Centers for Medicare & Medicaid Services

Center for Consumer Information and

Insurance Oversight (CCIIO)

EDGE Server Operations and Maintenance Manual (O&MM) – File Processing & Commands

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

List of Appendices

List of Figures

List of Tables

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.
STOP	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.

REGTAP
Registration for Technical Assistance Portal
My Dashboard
Training Events
Inquiry Tracking
Library
FAQs
Contact Us
About REGTAP
Log Out
Distributed Data Collection (DDC) for Risk Adjustment (RA) Including High Cost Risk Pool (HCRP)/EDGE Server
Get Adobe Reader

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
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.

Document	Summary
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) – Configuration, Validation & Application Errors	Provides issuers with the requirements for proper EDGE application configuration in order to maximize functionality.
EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures	Provides issuers with an overview of the operational support and backup procedures for both AWS and OP EDGE servers which is part of the disaster recovery process.
EDGE Server Operations and Maintenance Manual (O&MM) – Reference Data	Provides issuers with an overview of Global Refence Data and Plan refence Data.
EDGE Server File Ingest Error Codes Job Aid	Describes the log file ingest validation errors in the EDGE Server application in the MySQL EDGE_ERROR_LOG table on the EDGE server.
EDGE Server XML XSD Zip File Contents Job Aid	Lists the XML/XSD zip file contents for inbound and outbound reports
XML/XSD Inbound Files	Provides the structure and layout of the inbound files
XML/XSD Outbound Files	Provides the structure and layout of the outbound files

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

1.3 Technical Assistance

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

Table 1-3: Technical Assistance Table

Reason	Email Address or Website
Technical assistance for EDGE server data submission/processing, EDGE reports, EDGE calculations	EDGE_Server_Data@cms.hhs.gov
Financial Management (FM) Community* for webforms and notifications including: Truncation, Baseline, Quantity/Quality Outliers, EDGE Server Status Update, Attestation and Discrepancy, RA Reconsiderations, Archive, and EDGE Server Contacts update, including Chief Executive Officer (CEO) Designation.	ccrms-rari.force.com/financialmanagement
Policy, baseline, EDGE data quantity notifications, payments/charges, exempt filing, general information	RARIPaymentOperations@cms.hhs.gov
EDGE data quality notifications	EDGEdatareply@cms.hhs.gov
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 the Interface Control Document (ICD)) and the business validation rules outlined in the ESBR document (See the 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 Section 4 - Appendices.

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.

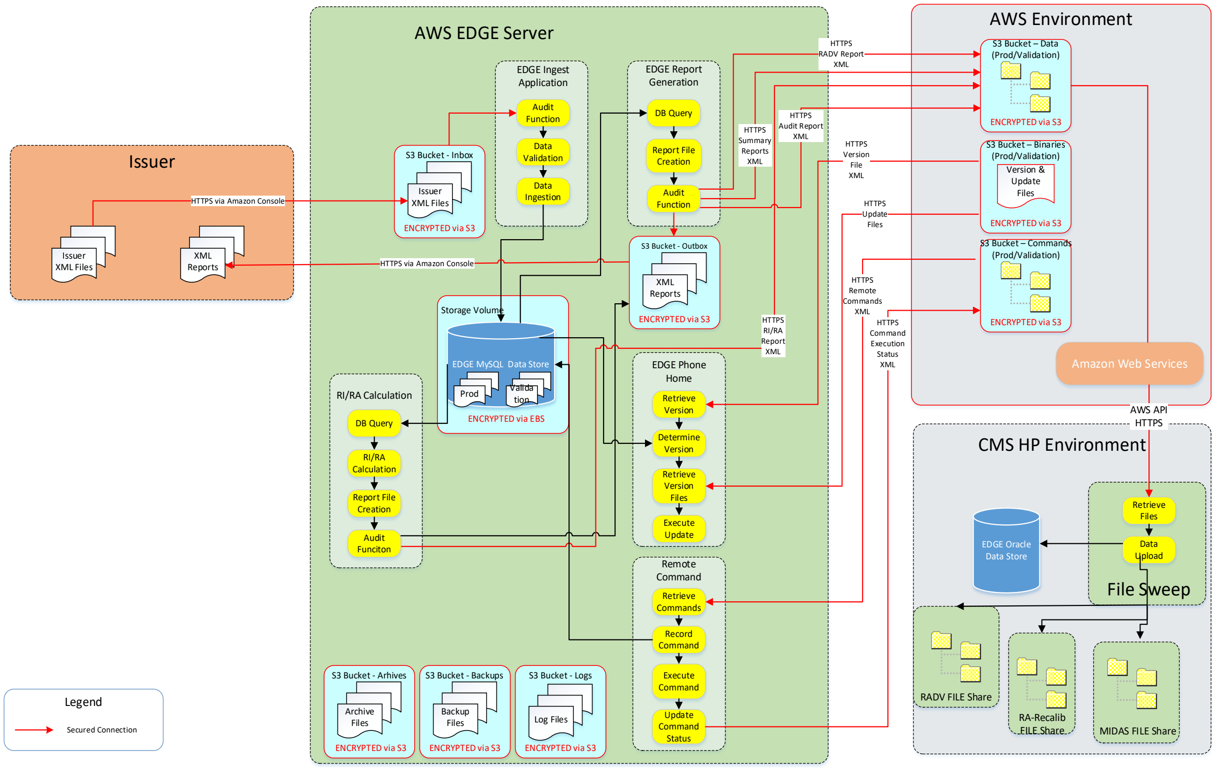


Figure 2-1: AWS EDGE Server Data Flow

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.

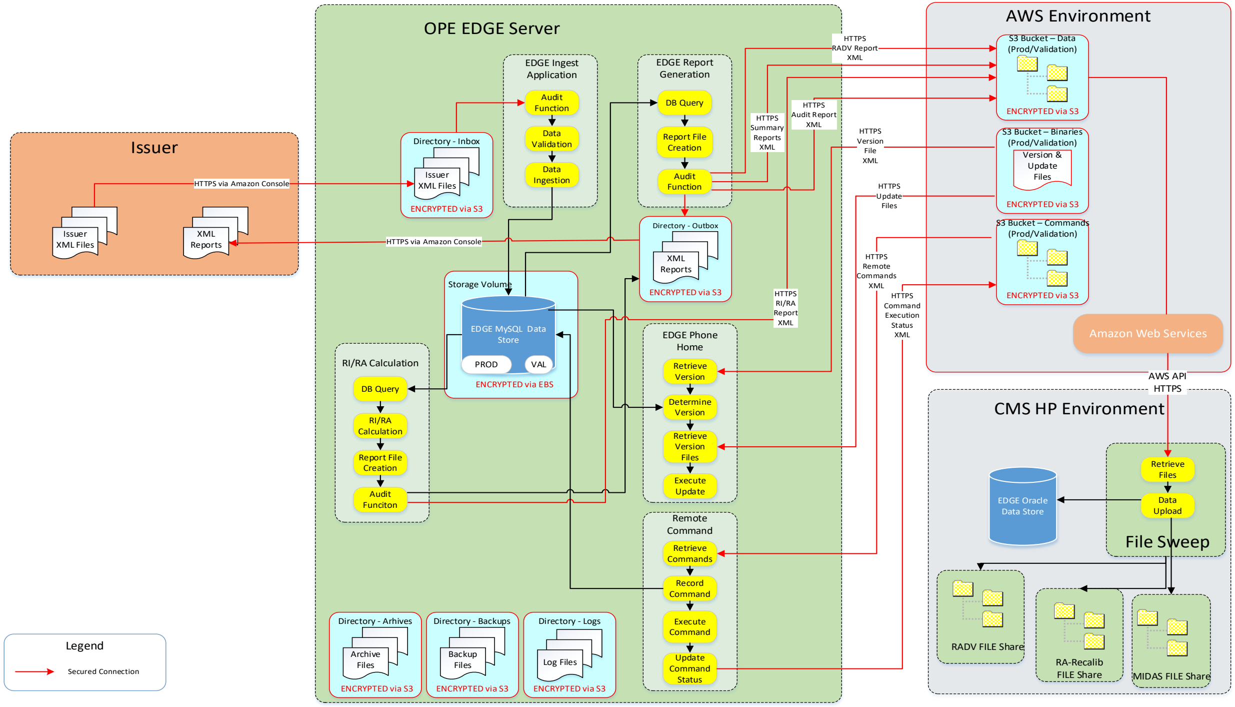


Figure 2-2: On-Premise EDGE Data Flow

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
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

