



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

EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures

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	4
1.1 Conventions	5
1.2 Additional Resources	6
1.3 Technical Assistance	8
Section 2 - System Overview	10
2.1 Functional System Overview	10
2.1.1 Issuer Responsibilities and Infrastructure Overview	11
2.1.2 Architecture	13
2.1.3 System Software Specifications	15
2.1.4 Application Users	16
2.1.5 Application Directories	16
2.1.6 Application Binary Files	17
2.2 Data Model & Dictionary	20
Section 3 - Backup and Maintenance Procedures	23
3.1 Backup and Data Retention Policy	23
3.1.1 Backup Command	25
3.1.2 Pre-Step Checklist	26
3.1.3 Executing the Backup Command - AWS Server	26
3.1.4 Executing the Backup Command - On-Premise Server	32
3.1.5 Restoring from Backup Files	34
3.2 Disaster Recovery	34
3.2.1 Inform CMS of the Disaster Recovery Event	35
3.2.2 Recreate Server	36
3.2.3 Backup Restoration	36
3.2.4 Backup Verification	36
3.3 Annual Archive Process	36
3.3.1 Pre-Archive Steps	38
3.3.2 Archive Steps	44
3.4 Truncation Requests	48
3.4.1 Truncation Request Approval	48
3.4.2 Executing a Truncation Script	50
3.5 EDGE Server Application and Software Stack Version Updates	50

List of Figures

Figure 1-1: REGTAP.....	6
Figure 2-1: AWS EDGE Server Data Flow	14
Figure 2-2: On-Premise EDGE Data Flow	15
Figure 3-1: AWS Account - EC2	26
Figure 3-2: AWS Account - Running Instances	27
Figure 3-3: AWS Account - Instance State	27
Figure 3-4: AWS Account - Public IP Address.....	27
Figure 3-5: Logging into PuTTY.....	28
Figure 3-6: DB Schemas	28
Figure 3-7: Backup Command Prompt for AWS Server.....	28
Figure 3-8: AWS S3 Folder.....	29
Figure 3-9: S3 Backup Folder.....	29
Figure 3-10: Verify Creation of Backup Files	30
Figure 3-11: S3 Folder Page	30
Figure 3-12: Backup Folder Link.....	30
Figure 3-13: Selecting Backup File (Image 1 of 3).....	31
Figure 3-14: Selecting Backup File (Image 2 of 3).....	31
Figure 3-15: Selecting Backup File (Image 3 of 3).....	31
Figure 3-16: Saving the Backup File.....	32
Figure 3-17: Navigate to opt/edge/bin folder.....	32
Figure 3-18: OP Backup Command Prompt	32
Figure 3-19: Ingest Backup Command	32
Figure 3-20: Confirming Creation of Backup File for OP Extraction.....	33
Figure 3-21: Log in to WinSCP	33
Figure 3-22: Ingest Folder	34
Figure 3-23: Edge.properties - DB User (Image 1 of 2)	38
Figure 3-24: Edge.properties - DB User (Image 2 of 2)	38
Figure 3-25: Schemas Check	39
Figure 3-26: MySQL - DB User Login	40
Figure 3-27: Schema Storage Space.....	41
Figure 3-28: DB Mount Points	41
Figure 3-29: DB Backup - Space Check	42
Figure 3-30: Obtain root password	42
Figure 3-31: MySQL Login for Remote Command Execution	43
Figure 3-32: Grant Privileges.....	43
Figure 3-33: Show Grants.....	44
Figure 3-34: Local Edge Commands to Execute the Remote Command	45
Figure 3-35: Command Execution Confirmation	45
Figure 3-36: Command Execution Confirmation	46
Figure 3-37: Backup Completion Confirmation	47
Figure 3-38: Welcome Page of Truncation Request Web Form	50

List of Tables

Table 1-1: Conventions Table.....5

Table 1-2: Key Documents7

Table 1-3: Technical Assistance Table9

Table 2-1: EDGE Server Schemas13

Table 2-2: Software Stack Components15

Table 2-3: EDGE Server Application Users16

Table 2-4: Application Directories16

Table 2-5: Binary Files.....17

Table 2-6: Data Model & Dictionary21

Table 3-1: Disaster Recovery Responsibilities35

Table 3-2: Current EDGE Server Supported Software51

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: Text	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](#) (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/> 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).
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.
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

Document	Summary
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 Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning	Provides issuers with 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, it provides steps on how to set up an AWS or OP server, as well as how to migrate servers after provisioning.
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) – 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:

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

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
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 Designate's 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 in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – HIOS, ESM & Provisioning](#). 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 in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – HIOS, ESM & Provisioning](#).

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.

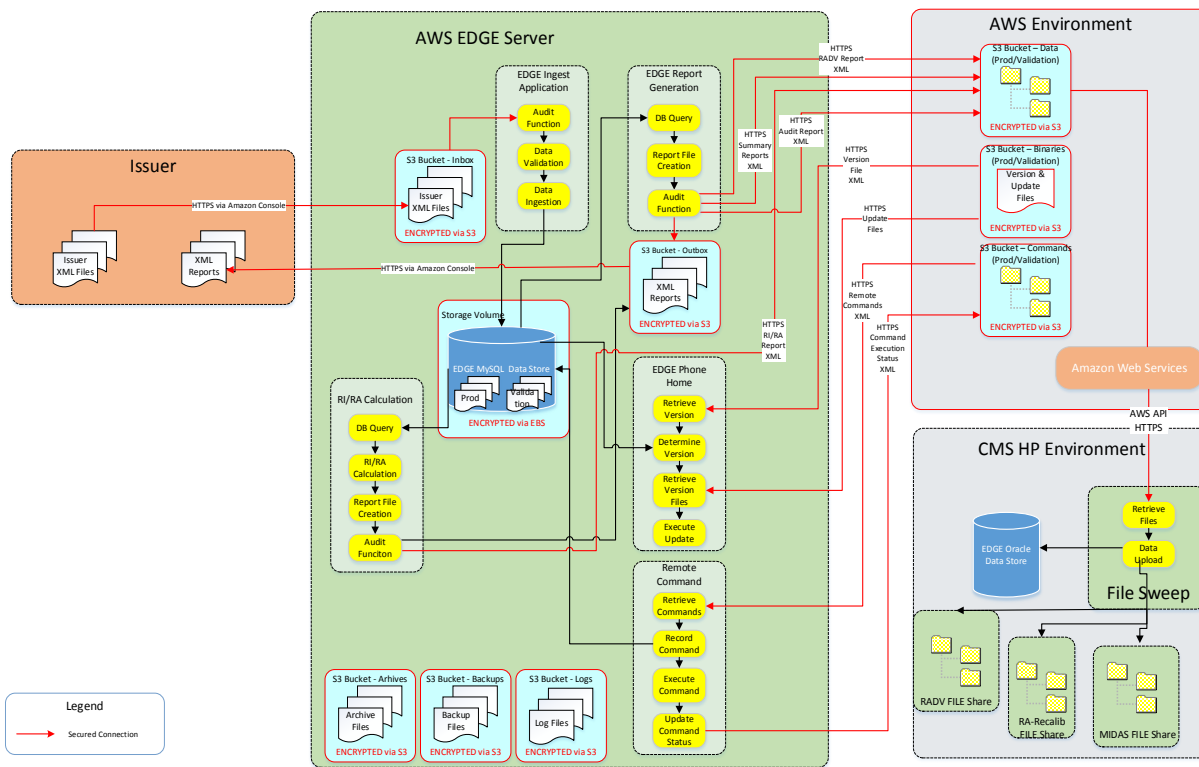


Figure 2-1: AWS EDGE Server Data Flow

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.

