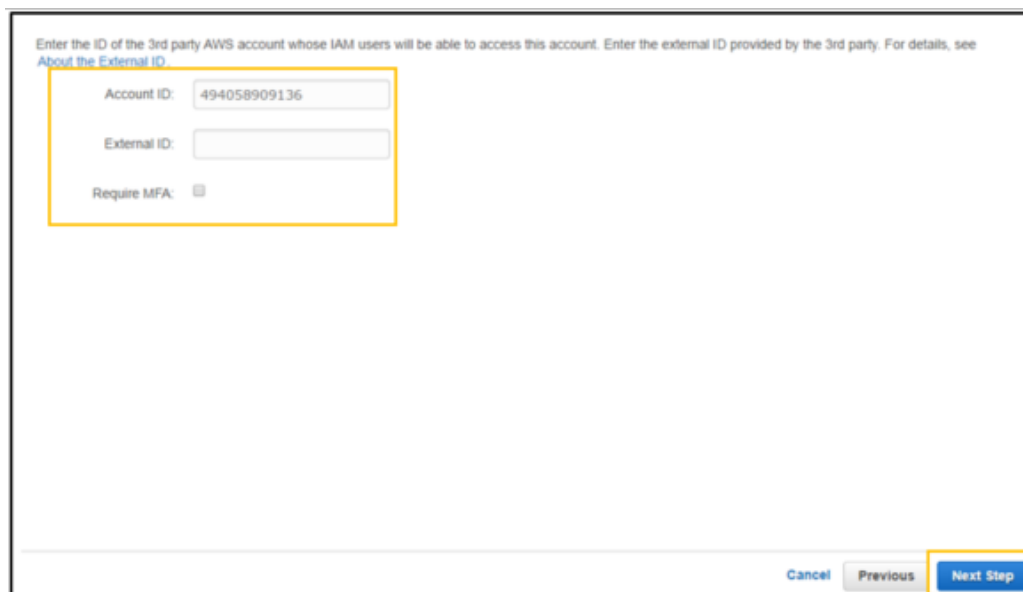
AWS account to access this account.



The screenshot shows the 'Create Role' wizard in the AWS IAM console. The progress bar at the top indicates the current step is 'CONFIGURE ROLE'. Under 'Select Role Type', the 'Role for Cross-Account Access' radio button is selected. Below this, two options are listed: 'Provide access between AWS accounts you own' and 'Allows IAM users from a 3rd party AWS account to access this account.' The second option is highlighted with a yellow box, and its 'Select' button is also highlighted with a yellow box.

Figure 3-20: Select Role Type

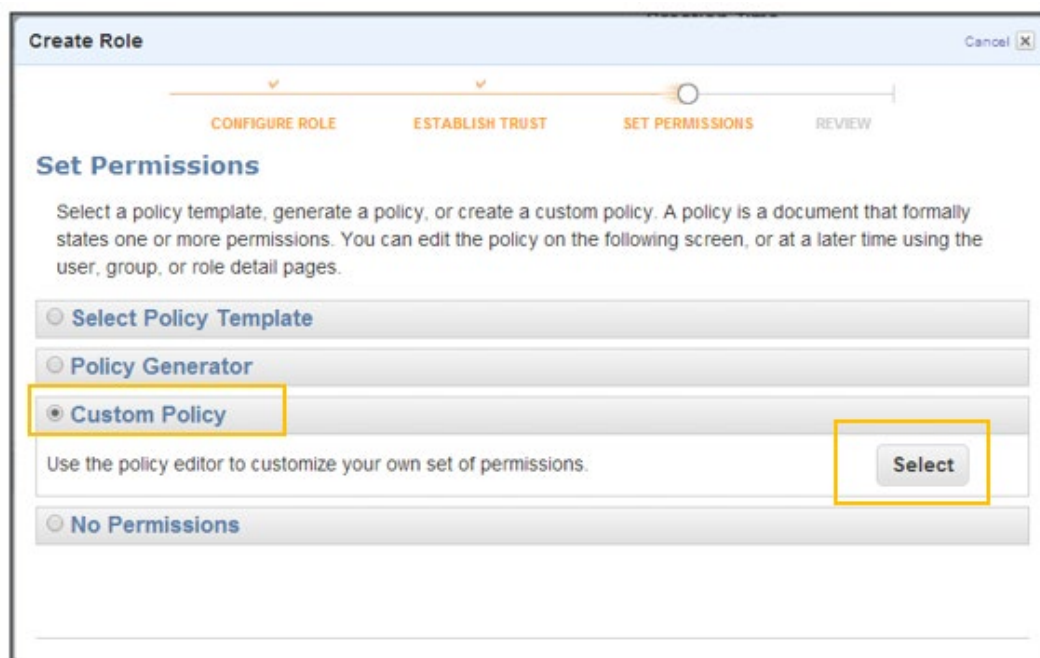
10. In the next window **<CMS Account number>** from **Account Settings** in the **Account ID** text box and your account ID in **External ID**. Click on **Next Step**.
Note: **494058909136** was used as the example CMS Account Number



The screenshot shows the 'Enter Account IDs' step in the AWS IAM console. The 'Account ID' field is populated with '494058909136'. The 'External ID' field is empty. The 'Require MFA' checkbox is unchecked. The 'Next Step' button at the bottom right is highlighted with a yellow box.

Figure 3-21: Enter Account IDs

11. Select **Custom Policy** and click **Select**.

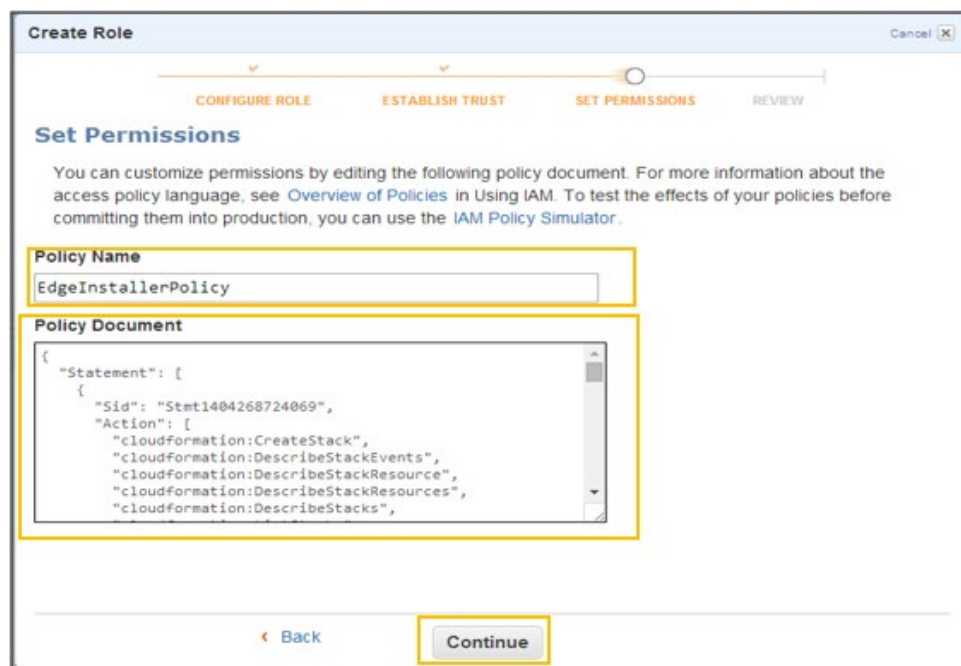


The screenshot shows the 'Create Role' wizard with the 'Set Permissions' step selected. The 'Custom Policy' option is chosen, and the 'Select' button is highlighted. The text below the options reads: 'Use the policy editor to customize your own set of permissions.'

Figure 3-22: Set Permissions - Custom Policy

12. Enter “**EdgeInstallerPolicy**” in the **Policy Name** field.
13. In the **Policy Document** text box, copy/paste the text inside the EDGE Installer Policy document. Once finished, click **Continue** button.

The EDGE Installer Policy Data is posted in Appendix A: Installer Policy Data in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – Configuration, Validation & Application Errors](#).



The screenshot shows the 'Create Role' wizard with the 'Set Permissions' step selected. The 'Policy Name' field contains 'EdgeInstallerPolicy' and the 'Policy Document' text box contains the following JSON policy document:

```
{
  "Statement": [
    {
      "Sid": "Stm1404268724069",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ]
    }
  ]
}
```

The 'Continue' button is highlighted.

Figure 3-23: EdgeInstallerPolicy- Custom Permissions

14. Review/Edit the role information if necessary. If correct, select **Create Role**.

Figure 3-24: Final Review Page

Generate Key Pair

A Key Pair will be used to establish connection to the AWS EDGE instance. This Key Pair File must be secured and accessible to execute the provisioning process.

When Amazon EC2 key pairs are generated by AWS, both the private and public key of the RSA key pair are presented. **You must download and store the private key of the Amazon EC2 key pair in a secure location such as an S3 bucket that has a least privilege policy.** Ultimately, issuers should store the key pair in accordance with their organizations security policy.



Note: AWS does not store the private key. CMS cannot obtain your key pair. If the key pair is lost, you will not be able to sign into your EDGE server.

The same Key Pair can be used for multiple EDGE server instances in the same region but all instances **MUST** be in same region. If an EDGE server instance is in a different region, a separate Key Pair is required for each instance.

15. On the AWS home page, click on **All AWS Services**, and then click on **EC2**.

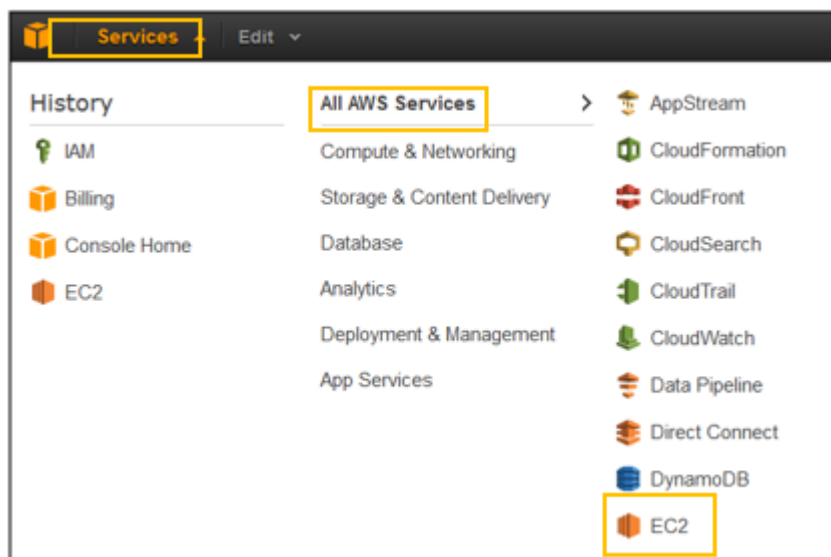


Figure 3-25: Services Dropdown with All AWS Services Selected

16. Click on **Key Pairs** on the left side of the screen.

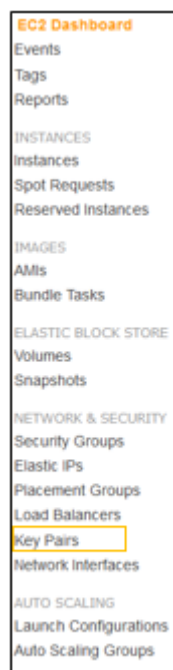


Figure 3-26: EC2 Dashboard Options

17. Issuers will now click **Create Key Pair** button.



Figure 3-27: Create Key Pair

18. Name the key pair **“EdgeServer”** and then click **Create** button.



Figure 3-28: Create Key Pair Name

19. A pop-up window will appear to either **Save the File** or **Open it**.

You **MUST** save the file at this point in time and should keep the file saved on their computer.

A Key Pair Name has been created.



Note: If the key pair file is lost, you will be unable to connect to the server. Neither CMS nor AWS will be able to retrieve the key pair and your server will need to be re-provisioned.

3.5 HIOS ESM Roles

All users must register for a HIOS Issuer ID and/or a Company. The user's role will dictate the level of access in the ESM. Please note, a user may not register for issuer and TPA roles at the same time.

The following roles are available for issuers and TPAs. The sections that follow include the steps for assigning these roles for an organization.



Note: Issuers acting as a TPA must identify themselves in HIOS as an EDGE server TPA by editing their organization in HIOS.

Issuer EDGE Registration Request Submitter

- Submits and manages EDGE server registration requests
- Retrieves provisioning scripts/EDGE installation kit

Issuer EDGE Registration Request Approver

- Approves EDGE server registration requests
- Responsible for viewing the RA and RI payment reports

TPA EDGE Registration Request Submitter

- Enters EDGE Server details when selected and approved by an issuer
- Retrieves provisioning scripts/EDGE installation kit



Note: Only HIOS users that have the Issuer EDGE Registration Request Approver role will be able to view reports uploaded to the ECM. Issuer Submitters and TPAs will not be able to access or view payment reports.

All TPAs:

- All TPAs must register for an organization HIOS Issuer ID or a Company (FEIN/TIN).
- TPAs must then request in HIOS an EDGE server user role:
 1. TPA EDGE Registration Submitter
 - a. Role that updates EDGE server requests with TPA details

Amazon EDGE Server Issuers/TPAs:

1. Register for an AWS Account (select support level).
2. Request a Business Associate Agreement (BAA) by sending an email to: aws-edge@amazon.com.
3. Contact Amazon to set up alternate payment options.

OP EDGE Server Issuers/TPAs:

- Obtain and configure OP server:
 1. Choose physical or virtual server.
 2. Install and configure software.
 - a. OP server provisioning steps can be found in [Section Figure 3-24: OP Server Set Up](#)
 - b. [3.3.1 Server Setup](#). Latest software requirements for Red Hat Enterprise Linux, MySQL, and Oracle Java can be found in Section 3.5: Server Application and Software Stack Version Updates in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – Backup & Maintenance Procedures](#).
 3. Configure firewall rules.
 4. Set up file directories.

HIOS Role Management General Guidelines:

- Each HIOS user account can only have one (1) role assigned to it.
- If you are registered in HIOS but do not have an assigned EDGE server user role, you can simply request to have the appropriate role.
- The Issuer EDGE Registration Request Submitter, Issuer EDGE Registration Request Approver and TPA EDGE Registration Request Submitter roles cannot be assigned to the same HIOS user.
- If you have an existing EDGE server role assigned to your account in HIOS (e.g., Issuer EDGE Registration Request Submitter role), you will not be able to request a second role.
- In order to reassign a role, you will need to delete the Issuer EDGE Registration Request Submitter role from your HIOS account in order to request the Issuer EDGE Registration Request Approver role.



Note: Issuers who need assistance with obtaining, deleting or editing HIOS IDs or EDGE roles should contact the CMS Help Desk at CMS-855-1515 or CMS_FEPS@cms.hhs.gov.

3.5.1 Assigning an EDGE Server Role to HIOS User

The following steps will provide issuers and TPAs guidance on how to assign a HIOS ESM Role to their username.

All issuers and TPAs will need to first access the HIOS portal through the [CMS Enterprise Portal](#) to then access the EDGE Registration site.

1. First, navigate to the CMS Enterprise Portal homepage at <http://portal.cms.gov>. If you are a new user, create a user using the **New User Registration** button. For existing users, enter your HIOS User ID and Password on the login screen. Read the **Terms and Conditions**, and then click the **Agree to our Terms & Conditions** button. Then click the **Login** button.

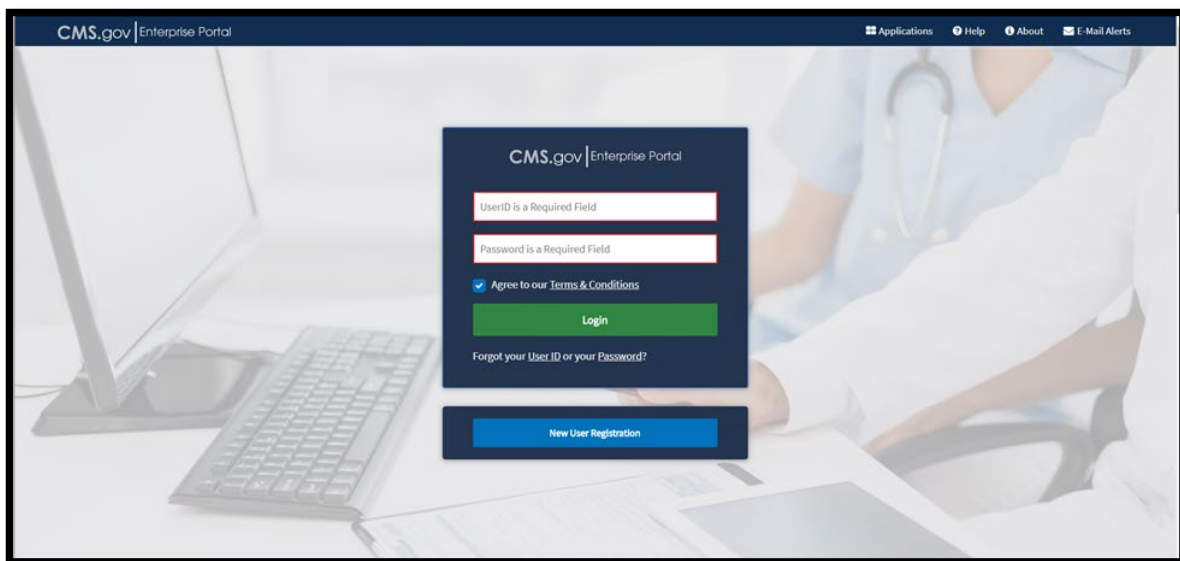


Figure 3-29: CMS Enterprise Portal Homepage, Login, and Terms and Conditions

2. Select a Multi Factor Authentication (MFA) Device Type to verify your identity through the MFA process. After receiving the code through a secondary device, enter the security code and click the Log In button.

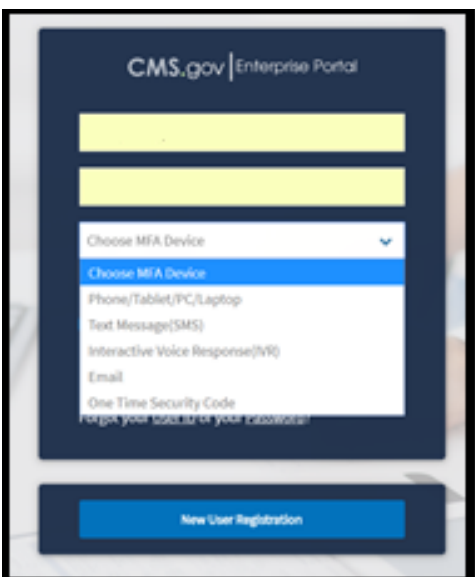


Figure 3-30: MFA Security Code

From the portal homepage, click the **HIOS** button. Then click **Overview**.

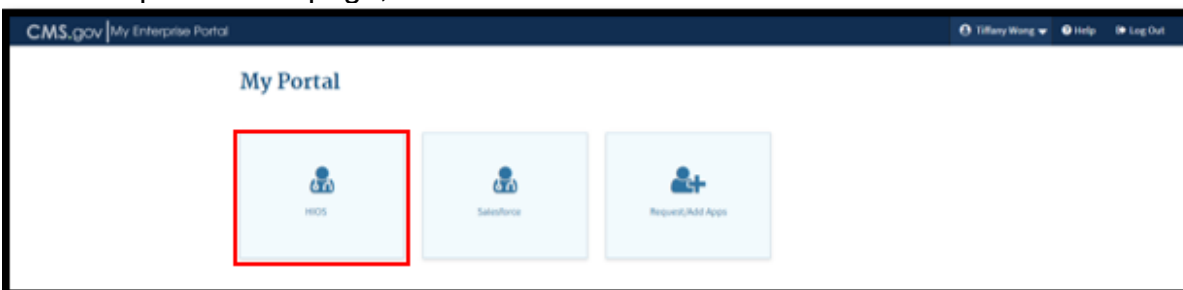


Figure 3-31: HIOS Button

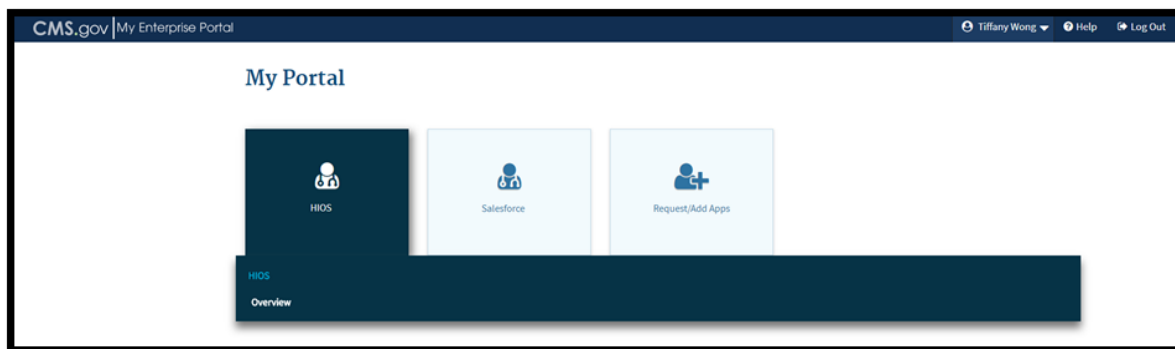


Figure 3-32: HIOS Button (Expanded Menu)

3. Under the **Plan Management and Market Wide Functions** section, click the **Access Plan Management and Market Wide Functions** link.

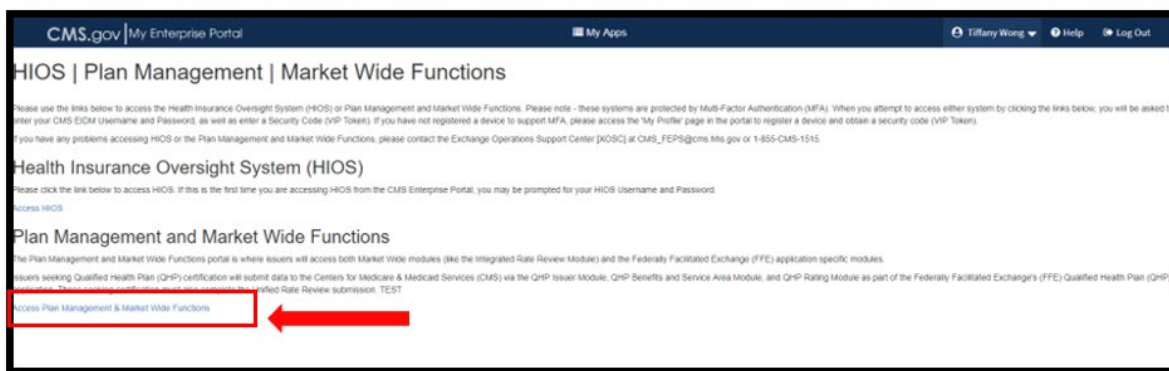


Figure 3-33: Access Plan Management & Market Wide Functions Link

4. Read the **Terms of Use** and then click the **Accept** button.

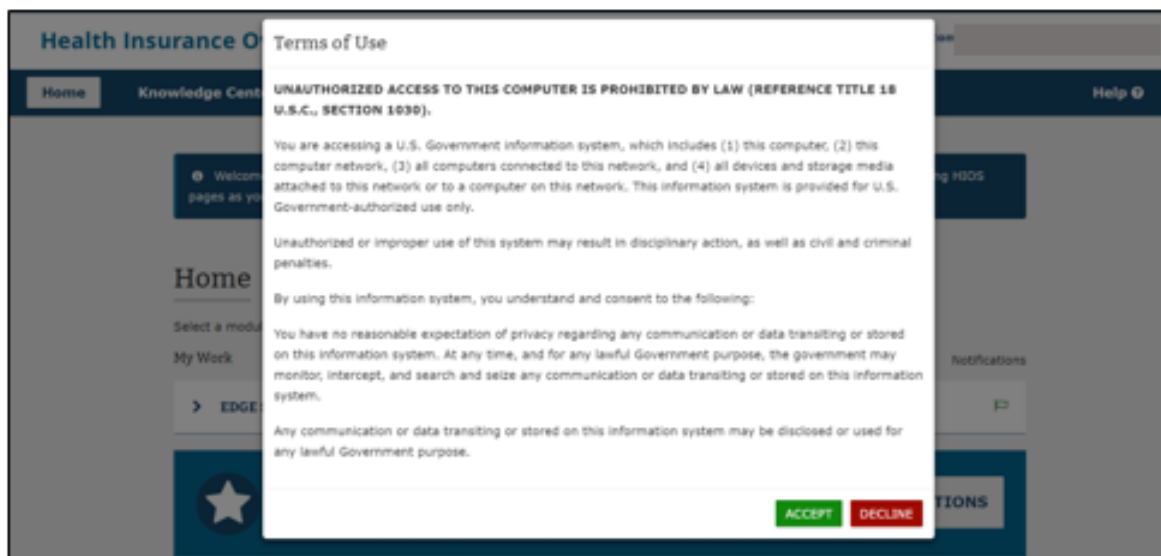


Figure 3-34: Terms of Use

5. After logging in, click on your username and then click the **Manage Roles** tab.

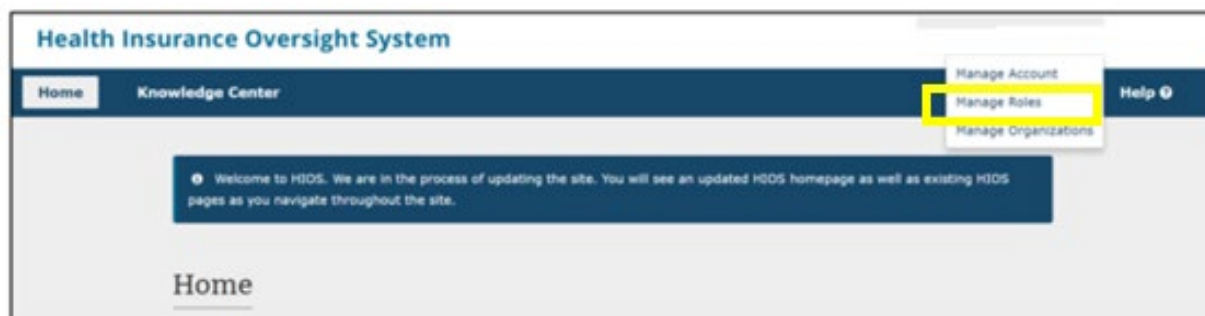


Figure 3-35: Manage Role Tab

6. Click the **Add a new role** tab at the top of the page.

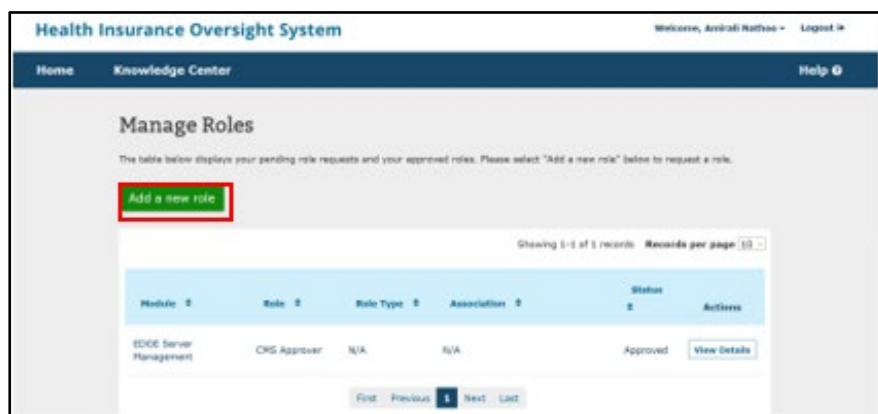


Figure 3-36: Request Role Tab

7. Select **EDGE Server Management (ESM)** and click **Next**



Figure 3-37: EDGE Server Management (ESM)

3.5.1.1 Issuer EDGE Registration Request Submitter or Issuer EDGE Registration Request Approver role

- Select **Issuer EDGE Registration Request Submitter** or **Issuer EDGE Registration Request Approver** role and click **Next**

Home Knowledge Center Help

Request a Role

Please note, a field with an asterisk (*) before it is a required field. For a detailed description of each module and available roles, please visit the [Browse by Module](#) page in the Knowledge Center.