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

2.1.6 Application Binary Files

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

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

Table 2-5: Binary Files

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

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

Binary Name	Description
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

Schema Name	Description	Data Model Link	Data Dictionary Link
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 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 - Operations

This section provides instruction for issuers to execute the EDGE operational activities including file processing, local and remote command execution, configuration management, and application errors.

3.1 File Processing

Issuers submit enrollment, pharmacy, medical and supplemental files to the EDGE server. After a file has completed processing, outbound XML files are produced and sent to the issuer. Notification of success or failure of every submitted record will be communicated in the outbound detail reports. Issuers are responsible for reviewing the outbound error file reports to identify any issues in their submission process.

Refer to Section 4 - Appendices for more information about Data Quantity and Quality Evaluation, file layout as described in the ICD, as well as XSDs and example XML files.

3.1.1 EDGE Server Business Rules

The EDGE Server Business Rules (ESBR) document 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.

3.1.2 Interface Control Document

The Interface Control Document (ICD) available on REGTAP includes the necessary information required to effectively define the CMS-EDGE server system interface. 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.

The RARI ICD Addenda is an addendum to the ICD that includes the file layouts and data element definitions/formats for the RA, RI and analytic XML reports generated by the EDGE server.

3.1.3 File Ingest Overview

Issuers upload enrollment claims and supplemental diagnosis files. The EDGE server software applies the verification edits outlined in the Interface Control Document (ICD) and the EDGE Server Business Rules (ESBR). Enrollment files must be full files; pharmacy claim, medical claim and supplemental diagnosis files must be incremental.

XML files are the only method of data submission. CMS has established an inbound file naming convention that must be used and is defined in the ICD. File layouts and requirements related to data submission are outlined in the ICD and ESBR processing time is only limited by the size of the environment that is used by the issuer.

Outbound Report Overview

Outbound XML reports include the results of file processing which are generated after inbound XML files are submitted, processed and verified. Outbound XML files will be available to the issuer in order to review and analyze the processing results of the enrollment, claims and supplemental diagnosis information submitted for RI and RA processing.

Three (3) types of reports will be produced:

- EDGE Server File Accept-Reject Report
- EDGE Server Summary Accept-Reject Report
- EDGE Server Detail Error Report

Issuers can identify the type of outbound file produced by the two (2) letter code provided in the standard outbound file naming convention. The list below provides the two (2) letter code and the corresponding file type.

- ‘EH’ - EDGE Server File Accept - Reject Report for Enrollment
- ‘MH’ - EDGE Server File Accept - Reject Report for Medical Claims
- ‘PH’ - EDGE Server File Accept - Reject Report for Pharmacy Claims
- ‘SH’ - EDGE Server File Accept - Reject Report for Supplemental Files
- ‘ES’ - EDGE Server Enrollment Summary Accept - Reject Report
- ‘MS’ - EDGE Server Medical Claim (MC) Summary Accept - Reject Report
- ‘PS’ - EDGE Server Pharmacy Summary Accept - Reject Report
- ‘SS’ - EDGE Server Supplemental Diagnosis Summary Accept - Reject Report
- ‘MD’ - EDGE Server Medical Claim (MC) Detail Error Report
- ‘PD’ - EDGE Server Pharmacy Claim Detail Error Report
- ‘ED’ - EDGE Server Enrollment Detail Error Report
- ‘SD’ - EDGE Server Supplemental Diagnosis Detail Error Report

Test, Production, and Validation Zones

The test zone will allow users to test files and identify errors. File processing that occurs in the test zone will produce the same file outputs; however, no files are sent to CMS.

Files will be routed to the test and production zone based on the zone indicator included in the file name **(“T” for test, “P” for production, “V” for validation - see below)**. Refer to the ICD for the full additional information on the file naming convention rules.

- **Test File Name Format:** 12345.HE.D04022014T091533.**T**.xml
- **Production File Name Format:** 12345.HE.D04022014T091533.**P**.xml
- **Validation File Name Format:** 12345.HE.D04022014T091533.**V**.xml

Issuers will receive outbound summary reports from the test, production, and validation zones. CMS will only receive outbound files from the production zone using a push method.

File Ingest Cautions

Prior to executing file ingest, issuers and TPAs should be aware of the following issues that could cause file ingest to fail:

- EDGE Application is not running the latest version
- Internet is not connected
- XML is not valid according to the XSD

This concludes the file ingest overview. The next two (2) section will cover the submission of inbound files to AWS and OP EDGE servers.

3.1.4 Submitting Files for Processing - AWS EDGE Servers

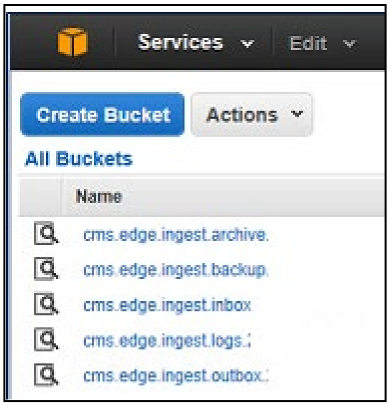
The section provides an overview of the steps that Amazon EDGE server issuers will take to upload enrollee and claims files to their AWS S3 bucket and generate outbound reports. Before submitting files, issuers should confirm successful provisioning and verify they are connected to their server instance as outlined in Section 3.8.6: AWS EDGE Server Provisioning in the EDGE Server Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning. Once issuers confirm they are connected to the AWS EDGE server instance and confirmed the server is functioning, they can begin submitting files for processing.

AWS EDGE Server File Directories

The following information provides Amazon EDGE server issuers an overview of the Amazon S3 bucket structure. Amazon S3 provides a highly durable and available store for a variety of content, ranging from web applications to media files. The EDGE server S3 bucket is created through initial server set up. If a user hosts several servers, each server will be displayed in the S3 bucket.

File processing is automatically initiated when an issuer uploads the inbound file and it is uploaded to the EDGE Server S3 bucket and when the Amazon EDGE server is started and running. Amazon S3 service authentication, authorization and SSL/TLS encryption, and server-side encryption at rest policies are used to protect issuer data being transmitted between the issuer EDGE server and source/target S3 buckets. Within the Amazon S3 bucket, issuers will find the following folders:

- Archive
- Backup
- Inbox
- Logs
- Outbox



Name
cms.edge.ingest.archive.
cms.edge.ingest.backup
cms.edge.ingest.inbox
cms.edge.ingest.logs.
cms.edge.ingest.outbox.