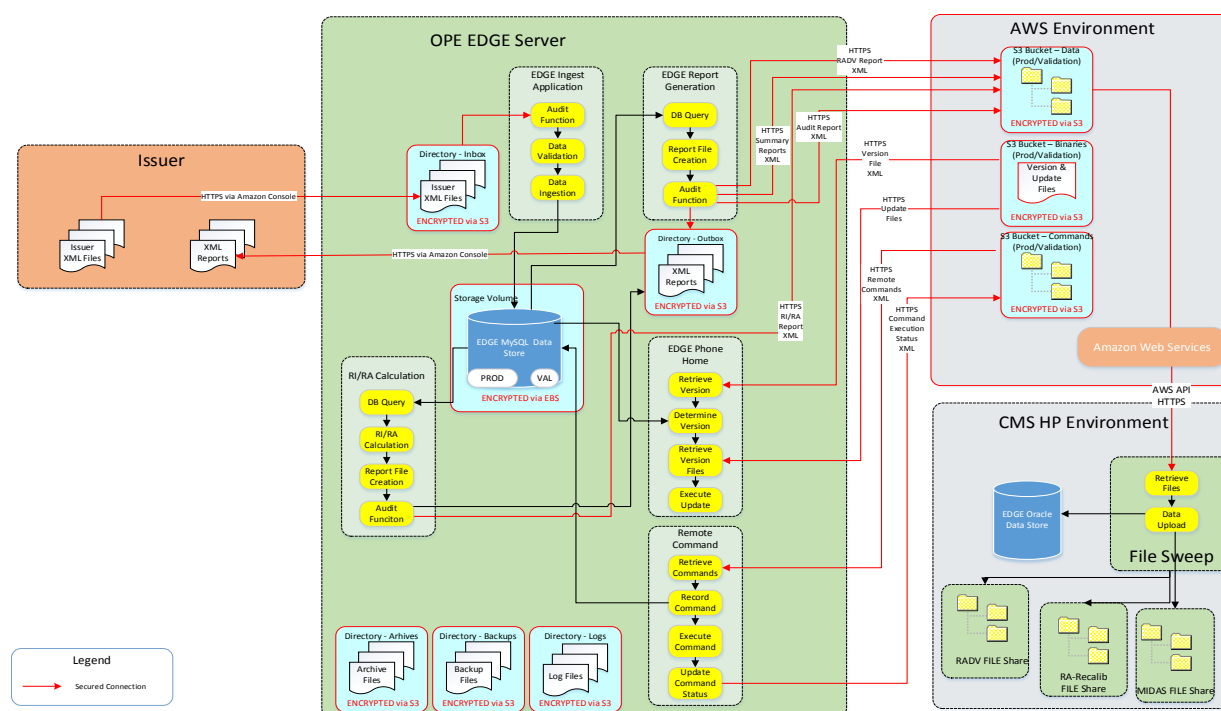


Figure 2-2: On-Premise EDGE Data Flow

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

Area	Vendor	Product
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
/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

Directory	Description
/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

Binary Name	Description
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
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

Binary Name	Description
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
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

Binary Name	Description
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
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 - Backup and Maintenance Procedures

Issuers are responsible for backing up their EDGE server data as a part of a complete disaster recovery process. The operational support and backup procedures for both AWS and OP EDGE servers are the responsibility of the issuer's operations teams.

A local command has been provided to back up the EDGE Server MySQL database server, as will be described in [Section: 3.1.1 Backup Command](#). However, the issuer's operations team is responsible for executing this command and placing the resulting backup file onto a safe repository. Issuers can either use the CMS provided backup command or follow their own backup processes.

Overall, issuer backups will help support the following critical EDGE functions:

- Restoration activities
- Verification, investigation and meeting internal audit requirements
- Supporting discrepancies and appeals that may be filed
- Retention of inbound and outbound data files that contributed to the final calculations.

The following sections describe CMS' backup policy guidance, how to backup EDGE server data and how to restore the data from a backup file.

3.1 Backup and Data Retention Policy

EDGE server issuers are required to retain all original data stored in their MySQL data tables for a period of 10 years. Issuers must maintain their MySQL data on the EDGE server for a period of three (3) years after the applicable benefit year to comply with any RA, HCRP, or RI program initiatives or activities identified by CMS. This data may not be backed-up and saved to another server until the three (3) year data requirement has been met or as instructed by CMS. The data must be active and query-able by HHS, the OIG, the Comptroller General or their designees for purposes of verification, investigation, audit or other review. This may include, but is not limited to, queries on current year data and archived data for activities such as ad hoc reports, data research, discrepancies and/or appeals. Afterwards, the issuer can disconnect their data but are required to retain any original data stored in their MySQL data tables for a total of 10 years after the date the data is reported.

For example, for BY2018, data must be retained on an active EDGE server until June 30, 2021. The 10-year data retention requirement is met 10 years after the final calculation of a benefit year and, therefore, BY2018 data must be retained until June 30, 2029.

Required:

- EDGE servers' data are backed up after each CMS-executed RA, HCRP, and RI run. Backups must also be moved to a secure external location off the server in order for the data to be retrievable and accessible in case of catastrophic system failure.
- Issuers must move backed-up final EDGE data SQL tables to an external source after the final RA and RI calculations are run in May.
- Storing a backup on the EDGE server is not sufficient.
- Storage of the EDGE data SQL tables is the minimum requirement to meet the data retention policy.

After the final RA and RI calculations are run each calendar year, CMS will require that all issuers complete the Attestation and Discrepancy Form to attest that they have performed the backup function to an external location. Additionally, issuers will need to attest that they have verified that their data has been backed-up and is available for future use if need be.

TPA Considerations:



Issuers may engage with a TPA to assist with RA and RI obligations under 45 CFR§153.620(b) and 153.410(c) should ensure any contracted parties have the appropriate backup procedures in place. CMS strongly recommends that issuers who rely upon a TPA ensure any agreement made with a TPA includes provisions that outline the parties' respective obligations related to data retention and whether such data will be retained by the TPA or transferred to the issuer (should there be a termination of the relationship or the termination of business) for the duration of the data retention period. Issuers who do not comply with backup requirements and experience a loss of data that is irretrievable, may receive adverse audit findings where applicable. CMS will not be extending file submission deadlines for issuers who have failed to back up their data in accordance with these instructions.

Recommendations:

CMS strongly recommends that issuers back up the MySQL tables and all inbound and outbound reports frequently for at least the entire reporting period for a coverage year and for the purpose of troubleshooting and to support the discrepancy and appeals process. Data are backed up after CMS staged RA and RI commands. However, CMS encourages issuers to run the backup command as frequently as needed and should occur whenever issuers are making system changes (e.g., software/hardware changes, migrations, etc.). Once the backup command is executed as detailed in this section, backups are automatically created in the `cd/opt/edge/ingest/backup` folder when RA and RI calculation is executed by CMS.

Issuers are ultimately responsible for data submission, retention and storing backups in a safe and accessible location. Issuers may engage with a TPA to assist with RA and RI obligations and should ensure any contracted parties have the appropriate backup procedures in place. CMS strongly recommends that issuers who rely upon a TPA ensure any agreement made with a TPA includes provisions that outline the parties' respective obligations related to data retention

If the host of the EDGE server is changed during the three (3) year data retention period, the data must be migrated to the new active server for that HIOS ID for the duration of the data retention period. After this period, the determination in maintaining the EDGE server is at the discretion of the owner. If an issuer switches from one (1) TPA to another TPA, the issuer must move their entire data backup using the same issuer ID to the new server that they plan on using to submit EDGE server data for RA/RI. The second TPA is then responsible for maintaining their MySQL data in an active, query-able status.

Issuers will need to ensure three (3) years of data is accessible on a single active EDGE server regardless of the party responsible for maintaining or storing the EDGE server data except as

outlined below. After three (3) years, the data may be stored as .sql files in a location of the issuer's choice. For example,

- Market Year = 2014, 3 Yr Date Retention End Date = 6/30/2018, 10 Yr Data Retention End Date = 6/30/2026
- Market Year = 2015, 3 Yr Date Retention End Date = 6/30/2019, 10 Yr Data Retention End Date = 6/30/2027
- Market Year = 2016, 3 Yr Date Retention End Date = 6/30/2020, 10 Yr Data Retention End Date = 6/30/2028

3.1.1 Backup Command

The “**edge dbbackup**” command creates a backup of the MySQL database schemas on the EDGE server. The same command can be executed by the issuer from the command line for both AWS and OP EDGE servers. Sections 5.1.3: Executing the Backup Command - AWS and 5.1.4: Executing the Backup Command - On-Premise will provide more details towards executing the command for the issuer's specific server type.

In the command prompt in PuTTY, simply type in the backup command without input parameters.

- `./edge dbbackup`

The backup command **will** include:

1. All common and production database schemas that exist on the server for the current processing year.
 - a. e.g. EDGE_SRVR_COMMON and EDGE_SRVR_PROD
2. Any archived and previously backed up database schemas that have been created for past years.
 - a. e.g. EDGE_SRVR_COMMON_2014 and EDGE_SRVR_PROD_2014

The backup command **will not** include:

1. XML ingest files submitted to the EDGE server for processing.
2. Any XML output reports generated by the EDGE server.
3. Any data submitted to the test and validation zone

Issuer's Responsibilities:

1. The backup command will not back up any XML ingest files submitted to the server or output XML files generated by the server. CMS recommends that the issuer backs up the XML ingest files submitted to the server for processing and the generated XML output files for the current processing year and any year for which they have submitted an appeal, in the event that the XML files are needed for research.
2. Once the backup files are generated, it is the issuer's responsibility to store the database tables and files in a secure location, off the EDGE server, in a manner that meets their internal IT backup policies.

3.1.2 Pre-Step Checklist

Prior to executing the EDGE command to conduct the backup, complete the pre-step checklist below to ensure an environment suitable to conduct the backup exist.

1. Ensure there is a valid working server available.
2. Ensure the server is running in AWS EC2 (For AWS Servers).
3. Download and install the PuTTY application from the web [here](#).
4. Download and install WinSCP or any File Transfer Protocol (FTP) client of your choice.