Please note, you must first have an organization registered in HIOS in order to request access to a module.

- 1 Select a module EDGE Server Management [Revisit this step](#)
- 2 Select a role
* Please select the role below:
☐ Issuer EDGE Registration Request Submitter
☐ TPA EDGE Registration Request Submitter
☒ Issuer EDGE Registration Request Approver
[NEXT](#)
- 3 Add association
- 4 Confirm your request

Figure 3-38: Issuer EDGE Registration Request Approver Role

- b. Enter the **HIOS Issuer ID** to which the Issuer EDGE Registration Request Submitter/Issuer EDGE Registration Request Approver role will be associated. Click **Search** to confirm/process the Issuer ID.

1 Select a module EDGE Server Management [Revisit this step](#)

2 Select a role Issuer EDGE Registration Request Approver [Revisit this step](#)

3 Add association

To add an Association to this role request, you must search for it in the system.

* Association Type
* **HIOS Issuer ID**

* Search for association

Please enter the HIOS Issuer ID below and select the Search button. Once an Issuer is found, select the "Add" button to associate the Issuer to the role. The HIOS Issuer ID must be a 5 digit, numeric value. You must add at least 1 Issuer and may add up to 10 Issuers per submission.

99999 [SEARCH](#)

[NEXT](#)

0 ITEMS ADDED TO REQUEST

Figure 3-39: Enter Issuer ID

- c. If all the information entered is correct, click the **Add** button to process the request, and then click **Next**.

3 Add association

To add an Association to this role request, you must search for it in the system.

* Association Type
* HIOS Issuer ID

* Search for association
Please enter the HIOS Issuer ID below and select the Search button. Once an issuer is found, select the "Add" button to associate the Issuer to the role. The HIOS Issuer ID must be a 5 digit, numeric value. You must add at least 1 Issuer and may add up to 10 Issuers per submission.

84639 SEARCH

Showing results for "84639"

84639 - Amin Agha (HI) Add

0 ITEMS ADDED TO REQUEST

NEXT

Figure 3-40: Review/Continue Button

- d. On the next page, you will be able to review the role request a final time before submitting. If all the information is correct, click the **Submit** button.

4 Confirm your request

Please select "Submit" to complete your request.

MODULE
EDGE Server Management

ROLE
Issuer EDGE Registration Request Submitter

ASSOCIATIONS
HI 84639

SUBMIT RESET

Figure 3-41: Submit Request

- e. After submitting the request, you will be taken to a confirmation page confirming the request has been submitted for CMS approval.

View Existing Role Request Role

Request Role

Confirm
Your role request has been submitted for approval, please log back in within 1 to 2 business days to check the status of your request.

All fields are required.

Please select a Module from the drop-down list below and follow the prompts to submit a role request. For a description of each module, select [Module Descriptions \(PDF - 835KB\)](#)

Module: --Select Module--

Figure 3-42: Confirmation Page



Note: No email or message will be sent to users when roles are approved. As the confirmation page indicates, approval may take one (1) to two (2) business days.

Users will need to log back into HIOS and access the **Manage Roles** tab in the **Welcome, <username>** dropdown to confirm approval.

From the HIOS site, you can view any existing roles you currently have associated with your HIOS account on the Manage Roles tab.

The screenshot displays the 'Manage Roles' interface in the Health Insurance Oversight System. At the top, there's a navigation bar with 'Home' and 'Knowledge Center' links. A user menu is open, showing options: 'Manage Account', 'Manage Roles', 'Request a Role', and 'Manage Organizations'. The main heading is 'Manage Roles', followed by a brief instruction: 'The table below displays your pending role requests and your approved roles. Please select "Add a new role" below to request a role.' Below this is a green button labeled 'Add a new role'. A table shows one record: 'EDGE Server Management' with role type 'QRBApprover' and status 'Approved'. The table has columns for Module, Role, Role Type, Association, Status, and Actions. A 'View Details' button is next to the role. At the bottom, there are pagination controls: 'First', 'Previous', '1' (selected), 'Next', and 'Last'.

Figure 3-43: View Roles



Note: If you have an existing EDGE server role assigned to your account in HIOS (e.g., Issuer EDGE Registration Request Submitter role), you will not be able to request the Issuer EDGE Registration Request Approver or TPA EDGE Registration Request Submitter role as users can only have one (1) assigned EDGE server role in HIOS.

3.5.1.2 TPA EDGE Registration Submitter role

- a. Select **TPA EDGE Registration Submitter** role and click **Next**.

Request a Role

Please note, a field with an asterisk (*) before it is a required field. For a detailed description of each module and available roles, please visit the [Browse by Module](#) page in the Knowledge Center.

Please note, you must first have an organization registered in HIOS in order to request access to a module.

1 Select a module EDGE Server Management [Revisit this step](#)

2 Select a role

* Please select the role below:

- ☐ Issuer EDGE Registration Request Approver
- ☐ Issuer EDGE Registration Request Submitter
- ☒ TPA EDGE Registration Submitter

[NEXT](#)

Figure 3-44: Request a Role

- b. Enter the **Organization Federal EIN/TIN** to which the TPA EDGE Registration Submitter role will be associated. Click **Search** to confirm/process the Issuer ID. If all the information entered is correct, click **Next**.

1 Select a module EDGE Server Management [Revisit this step](#)

2 Select a role TPA EDGE Registration Submitter [Revisit this step](#)

3 Add association

To add an Association to this role request, you must search for it in the system.

* Association Type

- ☒ Organization with FEIN

* Search for association

Please enter the Organization Federal EIN/TIN below. The Federal EIN/TIN must be a 9 digit, numeric value.

713112233 [SEARCH](#)

Showing results for "713112233"

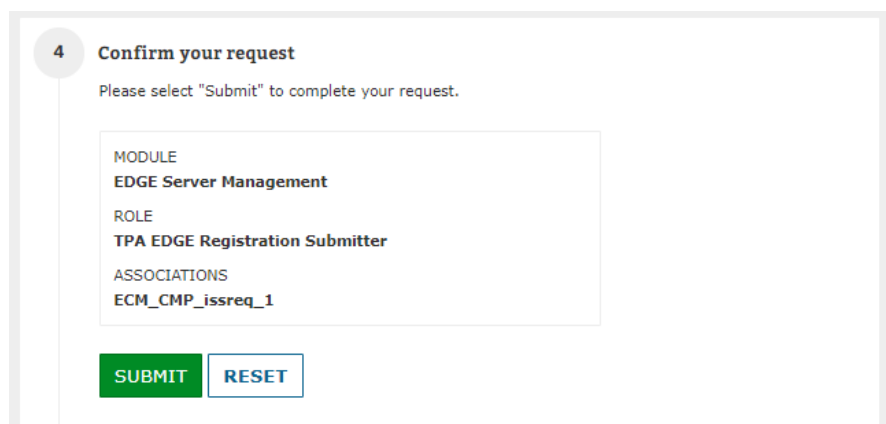
* ASSOCIATION

- ☒ 713112233 - ECM_CMP_issreq_1 (VA)

[NEXT](#)

Figure 3-45: Enter Issuer ID

- c. On the next page, you will be able to review the role request a final time before submitting. If all the information is correct, click the **Submit** button.



4 Confirm your request

Please select "Submit" to complete your request.

MODULE
EDGE Server Management

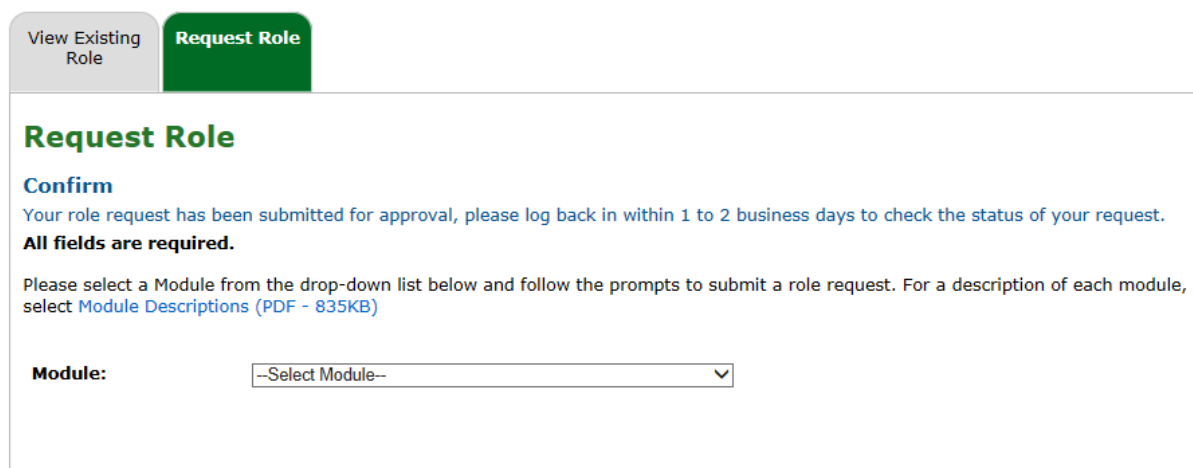
ROLE
TPA EDGE Registration Submitter

ASSOCIATIONS
ECM_CMP_issreq_1

SUBMIT **RESET**

Figure 3-46: Submit Request

- d. After submitting the request, you will be taken to a confirmation page confirming the request has been submitted for CMS approval.



View Existing Role **Request Role**

Request Role

Confirm

Your role request has been submitted for approval, please log back in within 1 to 2 business days to check the status of your request.

All fields are required.

Please select a Module from the drop-down list below and follow the prompts to submit a role request. For a description of each module, select [Module Descriptions \(PDF - 835KB\)](#)

Module:

Figure 3-47: Confirmation Page



Note: No email or message will be sent to users when roles are approved. As the confirmation page indicates, approval may take one (1) to two (2) business days.

Users will need to log back into HIOS and access the **Manage Roles** tab in the **Welcome, <username>** dropdown to confirm approval.

From the HIOS site, you can view any existing roles you currently have associated with your HIOS account on the Manage Roles tab.

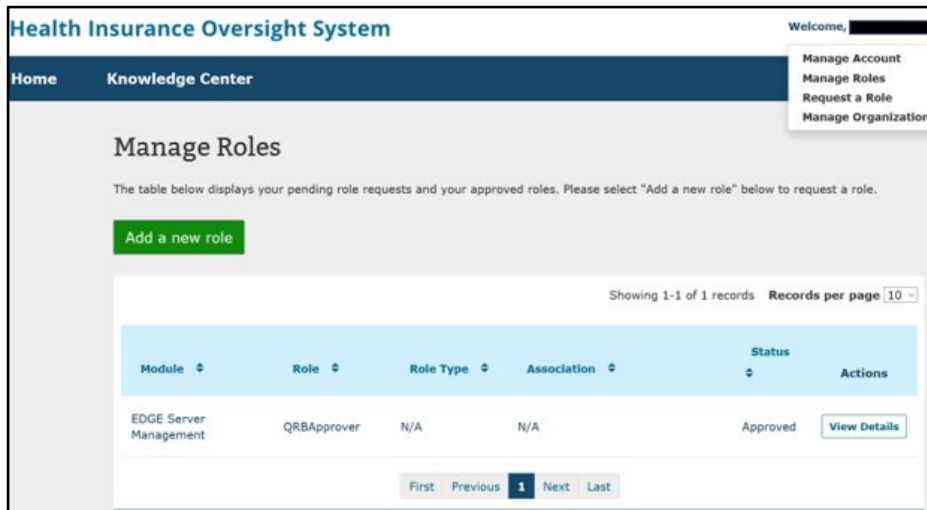


Figure 3-48: View Roles



Note: If you have an existing EDGE server role assigned to your account in HIOS (e.g., Issuer EDGE Registration Request Submitter role), you will not be able to request the Issuer EDGE Registration Request Approver or TPA EDGE Registration Request Submitter role as users can only have one (1) assigned EDGE server role in HIOS.

3.6 Accessing the ESM Website

This section provides detailed steps to access the ESM through HIOS.

Pre-Requisites for Registration: Setup Considerations

Use one (1) of the following browsers for optimum usability in the EDGE Server Registration site:

- Internet Explorer, Versions 9, 10 and 11
- Firefox, Version 32.0.2
- Google Chrome, Version 37

Issuers: All issuers must register for a HIOS Issuer ID. Issuers acting as a TPA must identify themselves in HIOS as an EDGE server TPA by editing their organization in HIOS.

TPAs: All TPAs must register for an organization HIOS Issuer ID or a Company (FEIN/TIN). TPAs must then request in HIOS an EDGE server user role.

Accessing the EDGE Server Registration Site

The following steps will provide issuers and TPAs guidance on how to initially access the EDGE Registration Site.

All issuers and TPAs will need to first access the HIOS portal through the [CMS Enterprise Portal](#) to then access the EDGE Registration site.

1. First, navigate to the CMS Enterprise Portal homepage at <http://portal.cms.gov>. If you are a new user, create a user using the **New User Registration** button. For existing users, enter your HIOS User ID and Password on the login screen. Read the **Terms and Conditions**, and then click the **Agree to our Terms & Conditions** button. Then click the **Login** button.

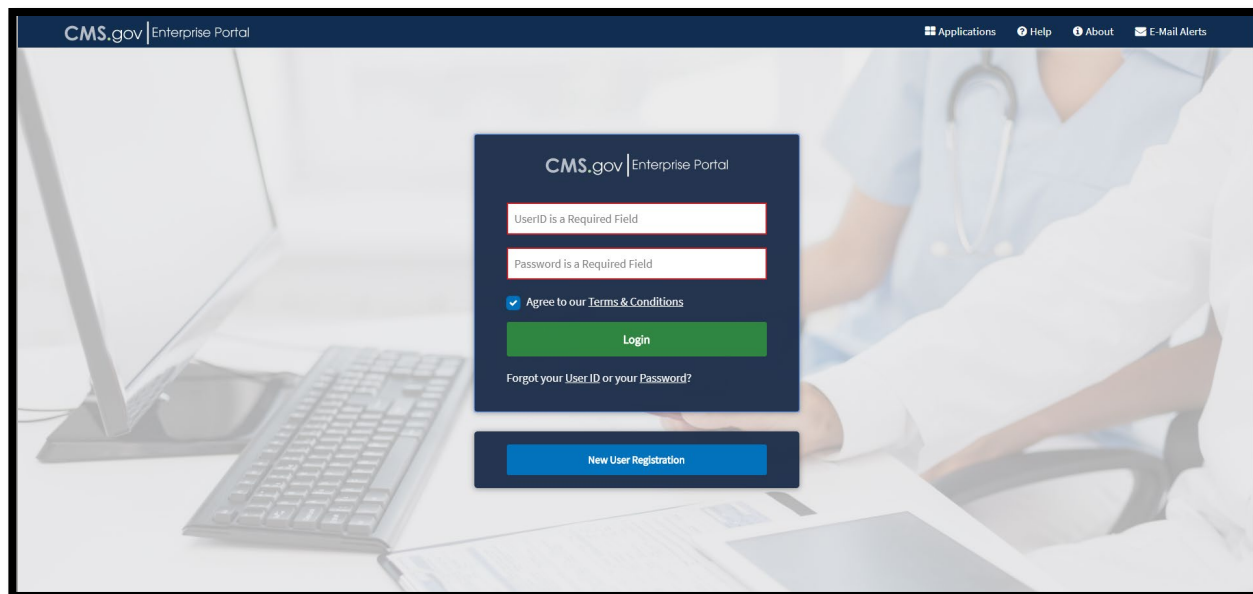


Figure 3-49: CMS Enterprise Portal Homepage, Login, and Terms and Conditions

2. Select a Multi Factor Authentication (MFA) Device Type to verify your identity through the MFA process. After receiving the code through a secondary device, enter the security code and click the Log In button.

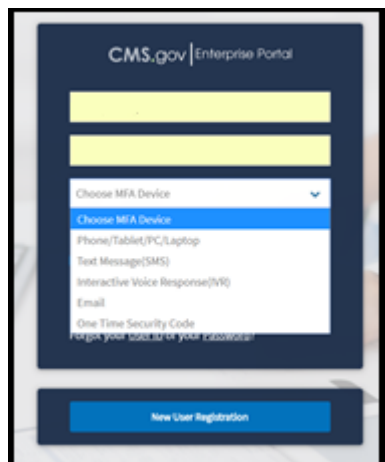


Figure 3-50: MFA Security Code

From the portal homepage, click the **HIOS** button. Then click **Overview**.

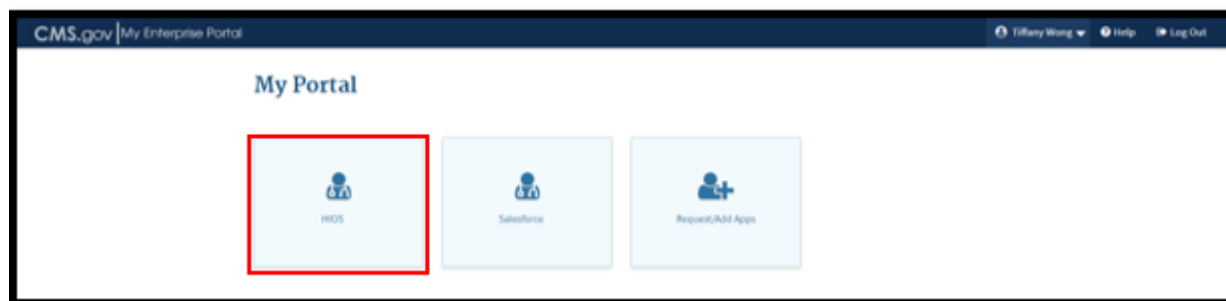


Figure 3-51: HIOS Button

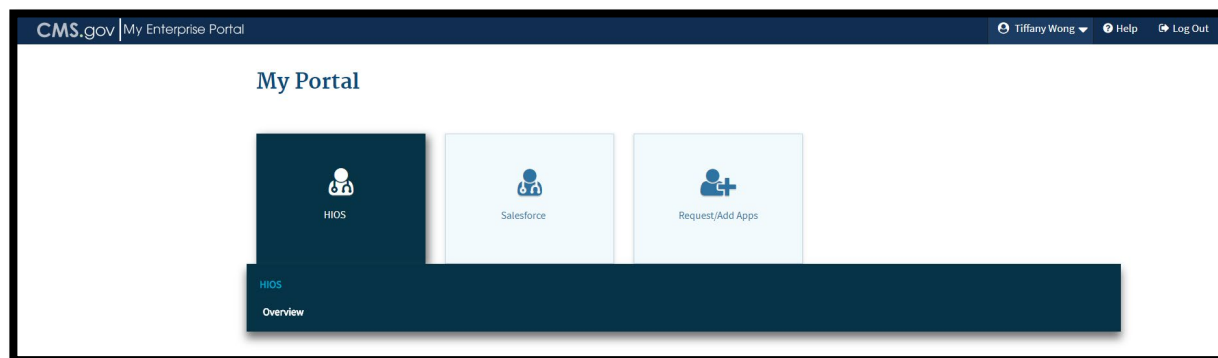


Figure 3-52: HIOS Button (Expanded Menu)

- Under the **Plan Management and Market Wide Functions** section, click the **Access Plan Management and Market Wide Functions** link.

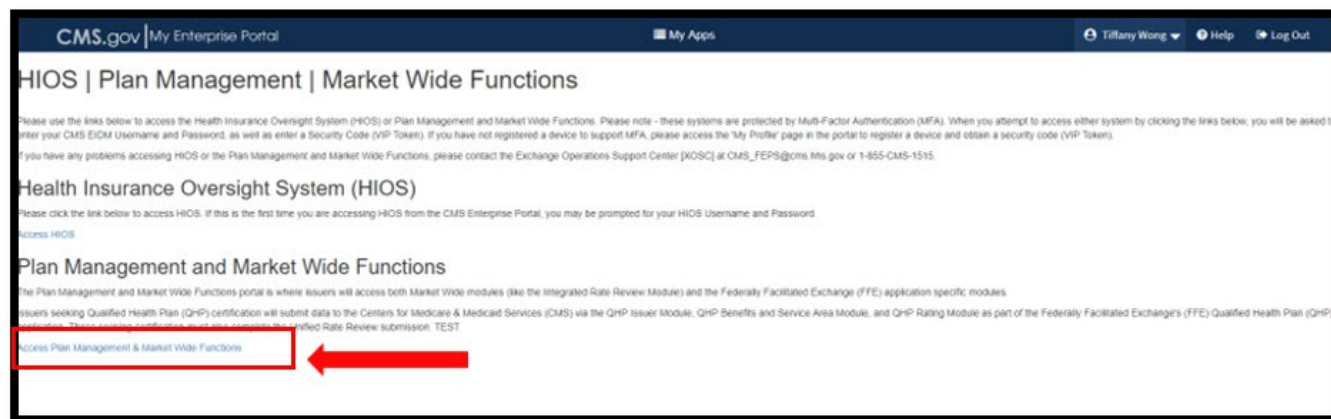


Figure 3-53: Access Plan Management & Market Wide Functions Link

- Read the **Terms of Use** and then click the **Accept** button.