Figure 3-1: AWS S3 Bucket Structure

Distribution of Outbound Data Files

- Amazon EDGE server issuer reports will be delivered to the AWS S3 bucket configured for the issuer.
- Summary reports for Amazon EDGE servers will be pushed to the CMS AWS S3 bucket.
- Issuers will receive outbound files from both the test and production zones.

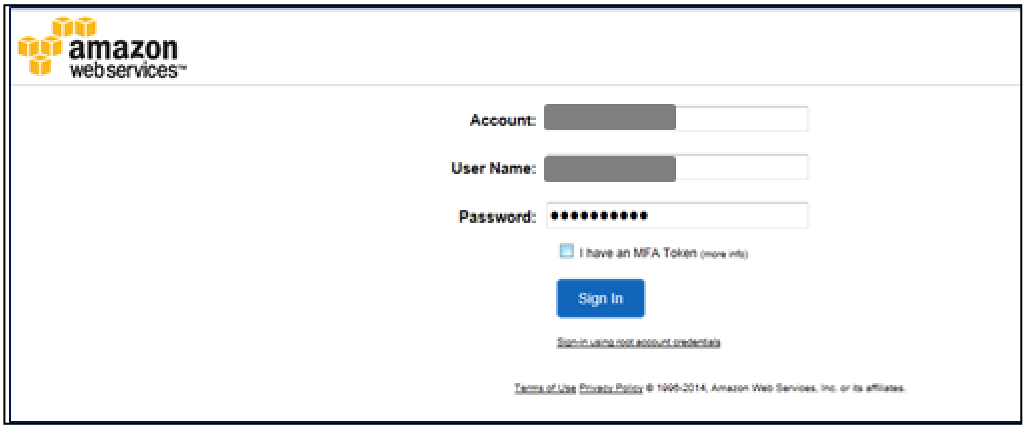
File Ingest Steps

Prior to executing file ingest, issuers and TPAs should be aware of the following issues that could cause file ingest to fail:

- EDGE Application is not running the latest version
- Internet is not connected
- XML is not valid according to the XSD

The following steps provide issuers using Amazon EDGE instance guidance on how to access their AWS S3 bucket, upload files to their S3 bucket inbox, and generate outbound reports to their S3 bucket outbox.

1. To begin uploading files to your EDGE server, first log into their AWS account.



Account: [redacted]

User Name: [redacted]

Password: ●●●●●●●●●●●

□ I have an MFA Token (more info)

amazon web services
Sign In
Sign-in using root account credentials
Terms of Use Privacy Policy © 1996-2014, Amazon Web Services, Inc. or its affiliates.

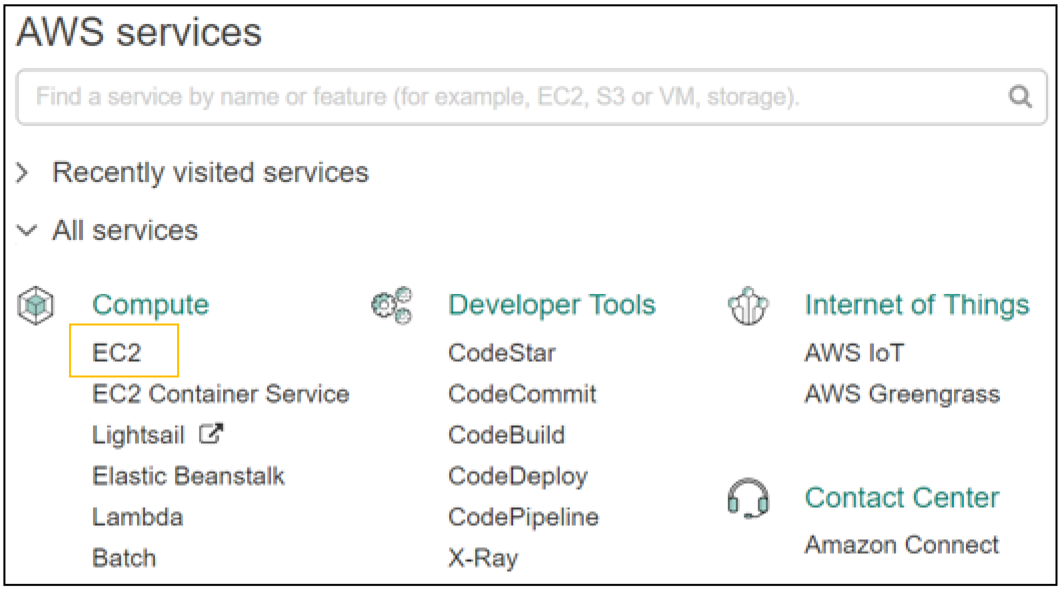
Figure 3-2: Amazon Web Services - Login Screen

Start Server Instance

In order to avoid continuous usage charges for a server instance, issuers have the ability to **"Start"** and **"Stop"** a server instance. This prevents a server from running and incurring cost when it is not being used.

Before processing your files, please remember to **"Start"** your server instance to ensure the server is running.

2. To start a server instance, from the AWS homepage, click **EC2** from the menu at the top left-hand side of the screen.



AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

> Recently visited services

All services

Compute
- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

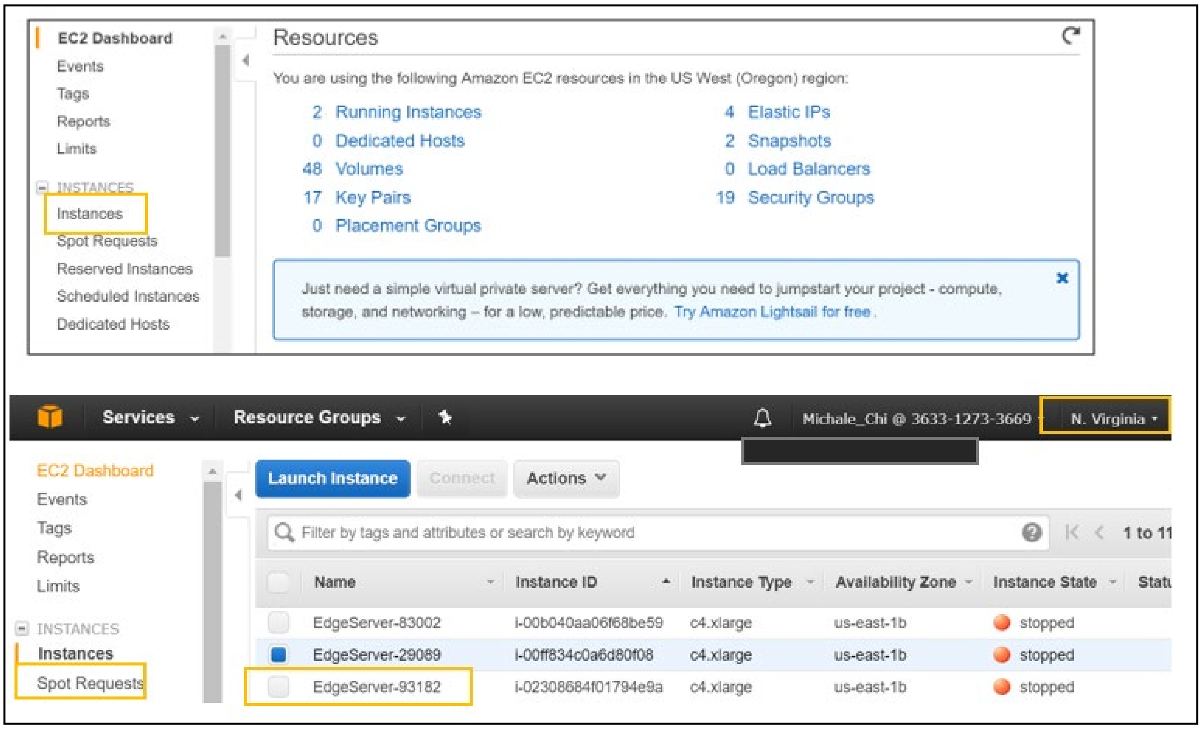
Developer Tools
- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Internet of Things
- AWS IoT
- AWS Greengrass

Contact Center
- Amazon Connect

Figure 3-3: Select EC2

3. Next, click **Instances** at the top left-hand side of the screen, verify you are in the correct region and from the list of server instances, select the box next to your server instance.



Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

2	Running Instances	4	Elastic IPs
0	Dedicated Hosts	2	Snapshots
48	Volumes	0	Load Balancers
17	Key Pairs	19	Security Groups
0	Placement Groups		

Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free.

[redacted]

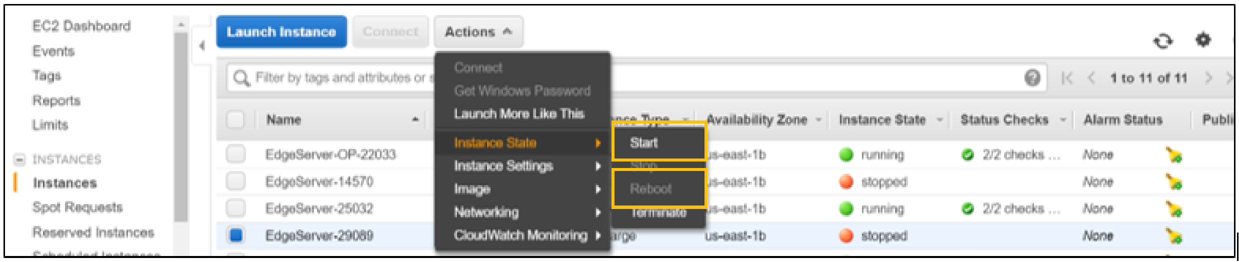
Filter by tags and attributes or search by keyword

1 to 11

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Statu
□	EdgeServer-83002	i-00b040aa06f68be59	c4.xlarge	us-east-1b	● stopped	
■	EdgeServer-29089	i-00ff834c0a6d80f08	c4.xlarge	us-east-1b	● stopped	
□	EdgeServer-93182	i-02308684f01794e9a	c4.xlarge	us-east-1b	● stopped	

Figure 3-4: Select Server Instance

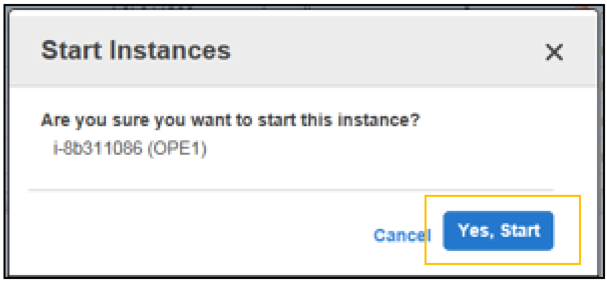
4. Once you have selected your server instance, click the **Actions** dropdown menu at the top of the page and then select **Start**.



Name	...nce Type	Availability Zone	Instance State	Status Checks	Alarm Status	Publi
EdgeServer-OP-22033		us-east-1b	running	2/2 checks ...	None	
EdgeServer-14570		us-east-1b	stopped		None	
EdgeServer-25032		us-east-1b	running	2/2 checks ...	None	
EdgeServer-29089	...arge	us-east-1b	stopped		None	

Figure 3-5: Start Server Instance

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



Are you sure you want to start this instance?
i-8b311086 (OPE1)

Figure 3-6: Confirm Start

6. Once you have confirmed your server instance is **“Started” (running),** navigate to the AWS Home Page by clicking the image and access your AWS S3 bucket by clicking **S3** located in the **Storage and Content Delivery** sub section of the menu.