3.1.3 Executing the Backup Command - AWS Server

Amazon offers options for storing MySQL tables and files outside the S3 bucket. Amazon EDGE server issuers can export and store EDGE MySQL tables and files off the AWS EDGE server to a location of their choice.



Note: Issuers should not permanently store backups within the EDGE server S3 bucket and should note that increasing Amazon S3 storage can result in deletion of existing S3 files and irretrievable loss of data. Contact your FM Service Representative before attempting to increase your Amazon S3 storage.

The following steps will guide you through executing the local backup command for AWS servers for extraction of XML (input/output) files.

Logging into PuTTY

PuTTY will allow issuers to log into their server once the server has been provisioned. This will allow issuers to run the “**edge dbbackup**” command to back up their files and schemas and log into MySQL to query their database for reference data and files ingested in the PROD schemas.

Below are steps to retrieve the server IP address, create a PuTTY session, and log into the server.

1. Log into your AWS account.
2. Navigate to EC2.

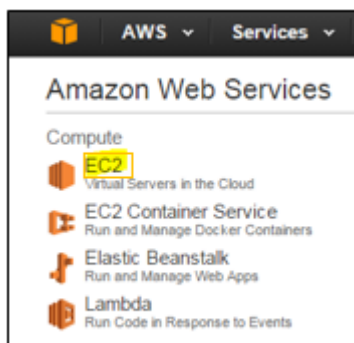


Figure 3-1: AWS Account - EC2

3. Click on “Running Instances”.

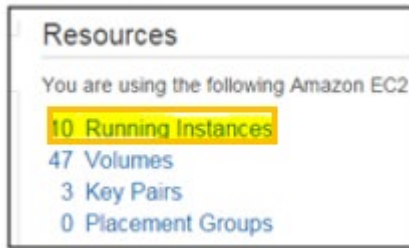


Figure 3-2: AWS Account - Running Instances

4. Identify your server and confirm that the “Instance State” is “running”. If the “Instance State” is “stopped”, then you must first start the instance by right clicking on the instance row and selecting Instance State > Start as seen in the screenshot below:

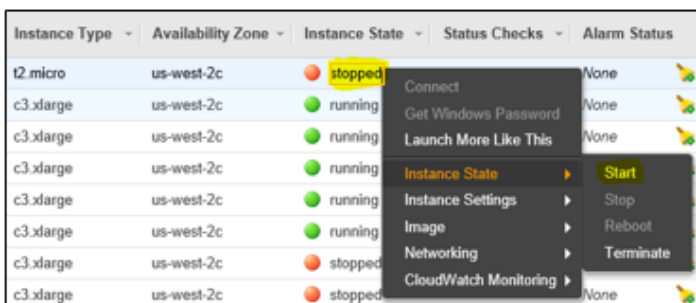


Figure 3-3: AWS Account - Instance State

5. After confirming the server is running, retrieve the public IP address for your server as seen below:

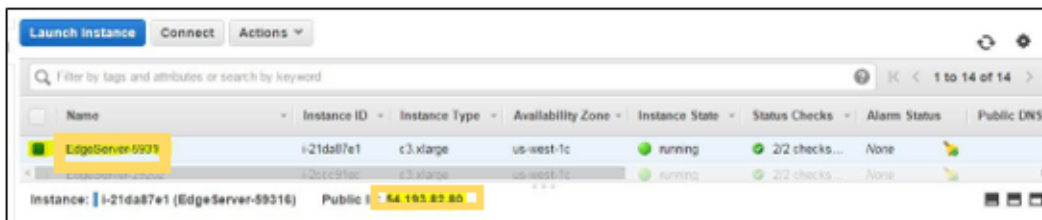


Figure 3-4: AWS Account - Public IP Address

- a) In the PuTTY screen under Host Name (or IP address), enter the IP address you retrieved from AWS.
- b) Enter the Host Name (or IP address): ec2-user@xx.xxx.xxx.xxx
- c) Enter any name for the server under “Saved Sessions”.
- d) Click on “Auth” under category in the left side panel.
- e) Click on “Browse” and select your .ppk key file.
- f) Click on “Session” under category in the left side panel.
- g) Click on “Save” to save your new PuTTY session.

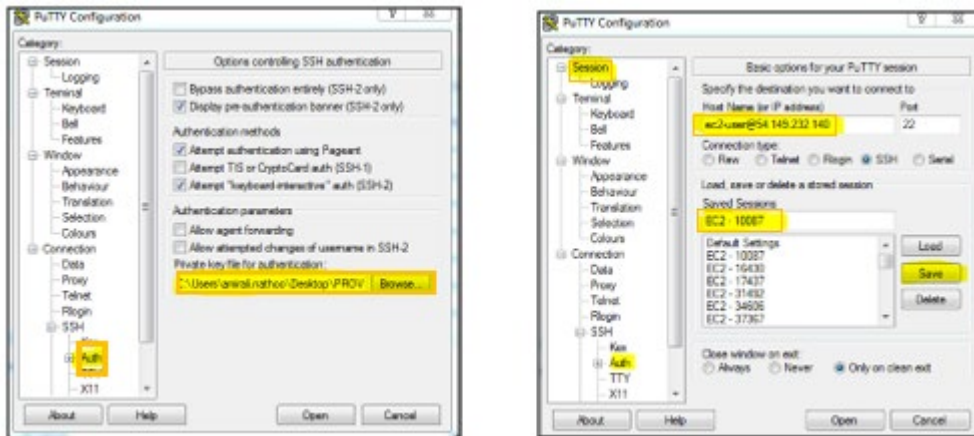


Figure 3-5: Logging into PuTTY

Verifying the Schema Information

This step will verify all your schema information before you begin the backup process.

6. Log in to your server using the above PuTTY instructions.
7. Log in to MySQL.
8. At the MySQL prompt, enter the following command:

- show schemas

```
mysql> show schemas;
+-----+
| Database |
+-----+
| information_schema |
| EDGE_SRVR_COMMON |
| EDGE_SRVR_COMMON_2015 |
| EDGE_SRVR_PROD |
| EDGE_SRVR_PROD_2015 |
| EDGE_SRVR_TEST |
| EDGE_SRVR_TEST_2015 |
| mysql |
| test |
+-----+
9 rows in set (0.00 sec)
```

Figure 3-6: DB Schemas

9. Verify all your schemas are present.
10. At the MySQL command prompt, exit back to the UNIX command prompt by executing:
 - quit
11. At the command prompt, type the command:
 - ./edge dbbackup
 and press “enter”.

```
[ec2-user@edgeserver-2006380 ~]$ ./edge dbbackup
```

Figure 3-7: Backup Command Prompt for AWS Server

12. Wait for the backup process to complete successfully.

Verifying the Backup for an AWS Server

This step will verify that the backup was successfully created in the AWS backup bucket in the S3 Bucket.

13. Log in to the AWS website. The link will be the same one used to ingest your XML files.

14. Navigate to the S3 Folder on the home page.



Figure 3-8: AWS S3 Folder

15. Inside the S3 Folder, navigate to the backup folder link.

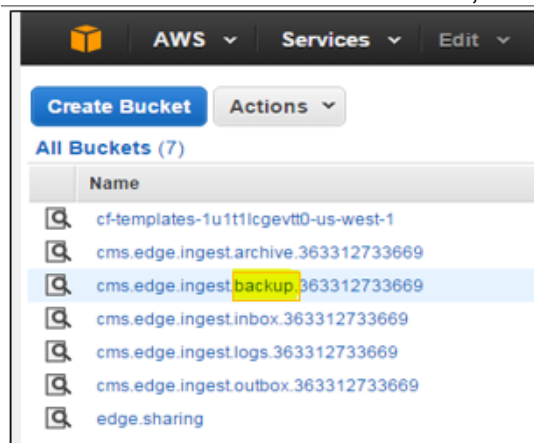


Figure 3-9: S3 Backup Folder

16. Select your server ID and click on it to enter the folder.

17. Verify that your backup is visible inside the folder.

- Verify the backup for all your schemas are created with *IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql*
- Verify the date the backup files were created (Should be current date and time).



The screenshot shows the AWS S3 console interface. At the top, there are tabs for 'None', 'Properties', and 'Transfers'. Below the tabs, the path is '/ cms.edge.ingest.backup.363312733669 / 14570'. A table lists several backup files with columns for Name, Storage Class, Size, and Last Modified.