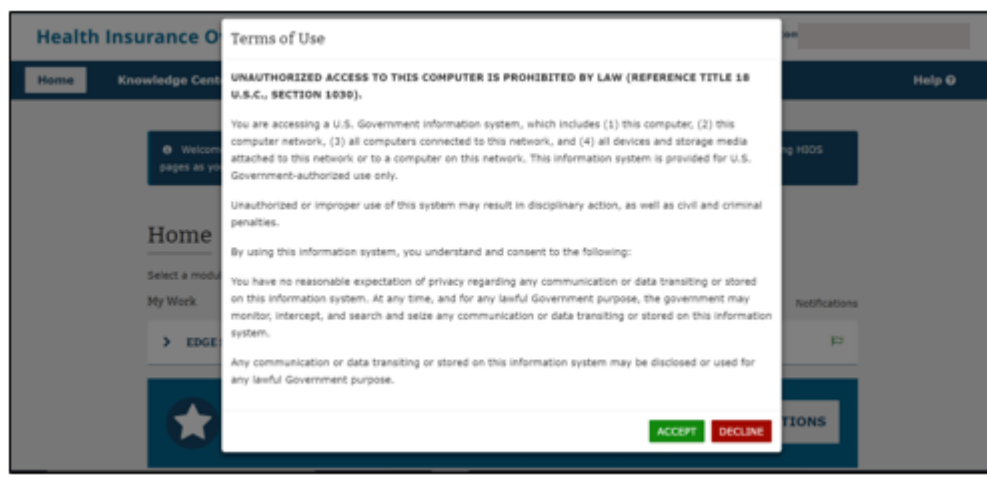


Figure 3-54: Terms of Use

5. Under **Home**, select the **EDGE Server Management** button.

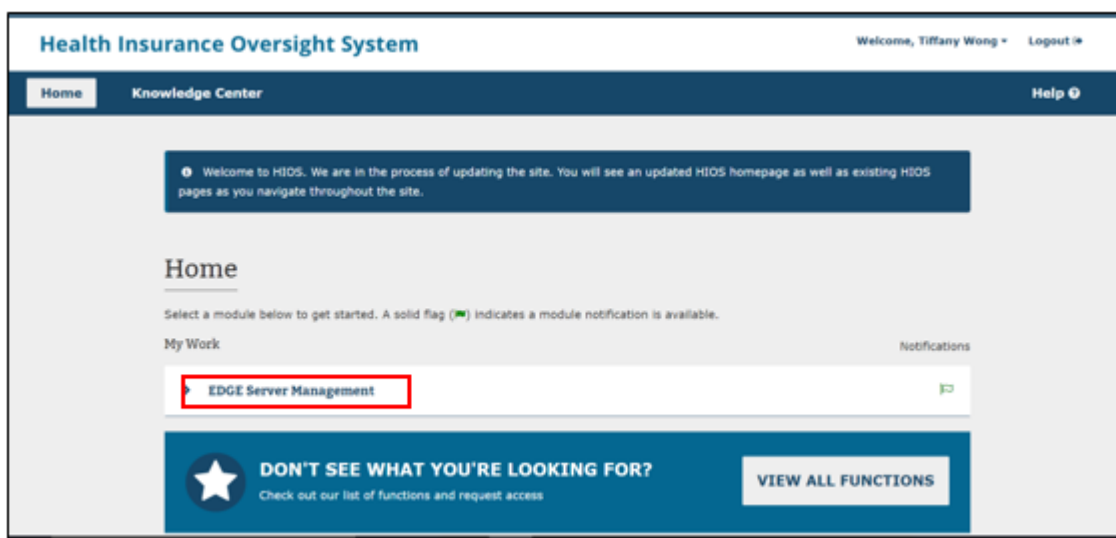


Figure 3-55: EDGE Server Management

6. Click the **Launch This Module** button.

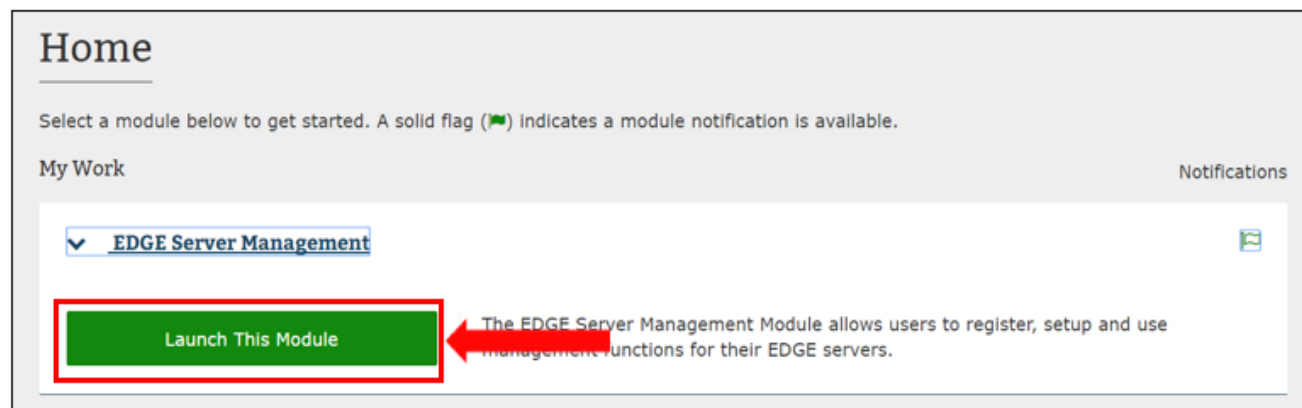


Figure 3-56: Launch This Module on ESM

- Click the **Access the EDGE Server Management Application** button.



Figure 3-57: Access the EDGE Server Management Application

- The next page is the **EDGE Server Home**, where you will be able to setup and use management functions for the EDGE server.

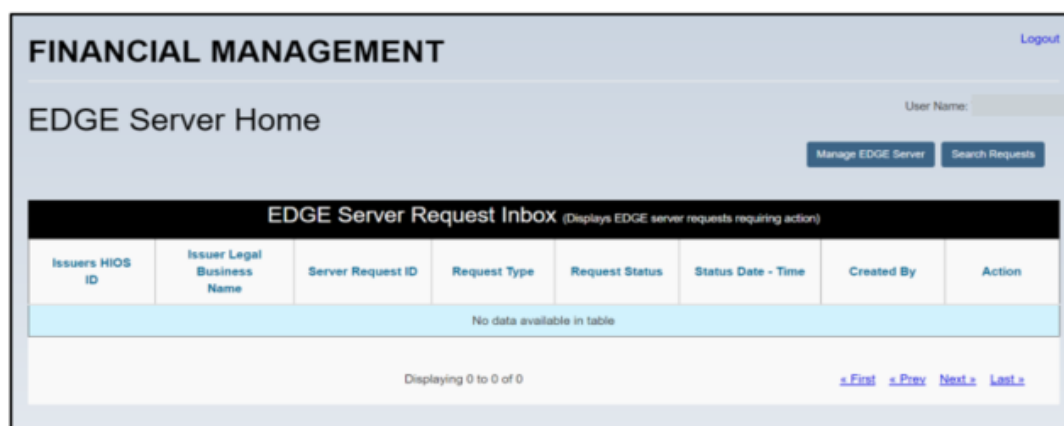


Figure 3-58: EDGE Server Home

3.7 EDGE Server Contacts

During the registration and set-up process in the ESM module, issuers are required to enter contact information. The ESM is no longer the repository used by CMS for contacting issuers with EDGE servers, therefore, the information in the ESM does not need to be maintained or updated after provisioning has been completed.

CMS requests that issuers maintain an accurate list of contacts for each company through the FM Community. The FM Community allows CEO designates and Alternate CEO designates to add, edit and replace EDGE server contacts.

This information helps CMS ensure that the appropriate contacts respond to the EDGE Server Outbound Reports and are the individuals permitted to report any formal discrepancies. EDGE server contact information is also used to notify issuers of various EDGE activities/milestones, communicate the quantity and quality of EDGE data and to report discrepancy and appeal decisions. CMS requests that CEO, or Alternate CEO designates, provide and/or confirm the current EDGE server contacts, including EDGE technical/TPA contacts.

3.8 EDGE Server Registration Overview

This section details the steps required to access the CMS EDGE server registration site and submit a request to provision an EDGE server. OP and AWS Servers use the same steps for Registration.



Note: Server Registration is required for both OP and AWS servers. For OP servers, skip the steps regarding AWS Server Details. For AWS servers, please complete the below steps.

The steps outlined below for the EDGE server registration process are divided into three (3) scenarios based on the type of access you will have in the site:

1. Issuer EDGE Registration Request Submitter
 - a. Create Self-Hosted Server Requests
 - b. Create TPA-Hosted Server Requests
2. Issuer EDGE Registration Request Approver
 - a. An Issuer EDGE Registration Request Submitter must have submitted a request before the Issuer EDGE Registration Request Approver can take an action.
3. TPA EDGE Registration Submitter
 - a. At least one (1) Issuer EDGE Registration Request Submitter and Issuer EDGE Registration Request Approver must have selected a TPA before a TPA EDGE Registration Submitter can enter server details.

All issuers and TPAs will need to log into the EDGE Server Registration Site, as detailed in [Section 3.6 Accessing the ESM Website](#), to complete a request to provision an EDGE server.

There can only be one (1) active request per issuer HIOS ID, as each issuer HIOS ID must have one (1) EDGE server. Issuers will be required to provide the following information on the request screen:

- Enter details for two (2) POC (typically server administrators) for the EDGE server they are registering.
- Indicate whether the server is self-hosted or TPA hosted.
- Signed Data Attestation Agreement. License agreements must be signed by someone who has the authority to legally and financially bind your organization.

ATTENTION TPAs:

Uploading a TPA Agreement through the EDGE Server Registration Site:



Once TPAs have access to the EDGE Server Registration site, please remember to log in and upload your signed TPA Agreement through your EDGE server home page. License agreements must be signed by someone who has the authority to legally and financially bind your organization.

Before issuers can select their TPA for managing their EDGE server, a signed agreement for the corresponding TPA must be uploaded through the EDGE Server Registration site. If the agreement is not uploaded, the TPA name and HIOS ID will not be available for selection when issuers create EDGE server requests. This document is separate from the data agreement uploaded by the issuer.

Issuers are encouraged to coordinate with their selected TPA prior to creating an EDGE server request to ensure the necessary signed TPA agreement has been uploaded in the EDGE Server Registration site. This document must be uploaded by the TPA in order for issuers to select them when creating an EDGE server request.

3.8.1 Issuer EDGE Registration Request Submitter (aka: Issuer Submitters)

3.8.1.1 Create a New EDGE Server Request - SELF-HOSTED

The following steps provide Issuer Submitters guidance on how to submit an EDGE server provisioning request for a server that will be self-hosted.

1. From the EDGE Registration home screen, click the **Create EDGE Server Request** button in top right corner to create a new request.



Figure 3-59: Create EDGE Server Request Button



Note: Any new request will be rejected if there is an existing active request for the same HIOS Issuer ID. The registration site allows only one (1) active server request for each HIOS Issuer ID.

2. Select their **HIOS Issuer ID** from the **Issuer-ID Name** dropdown menu and then enter their EDGE server POC information.

Two (2) POCs are required and up to four (4) POCs may be added. If more than two (2) POCs are needed, click the **Additional POCs** link at the bottom to open additional set of POC information fields.



Note: During the registration and set-up process in the ESM module, issuers are required to enter contact information. The ESM is no longer the repository used by CMS for contacting issuers with EDGE servers, therefore, the information in the ESM does not need to be maintained or updated after provisioning has been completed. Please see [Section 3.7 EDGE Server Contacts](#) for more information.

Figure 3-60: EDGE Server Request POC Page

3. Issuers who will be self-hosting an EDGE server, should select the **No** button in the TPA information section.

Note: When selecting **No**, the **Select TPA** drop down box and TPA POC will be disabled.

Figure 3-61: TPA Information

4. In the EDGE Server Detail section, select either **AWS** or **On Premise** for their server type from the **Select Server Type** dropdown menu.



EDGE Server Details

Select Server Type:

Figure 3-62: Select Server Type

5. Enter a name for their EDGE server in the **EDGE Server Name** field. There is no specific guidance on what to name your server.



EDGE Server Details

Select Server Type:

EDGE Server Name:

Figure 3-63: EDGE Server Name

Issuer Submitters setting up an OP EDGE server do not need to enter any additional information. Once you select **On Premise** for server type and enter a server name, the **AWS Details** fields will be disabled.



EDGE Server Details

Select Server Type:

EDGE Server Name:

AWS Details

Account Number and Key Name must be entered exactly as they appear in AWS. Incorrect entries will cause provision to fail.

AWS Account Number:

Key Name:

EDGE Server Size:

AWS Region:

Figure 3-64: On-Premise Server Details

Issuers setting up an Amazon EDGE server will need to add the following additional AWS specific information created in [Section 3.4: Server Set-Up - AWS](#)

EDGE Server Details

Select Server Type: AWS

EDGE Server Name: AWS Server

AWS Details

Account Number and Key Name must be entered exactly as they appear in AWS. Incorrect entries will cause provision to fail.

AWS Account Number:

Key Name:

EDGE Server Size: Small

AWS Region: Virginia

Figure 3-65: AWS Server Details

- **AWS Account Number** - This is the issuer's AWS account number provided by AWS. This is NOT the CMS Account Number.
- **Key Name** - The name of the SSH key pair that is associated with the issuer's AWS account that will be used to connect to the provisioned EDGE server instance. The Key Pair Name was created when executing [Section 3.4.2: Request an AWS Edge Server Instance](#).



Note: AWS does not store the private key. CMS cannot obtain your key pair. If the key pair is lost, you will not be able to sign into your EDGE server.

- **AWS Region** - The region in which the EDGE server will reside are:
 - Virginia (us-east-1)
 - California (us-west-1)
 - Oregon (us-west-2)

It is suggested that issuers select the region closest to their location.

- **EDGE Server Size** - The size of the EDGE server. This defines the computing power of the provisioned instance. Please see [Section 3.4.1 AWS Account Setup](#) for additional information about size.
 - Small
 - Medium
 - Large
6. After entering all EDGE Server details, upload the **Issuer Attestation Agreement** for the request. This agreement must be uploaded for every EDGE Server Request submitted. License agreements must be signed by someone who has the authority to legally and financially bind your organization.

Download the **Agreement** template by selecting the **Download Attestation Template** button.



The screenshot shows the 'Issuer Attestation' interface. At the top, there are three buttons: 'Download Attestation Template' (highlighted with a yellow box), 'Upload Attestation', and 'Download Signed Data Attestation'. Below these buttons are three action buttons: 'Back', 'Save', and 'Submit Request'. At the bottom, there is a 'Comments History' section with a table header containing 'Comment', 'User', and 'Date - Time'.

Figure 3-66: Download Attestation Agreement Template

A pop-up window will appear asking to download a PDF document. Download the template, review and sign the agreement and save the document for uploading.

7. Before uploading the **Issuer Attestation Agreement**, click the **Save** button to save the current request and enable the **Upload Attestation** button.



The screenshot shows the 'Issuer Attestation' interface. The 'Save' button is highlighted with a yellow box. The other buttons and layout are the same as in Figure 3-66.

Figure 3-67: Save Request

8. Scroll down to the bottom of the request screen and click the **Upload Attestation** button.



The screenshot shows the 'Issuer Attestation' interface. The 'Upload Attestation' button is highlighted with a yellow box. The other buttons and layout are the same as in Figure 3-66.

Figure 3-68: Upload Attestation Agreement

9. In the Upload window, click **Choose File** and select the saved and signed agreement. Once selected, click **Upload Attestation** button.

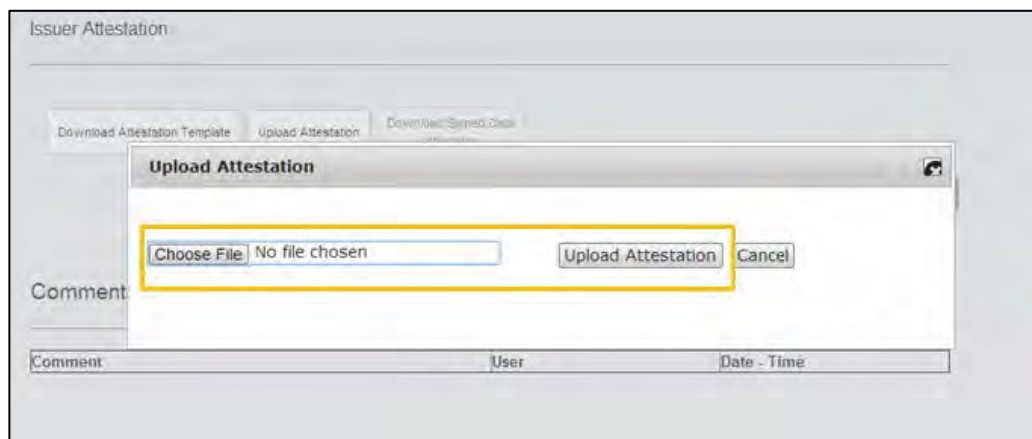


Figure 3-69: Attach and Upload Attestation Agreement

Once uploaded, the Issuer Submitter will see the message “**Successfully uploaded the file**”.

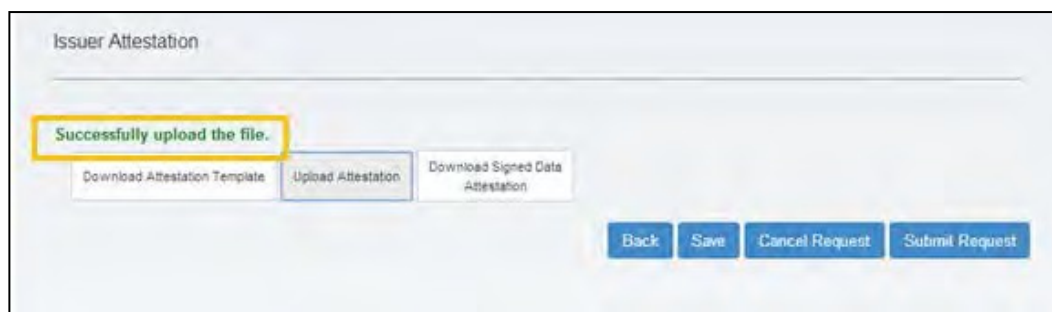


Figure 3-70: Successfully Uploaded the File Message

10. After uploading the agreement click the **Submit Request** button. At this point, the request cannot be updated by the Issuer Submitter.



Figure 3-71: Submit Request

11. Once submitted, Issuer Submitters will be taken back to their homepage.
The request is now sent to the Issuer Approver for review and approval. Issuer Submitters can track the status of their request using the **Search Requests** function. Refer to the IV **Track Request Status** section for how to search for requests.



Figure 3-72: Homepage

3.8.1.2 Create a New EDGE Server Request - TPA-HOSTED

The following steps provide Issuer Submitters guidance on how to submit an EDGE Server request for a server that will be hosted by a TPA. Issuer EDGE Registration Request Submitters will need to initiate these requests and have them approved by the Issuer Approver before the TPA can enter the server details.



Note: All TPAs should be registered in HIOS before Issuer EDGE Registration Request Submitters begin submitting requests for EDGE servers that will be hosted by a TPA. Only registered TPAs will be available for Issuer EDGE Registration Request Submitters to select when creating the request.

1. From the home screen, click **Create EDGE Server Request** button in top right corner to create a new request.

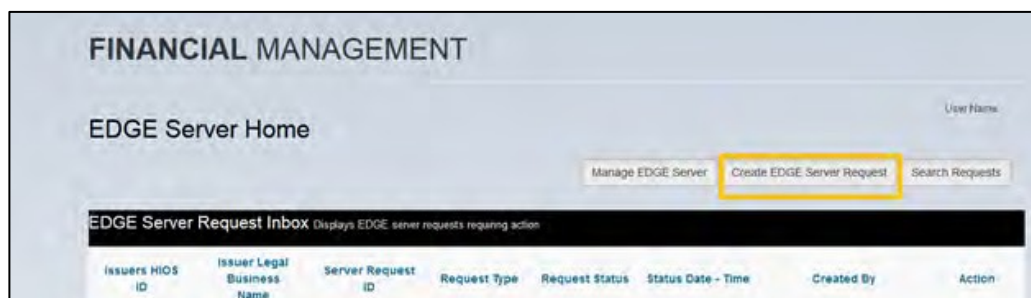


Figure 3-73: Create EDGE Server Request Button

2. Select the **HIOS Issuer ID** from the **Issuer-ID Name** dropdown menu and then enter their EDGE server POC information.
 - Two (2) POCs are required.



Note: During the registration and set-up process in the ESM module, issuers are required to enter contact information. The ESM is no longer the repository used by CMS for contacting issuers with EDGE servers, therefore, the information in the ESM does not need to be maintained or updated after provisioning has been completed. Please see [Section 3.7 EDGE Server Contacts](#) for more information.

Figure 3-74: EDGE Server Request POC Page

3. Select **YES** in the TPA information section to indicate a **TPA-hosted** EDGE server and then select an approved TPA from the dropdown.

Issuer Submitters who select a TPA Hosted EDGE server will not be able to populate the EDGE server details section. The section must be completed by the TPA after the Issuer EDGE Registration Request Approver has confirmed the request.

Figure 3-75: Select TPA



Note: The TPA drop down menu is only populated with valid TPAs (registered in HIOS) and is sorted by name and HIOS ID. If a TPA is not listed the issuer should first contact the TPA to confirm they have registered in HIOS and have obtained a HIOS ID. If they have not done so, the TPA will not be listed in the dropdown menu.

Figure 3-76: EDGE Server Details

The specific EDGE Server details will be entered by the requested TPA once approved and the EDGE Server Detail fields will be disabled for the Issuer EDGE Registration Request Submitter.

4. After indicating the EDGE server will be TPA hosted, upload the **Issuer Attestation Agreement** for the request. License agreements must be signed by someone who has the authority to legally and financially bind your organization.
 - a. Download the template by selecting the **Download Attestation Template** button

Figure 3-77: Download Attestation Agreement Template

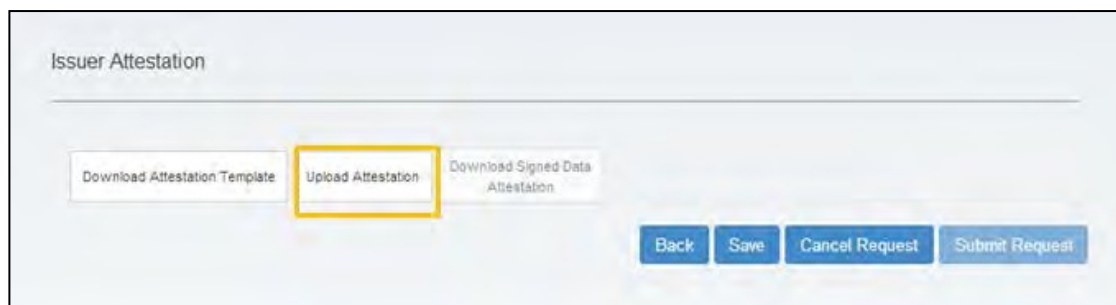
- b. A pop-up window will appear asking to download a PDF document. Download the template, review and sign the agreement and save the document for uploading.
- c. Before uploading the **Issuer Attestation Agreement**, click the **Save** button to save enable the **Upload Attestation** button.



The screenshot shows the 'Issuer Attestation' interface. At the top, there are three buttons: 'Download Attestation Template', 'Upload Attestation', and 'Download Signed Data Attestation'. Below these, there are three blue buttons: 'Back', 'Save', and 'Submit Request'. The 'Save' button is highlighted with a yellow rectangle. At the bottom, there is a 'Comments History' section with a table header containing 'Comment', 'User', and 'Date - Time'.

Figure 3-78: Save Request

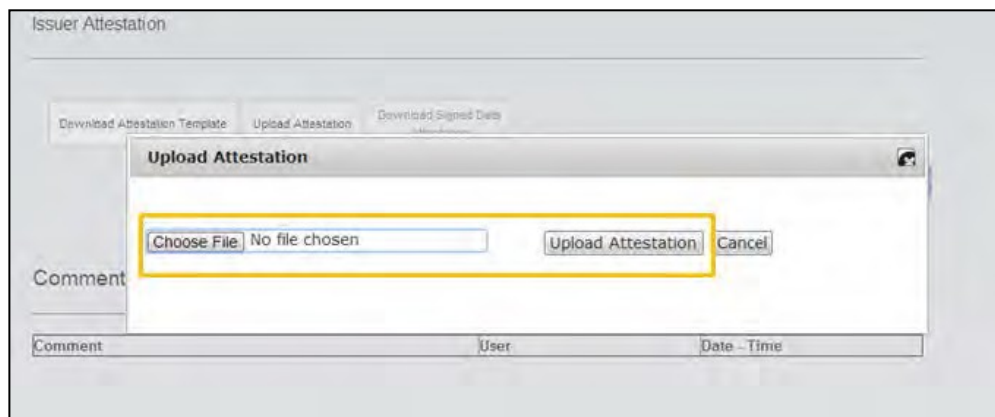
- d. Scroll to the bottom of the request screen and click the **Upload Attestation** button.



The screenshot shows the 'Issuer Attestation' interface. At the top, there are three buttons: 'Download Attestation Template', 'Upload Attestation', and 'Download Signed Data Attestation'. The 'Upload Attestation' button is highlighted with a yellow rectangle. Below these, there are four blue buttons: 'Back', 'Save', 'Cancel Request', and 'Submit Request'.

Figure 3-79: Upload Attestation Agreement

- e. In the Upload window, click **Choose File** and select the saved and signed agreement. Once selected, click **Upload Attestation** button.



The screenshot shows the 'Issuer Attestation' interface with the 'Upload Attestation' dialog box open. The dialog box has a title bar 'Upload Attestation' and a close button. Inside the dialog, there is a 'Choose File' button, a text field showing 'No file chosen', and two buttons: 'Upload Attestation' and 'Cancel'. The 'Choose File' button is highlighted with a yellow rectangle. The background shows the 'Issuer Attestation' interface with the 'Upload Attestation' button highlighted.