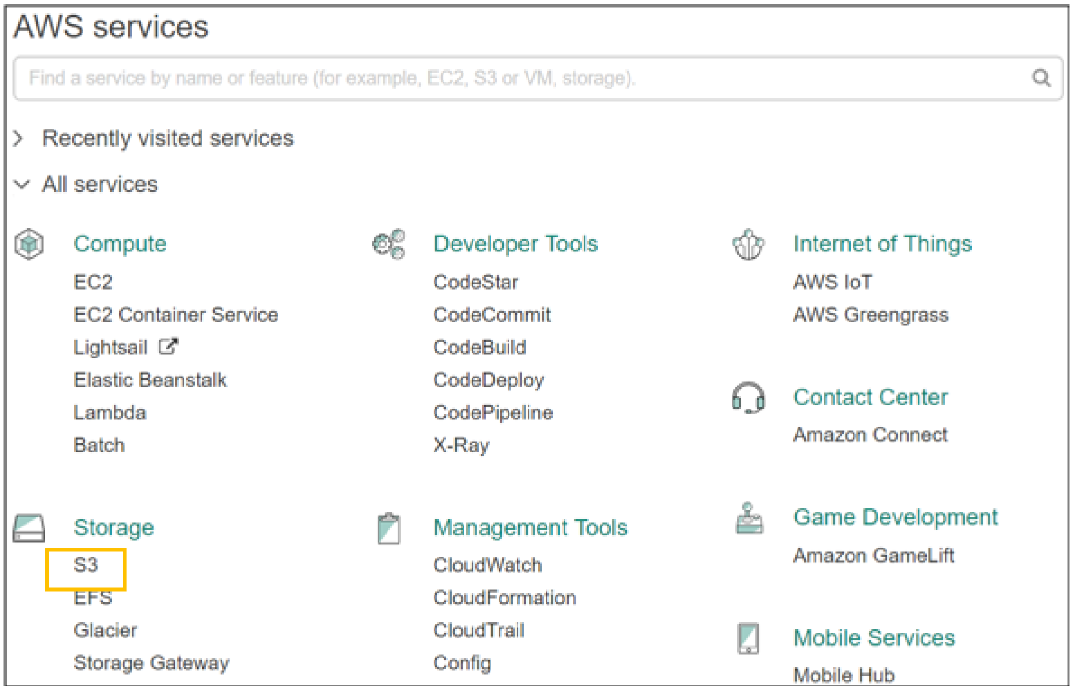


Figure 3-7: AWS Home Screen - Select S3

7. Issuers will then need to access their inbox by selecting ‘**cms.edge.ingest.inbox**’ from the list of S3 Buckets.

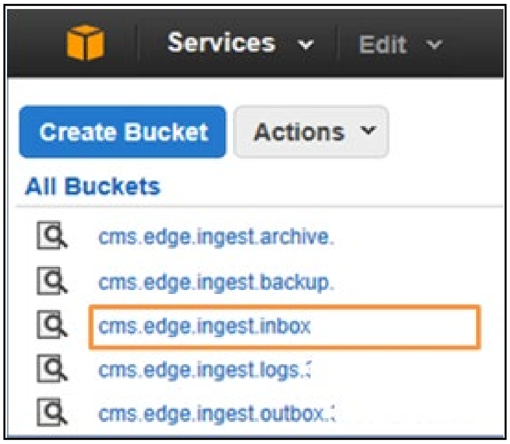


Figure 3-8: Select S3 Buckets Inbox

8. In the next screen, issuers will select their **Issuer ID** from the displayed list.

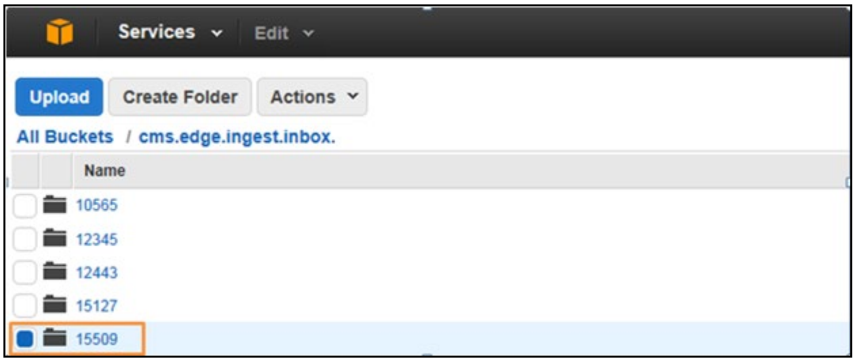


Figure 3-9: Select Issuer ID

9. From the inbox screen, issuers will see their Inbox folder is empty as files are moved to the archive folder after processing. To begin uploading files, first, click the ‘**Upload**’ button at the top left.

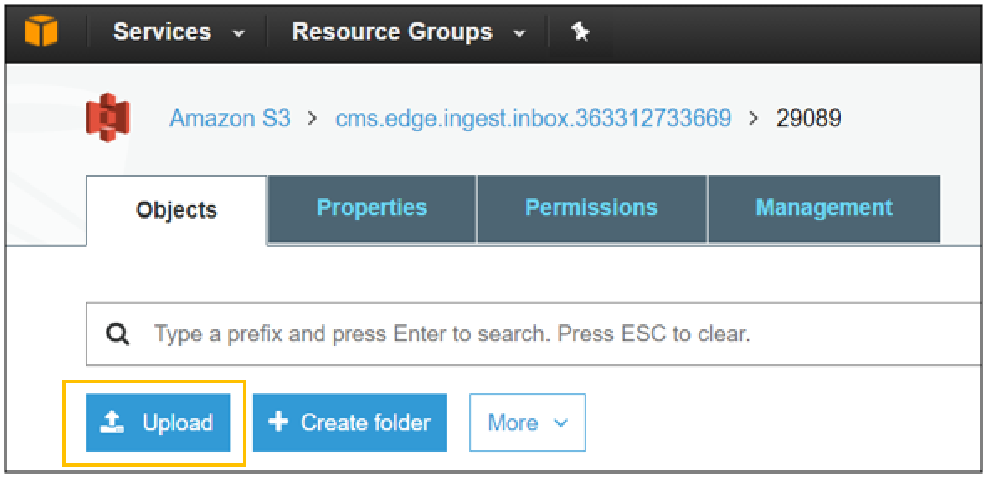

Services
Resource Groups
Amazon S3 > cms.edge.ingest.inbox.363312733669 > 29089
Objects
Properties
Permissions
Management
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
More

Figure 3-10: Select Upload

10. In the **Upload** window, issuers can now begin attaching files. Issuers will click the **Add Files** link to select files to upload from their computer.

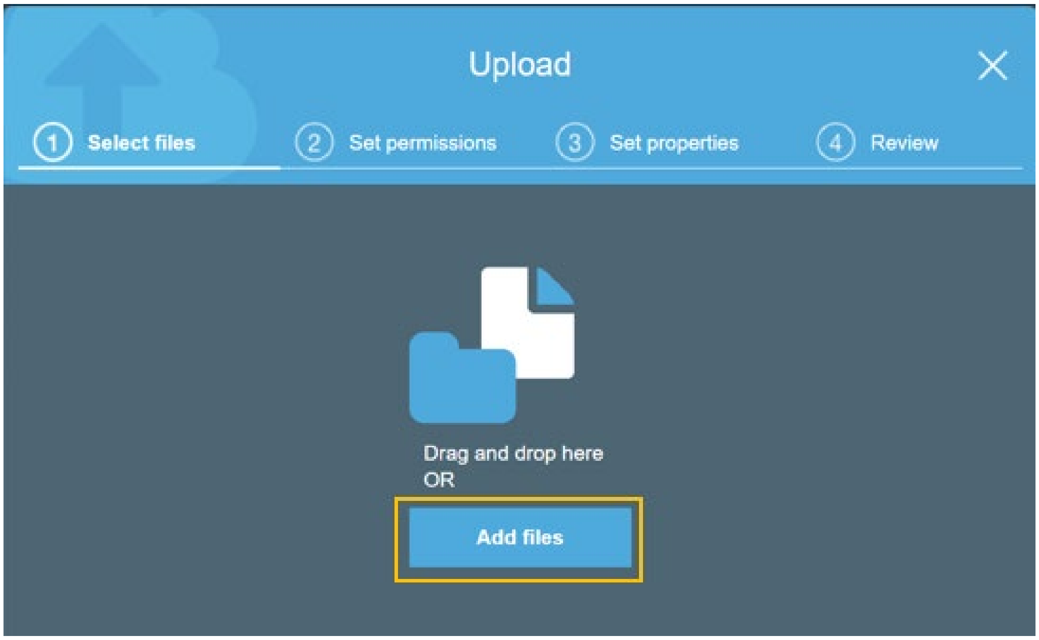
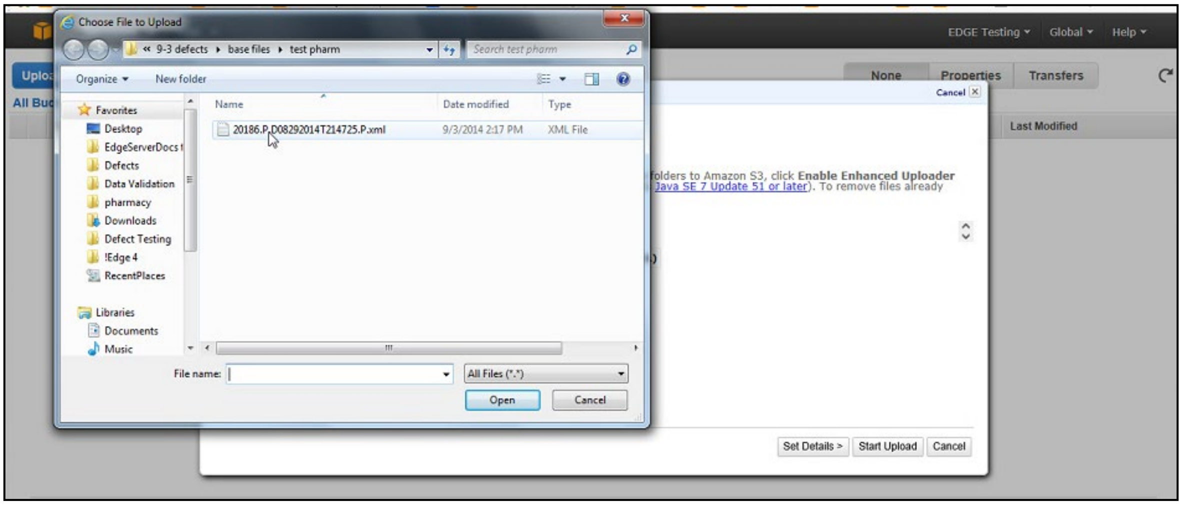


Figure 3-11: Upload - Select Files and Folder

11. In the **Choose File to Upload** window, select the enrollment or claims files to upload that are saved locally on your computer.