Name	Storage Class	Size	Last Modified
14570_EDGE_SRV_COMMON_LOCAL_BACKUP.D10052015T090733.spl	Standard	21.8 MB	Mon Oct 05 21:07:37 GMT-400 2015
14570_EDGE_SRV_COMMON_2014_LOCAL_BACKUP.D10052015T090733.spl	Standard	802 bytes	Mon Oct 05 21:07:40 GMT-400 2015
14570_EDGE_SRV_PROD_LOCAL_BACKUP.D10052015T090735.spl	Standard	73.2 KB	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRV_PROD_2014_LOCAL_BACKUP.D10052015T090733.spl	Standard	800 bytes	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRV_TEST_LOCAL_BACKUP.D10052015T090735.spl	Standard	73.2 KB	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRV_TEST_2014_LOCAL_BACKUP.D10052015T090733.spl	Standard	800 bytes	Mon Oct 05 21:07:41 GMT-400 2015

Figure 3-10: Verify Creation of Backup Files

Accessing your Backup files from an AWS Server



Note: It is important that issuers download and store the backup that is generated, as well as any ingest files under /opt/edge/ingest/archives/ and any reports not saved by the backup command, in a secure location that meets the issuers' internal IT backup policies.

To access the backup files that are generated, please follow the steps below:

18. Log into the AWS Website. The link will be the same link used to ingest your XML files.
19. Navigate to the S3 Folder on the home page.



Figure 3-11: S3 Folder Page

20. Inside the S3 Folder, navigate to the backup folder link.

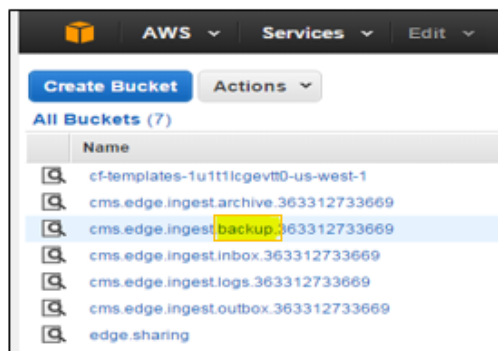


Figure 3-12: Backup Folder Link

21. Select your Server ID and click on it to enter the folder.
22. Select the backup file by selecting the square box on the left-hand corner in front of the files
(All the files cannot be downloaded at once in this step. All files must be individually selected and downloaded.)

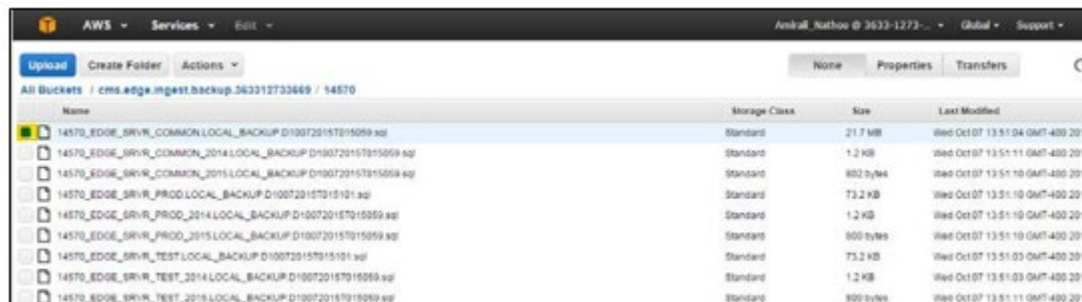


Figure 3-13: Selecting Backup File (Image 1 of 3)

23. Right click on the selected file and click on the **Download** link.

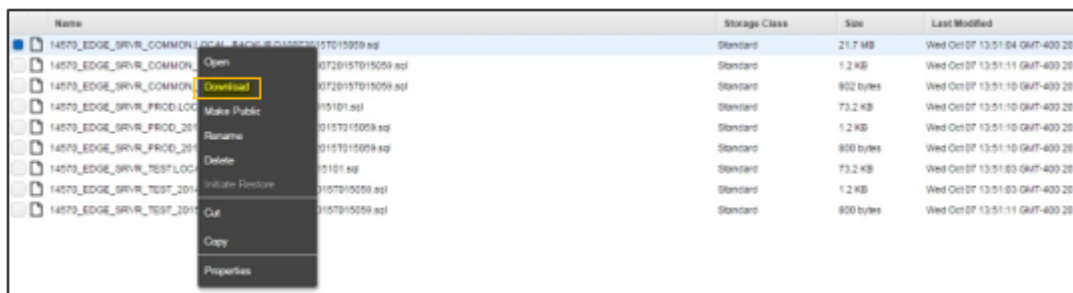


Figure 3-14: Selecting Backup File (Image 2 of 3)

24. Right click on the **Download** link displayed and click **Save link as...**

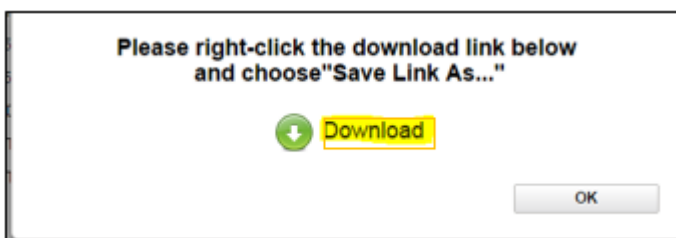


Figure 3-15: Selecting Back up File (Image 3 of 3)

25. A window prompt will be displayed to save your file in the secure location of your choice. Select the location and click **Save**. Make sure the file is saved as a .SQL type.



Figure 3-16: Saving the Backup File

3.1.4 Executing the Backup Command - On-Premise Server

The following steps will guide you through executing the local backup command for OP servers. These command prompts assist issuers in extracting their XML (output/input) files not included in the local backup tool for disaster recovery purposes



Note: Issuers are responsible for implementing their own IT backup and storage solutions.

26. Connect to the OP EDGE server using PuTTY or your preferred SSH client.
27. Navigate to the **cd /opt/edge/bin** folder.

```
[ec2-user@edgeServer-29089 backup]$ cd /opt/edge/bin
```

Figure 3-17: Navigate to opt/edge/bin folder

28. At the command prompt, execute the command:

- `./edge dbbackup`

```
[ec2-user@HPT1_OP_80991 bin]$ ./edge dbbackup
```

Figure 3-18: OP Backup Command Prompt

29. Wait for the back-up process to complete successfully.

Verifying the Backup for an OP Server

This step will verify that the backup was successfully created in the OP server's backup bucket

30. Log in to the OP server.
31. Execute the following commands to navigate to the backup folder and view contents:

- `cd /opt/edge/ingest/backup`
- `ll`

```
[ec2-user@edgeServer-29089 ~]$ cd /opt/edge/ingest/backup
You have new mail in /var/spool/mail/ec2-user
[ec2-user@edgeServer-29089 backup]$ ll
```

Figure 3-19: Ingest Backup Command

32. Verify that your backup is visible inside the folder.
 - a. Verify the backup for all your schemas are created with *IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql*
 - b. Verify the date the backup files were created with the current date and time.

```
[ec2-user@HPT1_OP_80991 backup]$ ll
total 64396
-rw-rw-r--. 1 ec2-user ec2-user 791 Oct 6 13:17 80991_EDGE_SRV_COMMON_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user 22914528 Oct 6 13:17 80991_EDGE_SRV_COMMON.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user 789 Oct 6 13:17 80991_EDGE_SRV_PROD_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user 78009 Oct 6 13:17 80991_EDGE_SRV_PROD.LOCAL_BACKUP.D10062015T011742.sql
-rw-rw-r--. 1 ec2-user ec2-user 789 Oct 6 13:17 80991_EDGE_SRV_TEST_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user 78009 Oct 6 13:17 80991_EDGE_SRV_TEST.LOCAL_BACKUP.D10062015T011741.sql
```

Figure 3-20: Confirming Creation of Backup File for OP Extraction

Saving your Backup Files from an OP Server



Note: It is important that issuers download and store the backup that is generated and any reports not saved by the backup command in a secure external location that meets issuers' internal IT backup policies. To save the backup files that are generated, please follow the steps below.