Figure 3-80: Attach and Upload Attestation Agreement

- f. Once uploaded, a message **“Successfully uploaded the file”** message will appear.

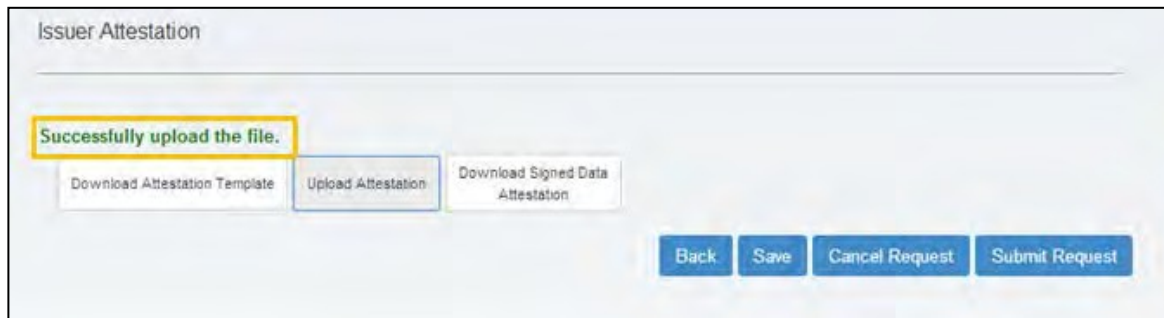


Figure 3-81: Successfully Uploaded the File Message

5. After uploading the agreement, Issuer Submitters are ready to submit the request for review and approval by the Issuer EDGE Registration Request Approver. Click the **Submit Request** button.



Figure 3-82: Submit Request

Issuer Submitters will be taken back to their homepage.

The request is sent to the Issuer Approver for review and approval before being sent to the TPA Submitter to enter the server details.

Issuer Submitters can track the status of their request using the **Search Requests** function. Please see From **the homepage**, click the Search Requests button to open the search request screen.

3.8.1.3 Updating a Rejected Request

If a request is rejected by an Issuer Approver, TPA Submitter or CMS Approver for any reason, it will return to the Issuer Submitter's homepage. Issuer Submitters will need to open the request, update the request per the comments made by the user rejecting it and then re-submit the request.



Note: No notification is sent to the Issuer Submitter. Issuer Submitters should check the status of their request periodically.

1. Issuer Submitters will see rejected requests on the homepage with one (1) of the following statuses:
 - **Org Rejected** (rejected by the Issuer Approver)
 - **Host Rejected** (rejected by the TPA Submitter - TPA-Hosted Servers ONLY)
 - **CMS Rejected** (rejected by CMS Approver)

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
99429	ABC	106101	New AWS Server	Org Rejected	8/26/14 4:42:07 PM	IR	view
99429	ABC	106101	New AWS Server	Host Rejected	8/26/14 4:34:22 PM	IR	view
99428	ABC	106102	New AWS Server	CMS Rejected	8/26/14 4:38:02 PM	IR	view

Figure 3-83: Rejected Requests in Issuer EDGE Registration Request Submitter's Inbox

2. Select **View**, under the **Action** column, to view the reason for rejection.

99429	ABC	106101	New AWS Server	Org Rejected	8/26/14 4:42:07 PM	IR	view
-------	-----	--------	----------------	--------------	--------------------	----	------

Figure 3-84: Open Request

3. Update the request per the rejection comments and re-submit following the standard submission process outlined in the previous steps.

3.8.1.4 Track Request Status

Once a request has been submitted, the request will move along one (1) of the following paths:

- Self-Hosted
- TPA-Hosted

Table 3-4: Self-Hosted Path

Step	Request Status
Request submitted to Issuer Approver	Pending Org Approval
Approved by Issuer Approver and sent to CMS Approver	Pending CMS Approval
Approved by CMS and provisioning pending	Pending Provisioning

Table 3-5: TPA-Hosted Path

Step	Request Status
Request submitted to Issuer Approver	Pending Org Approval
Approved by Issuer Approver and sent to TPA Submitter to complete	Pending Host Server Details
TPA Submitter submits to CMS for approval	Pending CMS Approval
Approved by CMS and provisioning pending	Pending Provisioning

Issuer Submitters can track the status of their request using the Search Requests function. From the homepage, click the Search Requests button to open the search request screen. Please refer to [Section 3.8.4: EDGE Server Management Console Server Status Tracking for further details.](#)

3.8.2 Issuer EDGE Registration Request Approver

Once an EDGE server request has been submitted by the Issuer Submitter, the request will appear on the Issuer Approver's homepage. Requests in the Issuer EDGE Registration Request Approver's homepage can either be newly submitted requests or previously submitted requests that have been rejected and re-submitted back to the Issuer EDGE Registration Request Approver for approval.



Note: There is no notification feature to alert Issuer Approvers of pending requests. Issuer Approvers should check their EDGE server homepage regularly.

The Issuer Approver reviews the request and confirms that a new EDGE server has been requested.

- From the homepage, Issuer Approvers will see the EDGE registration status inbox with active EDGE requests pending approval with a status **Pending Org Approval**.

FINANCIAL MANAGEMENT

EDGE Server Home

User Name: JA

Manage EDGE Server Search Requests

EDGE Server Request Inbox Displays EDGE server requests requiring action

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
99427	ABC	106100	New AWS Server	Pending Org Approval	8/26/14 4:16:21 PM	IR	view
99429	ABC	106101	New AWS Server	Pending Org Approval	8/26/14 4:19:15 PM	IR	view
99428	ABC	106102	New AWS Server	Pending Org Approval	8/26/14 4:20:02 PM	IR	view

Showing 1 to 3 of 3 entries

« First « Prev 1 Next » Last »

Figure 3-85: Issuer EDGE Registration Request Approver Homepage

- Select **View** in the **Action** column of their EDGE registration status inbox to open a request to approve.

FINANCIAL MANAGEMENT

EDGE Server Home

User Name: JA

Manage EDGE Server Search Requests

EDGE Server Request Inbox Displays EDGE server requests requiring action

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
99427	ABC	106100	New AWS Server	Pending Org Approval	8/26/14 4:16:21 PM	IR	view

Figure 3-86: Open Request

- When the Request Approval Screen opens, Issuer Approvers will have View-Only mode. The Issuer Approver will review the request and confirm the accuracy of information entered by the Issuer Submitter.

FINANCIAL MANAGEMENT

EDGE Server Request Approval

User Name: JA

Back to EDGE Server Home

Issuer-ID Name99427-issuer99427

Request ID106100

Request StatusPENDING_ORG_APPROVAL

Issuer Point of Contact

All fields marked with an asterisk[*] are required.

Primary Point of Contact

PrefixMr

Emailemail@tst.com

First NameTestFirst

Phone Number3017402313

Last NameTestLast

Job TitleManager

Secondary Point of Contact

PrefixMr

Emailjss@yahoo.com

First NameSecondFirst

Phone Number2402348241

Last NameSecondLast

Job TitlePM

Additional POCs

Figure 3-87: Request Approval

- Issuer Approvers must either Approve or Reject the Request.
 1. **Rejected Request** - Issuer Approvers will need to provide an explanation as to why the request is being rejected in the Comments section and then click **Reject Request**.

Comments

Comment

User

Date - Time

New Comments:

Rejecting this request

Back

Download Signed Issuer Attestation

Approve Request

Reject Request

Status History

Action	Status	User	Date - Time
Submitted	Pending Org Approval	JR	8/26/14 4:16:21 PM
Created	Draft	JR	8/26/14 4:12:42 PM

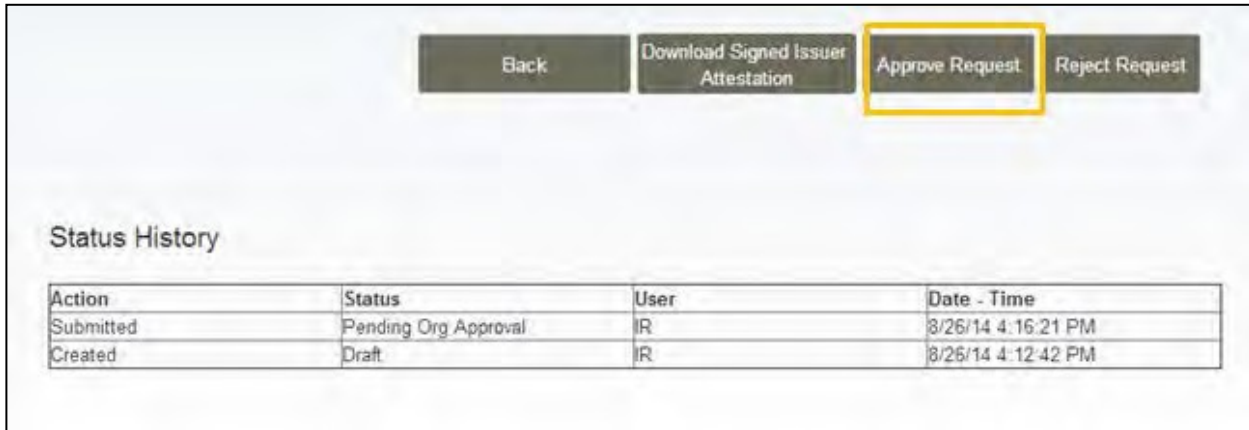
Figure 3-88: Reject Request

Contact Edge_Server_Data@cms.hhs.gov for technical assistance.

73

Rejected Requests will return to the Issuer EDGE Registration Request Submitter to make corrections and then send back to the Issuer EDGE Registration Request Approver to approve.

2. **Approved Request** - Issuer Approvers can click the **Approve Request** button.



The screenshot shows a user interface with four buttons: 'Back', 'Download Signed Issuer Attestation', 'Approve Request' (highlighted with a yellow box), and 'Reject Request'. Below these buttons is a section titled 'Status History' containing a table with the following data:

Action	Status	User	Date - Time
Submitted	Pending Org Approval	IR	8/26/14 4:16:21 PM
Created	Draft	IR	8/26/14 4:12:42 PM

Figure 3-89: Approve Request

Approved requests will move to the next step in the process.

- Self-Hosted: Request will move to CMS Approver's inbox for review.



Note: After the server status is Pending CMS Approval for review, please email CMS_FEPS@hhs.gov to inform CMS a server request has been added. In the email, include the server HIOS ID and a request for approval.

- TPA-Hosted: Request will move to TPA Submitter's inbox for processing.
- Issuer Approvers can track the status of their request using the Search Requests function. From the homepage, click the Search Requests button to open the search request screen. Please refer to [Section 3.8.4: EDGE Server Management Console Server Status Tracking for further details](#).

3.8.3 TPA EDGE Registration Submitter

Once the EDGE server request has been approved by the Issuer Approver, the request will appear in the selected TPA's EDGE server homepage. TPA Submitters will complete the steps that follow to finish registering the EDGE server.



Note: There is no notification feature to alert TPA Submitters of pending requests. TPA Submitters should check the EDGE server homepage regularly.

If for any reason the request is invalid or needs to be rejected, TPA Submitters can select the **Reject Hosting Request** button and the request will return to the Issuer Submitter's homepage.

When rejecting the request, the TPA will need to enter comments explaining why the request is being rejected.

Requests on the TPA Submitter's homepage can either be newly submitted requests or previously submitted requests that have been rejected and re-submitted for update.

1. From the EDGE server Homepage, TPA Submitters will see the pending request with a status **Pending Hosted Server Details**.

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
15040		56064	New AWS Server	Pending Hosted Server Details	8/25/14 11:42:44 AM	EDTEST1@FFETEST.COM	view
39774		7210	New AWS Server	Provisioning Failed	8/22/14 5:10:18 PM	ACCNFM131@FFETEST.COM	view
99429	ABC	106101	New AWS Server	Pending Hosted Server Details	8/26/14 4:28:26 PM	IR	view

Figure 3-90: TPA EDGE Registration Submitter Homepage

2. Before processing requests, TPA Submitters will need to upload the TPA Attestation Agreement from the homepage.



Note: TPA EDGE Registration Submitters will need to upload a TPA Attestation Agreement for every issuer they are hosting. License agreements must be signed by someone who has the authority to legally and financially bind your organization.

3. In the lower right corner, under the **Manage TPA Attestation** section, click the **Download TPA Attestation Template** button.

Date Uploaded	File Name
25-08-2014	atte (1) (1) (1).pdf
20-08-2014	Edge_Reg_Data.pdf

Figure 3-91: Download TPA Attestation Agreement Template

A pop-up window will appear asking the user to download and save the PDF.

4. Click **Yes** and sign and save the agreement.
5. Click the Upload Signed TPA Attestation button.

Manage TPA Agreement

Select TPA

TPA ID - Name
42226

Download Signed TPA Agreement

Date Uploaded	File Name
25-08-2014	atte (1) (1) (1).pdf
20-08-2014	Edge_Reg_Data.pdf

Download TPA Attestation Template

Upload Signed TPA Attestation

Figure 3-92: Upload Signed TPA Attestation Agreement

6. In the upload window, click **Choose File** to select the saved and signed TPA Attestation Agreement form and then click **Upload Attestation** button to attach.

Data Agreement

Choose File No file chosen Upload Attestation Cancel

Figure 3-93: Upload Attestation Agreement



Note: TPA Submitters will be able to track all their uploaded documents in the **Download Signed TPA Attestation** section at the bottom of the homepage.

Download Signed TPA Agreement

Date Uploaded	File Name
25-08-2014	atte (1) (1) (1).pdf
20-08-2014	Edge_Reg_Data.pdf

Download TPA Attestation Template

Upload Signed TPA Attestation

Figure 3-94: Uploaded Attestations Agreement

Once the agreement has been uploaded, the TPA Submitter can begin processing a request.

7. Select the **View** from the **Action** column on the homepage for the request to process.



Figure 3-95 Select to View Request

8. Scroll down to the EDGE Server Details section to enter the server information.
9. Select either **AWS** or **On Premise** for their server type.

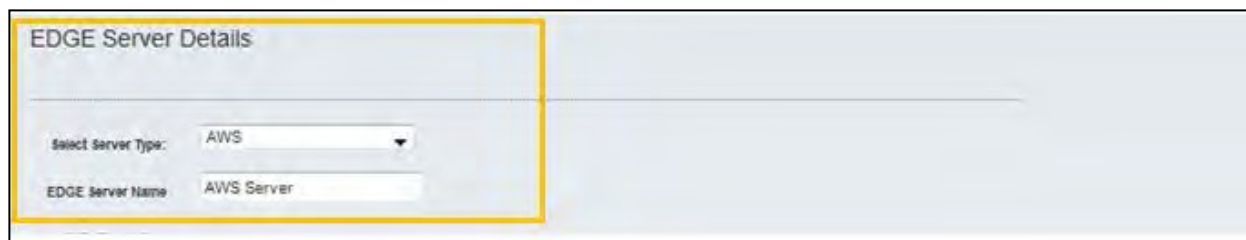
The screenshot shows the 'TPA Information' section with a form for 'Will this be a TPA hosted EDGE Server?' (yes/no), 'Select TPA:' (By Name and HIOS ID), and a dropdown for 'TPA Name - Paul Test Email TST'. Below this is the 'EDGE Server Details' section with a 'Select Server Type' dropdown menu, an 'EDGE Server Name' text field, and an 'AWS Details' section. The 'AWS Details' section includes a note: 'Account Number and Key Name must be entered exactly as they appear in AWS. Incorrect entries will cause provision to fail.' It contains fields for 'AWS Account Number', 'Key Name', 'EDGE Server Size' (dropdown), and 'AWS Region' (dropdown).

Figure 3-96: TPA EDGE Registration Submitters Request

The screenshot shows the 'EDGE Server Details' section of the form. It features a 'Select Server Type' label followed by a dropdown menu currently displaying 'Select Server Type'.

Figure 3-97: Select Server Type

10. Enter a name for their EDGE server in the **EDGE Server Name** field. There is no specific guidance or requirement for the EDGE server name.

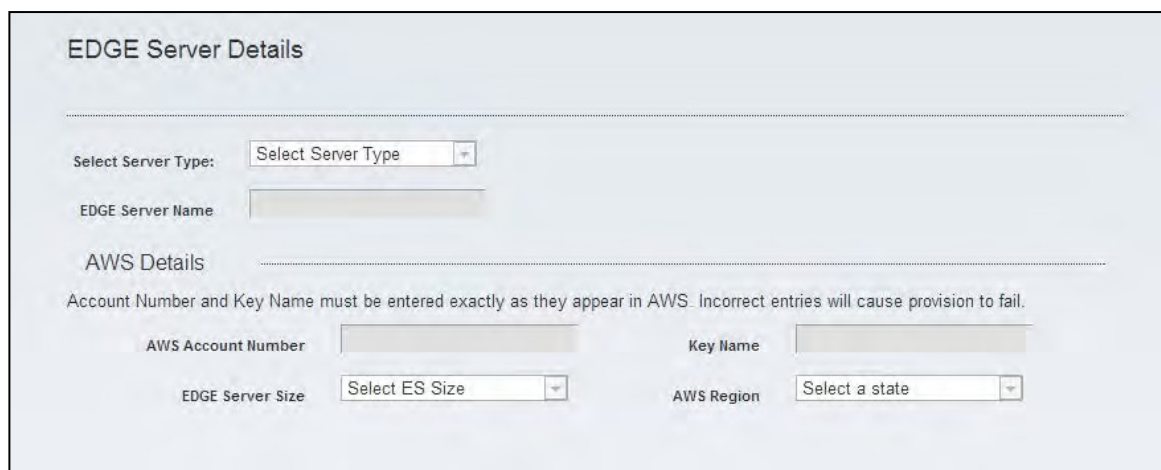


The screenshot shows a form titled "EDGE Server Details". It has two main sections. The first section contains a "Select Server Type:" dropdown menu with "AWS" selected, and an "EDGE Server Name" text input field with "AWS Server" entered. The second section is empty.

Figure 3-98: EDGE Server Name

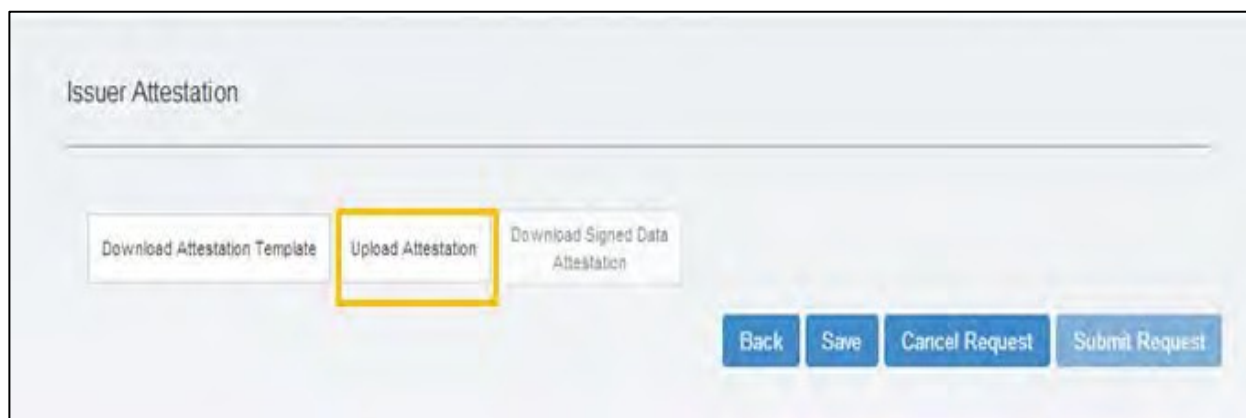
11. TPA Submitters setting up an **Amazon EDGE server** need to add the following AWS specific information:
- AWS Account Number
 - Key Name
 - AWS Region
 - EDGE Server Size

Note: TPA Submitters setting up an OP EDGE server do not need to enter any additional information.



The screenshot shows the "EDGE Server Details" form. The "Select Server Type:" dropdown is set to "Select Server Type". The "EDGE Server Name" field is empty. Below this is the "AWS Details" section, which includes a note: "Account Number and Key Name must be entered exactly as they appear in AWS. Incorrect entries will cause provision to fail." There are four input fields: "AWS Account Number", "Key Name", "EDGE Server Size" (a dropdown menu set to "Select ES Size"), and "AWS Region" (a dropdown menu set to "Select a state").

Figure 3-99: AWS Server Details



The screenshot shows the "Issuer Attestation" form. It has three buttons: "Download Attestation Template", "Upload Attestation" (highlighted with a yellow box), and "Download Signed Data Attestation". At the bottom right, there are four buttons: "Back", "Save", "Cancel Request", and "Submit Request".

Figure 3-100: AWS Details

12. After entering all appropriate EDGE Server details, click the **Submit** button to process the request.

If for any reason the request is invalid or needs to be rejected, TPA Submitters can select **Reject Hosting Request** button and the request will be returned to the Issuer Submitter's homepage. When rejecting the request, TPA Submitters will need to enter comments explaining why the request is being rejected.



The screenshot shows the 'Issuer Attestation' form. It includes buttons for 'Download Attestation Template', 'Upload Attestation', and 'Download Signed Data Attestation'. At the bottom right, there are four buttons: 'Back', 'Save', 'Reject Hosting Request', and 'Submit Request'. The 'Submit Request' button is highlighted with a yellow rectangular box.

Figure 3-100: Submit Button

3.8.3.1 Updating a Rejected Request

If a request is rejected for any reason, it will return to the Issuer Submitter's inbox. Issuer Submitters will need to open the request, update the request (if applicable) per the comments made by the user rejecting it and then re-submit to the Issuer Approver.

Once approved by the Issuer Approver, the request will be sent to the TPA Submitter to update any applicable information. If any of the required updates are to be made by the TPA Submitter, they will need to open the request, complete the updates and re-submit to CMS for approval.



The screenshot shows the 'FINANCIAL MANAGEMENT' section of the 'EDGE Server Home' page. It includes a header with 'User Name: TPA' and buttons for 'Manage EDGE Server' and 'Search Requests'. Below is the 'EDGE Server Request Inbox' which displays a table of requests requiring action. The 'Request Status' column in the table is highlighted with an orange box.

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
15040		56054	New AWS Server	Pending Hosted Server Details	8/25/14 11:42:44 AM	EDTEST1@FFETEST.COM	view

Figure 3-101: Rejected Requests in Submitter's Inbox

1. Select **View** next to the request to update.



Figure 3-102: Open Request

2. Update the request per the rejection comments and re-submit following the standard submission process outlined in the previous steps.

3.8.3.2 Track Request Status

Once a TPA-hosted request has been submitted, the request will move along the following path. TPA Submitters can track the status of their request using the below details:

Table 3-6: TPA-Hosted Path

Step	Request Status
1. Request submitted to Issuer Approver	Pending Org Approval
2. Approved by Issuer Approver and sent to TPA Submitter to complete	Pending Host Server Details
3. TPA Submitter submits to CMS for review and approval	Pending CMS Approval
4. Approved by CMS and provisioning pending	Pending Provisioning



Note: After receiving a server status of “Pending CMS Approval”, please email CMS_FEPS@hhs.gov to inform CMS a server request has been added. In the email, include the server HIOS ID and a request for approval.

TPA Submitters can track the status of their request using the Search Requests function. From the homepage, click the Search Requests button to open the search request screen. Please refer to [Section 3.8.4: EDGE Server Management Console Server Status Tracking for further details](#).

Confirm the request has a status of “Pending Provisioning” and continue to [Section 3.8.5 On-Premise EDGE Server Provisioning](#) for On Premise servers or [Section 3.8.6 AWS EDGE Server Provisioning](#) for AWS servers.

3.8.4 EDGE Server Management Console - Server Status Tracking

To track the status of an existing request after it has been submitted (server submission information in the following sections), Issuer Submitters, Issuer Approvers and TPA Submitters can use the search function on the homepage to search for requests or to monitor servers that are going through the provisioning process.

1. From the homepage, click the **Search Requests** button to open the search request screen.



Figure 3-103: Search Requests Button

2. At the EDGE Server Request Search screen, select the **Search Field** to search all requests and, if desired, specify the **Created Date Range** and click the **Search** button. All applicable results will display.

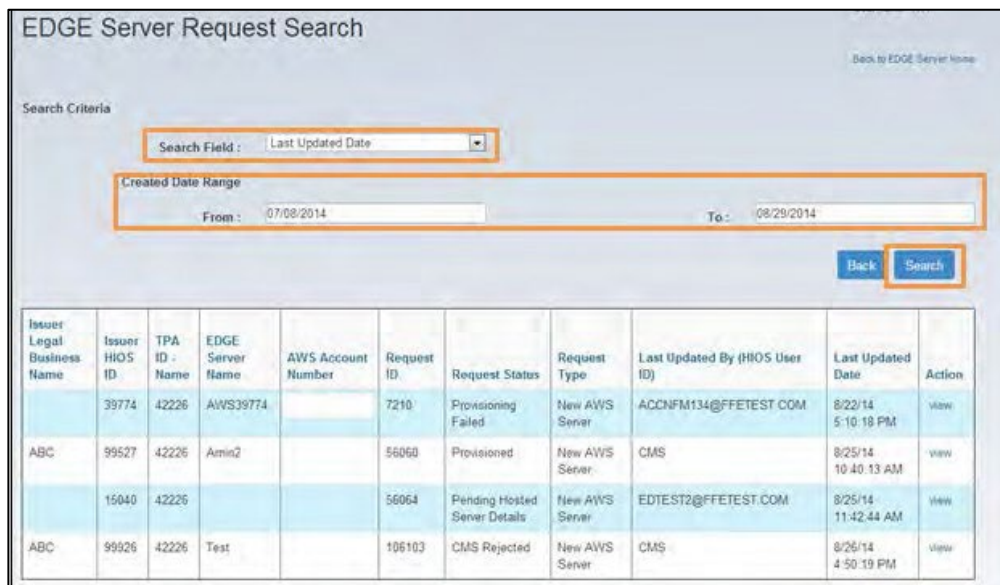


Figure 3-104: EDGE Server Request Search Screen

3.8.5 On-Premise EDGE Server Provisioning

This section provides an overview of the steps issuers must follow in order to successfully provision an OP EDGE server, confirm successful provisioning and connect to their server. It will also provide guidance on how to proceed in the event that provisioning fails.