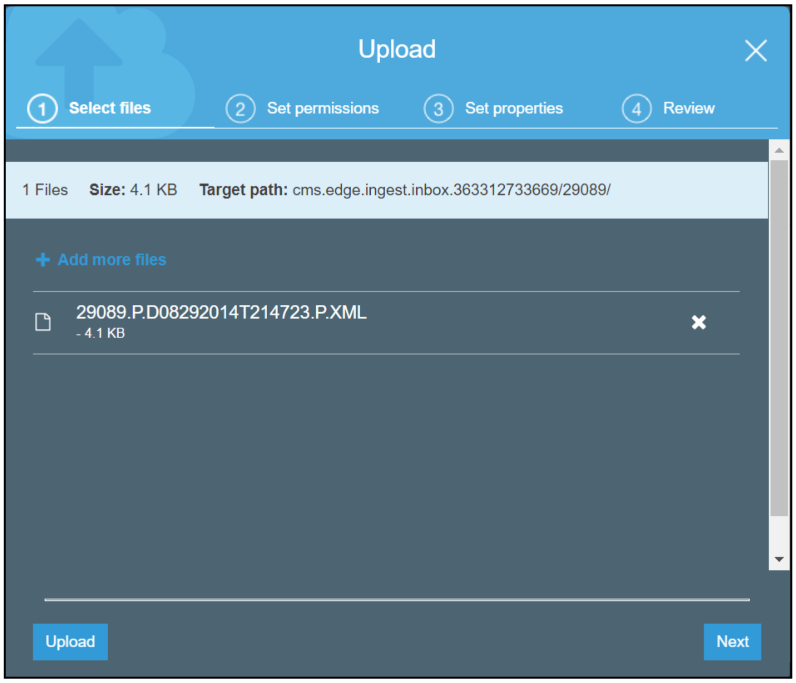


Name	Date modified	Type
20186.P.D08292014T214725.P.xml	9/3/2014 2:17 PM	XML File

folders to Amazon S3, click **Enable Enhanced Uploader** Java SE 7 Update 51 or later). To remove files already

Figure 3-12: Choose File to Upload

12. Once all files are attached for upload, click the **'Next'** button at the bottom of the screen until you reach the **Set Properties** page.

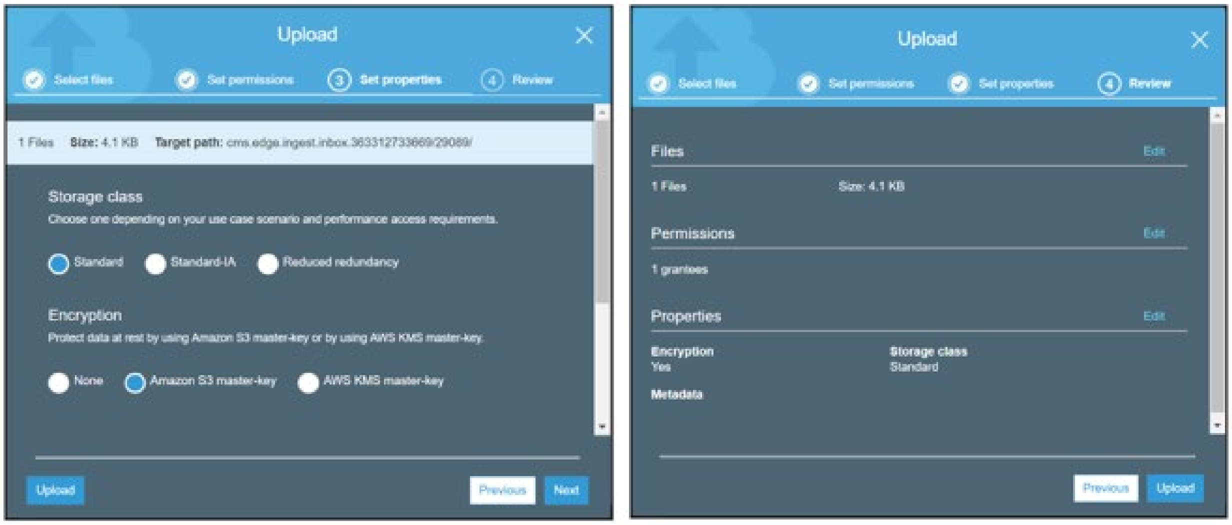


1 Files **Size:** 4.1 KB **Target path:** cms.edge.ingest.inbox.363312733669/29089/

29089.P.D08292014T214723.P.XML
- 4.1 KB

Figure 3-13: Attached File in Select Files

13. In the **Set Properties** window, select the **‘Amazon S3 master-key’** checkbox. This will ensure your uploaded files are encrypted on the server. Click **‘Next’**, and then click the **‘Upload’** button.



1 Files **Size:** 4.1 KB **Target path:** cms.edge.ingest.inbox.363312733669/29089/

Storage class

Choose one depending on your use case scenario and performance access requirements.

● Standard ○ Standard-IA ○ Reduced redundancy

Encryption

Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.

○ None ● Amazon S3 master-key ○ AWS KMS master-key

Files

1 Files Size: 4.1 KB

Permissions

1 grantees

Properties

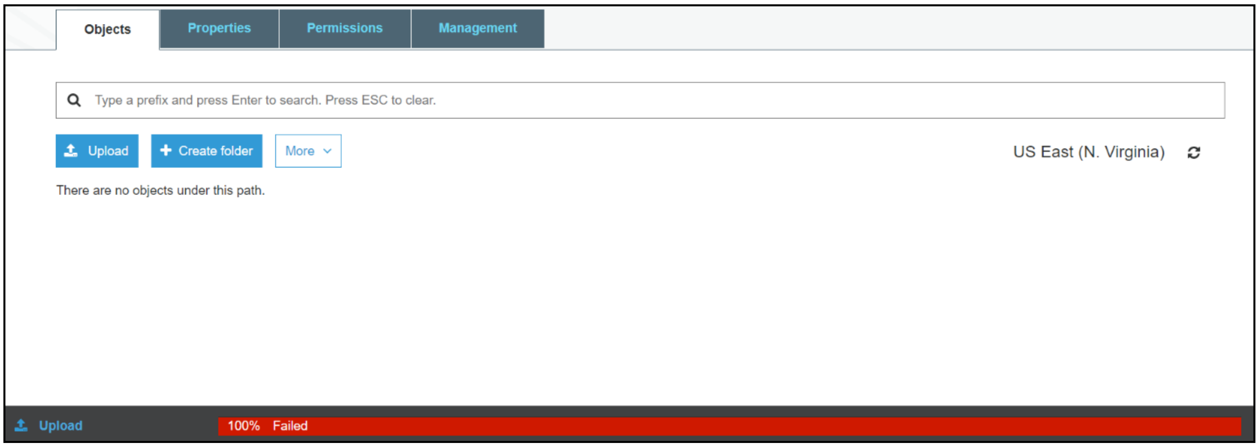
Encryption Yes

Storage class Standard

Metadata

Figure 3-14: Set Details and Upload

Note: If you do not enable the Server File Encryption noted in the above step and immediately click **‘Upload’** after attaching your file, file upload will fail, and you will receive the error message shown below. If this occurs, you will have to re-attach the file and upload again. Please remember to enable the server file encryption in the **Set Details** menu.