33. Retrieve your IP Address.
34. Log in to WinSCP.

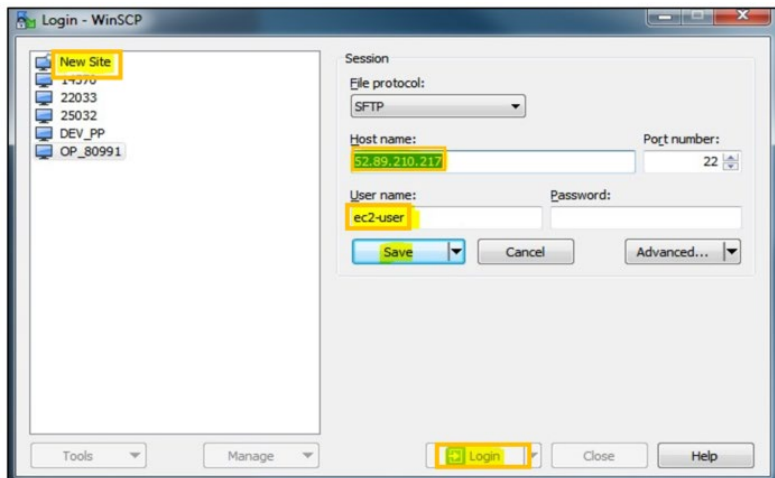


Figure 3-21: Log in to WinSCP

35. Click on the right-hand panel to highlight it. Navigate to `/opt/edge/ingest/backup`.

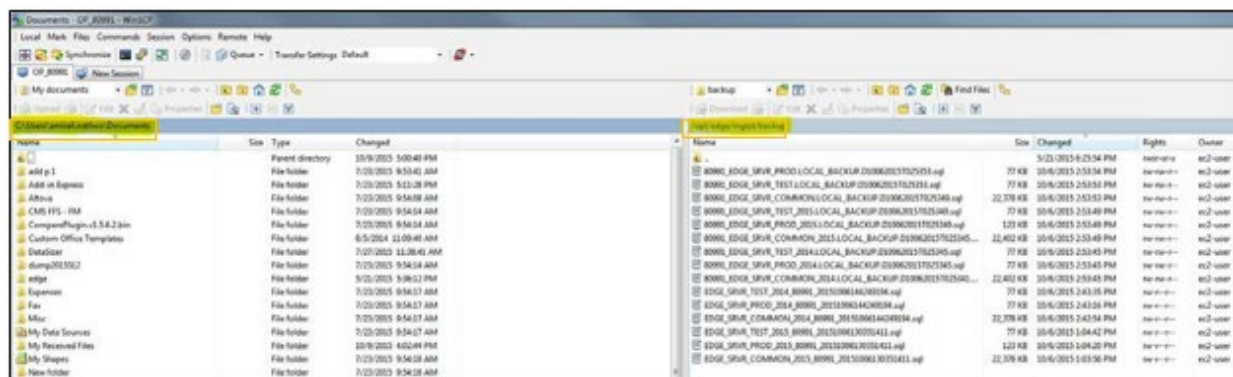


Figure 3-22: Ingest Folder

36. Click on the left-hand panel to highlight the window. Navigate to the location you want to save your files. Drag the files from the right window to the location on the left.

3.1.5 Restoring from Backup Files

Issuers must notify CMS immediately upon becoming aware of any issues with files, either stored or lost, which can create an access or retrieval problem. Notification will ensure that CMS is aware of any potential impacts to data submission, EDGE remote commands, reporting or other deadlines. CMS will also be able to better evaluate the issuer's specific scenario and develop an approach to resolve the issue that will minimize the risk of corrupting data.

Issuers must contact an FMCC Service Representative Team for technical assistance for both OP or AWS servers. CMS encourages issuers to report issuer-based problems as soon as possible so that, to the extent feasible, CMS can provide assistance to issuers to resolve those problems before the final data submission deadline. The FMCC Service Representative will work with the issuers to provide the best approach to resolve the specific scenario identified.



Note: AWS issuers should **NOT** contact Amazon for assistance in restoring their files until they have been instructed to do so by CMS.

FMCC representatives are available to answer any questions or assist issuers with this process. Issuers must notify CMS immediately upon becoming aware of an actual or potential loss of data, a need to perform recovery activities or, a need to increase the Amazon EDGE server memory. To contact an FMCC representative, email EDGE_Server_Data@cms.hhs.gov.

3.2 Disaster Recovery

CMS has established an EDGE Server Disaster Recovery Process in the event of a disaster or emergency that impacts an issuer's EDGE server. The purpose of this section is to outline the steps that are required to be performed on the EDGE server to assist issuers in resuming data submission and ensuring that the data is included in the RA and RI program calculations. The recovery process requires routine server backup as outlined in [Section 3: Backup and Maintenance Procedures](#).

The issuer's operational team is responsible for the day-to-day maintenance of their EDGE server environment. The issuer's operational teams will be responsible for the overall disaster recovery plan for the EDGE server environment. They will have the following responsibilities:

Table 3-1: Disaster Recovery Responsibilities

Task	Team	Description
Disaster recovery plan	Issuer Operation's Team	Create and maintain a disaster recovery process and procedures for restoring the EDGE server in case of a catastrophic data loss
Storing backup files	Issuer Operation's Team	Place backup files (e.g., application files, DB backup files, etc.) in accordance with the disaster recovery plan
Restore EDGE server environment	Issuer Operation's Team EDGE Server Help Desk	Ensure the EDGE server application has all necessary supported software and is on the latest EDGE version. Please see Section 3.5: EDGE Server Application and Software Stack Version Updates for more information. The EDGE Server help desk will only assist the issuer in provisioning or installing a new EDGE server in case of a catastrophic failure
Disaster Recovery Site, if applicable	Issuer Operation's Team	If applicable, the issuer's operational team will be responsible for maintaining an EDGE server disaster recovery site as outlined by the issuer's disaster recovery policies and procedures.

3.2.1 Inform CMS of the Disaster Recovery Event

Issuers must alert the FMCC Service Representative Team in the event of a catastrophic loss of the EDGE server. The FMCC representative assists issuers with immediate coordination and instructions on how to restore issuers' backup. To contact an FMCC representative, issuers should send an email to EDGE_Server_Data@cms.hhs.gov. Issuers may also open a ticket with AWS, if needed.

3.2.2 Recreate Server

The FMCC representative will reset the Issuer HIOS ID so that the existing server can be re-provisioned, upon CMS approval. The following sections explain the process to recreate the EDGE server, depending upon server type:

AWS: A new AWS server will be re-provisioned using the steps in Section 3.8.6: AWS EDGE Server Provisioning in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – HIOS, ESM, & Provisioning](#).

OP: Issuers should install the new server using the steps in Section 3.8.5: On-Premise EDGE Server Provisioning in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – HIOS, ESM, & Provisioning](#). They will need to download the following from the ESM console: 'edge.keys', 'edge.properties' and the installation kit and proceed with the re-provisioning as instructed in the documentations.

During the disaster recovery process, servers (either AWS or OP) should meet the set of software requirements outlined in the following sections before restoring backup files and installing the EDGE application software. Please see [Section 3.5 EDGE Server Application and Software Stack Version Updates](#) for the latest Red Hat Enterprise Linux (RHEL), MySQL and Java versions. Issuers who want to install a different version should first contact the FMCC Service Representative Team to ensure it complies with current CMS guidelines and EDGE software.

3.2.3 Backup Restoration

Issuers will work with the FMCC Service Representative Team for coordination and instructions to restore issuers' backup servers.

3.2.4 Backup Verification

The FMCC representatives will work with the issuer to execute the following series of steps to verify backup and to check if the application is up and running:

1. Verify the software version information
2. Verify if all databases are restored
3. Verify database schema information, check if the expected schemas are created and loaded with the data and check the table counts
4. Run basic EDGE commands and confirm the application is running

3.3 Annual Archive Process

The EDGE server data submission deadline for the previous benefit year is typically the last day in April. The [EDGE Server Timeline](#), available in the REGTAP Library (https://www.regtap.info/reg_library.php) provides the year specific deadlines for data submission. CMS implemented a blackout period after the submission deadline in order for the annual RA payments and charges processes to be performed. Once CMS has finished the benefit year payments and/or charges, a command will be sent to issuers' EDGE servers to archive the data on the server for future audit purposes. During the archive process, the production tables will be cleared and claim and supplemental data, already submitted and

accepted for the current benefit year, will be restored. This eliminates the need for data resubmission and will make the system ready for additional data for the current benefit year.

Note: For example, after the data submission deadline on April 30, 2018, the current benefit year will be 2019 and the previous benefit year will be 2018.

After the EDGE server data submission deadline, or the subsequent business day, all data submissions for the previous benefit year will be blacked out. However, during the blackout period, issuers will be able to submit medical claims, pharmacy claims, and supplemental diagnosis records for the current benefit year. Enrollment data for the current benefit year may **not** be submitted during the blackout period. Issuers will also not be able to execute the Risk Score Local Remote Command during the blackout period. All current benefit year claims and supplemental data submitted will be restored to the production tables during the archive process.

Records that will be restored include:

Any medical claim families where the latest claim in the claim family has a Statement Covers Through Date within the current benefit year. A claim family that meets these criteria will be restored regardless of whether the latest claim is active or inactive (void);

- Any supplemental records linked to a restored medical claim; and
- Any pharmacy claims with a Fill Date within the current benefit year.

Enrollment data will not be restored because enrollment submissions are full replacement files. Once the archive process is complete and the blackout is lifted (usually at the end of July), issuers may submit their enrollment files.

It is important to note that only the PROD and COMMON tables will be archived. All data in the PROD schema will be archived, including data from the previous benefit year and the current benefit year. If all current benefit year claim counts are not present in the production schema after the archive command, the command will fail and the FMCC team will perform outreach with next steps. The TEST zone and VALIDATION zone tables will not be archived.

Note: Beginning in July 2018, data archived for the new benefit year will be restored to the production tables eliminating the need for issuers to re-submit new benefit year data submitted prior to the archive.

Issuers who want to sync their PROD and TEST zone after the archive occurs will need to truncate the TEST zone to clear the tables. Section 3.2.3: Prod to Test and Prod to Validation Copy Command in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands](#) provides steps if issuers would like to sync their two (2) zones. Issuers who have received a TEST zone truncation script before, may use the same script. Refer to [Section 3.4.1: Truncation Requests](#) to request a truncation.