The below steps will provide issuers and TPAs an overview of how to provision an OP EDGE server by manually running installation scripts downloaded from the EDGE registration site, confirming successful installation and connecting to the EDGE server.

OP EDGE Server Provisioning

3.8.5.1 Download Installation Scripts

Once an OP 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 servers may begin the provisioning process. The following steps explain how to access the installation scripts to complete the provisioning process.

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



FINANCIAL MANAGEMENT							
EDGE Server Home							
Manage EDGE Server Create EDGE Server Request Search Requests							
EDGE Server Request Inbox Displays EDGE server requests requiring action							
Issuers HHOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
10297		106183	New Server Request	Pending Provisioning	9/15/14 10:25:04 AM	ZFMLOADTEST1991	view

Figure 3-105: Pending Provisioning

At this point, a batch job runs and will pick up the request and update the status to **Provisioning in Progress**. Once the request status updates to Provisioning in Progress, 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.

Click the **Search Requests** button at the top right.



Figure 3-106: Search Requests Button

2. In the Search Requests screen, select **Issuer HIOS ID** from the **Search Field** dropdown menu and enter your 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.

EDGE Server Request Search

User Name: ACCNFM123@FFETEST.COM

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Issuer HIOS ID Search Value : 15509

[Back](#) [Search](#)

Figure 3-107: Search Request Screen

3. The status of **Provisioning in Progress** indicates the OP EDGE server installation scripts are available. Click the **View** button from the **Action** column of the request to open the request and locate the On- Premise Installation scripts.

FINANCIAL MANAGEMENT

EDGE Server Request Search

User Name: ZFMLOADTEST1991

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Issuer HIOS ID Search Value : 15297

[Back](#) [Search](#)

Issuer Legal Business Name	Issuer HIOS ID	TPA ID Name	EDGE Server Name	AWS Account Number	Request ID	Request Status	Request Type	Last Updated By (HIOS User ID)	Last Updated Date	Action
	15297	Test1	Test1		156183	Provisioning In Progress	New Server Request	ZFMLOADTEST1991	9/15/14 11:05:54 AM	view

Figure 3-108: Provisioning in Progress

4. Download links for the three (3) files for OP EDGE server installation:
 - Installation Information
 - Deployment Script
 - Property File

Follow the instructions on the screen to download and install each of these scripts.

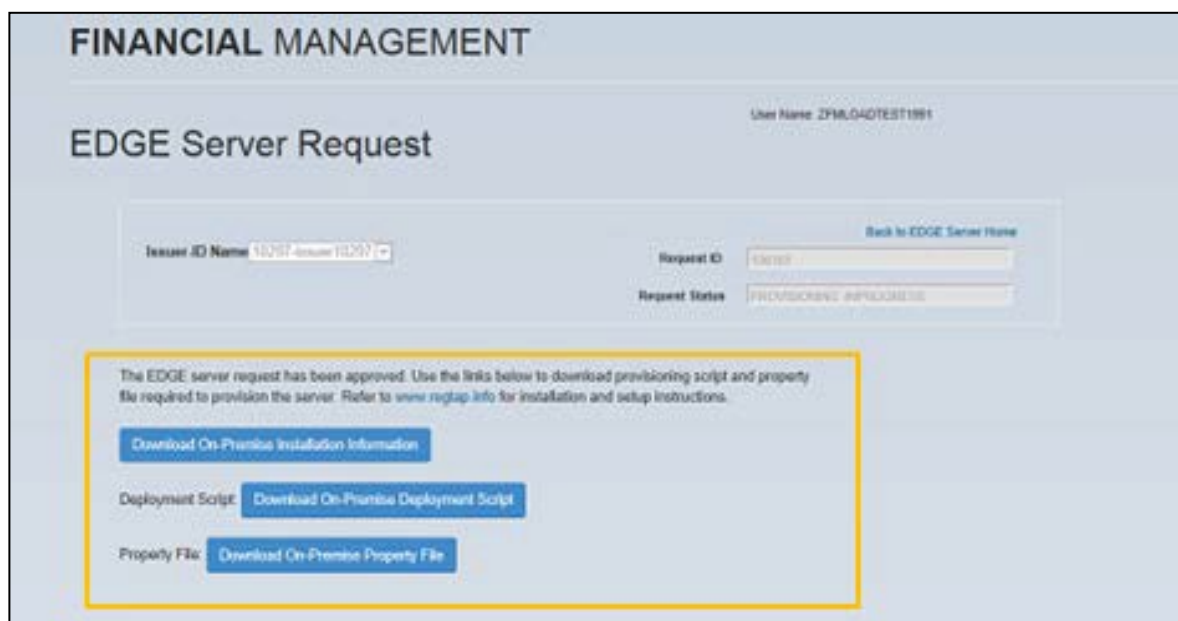


Figure 3-109: Download Provisioning Installation Scripts

Save the programs locally to your computer. Save the files in a secure location where they will be easily accessible for the subsequent steps.

3.8.5.2 Transfer Installation Scripts to OP EDGE Server, Connect to Server and Confirm Provisioning

Transfer the installation scripts downloaded from the EDGE Registration site to the server using WinSCP, connect to the server using PuTTY and confirm successful provisioning.

I. *Download WinSCP*

Issuers may use the Secure File Transfer Protocol (SFTP) client of choice to transfer the installation scripts from their computer to their server. WinSCP is a commonly used application for this purpose, and for sample purposes, the steps for downloading and configuring the tool are included here. Issuers will need to adapt these instructions if they choose to use a different SFTP client.



Note: WinSCP download page updates the user interface for the website often. Although the below figures may change, the steps are accurate.

1. Go to [WinSCP](#) website.

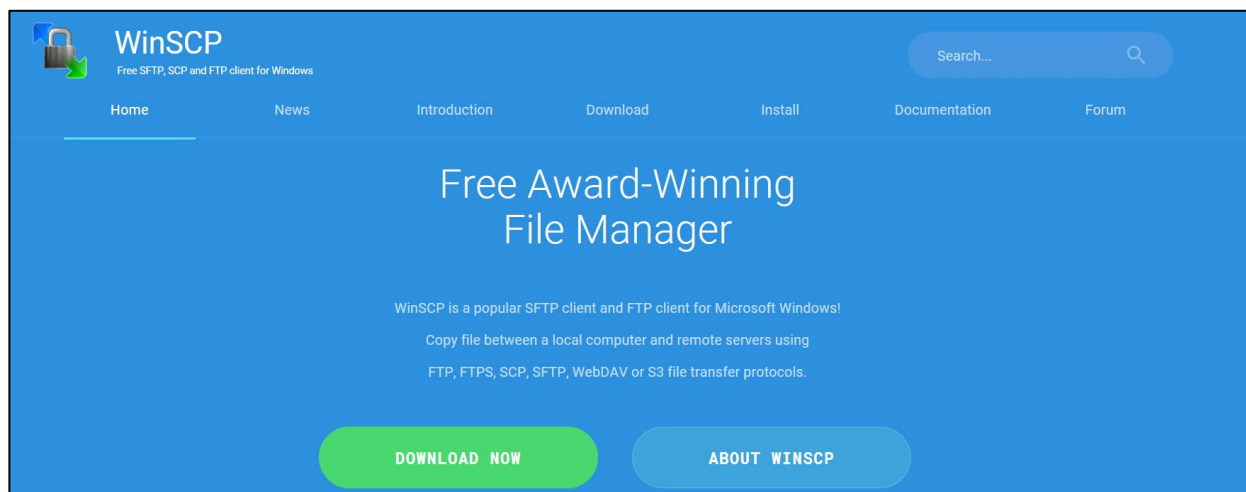


Figure 3-110: WinSCP Home Page

2. Click the **News** tab.



Figure 3-111: News Tab

3. Click the **Go to Download Page** link.

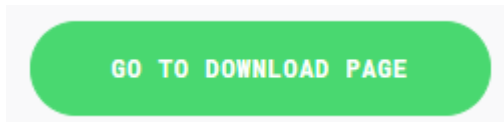


Figure 3-112: Go to Download Page Link

4. Click the **Download WinSCP** link and complete software setup.



Note: EDGE software is currently tested with WinSCP 5.13.6. If issuers run into issues with a later version, please contact edge_server_data@cms.hhs.gov.

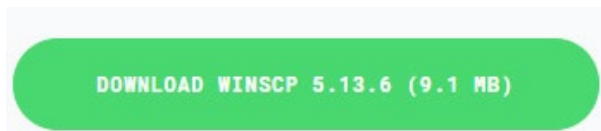


Figure 3-113: Download WinSCP

5. Click and download the **Installation Package** link on the screen:

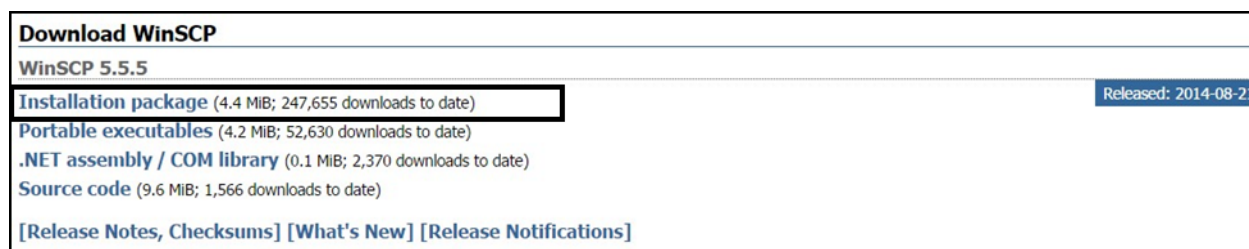


Figure 3-114: Download Installation Package

II. Run WinSCP

1. Open and run the WinSCP program downloaded in the previous step. After running the program, the following window will appear.

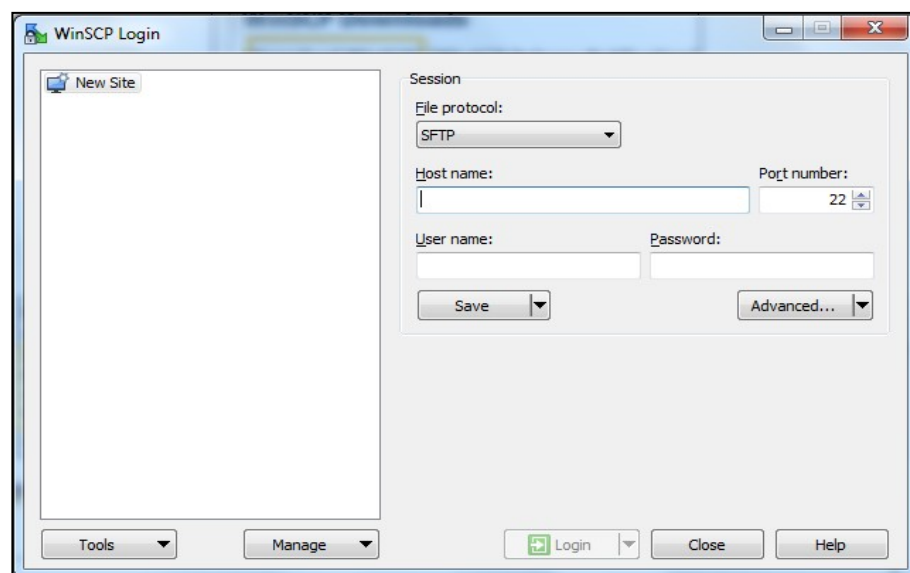


Figure 3-115: WinSCP Login Screen

2. In the WinSCP login window, enter the IP address for your server in the **Host Name** field. Then enter the name and password of your OP server in the **User Name** and **Password** fields. Click the **Login** button when finished.

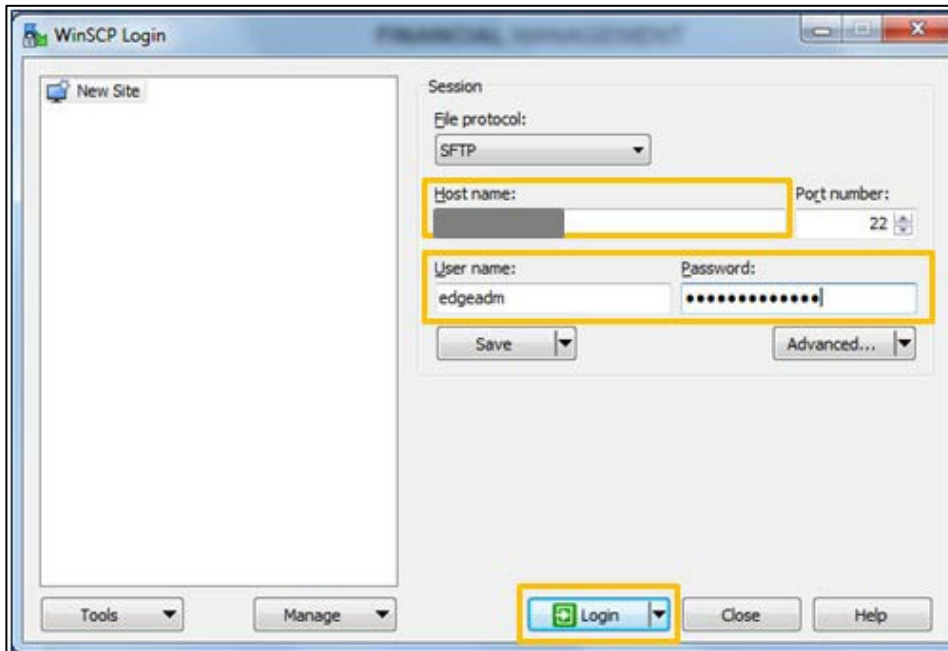


Figure 3-116: WinSCP Login Information

3. After clicking login, two (2) menus will appear side by side: Local computer files appear on the left side and OP server files appear on the right. Locate the three (3) files downloaded from the EDGE Registration site from the left side:

- EDGE property file
- EDGE key file
- EDGE application files

Click and drag the files from the left side (local computer) to the right side (server) and store the files in a location of your choice on the server side.

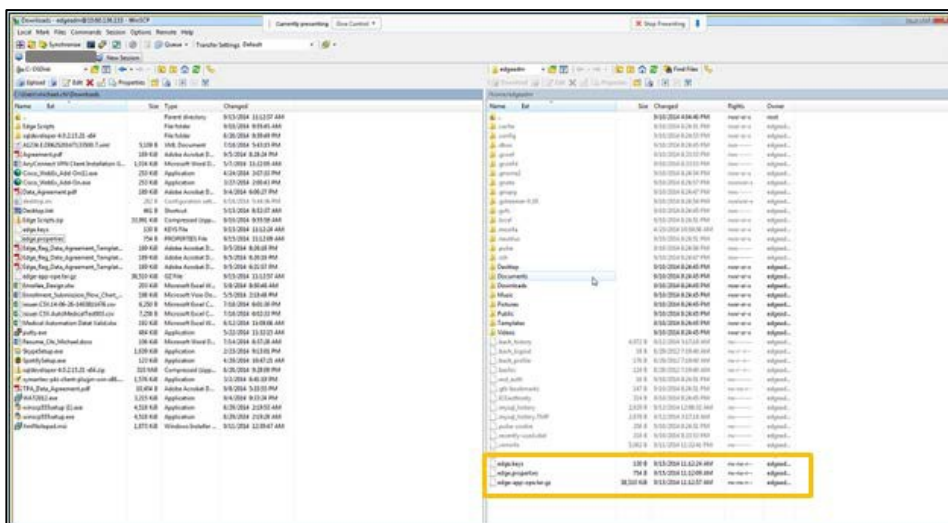


Figure 3-117: WinSCP Files and Folders

III. Download PuTTY

Issuers may use their SSH client of choice to log into the provisioned server.

PuTTY is a commonly used application for this purpose, and for sample purposes, the steps for downloading and configuring the tool are included here. Issuers will need to adapt the instructions that follow if they choose to use a different SSH client.

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

1. Go to www.putty.org
2. Click **You can download PuTTY here.**

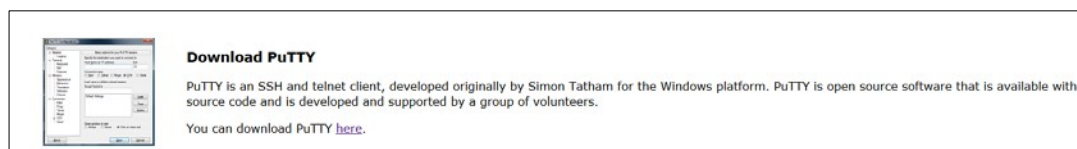


Figure 3-118: PuTTY Home Page

3. The PuTTY download page will appear with a link to download **putty.exe**.



Figure 3-119: PuTTY Download Page

4. After running PuTTY.exe, the PuTTY configuration window will appear.

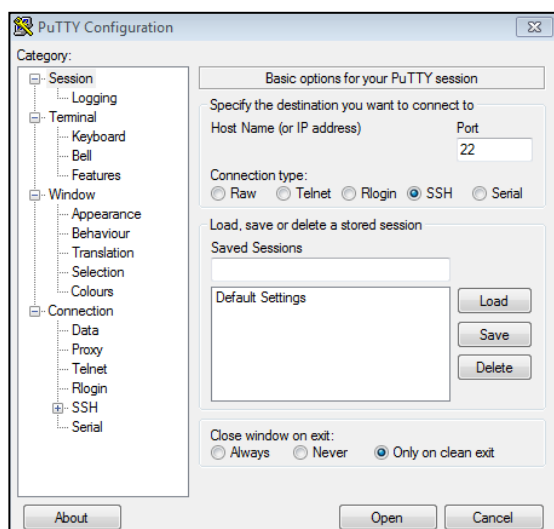


Figure 3-119: PuTTY Configuration Window

Run PuTTY.exe

1. Enter the IP address for the server into **Host Name (or IP Address)** field. Click the **Open** button when finished.

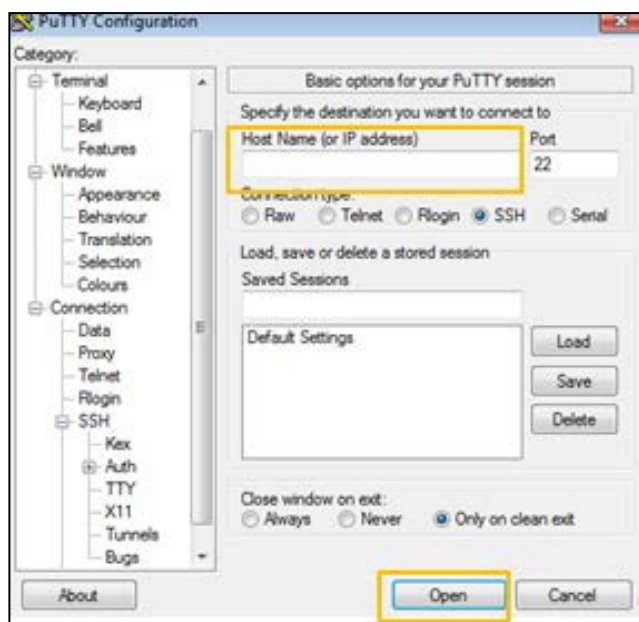


Figure 3-120: PuTTY Configuration - Add IP Address

2. Once the PuTTY program opens, enter your OP username and click **Enter**.

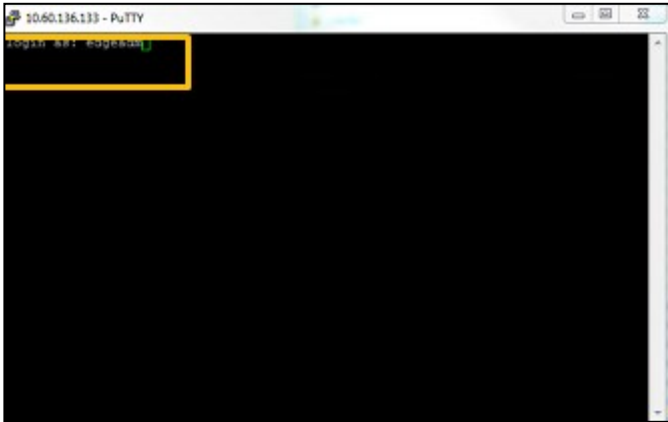


Figure 3-121: Enter Username for PuTTY

Enter your password and then click enter.

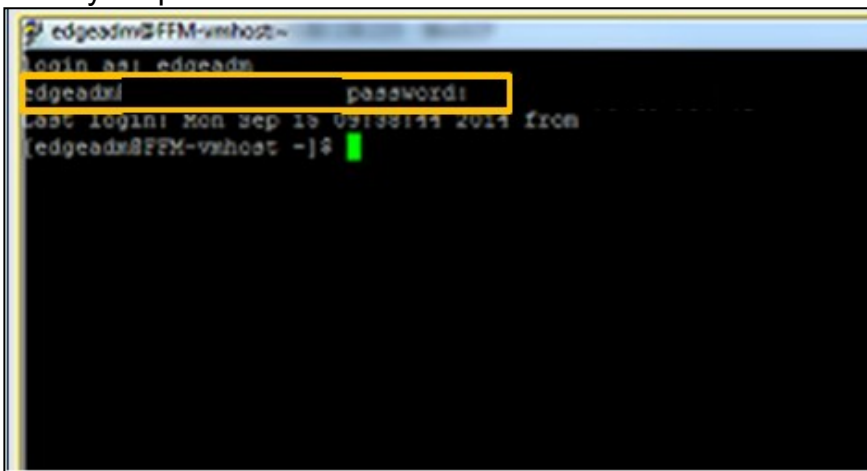


Figure 3-122: Enter Password for PuTTY

The EDGE installation program does not create any directories or move files so the creation of directories is recommended.



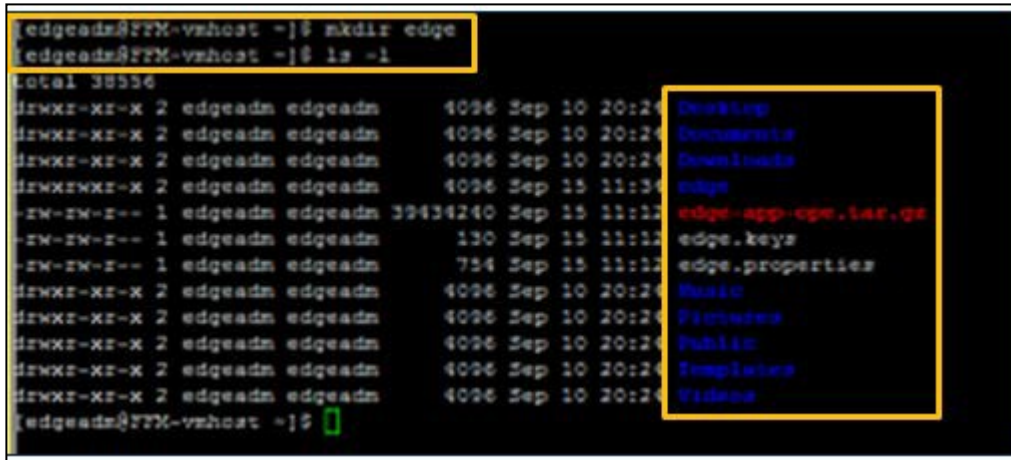
Note: Please do not copy the following commands to the command line directly from this document to avoid execution errors caused by Windows End of Line Conversion. Issuers can either type the commands in the command line or copy commands from this document to NotePad or TextPad, then copy it to the command line.

3. After connecting to the server, create a new directory where the EDGE application files downloaded from the EDGE Registration site. The recommended home location is /opt/edge.
 - a. Enter the following command to change current directory to “/opt”.
 - `cd /opt`and click **Enter**.
 - b. Enter the following command to create a new edge folder:
 - `mkdir edge`and click **Enter**.