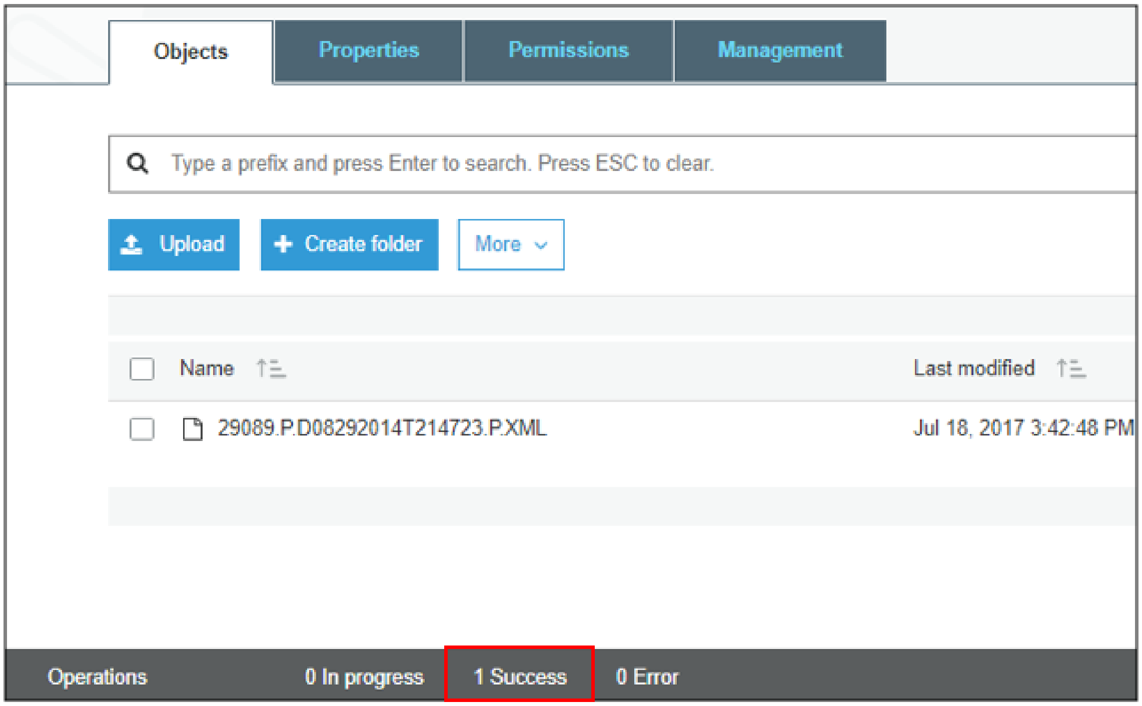


There are no objects under this path.

100% Failed

Figure 3-15: File Upload Error

After uploading the files, issuers will be taken back to their inbox and will see the upload progress of their files. The file is complete once the issuer sees a **"Success"** message at the bottom of the screen.

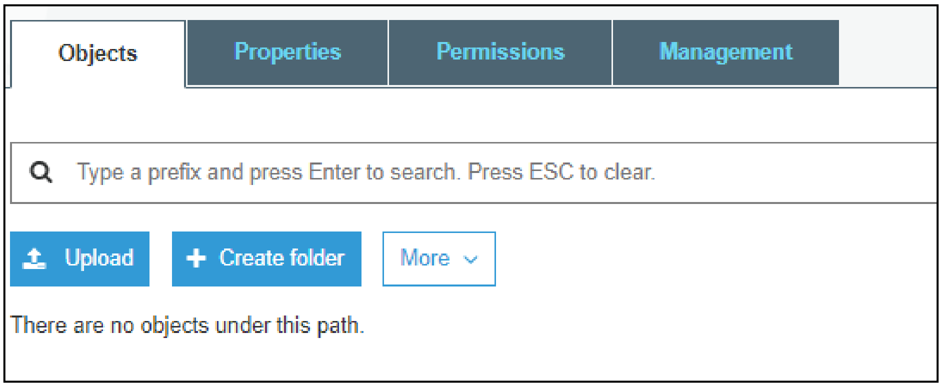


	Name	Last modified
□	29089.P.D08292014T214723.P.XML	Jul 18, 2017 3:42:48 PM

Operations 0 In progress 1 Success 0 Error

Figure 3-16: Upload Complete

An automatic CRON job or issuer initiated 'edge ingest' command will then pick up the file for processing. The results of the processing will be sent to the Outbound folder and the Inbound folder will be empty.

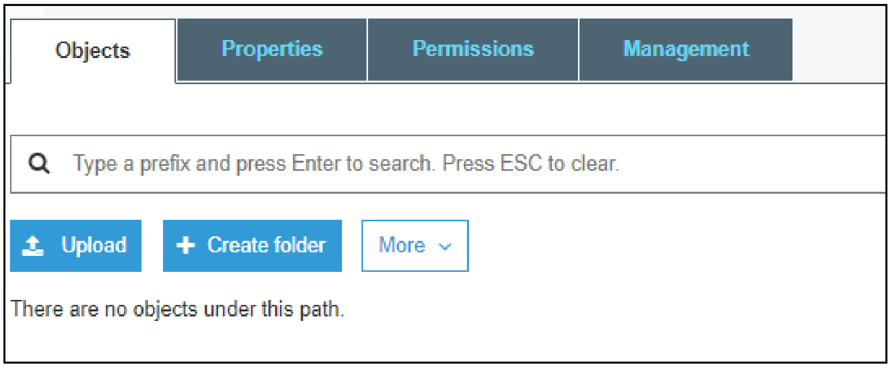


There are no objects under this path.

Figure 3-17: File Picked Up for Processing

Locate Outbound Reports

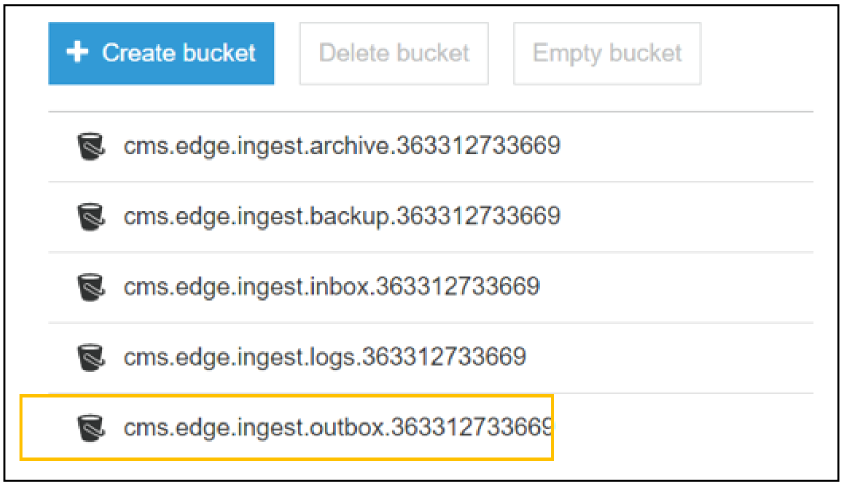
14. Once the file is cleared and the folder is empty this indicates that the file has processed completely, and the corresponding outbound reports have generated. Once complete, click the **'Amazon S3'** link in the top left to return to the S3 bucket main screen.



There are no objects under this path.