This section will provide issuers with instructions on the pre-archive steps necessary to successfully prepare their servers to execute the EDGE server remote command that will create the archive schemas to back up benefit year data that was used for RA and RI calculations. In addition, this section will provide instructions on the post-archive confirmations that are recommended to confirm a successful archive has occurred. Issuers should refer to CMS-published communications for the deadlines for executing these steps, to ensure a successful archive process.



Note: Issuers are required to attest, through the **Annual Archive Confirmation Web Form**, that the archive and the restoration of BY2019 data was successful.

Issuers should refer to CMS-published communications in the REGTAP library about the deadlines for executing these steps and attesting to the archive and restoration process.

Note: The following steps provide general guidance for the previous benefit year. This section will be revised each year for guidance to the current benefit year.

3.3.1 Pre-Archive Steps

Step 1: Identify 'DB User' from edge.properties along with 'DB password'

- Log into the server and access the properties file by entering:

- cd /opt/edge/config
- view edge.properties

```
[ec2-user@edgeserver-2906515 config]$ pwd
/opt/edge/config
You have mail in /var/spool/mail/ec2-user
[ec2-user@edgeserver-2906515 config]$ view edge.properties
```

Figure 3-23: Edge.properties - DB User (Image 1 of 2)

- Identify the value associated with the property, db_user and db_password, from edge.properties, using the EDGE application that connects to MySQL DB.

```
db_host=localhost
db_port=3306
db_user=edgedbuser
```

Figure 3-24: Edge.properties - DB User (Image 2 of 2)

The commands in the following steps use 'edgedbuser' as the db_user; however, this ID could vary based on issuer setup. Please use the db_user field in the following commands to substitute 'edgedbuser', if needed.

Step 2: Identify Custom Schemas, if Applicable

- Identify the custom schemas by checking the values associated with the following properties: These fields will be used in later steps to archive custom schemas:
 - db_common_schema
 - db_prod_schema

```
db_common_schema=EDGE_SRVR_COMMON_CUSTOM
db_test_schema=EDGE_SRVR_TEST_CUSTOM
db_prod_schema=EDGE_SRVR_PROD_CUSTOM
```

Figure 3-25: Schemas Check

Step 3: Validate Current Table Counts within Schemas

- The following steps outline how to confirm the count of the tables in the current schemas. This information is used to confirm that the new archive schemas are created successfully after the Archive command is executed.
 - a. Issuers need to validate the count of the tables within the current schemas. Please enter the following commands and save the table count so that it may be used to confirm that the new archive schemas are created successfully after the Archive command is executed.

- USE EDGE_SRVR_COMMON
- show tables;
- USE EDGE_SRVR_PROD
- show tables;

Step 4: Validate Current Record Counts within the Tables

The following steps outline how to calculate the current benefit year record counts submitted to the current production tables. This information will be used to confirm that the data for each benefit year is archived and the current benefit year data is restored to production after the Archive command is executed.

Issuers who have submitted prior benefit year data (e.g., 2017 data in July of 2018) and current benefit year (e.g., 2019 data in July of 2019), claims and supplemental diagnosis codes prior to the archive will not need to resubmit current benefit year data after the archive and blackout is lifted. The archive will restore (i.e. repopulate) the current benefit year data in the current production tables.



Note: Issuers must validate the current benefit year record counts within the current schemas. The record counts will be required when attesting that the Pre-Archive steps have been completed.

- a. CMS will deploy Ad Hoc remote commands which will contain the record counts needed to provide when completing the Pre-Archive Web Form. Please execute the commands on your EDGE server and make note of the counts. The queries to generate these counts are also located in Appendix H: Data Validation Queries for Archive Command in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands](#).
 - Execute the ad-hoc remote commands staged by CMS
 - a. Each ad-hoc command will produce a separate CSV file
 - b. Filename Format: <HIOSID>.ADHOC.D<YYYYMMDD>.T<HHMMSS>.txt
 - Save the ad-hoc results of the record counts to populate the Pre-Archive Web Form.

Step 5: Check Current Storage Space Usage by Database Schemas

Issuers should verify they have sufficient storage space to accommodate the archive data and the new benefit year data that will be restored and submitted. The following steps can be used to check the DB storage space currently used by DB schemas on the MySQL server.



Note: If there is insufficient space on the server, issuers may encounter problems executing the archive remote command. To address this, issuers will need to add additional storage to the MySQL DB mount point.

- Log in to the MySQL shell using the **db-user**, as shown below.

- `mysql --host localhost -u edgedbuser -p`

```
[ec2-user@edgeserver-2906515 config]$ mysql --host localhost -u edgedbuser -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 434815
Server version: 5.5.47 MySQL Community Server (GPL) by Remi

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Figure 3-26: MySQL - DB User Login

Steps to check current storage space, taken by DB schemas:

- Run the following **SQL** from MySQL shell to check storage space.
 - SELECT table_schema "Data Base Name",
sum(data_length + index_length) / 1024 /
1024 "Data Base Size in MB"
FROM information_schema.TABLES
GROUP BY table_schema;

```
mysql> SELECT table_schema "Data Base Name",
-> sum( data_length + index_length ) / 1024 /
-> 1024 "Data Base Size in MB"
-> FROM information_schema.TABLES
-> GROUP BY table_schema;
```

Data Base Name	Data Base Size in MB
EDGE_SRVR_COMMON	67.01562500
EDGE_SRVR_COMMON_V	66.84375000
EDGE_SRVR_PROD	3.73437500
EDGE_SRVR_TEST	2.95312500
EDGE_SRVR_VALIDATION	2.95312500
information_schema	0.15625000

```
6 rows in set (0.03 sec)
```

Figure 3-27: Schema Storage Space

- Based on DB size, issuers can increase the space available on the DB Mount points for the back-up schemas and also for the upcoming file ingests. The result from 'Data Base Size in MB' for the EDGE_SRVR_PROD schema provides issuers a guide to allocate required extra space to successfully execute the Archive remote command.



Note: The system capacity must be at least double the size of the EDGE_SRVR_PROD schema. However, issuers may consider allocating at least three (3) times the space taken by EDGE_SRVR_PROD schema.

To exit out of MySQL and navigate to the config folder, execute the following commands:

- exit
- cd /opt/edge/config

To check the available space, enter the following command:

- df -k /var/lib/mysql

Note: Depending on the MySQL installation, the mount point for MySQL may vary.

```
[ec2-user@edgeServer-29089 config]$ df -h /var/lib/mysql
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvdk        246G  1.2G  233G   1% /var/lib/mysql
[ec2-user@edgeServer-29089 config]$
```

Figure 3-28: DB Mount Points

- During archive process, the DB backup files will be written to **/opt/edge/ingest/backup**. It is recommended to allocate more space for the mount point for /opt/edge. Use the below command to check the available space:

- df -k /opt/edge

```
[ec2-user@edgeServer-29089 config]$ df -h /opt/edge
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvdk        246G  1.2G  233G   1% /opt/edge
You have new mail in /var/spool/mail/ec2-user
[ec2-user@edgeServer-29089 config]$
```

Figure 3-29: DB Backup - Space Check

If issuers encounter server storage space issues, the following error message will display in the error log files:

- java.io.IOException: No space left on device



Note: In such cases, additional storage space is required to be added. There is no difference between space and storage space. The command will fail when there is insufficient space. To resolve this error, issuers need to contact their internal infrastructure team to increase space.

Step 6: Verify Grant Permissions for 'DB User'

The following three (3) steps are prerequisites for executing the remote command. Permissions must be granted prior to executing the remote command.



Note: Please ensure the database user who will be executing the remote command has the appropriate permissions, as outlined below before executing.

- Obtain and save the root password before executing the following steps:

- cd /opt/edge/config
- ls -lart
- more .edge.root

```
[ec2-user@edgeServer-29202 edge]$ cd /opt/edge/config
[ec2-user@edgeServer-29202 config]$ ls -lart
total 32
-rwxr-xr-x. 1 ec2-user ec2-user  0 May 19 2017 completeConfiguration
-rwxr-xr-x. 1 ec2-user ec2-user 12 May 19 2017 .edge.root
-rw-r--r--. 1 ec2-user ec2-user 150 Jan 18 14:25 edge.keys.old
-rwxr-xr-x. 1 ec2-user ec2-user 150 Jan 18 14:25 edge.keys
-rwxr-xr-x. 1 ec2-user ec2-user 1124 Jan 18 15:51 edge.properties
-rw-r--r--. 1 ec2-user ec2-user 2246 Mar  6 14:15 logback.xml.bak
-rw-rw-r--. 1 ec2-user ec2-user 2246 May 24 15:27 logback.xml
drwxr-xr-x. 2 ec2-user ec2-user 4096 May 24 15:27 .
drwxr-xr-x. 13 ec2-user ec2-user 4096 May 24 15:36 ..
[ec2-user@edgeServer-29202 config]$ more .edge.root
```

Figure 3-30 Obtain root password

Log in into MySQL with **root** access and enter the following command: When prompted, enter the root password obtained in the previous step:

- `mysql -u root -p`