- c. Enter the following command to create a listing of all available files currently on the server:

- `ls -l`

and click **Enter**.



```
[edgeadm@FFM-vnhost ~]$ mkdir edge
[edgeadm@FFM-vnhost ~]$ ls -l
total 38556
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Desktop
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Documents
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Downloads
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 13 11:34 edge
-rw-rw-r-- 1 edgeadm edgeadm 39434240 Sep 13 11:12 edge-app-opc.tar.gz
-rw-rw-r-- 1 edgeadm edgeadm 130 Sep 13 11:12 edge.keys
-rw-rw-r-- 1 edgeadm edgeadm 754 Sep 13 11:12 edge.properties
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Music
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Pictures
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Public
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Templates
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Videos
[edgeadm@FFM-vnhost ~]$
```

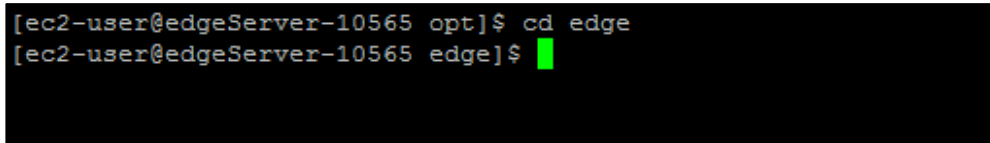
Figure 3-123: Create EDGE folder and Open Files

4. Enter command:

- `cd edge`

and then click **Enter**.

This will take the user to the **edge** folder created in the previous step. The folder will be empty since it was just created.



```
[ec2-user@edgeServer-10565 opt]$ cd edge
[ec2-user@edgeServer-10565 edge]$
```

Figure 3-124 Open EDGE Folder

5. Enter command:

- `tar xvf ~/edge-app-opc.tar.gz`

and click **Enter**.

This will unzip the OP Installation Information file downloaded from the EDGE Registration site. The script that runs will create different directories on your server, including the file inbox, file outbox, database and installation scripts.

```

edgeadm@RTM-vshost edge]$ tar xvf ~/edge-app-ope.tar.gz
...
bin/edge
config/
config/logback.xml
ingest/
  ingest/inbox/
  ingest/outbox/
  nstall/
  nstall/1.CREATE_DATASK_OBJECTS.sql
  nstall/hosts
  nstall/installApplication.sh
  nstall/issuer
  nstall/network
lib/
lib/afp3-common-6.5.0.jar
lib/annex-0.5.0.jar
lib/aspalliance-1.0.jar
lib/aws-java-sdk-1.7.11.jar
lib/bah-2.0b4.jar
lib/cglib-nodep-2.2.2.jar
lib/classmate-1.0.0.jar
lib/commons-beanutils-1.9.1.jar
lib/commons-codec-1.3.jar
lib/commons-collections-3.2.1.jar
lib/commons-configuration-1.7.jar
lib/commons-dbcp-1.4.jar
lib/commons-digester-1.8.1.jar
lib/commons-io-2.4.jar
lib/commons-lang-2.3.jar
lib/commons-logging-1.1.1.jar
lib/commons-pool-1.6.4.jar
lib/easymock-3.2.jar
lib/edge-application.jar

```

Figure 3-125: Unzip On-Premise Installation Information File

6. Next, enter command:

- `cd config/`

and click **Enter**.

This opens the Config folder needed to load and run the Property file.

```

[ec2-user@edgeServer-10565 edge]$ cd config/
[ec2-user@edgeServer-10565 config]$ 

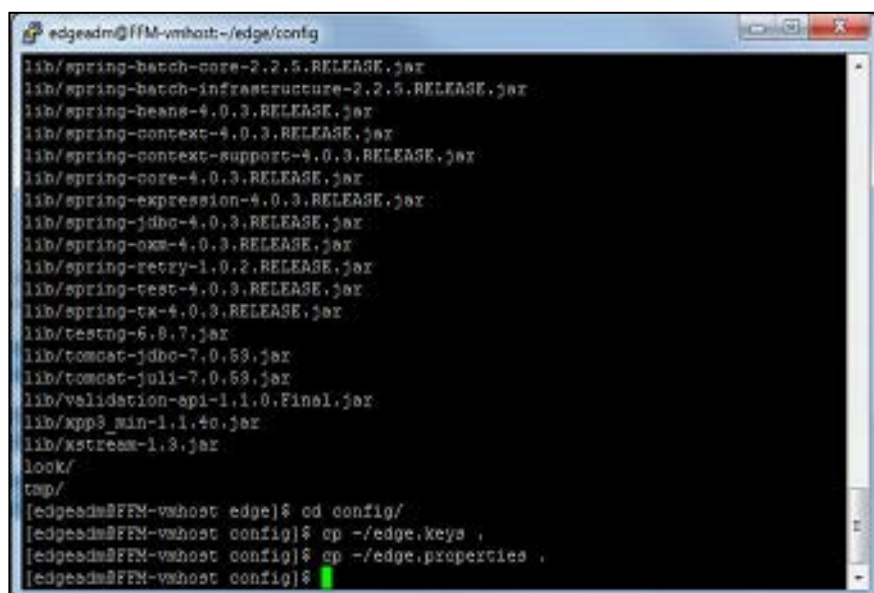
```

Figure 3-126 Open Config Folder

7. Enter commands:

- `cp ~/edge.keys .`
- `cp ~/edge.properties .`

This will open the Deployment Script and Property file downloaded from the EDGE Registration site.



```
edgeadm@ffm-vmhost:~/edge/config
lib/spring-batch-core-2.2.5.RELEASE.jar
lib/spring-batch-infrastructure-2.2.5.RELEASE.jar
lib/spring-beans-4.0.3.RELEASE.jar
lib/spring-context-4.0.3.RELEASE.jar
lib/spring-context-support-4.0.3.RELEASE.jar
lib/spring-core-4.0.3.RELEASE.jar
lib/spring-expression-4.0.3.RELEASE.jar
lib/spring-jdbc-4.0.3.RELEASE.jar
lib/spring-orm-4.0.3.RELEASE.jar
lib/spring-retry-1.0.2.RELEASE.jar
lib/spring-test-4.0.3.RELEASE.jar
lib/spring-tx-4.0.3.RELEASE.jar
lib/testing-6.0.7.jar
lib/tomcat-jdbc-7.0.53.jar
lib/tomcat-juli-7.0.53.jar
lib/validation-api-1.1.0.Final.jar
lib/xpp3_min-1.1.4c.jar
lib/xstream-1.3.jar
lock/
tmp/
[edgeadm@ffm-vmhost edge]$ cd config/
[edgeadm@ffm-vmhost config]$ cp -r /edge.keys .
[edgeadm@ffm-vmhost config]$ cp -r /edge.properties .
[edgeadm@ffm-vmhost config]$
```

Figure 3-127: Open Deployment Script and Property File

8. Next, enter command:

- `vi edge.properties`

then click **Enter**.

This will open the Properties file in an editable format in PuTTY as shown below.

```

issuer=10565
edgeserver=
edgerequestid=
region=us-west-1
edgeserver_size=Large
db_host=localhost
db_port=3306
db_user=edgedbuser
db_password=
batch_outbound_reports_es_id=EdgeServer_10565
batch_outbound_reports_es_version=100
batch_location=${EDGE_HOME}
local_file_ingest=${batch_location}/ingest
batch_csv_file_location_path=${local_file_ingest}/appdata
batch_archive_file_location_path=${local_file_ingest}/archives
batch_input_xml_file_path=${local_file_ingest}/inbox/
batch_outbound_reports_cms_path=${local_file_ingest}/outbox/cms/
batch_outbound_reports_issuer_path=${local_file_ingest}/outbox/issuer/
#aws_s3_bin=edge.binaries.edge2.test
aws_s3_bin=edge.binaries.edge0.test
aws_s3_data=edge.data.edge2.test
aws_s3_command=edge.commands.edge2.test
#aws_s3_bin_validation=edge.binaries.edge2.validation
aws_s3_bin_validation=edge.binaries.edge0.validation
aws_s3_data_validation=edge.data.edge2.validation
aws_s3_command_validation=edge.commands.edge2.validation
aws_s3_inbox=cms.edge.ingest.inbox.363312733669
aws_s3_outbox=cms.edge.ingest.outbox.363312733669
aws_s3_archive=cms.edge.ingest.archive.363312733669
aws_s3_logs=cms.edge.ingest.logs.363312733669
aws_s3_backup=cms.edge.ingest.backup.363312733669
showBuidNumber=True
phoneHomeResponse=phoneHomeResponse-ES27.json
#db_common_schema=EDGE_SRVR_COMMON_2016
#db_prod_schema=EDGE_SRVR_PROD_2016
#db_test_schema=EDGE_SRVR_TEST_2016

```

Figure 3-128: Open Properties File in Editable Format

9. Enter

- i

in order to edit the file (text). Enter a password in the **dbPassword** field.

This password field will be blank when first running the program. Enter a password and save this password to a secure location. This password will be used to log into the database.

Note: db_password, edgerequestid, and edgeserver fields should have an associated value on issuers' servers but is hidden in the figure.



Note: Issuers own the OP servers and are responsible for its maintenance, including passwords. Issuers will need to reinstall MySQL if dbPassword is lost. For issuers who have provisioned servers, they can see the password in their properties file.

```

issuer=10565
edgeserver=
edgerequestid=
region=us-west-1
edgeserver_size=Large
db_host=localhost
db_port=3306
db_user=edgedbuser
db_password=
batch_outbound_reports_es_id=EdgeServer_10565
batch_outbound_reports_es_version=100
batch_location=${EDGE_HOME}
local_file_ingest=${batch_location}/ingest
batch_csv_file_location_path=${local_file_ingest}/appdata
batch_archive_file_location_path=${local_file_ingest}/archives
batch_input_xml_file_path=${local_file_ingest}/inbox/
batch_outbound_reports_cms_path=${local_file_ingest}/outbox/cms/
batch_outbound_reports_issuer_path=${local_file_ingest}/outbox/issuer/
#aws_s3_bin=edge.binaries.edge2.test
aws_s3_bin=edge.binaries.edge0.test
aws_s3_data=edge.data.edge2.test
aws_s3_command=edge.commands.edge2.test
#aws_s3_bin_validation=edge.binaries.edge2.validation
aws_s3_bin_validation=edge.binaries.edge0.validation
aws_s3_data_validation=edge.data.edge2.validation
aws_s3_command_validation=edge.commands.edge2.validation
aws_s3_inbox=cms.edge.ingest.inbox.363312733669
aws_s3_outbox=cms.edge.ingest.outbox.363312733669
aws_s3_archive=cms.edge.ingest.archive.363312733669
aws_s3_logs=cms.edge.ingest.logs.363312733669
aws_s3_backup=cms.edge.ingest.backup.363312733669
showBuidNumber=True
phoneHomeResponse=phoneHomeResponse-ES27.json
#db_common_schema=EDGE_SRVR_COMMON_2016
#db_prod_schema=EDGE_SRVR_PROD_2016
#db_test_schema=EDGE_SRVR_TEST_2016
-- INSERT --

```

Figure 3-129: Enter New Password for Database

10. The OP EDGE server property “**edgeserver_size**” determines how much memory is allocated for your application. By default, the “**edgeserver_size**” property is set to “S” (small). The possible values for this property are:

- “S” (Small) = 3 GB RAM
- “M”(Medium) = 4 GB RAM
- “L” (Large) = 5 GB RAM

To improve the performance of your OP EDGE server, you can increase your server size settings to process files faster. To adjust the size of the property “**edgeserver.size**”, please execute the following:

1. Execute the following command:

```
vi /opt/edge/config/edge.properties
```

2. Locate the line with the property “**edgeserver_size**” and Modify the default value of “S” to “M” or “L” as necessary

```
edgerequestid=
region=us-west-1
edgeserver_size=Large
```

Figure 3-130: edgeserver_size field

Note: If you have multiple EDGE server MySQL instances, you can consolidate them into a single MySQL instance. This will help reduce the number of servers needed to procure and maintain. There are two (2) options for consolidating instances into a single MySQL instance:

- Consolidating servers before installing the EDGE application
- Migrating servers following the installation of the EDGE application

11. To consolidate issuers before installing the EDGE application, begin by editing the “**edge.properties**” on the server

a. Run the following command:

- `vi /opt/edge/config/edge.properties`

b. Once the list of properties display, add or modify the EDGE server properties to specify the following new database properties and set their values accordingly:

- `db_host = new_mysql_server_host`
- `db_port = <PORT Number>`
- `db_user = edgeapp_<ISSUER ID>`
- `db_password = <EDGE server password>`
- `db_common_schema = EDGE_SRVR_<ISSUER ID>_COMMON`
- `db_test_schema = EDGE_SRVR_<ISSUER ID>_TEST`
- `db_prod_schema = EDGE_SRVR_<ISSUER ID>_PROD`
- `db_validation_schema = EDGE_SRVR_<ISSUER ID>_VALIDATION`
- `db_common_schema_v = EDGE_SRVR_<ISSUER ID>_COMMON_V`

```
[ec2-user@edgeServer-29089 ~]$ vi /opt/edge/config/edge.properties
edgeserver_size=Small
db_host= new_mysql_server_host
db_port=
db_user=edgeapp_ISSUERID
db_password=
db_common_schema = EDGE_SRVR_ISSUERID_COMMON
db_test_schema = EDGE_SRVR_ISSUERID_TEST
db_prod_schema = EDGE_SRVR_ISSUERID_PROD
db_validation_schema = EDGE_SRVR_ISSUERID_VALIDATION
db common schema v = EDGE SRVR ISSUERID COMMON V
```

Figure 3-131: Add/Modify EDGE Properties

12. Next, click **ESC**, then type command:

- `:wq`

and click **Enter**.

This will save the file with the new password and exit the file.

```
#db_common_schema=EDGE_SRVR_COMMON_2016
#db_prod_schema=EDGE_SRVR_PROD_2016
#db_test_schema=EDGE_SRVR_TEST_2016
:wq
```

Figure 3-132: Save File and Exit

13. Change ownership of the /opt/edge and all the sub-directories and files to **edgeadm**. The **edgeadm** user must be configured to have “**sudo**” privileges. Enter command:

```
• chown -R edgeadm:edgeadm /opt/edge
```

14. Open the install folder by entering the following command:

```
• cd ../install/
```

and click **Enter**.

```
[edgeadm@FFM-vmlhost edge]$ cd config/
[edgeadm@FFM-vmlhost config]$ cp -r /edge.keys .
[edgeadm@FFM-vmlhost config]$ cp -r /edge.properties .
[edgeadm@FFM-vmlhost config]$ vi edge.properties
[edgeadm@FFM-vmlhost config]$ vi edge.properties
[edgeadm@FFM-vmlhost config]$ cd ../install/
```

Figure 3-133: Open Install Folder

Note: The following command will execute under only the two (2) conditions below:

- The user for the following commands must have MySQL root access and cannot be the same user that is defined in the edge.properties file as the db_user. If an additional user does not exist, then a new user ID must be created with root MySQL privileges for this purpose.
- Please do not copy commands to the Linux command line directly from this document to avoid execution errors caused by Windows End of Line Conversion that cause the command to fail. Issuers can either type the commands in the command line or copy commands from this document to NotePad or TextPad, then copy it to the command line.



15. Enter command:

```
• ./installApplication.sh -dbUser <DBA USER> - dbPassword <PASSWORD> and click Enter.
```

- The User ID specified in the **db_user** property must be different than the User ID configured in MySQL that will be used by the EDGE application. If the User ID is already configured in the database, the installation program will fail.
- The sudo command may prompt you to enter a password. If prompted, enter the same password that you used to log onto the server and click **Enter**.

The EDGE Application will now install and create the following:

- The User ID associated with the **db_user** property. The default value = **edgedbuser**
- The password for **edgedbuser** is set using **db_password** property
- All reference tables along with reference data under **db_common_schema**, including issuer specific reference data.
- The following schemas, along with their default values:
 - **db_common_schema** = **EDGE_SRVR_COMMON**
 - **db_test_schema** = **EDGE_SRVR_TEST**
 - **db_prod_schema** = **EDGE_SRVR_PROD**
 - **db_validation_schema** = **EDGE_SRVR_VALIDATION**
 - **db_common_schema_v** = **EDGE_SRVR_COMMMON_V**



Note: If you have changed the schema names in the properties file, then those will be the schema names that you see, rather than the default values indicated above. If more than one (1) schema is on a particular MySQL instance, the schemas can be differentiated by entering an Issuer ID in the property name. For example: **EDGE_SRVR_<ISSUER ID>_COMMON**

```
ec2-user@edge-dev-1 /opt/edge/install
[ec2-user@edge-dev-1 install]$ ./installApplication.sh -dbUser edgedbauser -dbPassword seswU5aC
```

Figure 3-134: Install EDGE Application

16. After clicking Enter, the script will run to install the EDGE application. The process can take two (2) to three (3) minutes to complete. Once finished, verify there are no error messages displayed. If no error messages display, provisioning was successful.

Contact the FMCC at EDGE_Server_Data@cms.hhs.gov if errors occurred.

```
14:39:31.961 [main] DEBUG o.a.h.i.c.PoolingClientConnectionManager - Connection released: [id: 1][route: {s}->https://edge.commands.dev.s
ive: 2; route allocated: 1 of 50; total allocated: 2 of 50]
14:39:31.961 [main] DEBUG c.a.s.s.m.t.XmlResponsesSaxParser - Parsing XML response document with handler: class com.amazonaws.services.s3
axParser$ListBucketHandler
14:39:31.962 [main] DEBUG c.a.s.s.m.t.XmlResponsesSaxParser - Examining listing for bucket: edge.commands.dev
14:39:31.965 [main] DEBUG com.amazonaws.request - Received successful response: 200, AWS Request ID: F652F7719FC24A0E
14:39:31.965 [main] DEBUG o.s.jdbc.core.JdbcTemplate - Executing SQL query [SELECT * FROM REMOTE_CMD_QUEUE WHERE REMOTE_CMD_STATUS='SCHED
TED_DT, EXTERNAL_CMD_ID]
14:39:31.965 [main] DEBUG o.s.jdbc.datasource.DataSourceUtils - Fetching JDBC Connection from DataSource
14:39:31.967 [main] DEBUG o.s.jdbc.datasource.DataSourceUtils - Returning JDBC Connection to DataSource
log4j:WARN No appenders could be found for logger (gov.hhs.cms.ff.fm.edge.app.command.impl.QueueCommandImpl).
log4j:WARN Please initialize the log4j system properly.
```

Figure 3-135: Confirm Successful Provisioning

Note: If you have already installed the EDGE application and want to consolidate issuers into a single MySQL instance, please execute the following steps:

17. Dump the existing MySQL data to flat files. Execute the following commands to dump data from current database to flat files:

```
mysqldump --user= <DB USER> --password= <PASSWORD> EDGE_SRVR_COMMON >
edge_common.sql
mysqldump --user= <DB USER> --password= <PASSWORD> EDGE_SRVR_TEST > edge_test.sql
mysqldump --user= <DB USER> --password= <PASSWORD> EDGE_SRVR_PROD > edge_prod.sql
mysqldump --user= <DB USER> --password= <PASSWORD> EDGE_SRVR_VALIDATION >
edge_validation.sql
mysqldump --user= <DB USER> --password= <PASSWORD> EDGE_SRVR_COMMON_V >
edge_common_v.sql
```

```
[ec2-user@edgeServer-29089 ~]$ mysqldump --user=edgedbuser --password=KFkgIJ9t EDGE_SRVR_COMMON > edge_common.sql;
mysqldump: [Warning] Using a password on the command line interface can be insecure.
You have new mail in /var/spool/mail/ec2-user
[ec2-user@edgeServer-29089 ~]$ mysqldump --user=edgedbuser --password=KFkgIJ9t EDGE_SRVR_PROD > edge_prod.sql;
mysqldump: [Warning] Using a password on the command line interface can be insecure.
[ec2-user@edgeServer-29089 ~]$ mysqldump --user=edgedbuser --password=KFkgIJ9t EDGE_SRVR_TEST > edge_test.sql;
mysqldump: [Warning] Using a password on the command line interface can be insecure.
[ec2-user@edgeServer-29089 ~]$ mysqldump --user=edgedbuser --password=KFkgIJ9t EDGE_SRVR_VALIDATION > edge_validation.sql;
mysqldump: [Warning] Using a password on the command line interface can be insecure.
[ec2-user@edgeServer-29089 ~]$ mysqldump --user=edgedbuser --password=KFkgIJ9t EDGE_SRVR_COMMON_V > edge_common_v.sql;
[ec2-user@edgeServer-29089 ~]$ ls -l
total 50604
-rw-r--r--. 1 root      root           81 Apr 11 18:14 1
-rw-rw-r--. 1 ec2-user ec2-user 25585210 Jul 19 13:41 edge_common.sql
-rw-rw-r--. 1 ec2-user ec2-user          0 Jul 19 13:40 edge_common_v.sql
-rw-rw-r--. 1 ec2-user ec2-user   118256 Jul 19 13:40 edge_prod.sql
-rw-rw-r--. 1 ec2-user ec2-user   118569 Jul 19 13:40 edge_test.sql
-rw-rw-r--. 1 ec2-user ec2-user   119365 Jul 19 13:40 edge_validation.sql
```

Figure 3-136: MySQL Data Dump Commands

18. Move the MySQL data generated by the data dump executed to the new target server. You may need to use WinSCP (or similar program) to download and upload files to the target server.
19. Create a new database on the target MySQL server by executing the following commands:

- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_COMMON
- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_TEST
- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_PROD
- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_VALIDATION
- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_COMMON_V

```

mysql> CREATE DATABASE EDGE_SRVR_ISSUERID_COMMON;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE DATABASE EDGE_SRVR_ISSUERID_TEST;
Query OK, 1 row affected (0.01 sec)

mysql> CREATE DATABASE EDGE_SRVR_ISSUERID_PROD;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE DATABASE EDGE_SRVR_ISSUERID_VALIDATION;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE DATABASE EDGE_SRVR_ISSUERID_COMMON_V;
Query OK, 1 row affected (0.00 sec)

mysql> USE EDGE_SRVR_ISSUERID_COMMON;
Database changed
mysql> SHOW TABLES;
Empty set (0.00 sec)

mysql> USE EDGE_SRVR_ISSUERID_TEST;
Database changed
mysql> SHOW TABLES;
Empty set (0.00 sec)

mysql> USE EDGE_SRVR_ISSUERID_PROD;
Database changed
mysql> SHOW TABLES;
Empty set (0.00 sec)

mysql> USE EDGE_SRVR_ISSUERID_VALIDATION;
Database changed
mysql> SHOW TABLES;
Empty set (0.00 sec)

mysql> USE EDGE_SRVR_ISSUERID_COMMON_V;
Database changed
mysql> SHOW TABLES;
Empty set (0.00 sec)

```

Figure 3-137: Create Databases

20. Create a new database user and configure this user to have access to the newly created database. It is recommended that you enter username:

- edgeapp_<ISSUER ID>

```

mysql> CREATE USER 'edgeapp_      '@localhost' IDENTIFIED BY '      ';
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE USER 'edgeapp_      '@' IDENTIFIED BY 'GreenEggs';
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_      _COMMON.* TO 'edgeapp_      '@localhost' IDENTIFIED BY '      ' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_      _COMMON.* TO 'edgeapp_      '@' IDENTIFIED BY '      ' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_      _TEST.* TO 'edgeapp_      '@localhost' IDENTIFIED BY '      ' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_      _TEST.* TO 'edgeapp_      '@' IDENTIFIED BY '      ' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_      _PROD.* TO 'edgeapp_      '@localhost' IDENTIFIED BY '      ' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_      _PROD.* TO 'edgeapp_      '@' IDENTIFIED BY '      ' WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

```

Figure 3-138: Create New Database User

21. Finally, load the data from the new target server to the newly created database tables. Execute the following commands:

- `sudo mysql EDGE_SRVR_<ISSUER ID>_COMMON <edge_common.sql`
- `sudo mysql EDGE_SRVR_<ISSUER ID>_TEST <edge_test.sql`
- `sudo mysql EDGE_SRVR_<ISSUER ID>_PROD <edge_prod.sql`
- `sudo mysql EDGE_SRVR_<ISSUER ID>_VALIDATION <edge_validation.sql`
- `sudo mysql EDGE_SRVR_<ISSUER ID>_COMMON_V <edge_common.v.sql`

```
ec2-user@Edge-31492-Test-Edge4-T1 ~]$ sudo mysql EDGE_SRVR_31492_COMMON < edge_common.sql
ec2-user@Edge-31492-Test-Edge4-T1 ~]$ sudo mysql EDGE_SRVR_31492_TEST < edge_test.sql
You have new mail in /var/spool/mail/ec2-user
ec2-user@Edge-31492-Test-Edge4-T1 ~]$ sudo mysql EDGE_SRVR_31492_PROD < edge_prod.sql
ec2-user@Edge-31492-Test-Edge4-T1 ~]$
```

Figure 3-139: Load Data to New Tables

IV. Configure CRON

1. You may elect to configure your OP EDGE server to pick up files automatically for processing, executing CMS deployed maintenance releases and commands, by setting up **CRON**.

In PuTTY, enter command: The following command displays black characters highlighted in gray

- `crontab -e`

and press **Enter**.

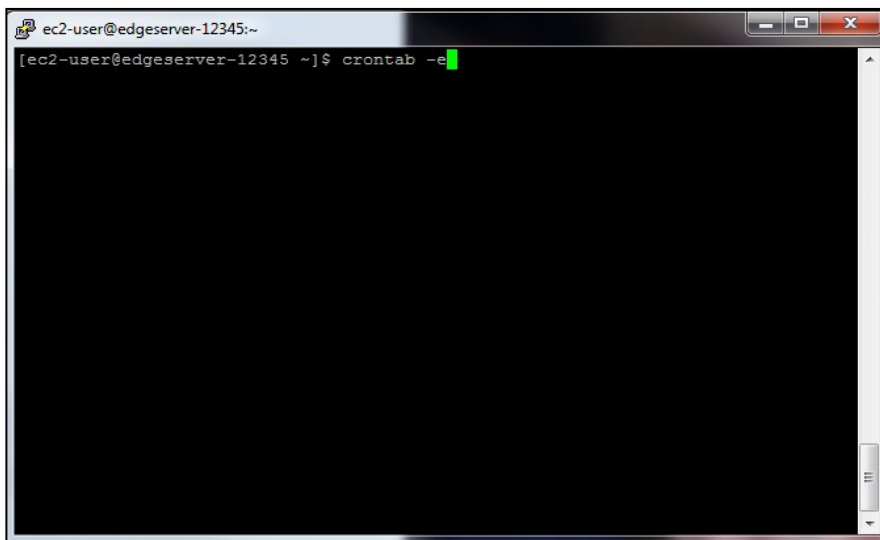


Figure 3-140: Enter CRON Command

2. Setup the timing for **cron** to run.

The configuration is setup to run **cron** every minute - you may choose to configure it to run on a different time. Press “i” and enter the following command:

- i
- */1 * * * * /opt/edge/bin/edge ingest

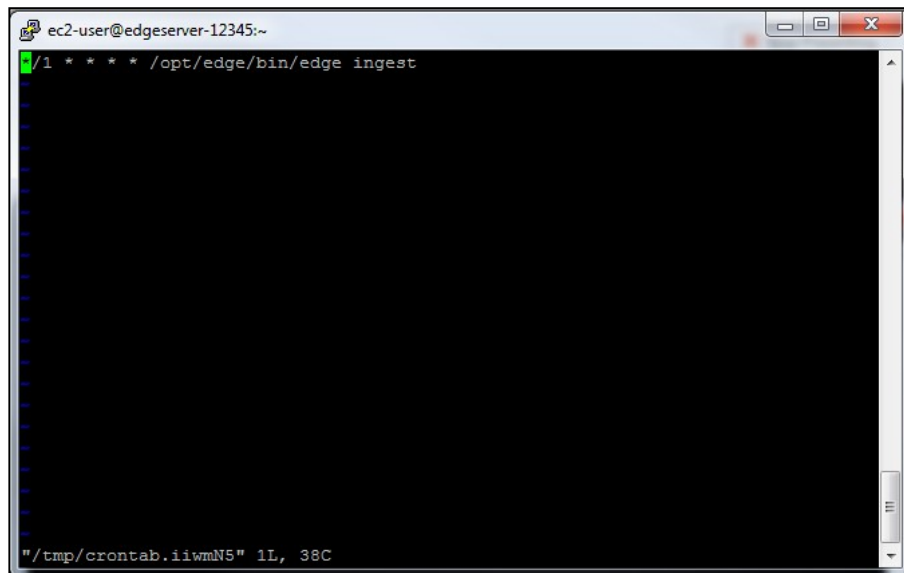


Figure 3-141: Configure Cron Timing

3. Press **ESC** and enter command the following command to save and exit the file:

- :wq

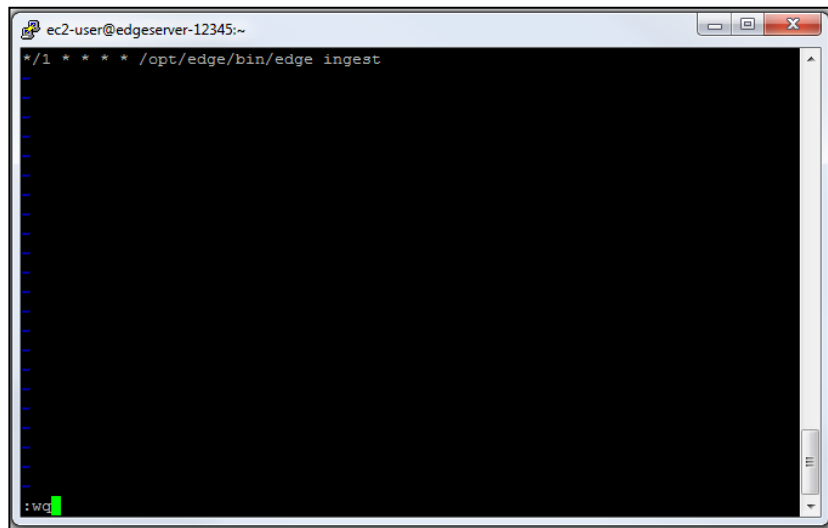


Figure 3-142: Save and Exit Cron

4. Once the script completes from **Step 2**, log back into the EDGE Registration site, search for your request and confirm that the status is now **Provisioned**.



Note: It will take between five (5) and 10 minutes from the time the script completes for the EDGE server request status to change to **PROVISIONED**.

FINANCIAL MANAGEMENT

EDGE Server Request Search

User Name: ZFMLOADTEST1991

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Issuer HIOS ID Search Value : 10297

[Back](#) [Search](#)

Issuer Legal Business Name	Issuer HIOS ID	TPA ID - Name	EDGE Server Name	AWS Account Number	Request ID	Request Status	Request Type	Last Updated By (HIOS User ID)	Last Updated Date	Action
	10297		Test1		106183	Provisioned	New Server Request	ZFMLOADTEST6236	9/15/14 12:06:29 PM	view

Figure 3-143: Confirm Provisioned Request

V. Provisioning Failed

If the OP provisioning script does not complete successfully, there is an error in the script and issuers will see error messages in the PuTTY program while attempting to install the EDGE application.



Note: Contact the FMCC team to determine the reason provisioning failed at EDGE_server_data@cms.hhs.gov.

Once the cause of the failure has been determined and the installation scripts have been updated, the request will return to a status of **Pending Provisioning**. The issuer can return back to the request, open it and download the updated installation scripts again and execute the provisioning process.

3.8.6 AWS EDGE Server Provisioning

This section provides the steps issuers must follow in order to successfully provision an AWS EDGE server, confirm successful provisioning, and connect to the EDGE server. It will also provide guidance on how to proceed in the event that provisioning fails.

Once an Amazon EDGE server request has been approved by CMS, the EDGE server is automatically provisioned in the AWS cloud using the details provided, by the issuer or TPA, during registration. The provisioning process itself is triggered by CMS approving the registration request through the EDGE Server 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.

Issuers with an Amazon EDGE server should confirm provisioning was successful by following the steps below.

I. 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. Log in and access the ESM using the steps in [Section 3.6 Accessing the ESM Website](#).

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

The screenshot shows the 'FINANCIAL MANAGEMENT' header and 'EDGE Server Home' sub-header. Below the header are three buttons: 'Manage EDGE Server', 'Create EDGE Server Request', and 'Search Requests'. A section titled 'EDGE Server Request Inbox' displays a table of requests. The table has columns: Issuers HIOS ID, Issuer Legal Business Name, Server Request ID, Request Type, Request Status, Status Date - Time, Created By, and Action. One entry is shown with a status of 'Pending Provisioning', which is highlighted by a yellow box. The status is also highlighted by a yellow box in the original image.

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
49693		106227	New AWS Server	Pending Provisioning	9/3/14 3:25:18 PM	EDREQUESTER8@FFETEST.COM	view

Showing 1 to 1 of 1 entries

Figure 3-144: Pending Provisioning

2. The information provided during the submission of the registration request is 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 to see the status of **Provisioning in Progress**.
3. Click the **Search Requests** button at the top right.

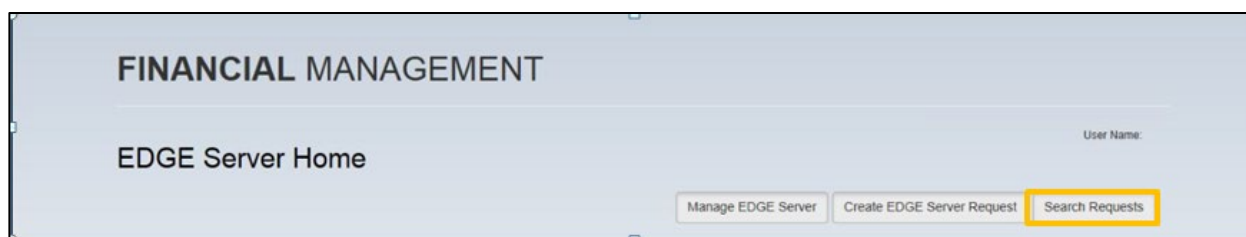


Figure 3-145: Search Requests Button

4. In the Search Requests screen, select **Issuer HIOS ID** from the **Search Field** dropdown menu and enter your HIOS Issuer ID in the **Search Value** Field. Click the **Search** button to display the results. Any active requests associated with your Issuer HIOS ID will display.

EDGE Server Request Search

User Name: ACCNFM123@FFETEST.COM

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Issuer HIOS ID Search Value : 15509

[Back](#) [Search](#)

Figure 3-146: Search Request Screen

- The request will display with a status of **Provisioning in Progress**. You can refresh the page periodically to track the status as it updates. When provisioning has completed, the status will change to **Provisioned**.



Note: The process described above typically takes about 60 minutes to complete. Issuers will be able to access their AWS accounts and confirm successful provisioning.

EDGE Server Request Search

User Name: EDCMSTEST1@FFETEST.COM

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Request ID Search Value : 106853

[Back](#) [Search](#)

Issuer Legal Business Name	Issuer HIOS ID	TPA ID - Name	EDGE Server Name	AWS Account Number	Request ID	Request Status	Request Type	Last Updated By (HIOS User ID)	Last Updated Date	Action
	26386	15040	Test		106853	Provisioning in Progress	New AWS Server	EDCMSTEST@FFETEST.COM	04/09/14 11:59:06	view

Figure 3-147: Provisioning in Progress

The status **Provisioned** indicates that the Amazon EDGE server has connected with the Phone Home service for the first time.

EDGE Server Request Search

User Name: EDTEST1@FFTEST.COM

Back to EDGE Server Home

Search Criteria

Search Field : Request ID Search Value : 106217

Back Search

Issuer Legal Business Name	Issuer HIOS ID	TPA ID - Name	EDGE Server Name	AWS Account Number	Request ID	Request Status	Request Type	Last Updated By (HIOS User ID)	Last Updated Date	Action
	34606		Amin		106217	Provisioned	New AWS Server	CMS	8/29/14 12:12:16 AM	view

Showing 1 to 1 of 1 entries

« First « Prev 1 Next » Last »

Figure 3-148: Server Provisioned Status

II. Provisioning Failed

The EDGE Server Registration site monitors the completion of the AWS provisioning script. If the provisioning script does not complete successfully 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.

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

FINANCIAL MANAGEMENT

EDGE Server Home

User Name:

Manage EDGE Server Create EDGE Server Request Search Requests

EDGE Server Request Inbox Displays EDGE server requests requiring action

Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
49693		106227	New AWS Server	Pending Provisioning	9/3/14 3:25:18 PM	EDREQUESTER8@FFTEST.COM	view

Showing 1 to 1 of 1 entries

« First « Prev 1 Next » Last »

Figure 3-149: Pending Provisioning

When provisioning has failed, the Issuer Submitter will need to contact the FMCC Team at EDGE_server_data@cms.hhs.gov to determine the cause of the failure. Your representative will provide more details on the cause of the failure and the resolution process. Errors may be related to EDGE Server Storage, insufficient capacity issues for AWS or incorrect AWS Region, and the issuer may need to open up a ticket with AWS in order to assist in supporting solution. Please update your FMCC representative on the progress.

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**.

3.8.6.1 Confirming Successful AWS EDGE Server Provisioning and Connecting to the Server

I. Download PuTTY

PuTTY is a commonly used application for connecting to your server. The steps for downloading and configuring PuTTY are described below. Issuers may use the SSH client of choice and adapt these instructions if they choose to use a different SSH client.

To download PuTTY to connect to the provisioned server:

6. Go to www.putty.org.
7. Click you can download PuTTY [here](#).

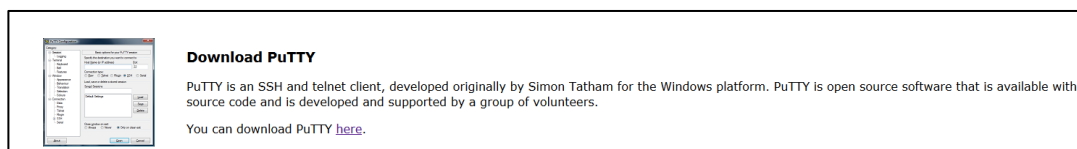


Figure 3-150: PuTTY Home Page

Download both **putty.exe** and **puttygen.exe**.

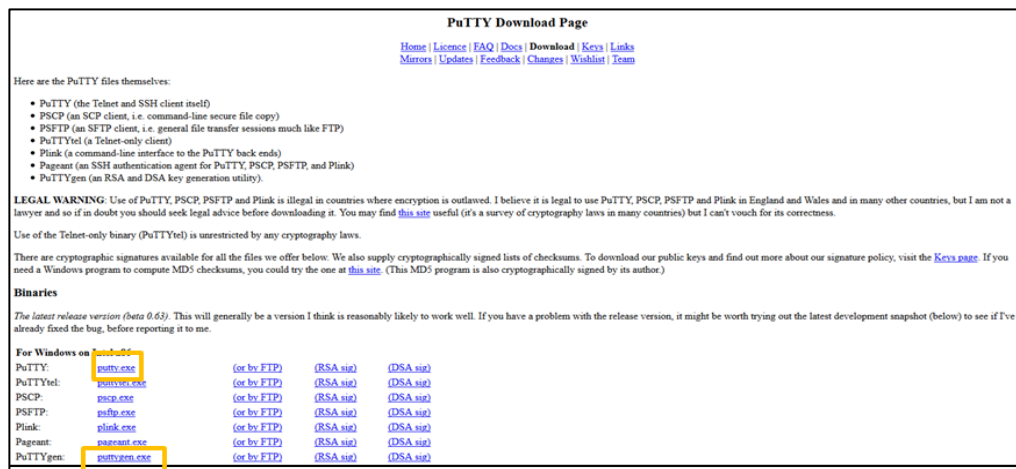


Figure 3-151: PuTTY Download Page

II. Configure Puttygen.exe

8. Open and run the puttygen.exe file. The **PuTTYgen Program Screen** window (shown below) will appear.
9. Click **Load** and then select the Key Pair file that was saved (.pem file) in [Section 3.4.2 Request an AWS EDGE Server Instance](#).

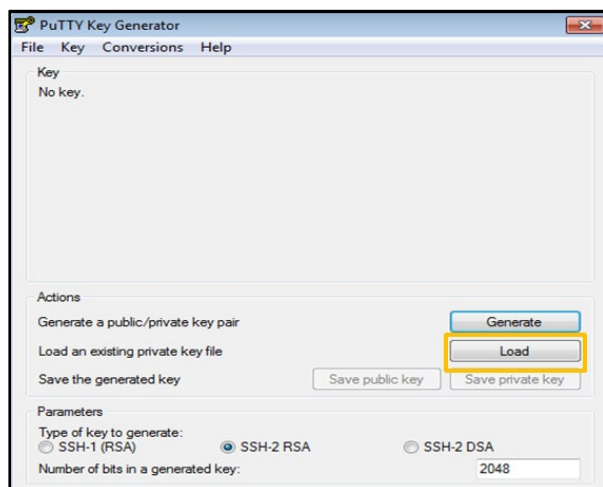


Figure 3-152: PuTTYgen Program Screen

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.

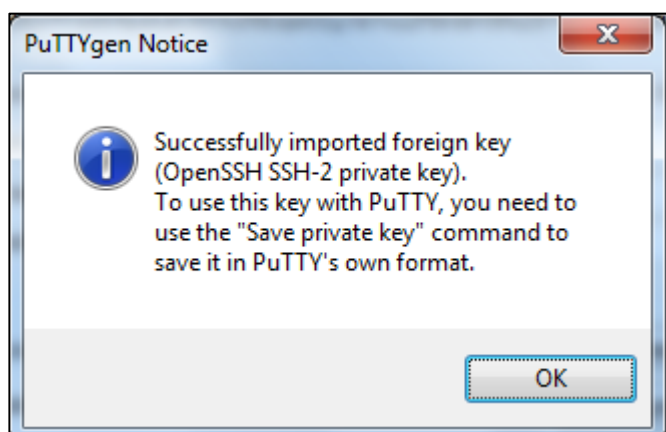


Figure 3-153: PuTTYgen Notice

10. Click **Yes** in the **PuTTYgen Warning** window to save the key without a passphrase and the **Save private key** button.

You may save the key with a passphrase if desired. The passphrase is not needed for successful AWS provisioning and helps the issuer with encryption. If the passphrase is lost, then CMS cannot retrieve it.



Figure 3-154: Save Private Key

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



Note: 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.

III. *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.

11. Log in to the AWS account, click **Services**, click **All AWS Services**, and then click **EC2**.

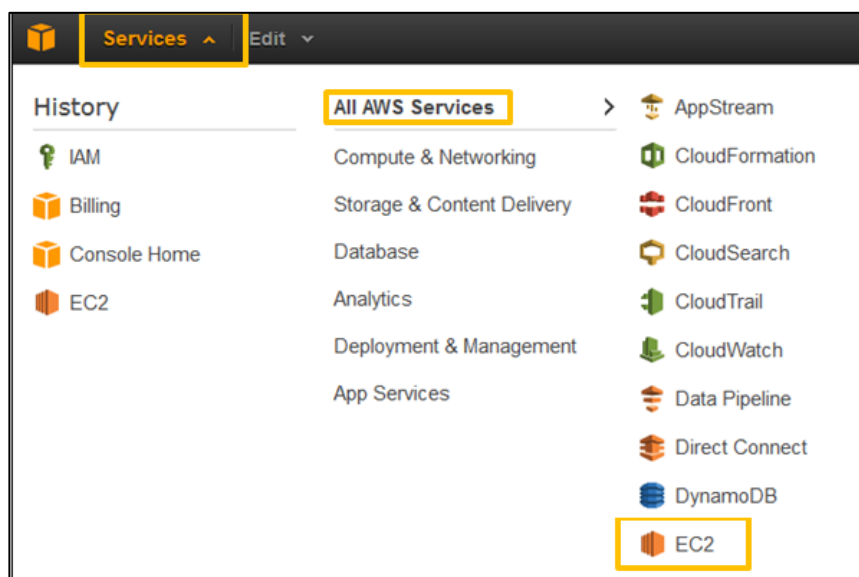


Figure 3-155: Services and All AWS Services Dropdowns

12. Click **Instances** on the upper left corner of the page.

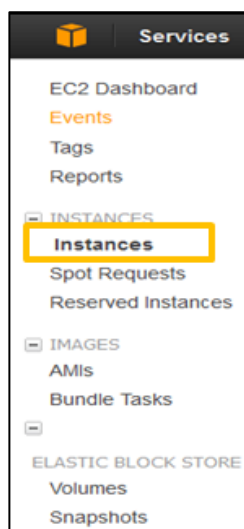


Figure 3-156: EC2 Options

13. Issuers will find the available EDGE server instances listed in the menu. If a user manages multiple servers, the user will see multiple EDGE server instances. Identify the correct server by finding the Issuer HIOS ID in the **Name** column on the right and an **Instance State** set to **running**.

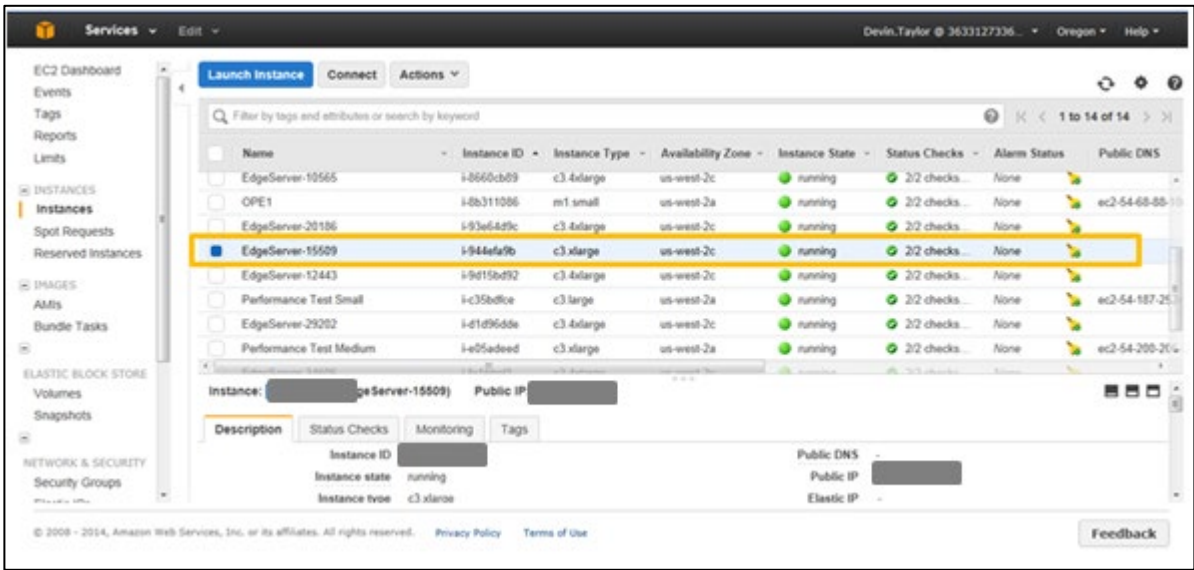


Figure 3-157: All Instances List

14. Select the **EDGE Server Instance**. You can 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. 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.

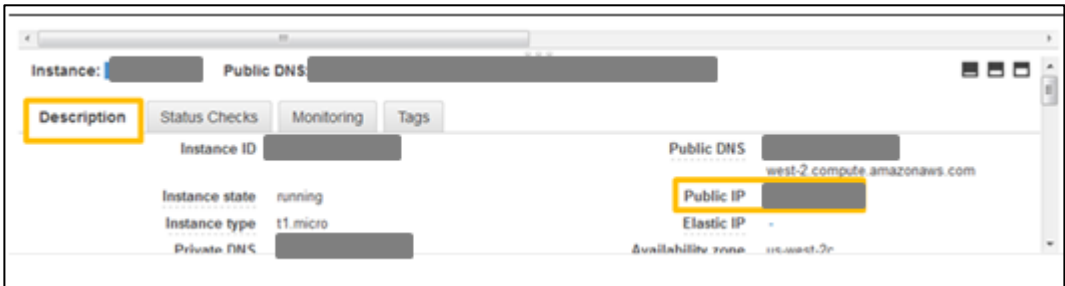


Figure 3-158: Public IP Address

15. Locate the PuTTY.exe file that was downloaded.

After running PuTTY.exe, the PuTTY configuration window will appear.

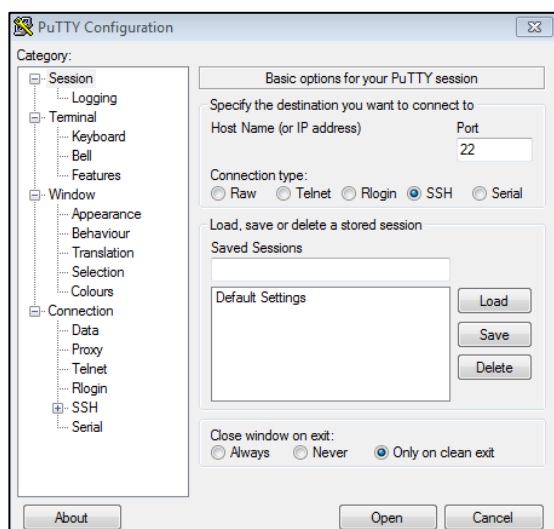


Figure 3-159: PuTTY Configuration Window

16. Select the **Connection type “SSH”** and then enter “ec2-user@<IP address>” into “Host Name (or IP address)”.

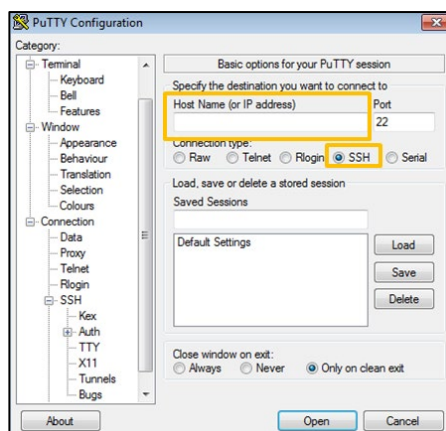


Figure 3-160: PuTTY Configuration - Add IP Address

17. Click the **SSH dropdown** from the Category list on the left side of the PuTTY Configuration window and then select **Auth**.