```
[ec2-user@edgeServer-43328 ~]$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2758148
Server version: 5.7.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Figure 3-31: MySQL Login for Remote Command Execution

1. Next, grant the required permissions to the database user in order to execute the archive process. Execute the following commands:

- `GRANT ALL PRIVILEGES ON EDGE_SRVR_COMMON_YYYY.* TO 'edgedbuser'@'localhost';`
- `GRANT ALL PRIVILEGES ON EDGE_SRVR_PROD_YYYY.* TO 'edgedbuser'@'localhost';`
- `FLUSH PRIVILEGES;`

Note: **YYYY** = the BY that is being archived. In July of 2018, CMS will archive BY2017 data.

```
mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_COMMON_2016.* TO 'edgedbuser'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON EDGE_SRVR_PROD_2016.* TO 'edgedbuser'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Figure 3-32: Grant Privileges

2. Next, verify that all the correct permissions were granted. **All of the permissions MUST be granted.** Enter the following commands to verify:

- `SHOW GRANTS FOR 'edgedbuser'@'localhost';`

```
mysql> SHOW GRANTS FOR 'edgedbuser'@'localhost';
+-----+
| Grants for edgedbuser@localhost |
+-----+
| GRANT USAGE ON *.* TO 'edgedbuser'@'localhost' |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_COMMON`.* TO 'edgedbuser'@'localhost' WITH GRANT OPTION |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_COMMON_V`.* TO 'edgedbuser'@'localhost' WITH GRANT OPTION |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_TEST`.* TO 'edgedbuser'@'localhost' WITH GRANT OPTION |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_PROD`.* TO 'edgedbuser'@'localhost' WITH GRANT OPTION |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_VALIDATION`.* TO 'edgedbuser'@'localhost' WITH GRANT OPTION |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_COMMON_2016`.* TO 'edgedbuser'@'localhost' |
| GRANT ALL PRIVILEGES ON `EDGE_SRVR_PROD_2016`.* TO 'edgedbuser'@'localhost' |
+-----+
8 rows in set (0.00 sec)
```

Figure 3-33: Show Grants

For issuers with CUSTOM SCHEMAS only

3. (Grant the required permissions to the database user for CUSTOM SCHEMAS to be ARCHIVED in order to execute the archive process.

- GRANT ALL PRIVILEGES ON <EDGE_SRVR_COMMON_CUSTOM>_YYYY.* TO '<edgedbuser>'@'localhost';
- GRANT ALL PRIVILEGES ON <EDGE_SRVR_PROD_CUSTOM>_YYYY.* TO '<edgedbuser>'@'localhost';
- FLUSH PRIVILEGES;

Note: YYYY = the BY that is being archived. In July of 2018, CMS will archive BY2017 data.



Note: This completes the Pre-Archive steps necessary to perform the archive.

Issuers must now complete the Annual Archive Confirmation Web Form in order for CMS to release the Archive Remote Command.

Issuers will be notified when the remote command is being deployed. Once the remote command is deployed, issuers may continue with the steps that follow.

3.3.2 Archive Steps

CMS will notify issuers via REGTAP when the remote command to archive will be staged. The remove command is not issued until all servers pass the steps mentioned above. Once CMS has confirmed all servers are ready to be archived, CMS will send the following remote command:

YEAR_END_BACKUP_DB

Step 7: Start Database Archive Process

The following steps outline how to execute the database archive remote command once it has been released by CMS.

To complete the database archive process, run a local edge command to execute the remote command released by CMS:

- Enter one (1) of the two (2) commands in the command window:
 - edge queue execute

- edge version

Note: DO NOT enter 'edge update' command, as this is only for application updates. The 'edge version' or 'edge queue execute' command is needed to trigger the remote command. If there is a CRON job running, the command will automatically be picked up.

```
[ec2-user@edgeserver-606103 ~]$ edge queue execute
```

OR

```
[ec2-user@edgeserver-606103 ~]$ edge version
```

Figure 3-34: Local Edge Commands to Execute the Remote Command

Step 8: Validate Remote Command Status is Executed

- After the remote command is finished executing, log into MySQL and navigate to the remote command queue table below to confirm the status is executed and the date/time stamp. Enter the following commands:

- mysql --host localhost -u edgedbuser -p
- USE EDGE_SRVR_COMMON
- SELECT * FROM REMOTE_CMD_QUEUE WHERE REMOTE_CMD_TYPE='YEAR_END_BACKUP_DB' and REMOTE_CMD_CREATED_DT > 'YYYY-06-30\G;

Note: **YYYY** = the current BY. Example: In July of 2018, this value should say 2018.

```
mysql> SELECT * FROM REMOTE_CMD_QUEUE WHERE REMOTE_CMD_TYPE= 'YEAR_END_BACKUP_DB' and REMOTE_CMD_CREATED_DT > '2017-06-01'\G;
+-----+-----+-----+-----+-----+-----+
| REMOTE_CMD_ID | REMOTE_CMD_STATUS | REMOTE_CMD_TYPE | REMOTE_CMD_CREATED_DT | REMOTE_CMD_SCHEDULED_AT | REMOTE_CMD_EXPIRES_ON |
+-----+-----+-----+-----+-----+-----+
| 86044         | EXECUTED          | YEAR_END_BACKUP_DB | 2017-06-14 14:14:16   | 2017-06-14 00:00:00     | NULL                  |
+-----+-----+-----+-----+-----+-----+
PARAMETERS: ("JOB_ID":"86044","YEAR":"2016","BATCH_ID":"S02-2016-00020","BATCH_TYPE":"YEAR_END_BACKUP_DB","ZONE_TYPE":"P")
RESULTS: NULL
CREATED_DT: 2017-06-14 14:15:13
UPDATED_DT: 2017-06-14 00:00:00
1 row in set (0.00 sec)
```

Figure 3-35: Command Execution Confirmation

Step 9: Validate New Archive Schemas and Tables within Archive Schemas Created

The following steps outline how to confirm the database archive process successfully created the new schemas. The new schemas will preserve the data used for the benefit year EDGE server calculations.

- In order to validate that the database archive process completed successfully, check to confirm the following schemas created in MySQL:
 - show schemas;
 - a. Confirm the following schemas exist:
 - i. **EDGE_SRVR_COMMON_YYYY**
 - ii. **EDGE_SRVR_PROD_YYYY**

Note: YYYY = the BY that is being archived. In July of 2017, CMS will archive BY2016 data.

```
mysql> show schemas;
+-----+
| Database |
+-----+
| information_schema |
| EDGE_SRVR_COMMON |
| EDGE_SRVR_COMMON_2014 |
| EDGE_SRVR_COMMON_2015 |
| EDGE_SRVR_COMMON_2016 |
| EDGE_SRVR_COMMON_V |
| EDGE_SRVR_PROD |
| EDGE_SRVR_PROD_2014 |
| EDGE_SRVR_PROD_2015 |
| EDGE_SRVR_PROD_2016 |
| EDGE_SRVR_TEST |
| EDGE_SRVR_VALIDATION |
| mysql |
| performance_schema |
| sys |
+-----+
15 rows in set (0.00 sec)
```

Figure 3-36: Command Execution Confirmation

The following steps outline how to confirm that the correct tables were created in the new archive schemas.

- After validating the new schemas created, issuers should validate that new tables within those schemas were also created. Please enter the following commands and confirm the table count with the table counts from [Step 3: Validate Current Table Counts within Schemas](#).

- show tables;
- USE EDGE_SRVR_PROD_YYYY
- show tables;



Note: Issuers are required to perform the following steps and attest to the successful archive and restoration of BY2019 data through the Annual Archive Confirmation Web Form.

Note: YYYY = the BY that is being archived. In July of 2018, CMS will archive BY2017 data.

Step 10: Validate Remote Command is Successful

- The below step outlines how to confirm the archive remote command completed successfully in the EDGE log files. Open the edge.log files by executing the following commands:
 - `cd /opt/edge/log`
 - `ls -l`
 - `view edge.log`
- If the archive process is completed successfully, please verify the following:
 - Archive backup status will show as COMPLETED and code as 200 in log file.



Note: If the archive command completed, but issuers do not see the success message, issuers should press the 'Page down' key to view more of the edge.log. The side scroll bar may not be sufficient, so it is recommended to use the 'Page down' key to view more of the edge.log.