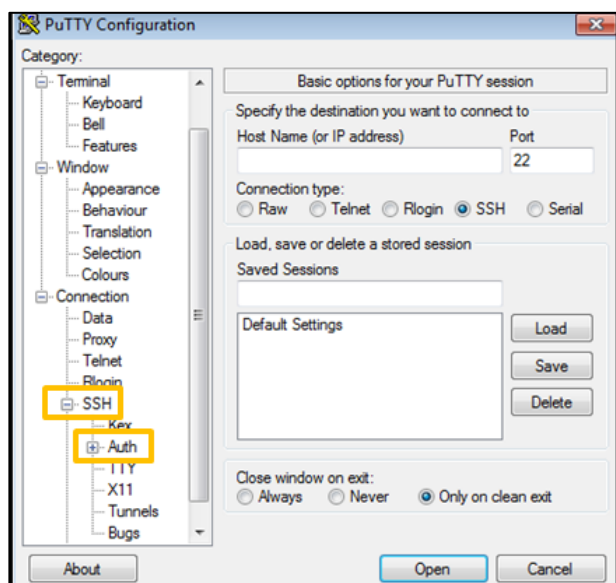


Figure 3-161: Category List on PuTTY Configuration Window

18. Authentication Options will appear. Click **Browse**.

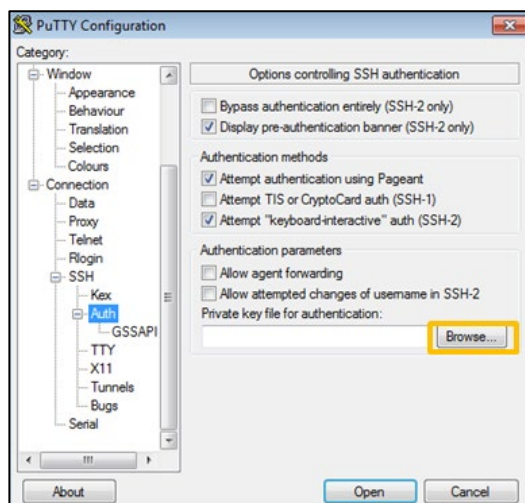


Figure 3-162: PuTTY Authentication Options

19. Locate the PuTTY Private Key and click **Open**.

The Private Key was created and saved in Step 3 of the Configure Puttygen.exe section above. This file should be in .ppk format.

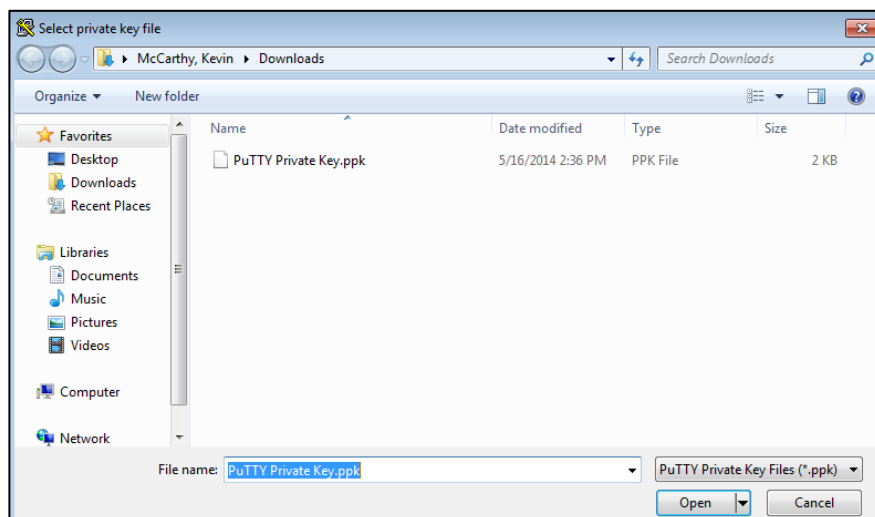


Figure 3-163: Browsing for PuTTY Private Key

20. After loading the Private Key file, save the 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.

21. In the PuTTY configuration window, click the **Session** option at the top right. Make sure the Host Name field is populated correctly with the name you entered. Enter a name for your session in the **Save Sessions** field and then click **Save**.

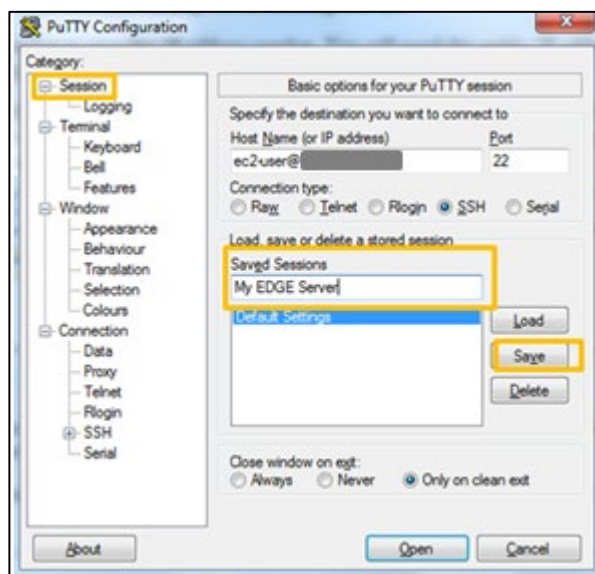


Figure 3-164: Save Session

22. The session will appear as shown below. Click **Open** in the PuTTY Configuration window to open the PuTTY program.

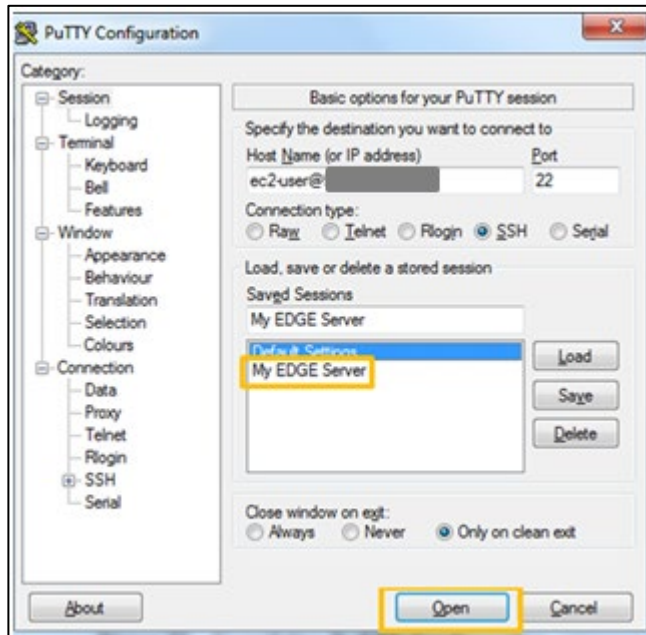


Figure 3-165: Completing PuTTY Configuration

23. 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.



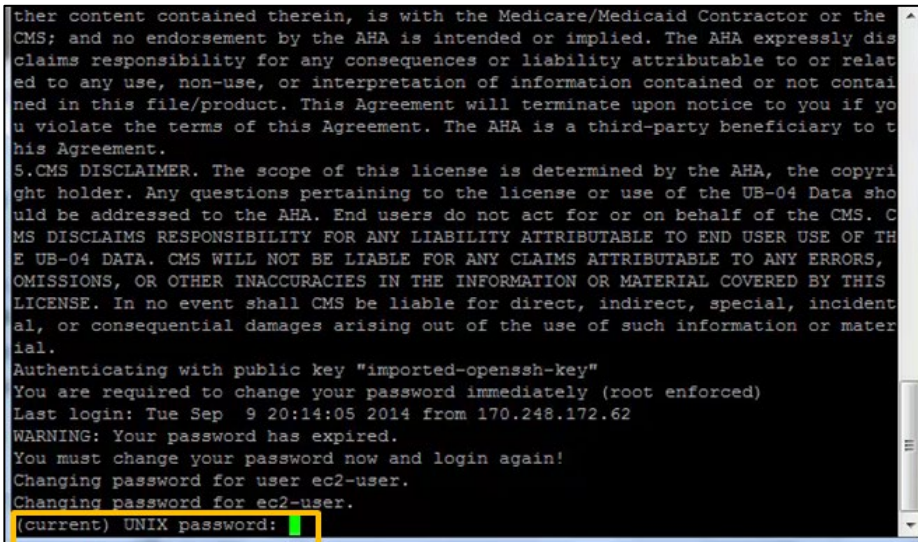
Figure 3-166: PuTTY Security Alert

IV. Connect to EDGE Instance and confirm functionality

When logging into the server for the first time, you will need to enter a password.

Enter the following in the PuTTY window: **edgeserver (enter as one [1] 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.



```
ther content contained therein, is with the Medicare/Medicaid Contractor or the
CMS; and no endorsement by the AHA is intended or implied. The AHA expressly dis
claims responsibility for any consequences or liability attributable to or relat
ed to any use, non-use, or interpretation of information contained or not contai
ned in this file/product. This Agreement will terminate upon notice to you if yo
u violate the terms of this Agreement. The AHA is a third-party beneficiary to t
his Agreement.
5.CMS DISCLAIMER. The scope of this license is determined by the AHA, the copyri
ght holder. Any questions pertaining to the license or use of the UB-04 Data sho
uld be addressed to the AHA. End users do not act for or on behalf of the CMS. C
MS DISCLAIMS RESPONSIBILITY FOR ANY LIABILITY ATTRIBUTABLE TO END USER USE OF TH
E UB-04 DATA. CMS WILL NOT BE LIABLE FOR ANY CLAIMS ATTRIBUTABLE TO ANY ERRORS,
OMISSIONS, OR OTHER INACCURACIES IN THE INFORMATION OR MATERIAL COVERED BY THIS
LICENSE. In no event shall CMS be liable for direct, indirect, special, incident
al, or consequential damages arising out of the use of such information or mater
ial.
Authenticating with public key "imported-openssh-key"
You are required to change your password immediately (root enforced)
Last login: Tue Sep 9 20:14:05 2014 from 170.248.172.62
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user ec2-user.
Changing password for ec2-user.
(current) UNIX password: 
```

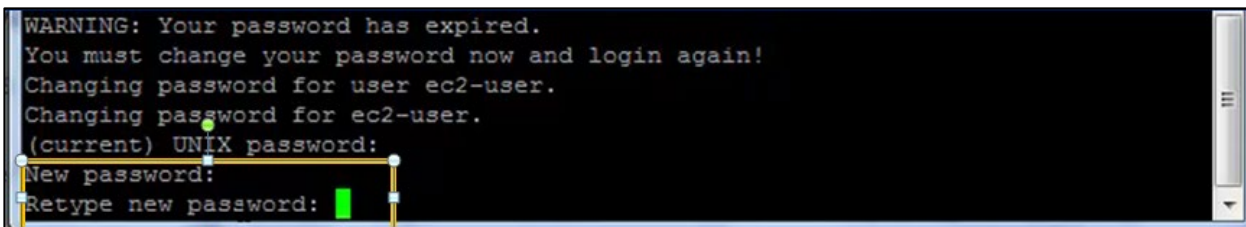
Figure 3-167: Enter Password

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

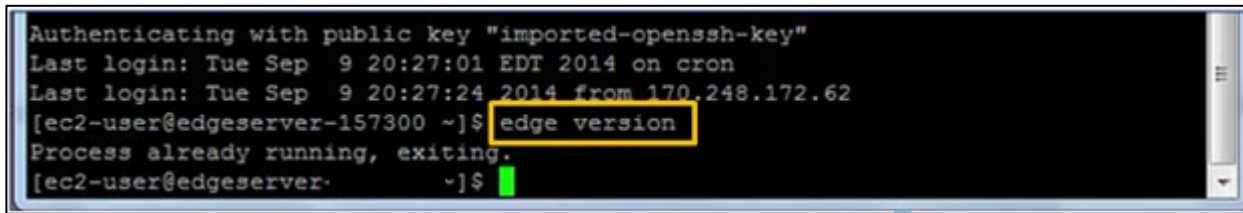


```
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user ec2-user.
Changing password for ec2-user.
(current) UNIX password:
New password:
Retype new password: 
```

Figure 3-168: 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.

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



```

Authenticating with public key "imported-openssh-key"
Last login: Tue Sep  9 20:27:01 EDT 2014 on cron
Last login: Tue Sep  9 20:27:24 2014 from 170.248.172.62
[ec2-user@edgeserver-157300 ~]$ edge version
Process already running, exiting.
[ec2-user@edgeserver-157300 ~]$

```

Figure 3-169: EDGE Version Command

25. The EDGE version command will check if the system is running on current version and will automatically generate database and application updates and/or execute CMS deployed commands.

V. *Enable Termination Protection*

By default, your server instance does not have termination protection enabled.



Note: 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 accidentally being terminated, enable termination protection on the server instance.

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

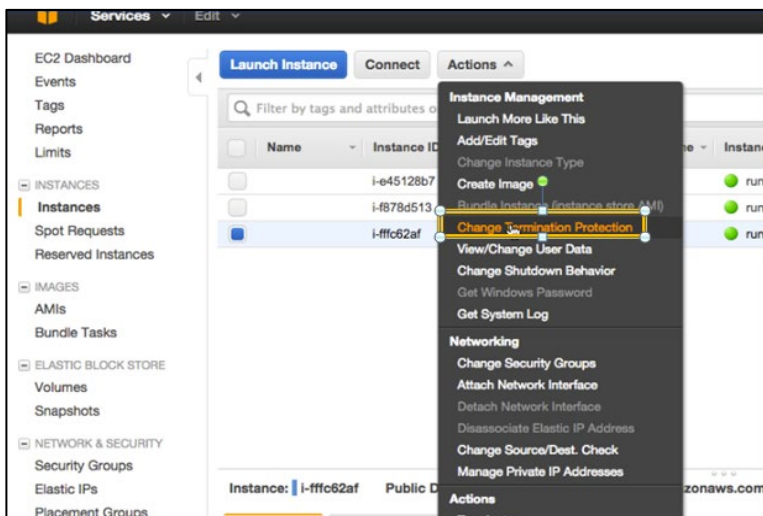


Figure 3-170: Select Change Termination Protection

27. A notification message will appear asking to confirm. Click **Yes, Enable** in the window.

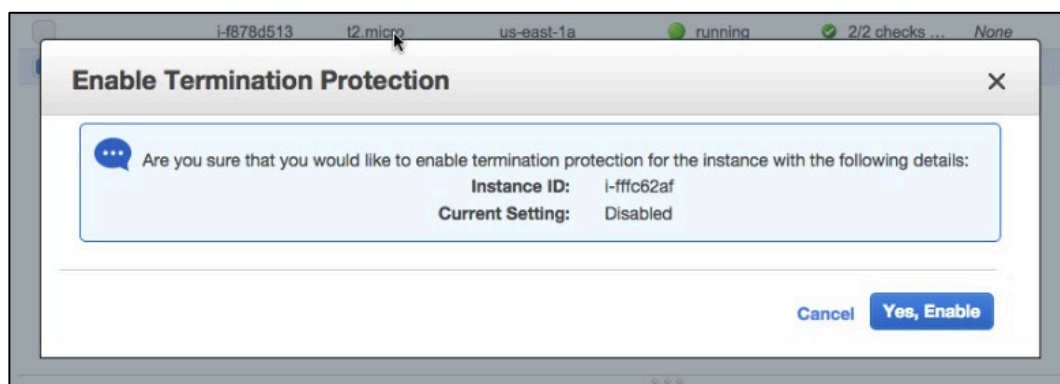


Figure 3-171: Enable Termination Protection

28. Once Termination Protection is enabled, selecting Terminate will produce the following message indicating the instance has **Termination Protection and will not be terminated**.

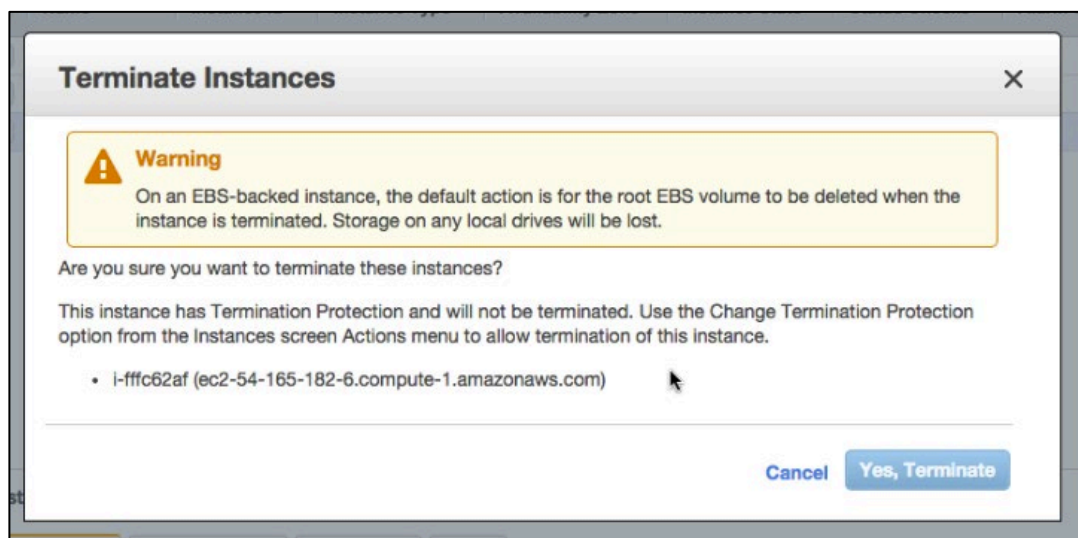


Figure 3-172: Terminate Instances Message

VI. Stop Server Instance

In order to avoid continuous usage charges for a server instance, CMS recommends issuers turn off the server instance when not in use.

29. To stop a server instance, from the AWS homepage, click **EC2** from the menu at the top left side of the screen.

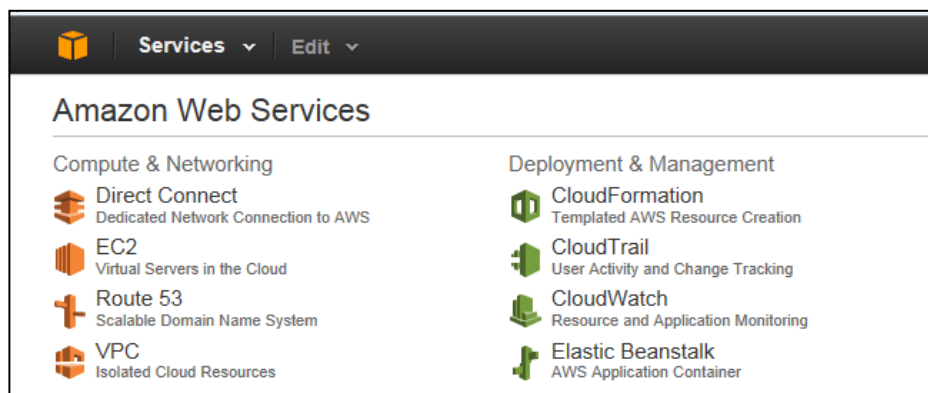


Figure 3-173: Select EC2

30. Click **Instances** on the left side of the screen and from the list of server instances, select the box next to your server instance. Then click **Actions** dropdown menu at the top of the page, hover over **Instance State**, then click **Stop**.

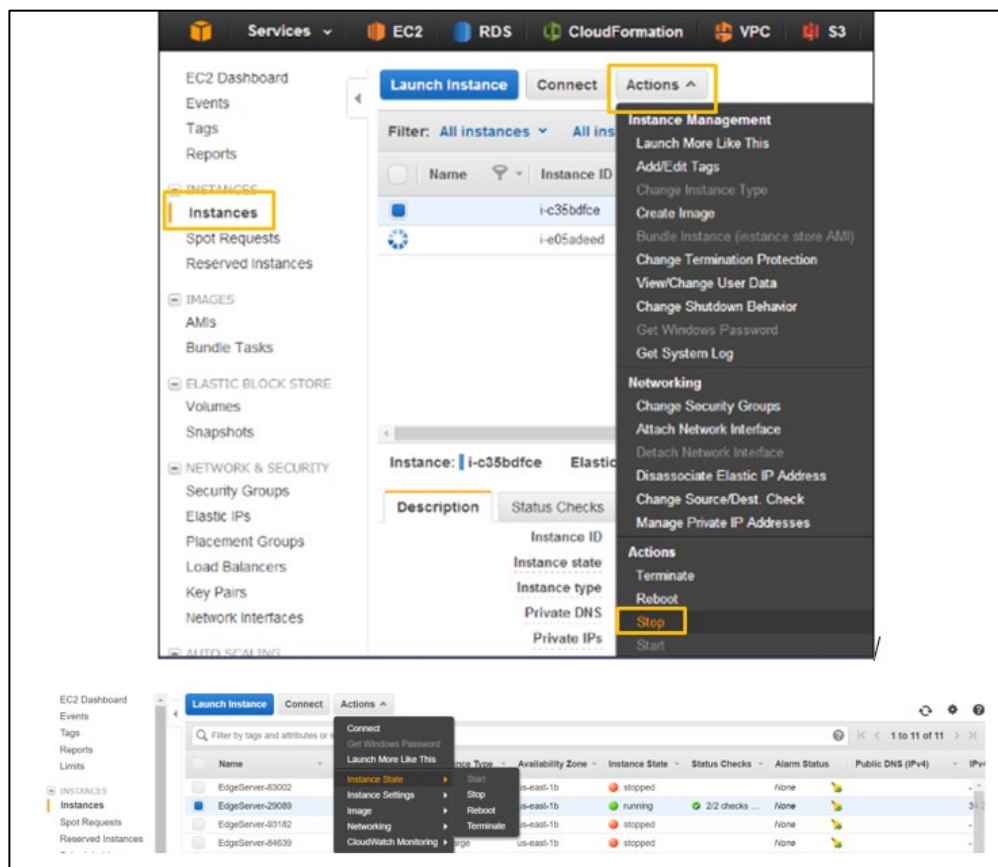


Figure 3-174: Stop Server Instance

A notification message will appear asking to confirm. Issuers should click **Yes, Stop** in the window.

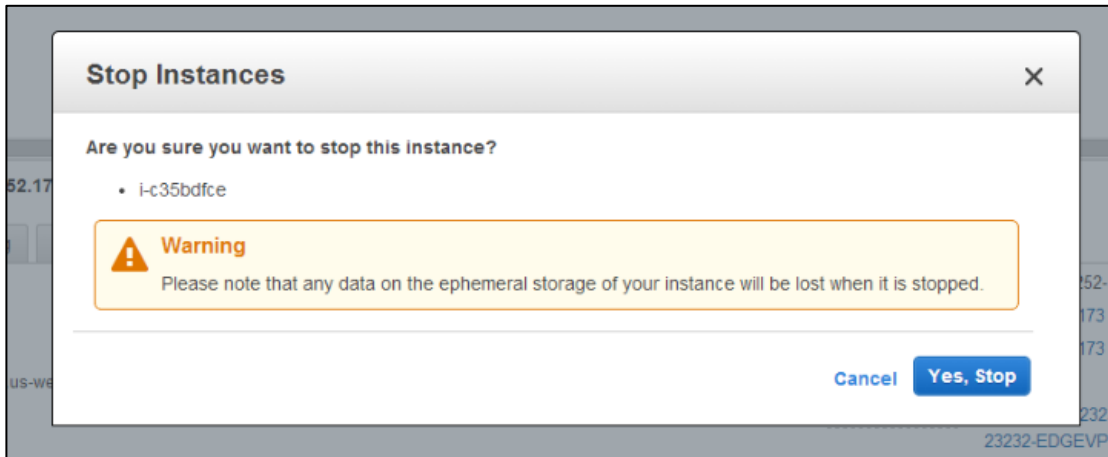


Figure 3-175: Confirm Stop Instance

This concludes information related to setting up the AWS EDGE server. The next section provides information related to server migration, from one (1) EDGE server option to another or from one (1) ownership to another (self-hosted or TPA), if needed.

3.9 Migration



Note: Issuers **must** contact CMS by emailing the FMCC mailbox at EDGE_Server_Data@cms.hhs.gov to create a migration ticket. This includes any self-hosted server or TPA changes. Please include the following subject line and detailed information in your email:

- Subject Line: "EDGE Server Migration - <Company Name>"
 - HIOS ID
 - EDGE Server ID
 - Server Name
 - Current Host
 - New Host
 - EDGE Server Size
 - AWS Region (If applicable)
 - Planned Migration Date
 - Reason for Migration

CMS must approve the migration request before the issuer performs any action.

Migrating before CMS approval can have detrimental effects on remote commands or the data archival process.

This section provides a high-level overview of the migration process for OP and AWS server options. [The EDGE Server Migration Job Aids](#) located in the REGTAP Library are organized according to the type of server to which the issuer is migrating. Each EDGE Server Migration Job Aid is divided into sub-sections, listed below, that provide pre-migration and migration steps for issuers who are self-hosted and for issuers who contract with TPAs.

Migrating to AWS

- AWS to AWS

Migrating to OP

- AWS to OP
- OP to OP

Server migration requests typically occur after the data archival black out period has been lifted in August, but please inform the FMCC if you would like to request a server migration at a different time during the year. When requesting a server migration, please consider that typical server migration can take **several** weeks. This timeframe is an especially important consideration when ending a contract with a TPA.

The FMCC representative will inform issuers once the server migration is approved by CMS. To expedite the server migration, old server data can be backed up while the new server software is being installed. Please refer to the migration job aids and contact your FMCC representation with any questions.