```
DB BACKUP Process is completed successfully!!!. Exiting with success code of 200
Printing FINAL BackupVO element details:
```

Figure 3-37: Backup Completion Confirmation

- Issuers will see empty PROD schemas, recreated with the expected number of tables with NO data in PROD schema.

Step 11: Validate Current and Previous Benefit Year Data in Archive and Prod Schemas

The following steps outline how to confirm the database archive process successfully restored the current benefit year claims and supplemental diagnosis code records. The new prod schemas will preserve the data used for the current benefit year EDGE server calculations and eliminate the need for issuers to resubmit current year data that was submitted prior to archive.

After validating the new schemas were created, issuers may validate that new tables within those schemas were also created.

Please enter the commands in Appendix H: Data Validation Queries for Archive Command in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands](#) and confirm the record count of restored current benefit year data with the record counts from [Step 4: Validate Current Record Counts within the Tables](#).

Step 12: Report Execution of Archive Command and Ingest Files for the New Benefit Year

Once the archive is successful and you have verified the count of restored records for the current benefit year, please log into the Annual Archive Confirmation Web Form and report the count of records restored. The Annual Archive Confirmation Web Form will include an Attestation confirming the number of records that were restored was accurate.

CMS will notify issuers when the blackout has been lifted so that issuers may start submitting new enrollment files, additional claims and supplemental diagnosis codes for the current benefit year.

3.4 Truncation Requests

Database truncation is a process by which issuers can delete claim, supplemental diagnosis and enrollment data that has been submitted to the EDGE server in the production, test or validation zones. Issuers have the option to request a complete truncation within a specific zone, or to delete data based on file type. Truncation does not allow deletion of the EDGE Server Common Schema Data Tables.

CMS reviews new truncation requests and truncation extension requests, then provides notification and instructions to issuers.



Note: If prior to September 20, 2019 you received a truncation script for the Test or Validation Zone for a benefit year (BY) 2018 HIOS ID that continues to participate in BY2019, you **must** request a new truncation script to truncate all files for that HIOS ID. Once approved for a benefit year, the Test and Validation Zone truncations can be reused for the remainder of the benefit year. If you requested to truncate by a specific file type and later wish to truncate by another file type, you must submit a new request.

Issuers may only perform truncation of data from the EDGE server using a CMS provided script. Please see the following sections for instructions on obtaining the scripts.



Note: Issuers may NOT create their own scripts to delete some or all of the EDGE server data. CMS has included coded functionality in the EDGE server software that creates a permanent record of all data submitted and used for calculations.

Truncation is not meant to be a form of data management and is made available to issuers to correct large scale systemic issues that cannot be resolved through the use of guidelines provided in the ESBR, such as the submission of void and replacement claims. Issuers should make every effort to use the appropriate method to correct data submitted to the server, as outlined in the ESBR.

3.4.1 Truncation Request Approval

CMS has developed an EDGE Server Truncation Request web form for issuers requesting an EDGE server truncation or an extension for a previously approved truncation request. The webform is located in the FM Community.



Note: Starting, September 23, 2019, all truncations requests must be completed in the EDGE Server Truncation Web form located within the FM Community. Previous links to the web form will no longer be accessible.

CMS Approval requirements to perform a database truncation in the production, test, or validation zones are as follows.

- To perform a truncation in the test or validation zones, issuers are only required to obtain a *one (1)-time approval*. After the initial approval, issuers can re-execute the truncation in test and validation for the remainder of the benefit year. To perform a truncation in the production zone, issuers must submit a new request each time they need to truncate production data.
 - Extensions for a previously approved truncation request must also be approved.
 - Requests for open ended time frames will not be approved. The date range for all truncation requests defaults to a standard seven (7) days.
- Issuers may submit more than one (1) HIOS ID and EDGE Server ID per request.



Note: Issuers will only be allowed to truncate one (1) file type at time or all the data at a time. If two (2) file types are requested during the same webform submission period, issuers must notify CMS when the first truncation is complete by replying to the truncation approval request for CMS to stage the second truncation.

A truncation request must be completed and submitted in a single session. It is recommended that you collect all necessary information before initiating the process. Issuers are required to submit the web form with the following information to request permission to truncate production data.

- Organization name
- Requestor's name
- HIOS ID number
- EDGE server ID number
- Issuer-stated reason for the request
- When do you plan to do the truncation?
- When do you plan to re-load your data?
- Are your new files ready for submission?
- Have you run your data through the test zone?
- What were the results?
- Have you performed a back-up of your data on an external location/site?

The [EDGE Server Truncation Web form Guide](#) will guide you through the truncation request process.

[HOME](#)
[MAINTENANCE](#)
[INQUIRIES](#)
[TRUNCATION](#)

EDGE Truncation

This page allows users to submit the EDGE Server Truncation Request Form in order to request a new EDGE Server truncation or to request an extension of a previously approved truncation request. Select the link below to proceed to the form.

This page also allows users to view the history of truncation requests associated with the company. Review the Truncation Request History table for additional details. [EDGE Server Truncation Request Form](#)

Truncation Request History

The table below lists the EDGE Server truncation requests previously submitted on behalf of your organization. Select the View link in the Action column to see all details related to the truncation request.

Action	Truncation Request ID	Request Type	Truncation Zone	HIOS IDs	Truncation Request Date	CMS Approved Truncation Start Date	CMS Approved Truncation End Date	Status
--------	-----------------------	--------------	-----------------	----------	-------------------------	------------------------------------	----------------------------------	--------

Figure 3-38: Welcome Page of Truncation Request Web Form

3.4.2 Executing a Truncation Script

Once CMS has provided approval for truncation, issuers can execute the approved command from the EDGE server Linux console in PuTTY (or SSH client of your choice). Any user who has access/permission to execute “**edge**” commands will be able to perform this step.

In all cases, the command will search for a file on the issuer-specific CMS AWS S3 bucket for permission to execute this command on or before a particular date.

3.5 EDGE Server Application and Software Stack Version Updates

CMS and issuers are responsible for ensuring the most current version of the EDGE Server Application and the supporting software, including the Red Hat operating system, MySQL and Java, are updated timely for successful data submission, program calculations and proper technical functioning of the server. Issuers are responsible for applying security and kernel patches on their servers and staying in accordance with the latest supported CMS versions, as indicated in the next section.

Updates to the EDGE Server Application

The EDGE server application software is periodically updated and release dates are scheduled and published for issuers in the [EDGE Server Maintenance Release Notes](#) located in the REGTAP Library.



Note: CMS makes every effort to deploy EDGE updates on Friday evenings between 8:00 p.m. and 11:59 p.m. ET. There may be occasions when CMS must deploy updates on a different day. Issuers will be notified as early as possible of any off-cycle deployment dates.

CMS will provide issuers with maintenance release notes in advance of deployment of new EDGE server application versions. Release notes include the following important information:

- EDGE server web registration site version number
- EDGE server application version number
- The version of the ICD that includes the technical specifications for ingest files and the reports produced after ingest files are processed
- The version of the ICD Addendum that includes the technical specifications for all reports produced upon execution of local or remote commands
- Release dates to the validation and production zones
- The functionality that was changed and the impact to issuers

When the new version is released, issuers can either manually execute the EDGE update command or enable CRON to pick up the release (see Section 3.2.1: Local commands in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands](#) and Appendix G: EDGE Server Reports and Local Commands in the [EDGE Server Operations and Maintenance Manual \(O&MM\) – File Processing & Commands](#)).

Issuers will need to validate they are on the correct EDGE version to ensure EDGE functionality is up-to-date. In most cases, new EDGE versions will be released to the validation zone first. The validation zone will serve as a pre-prod environment for CMS to test EDGE application releases with beta issuers, using their existing EDGE servers, prior to releasing the application to production. Selected Issuers may participate in beta testing the new EDGE functionality, however, CMS will not be able to support non-beta issuers performing activities in the validation zone prior to the completion of beta testing. Shortly after deployment to the validation zone, the new EDGE version will be released to the production and test zones.

Updates to the Software Stack Version and Supporting Software

The EDGE server application software is supported by MySQL, Java and RHEL operating system, and it is the issuer's responsibility to have currently supported software versions for both OP and AWS servers.

Table 3-2: Current EDGE Server Supported Software

Software	Supported Version
MySQL	5.7.16
Java	1.8
RHEL	7.3

CMS will monitor issuers to ensure their servers are on correct versions for supporting software. CMS runs weekly tests to ensure all security patches do not impact the EDGE application and advises issuers to stay on the versions listed in this section. When major software stack upgrades are needed to support the EDGE application, CMS will contact issuers in advance through [REGTAP](#) and webinars in order to prepare issuers for the upgrade. In this instance, CMS will assist issuers with AWS hosted servers when re-provisioning is needed.

The EDGE server is initially deployed with OS updates consistent with National Institute of Standards and Technology (NIST) moderate security standards. Issuers are responsible for following CMS minimum guidance for patching their EDGE server instances. Issuers should

follow leading practices for patching including keeping track of patch levels and dependencies, aiming to patch critical vulnerabilities in hours or days and subscribing to security mailing lists and news sources.

In addition to patching, issuers retain ownership of EDGE server instances and are responsible for:

- Security Group Management;
- Network ACLs' and
- Any issuer specific configuration.