Figure 3-18: Refresh Inbox

15. From the S3 bucket list, select the **'cms.edge.ingest.outbox'** link to open the Outbox folder.



cms.edge.ingest.archive.363312733669

cms.edge.ingest.backup.363312733669

cms.edge.ingest.inbox.363312733669

cms.edge.ingest.logs.363312733669

cms.edge.ingest.outbox.363312733669

Figure 3-19: Select Outbox

16. In the next screen, issuers will select their **Issuer ID** from the displayed list.

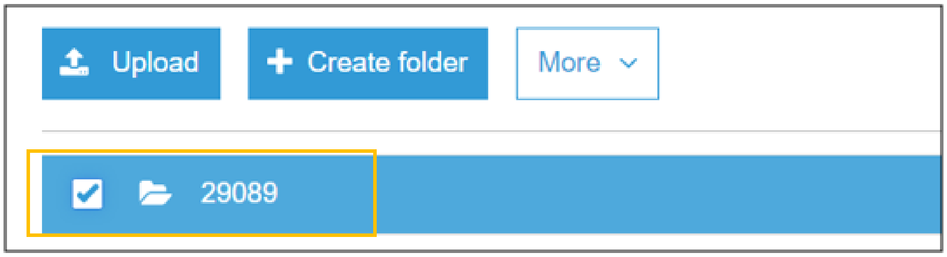
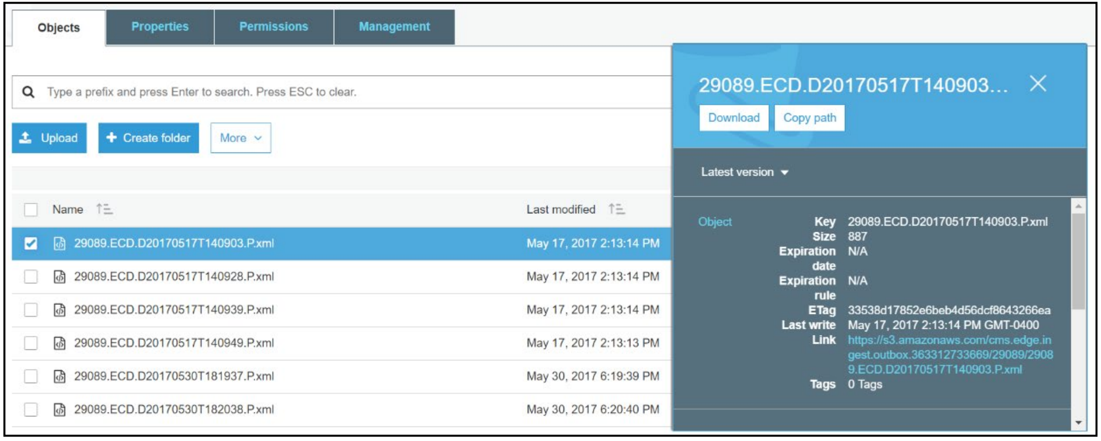


Figure 3-20: Select Issuer ID

a. In the Outbox screen, issuers will need to identify the outbound report that corresponds to the uploaded file by the **time/date** stamp and the file naming convention as described in Section 3.1.3 File Ingest Overview. To match an outbound report to the inbound report, issuers will need to download the file produced, open the file and look for the inbound File Identifier. To download a report, select the report by clicking the checkbox to the left and then right-click. Select **'Download'** from the pop-out menu.



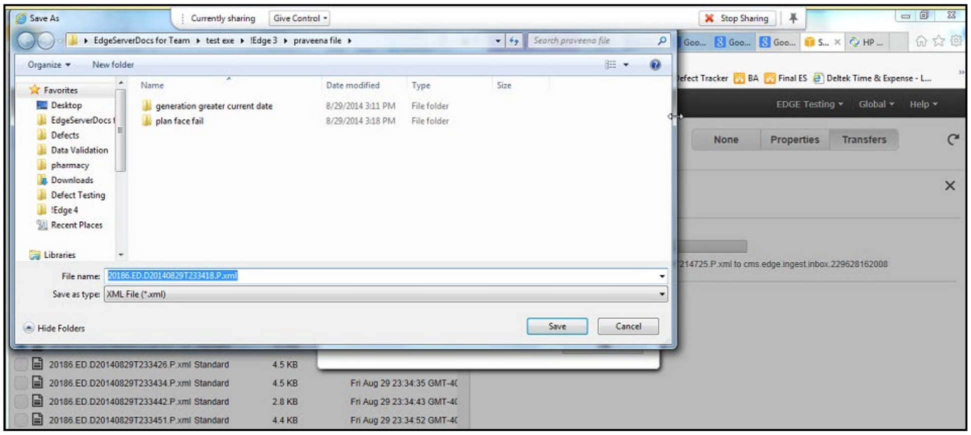
	Name	Last modified
☑	29089.ECD.D20170517T140903.P.xml	May 17, 2017 2:13:14 PM
□	29089.ECD.D20170517T140928.P.xml	May 17, 2017 2:13:14 PM
□	29089.ECD.D20170517T140939.P.xml	May 17, 2017 2:13:14 PM
□	29089.ECD.D20170517T140949.P.xml	May 17, 2017 2:13:13 PM
□	29089.ECD.D20170530T181937.P.xml	May 30, 2017 6:19:39 PM
□	29089.ECD.D20170530T182038.P.xml	May 30, 2017 6:20:40 PM

Object

Key	29089.ECD.D20170517T140903.P.xml
Size	887
Expiration date	N/A
Expiration rule	N/A
ETag	33538d17852e6beb4d56dcf8643266ea
Last write	May 17, 2017 2:13:14 PM GMT-0400
Link	https://s3.amazonaws.com/cms.edge.ingest.outbox.363312733669/29089/29089.ECD.D20170517T140903.P.xml
Tags	0 Tags

Figure 3-21: Locate and Download Report

17. In the **Save As** window, choose the appropriate file location for the outbound reports and save the files locally to your computer.



Name	Date modified	Type	Size
generation greater current date	8/29/2014 3:11 PM	File folder	
plan face fail	8/29/2014 3:18 PM	File folder	

File name: 20186.ED.D20140829T233418.P.xml

Save as type: XML File (*.xml)

214725.P.xml to cms.edge.ingest.inbox.229628162008

20186.ED.D20140829T233426.P.xml	Standard	4.5 KB	
20186.ED.D20140829T233434.P.xml	Standard	4.5 KB	Fri Aug 29 23:34:35 GMT-4(
20186.ED.D20140829T233442.P.xml	Standard	2.8 KB	Fri Aug 29 23:34:43 GMT-4(
20186.ED.D20140829T233451.P.xml	Standard	4.4 KB	Fri Aug 29 23:34:52 GMT-4(

Figure 3-22: Save Downloaded Report

Once saved, you will be able to open and review the outbound report results to validate that submitted data was processed successfully and does not contain any deficiencies.

Stop Server Instance

Once you receive the final notification that reports were sent to CMS for the files you have processed, you can stop your server instance in order to avoid incurring charges for having the server running. To stop a server instance, refer to the steps in VI: Stop Server Instance in Section 3.8.6: AWS EDGE Server Provisioning in the EDGE Server Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning.

This concludes the steps for submitting inbound files to an AWS EDGE Server. The next section will cover the submission of inbound files to an OP EDGE server.

3.1.5 Submitting Files for Processing - On-Premise EDGE Servers

The section provides an overview of the steps that OP EDGE server issuers will take to upload enrollee and claims files to their OP file directory and generate outbound reports. Before completing the steps highlighted in this document, issuers should have confirmed successful provisioning and verified they are connected to their server. Once issuers confirm they are connected to their EDGE server and confirmed the server is functioning, they can begin submitting files for processing.

OP EDGE Server File Directories

The following information provides OP EDGE issuers an overview of their file directory structure. File processing is initiated using scripts provided by CMS once the issuer uploads the inbound files to the physical/virtual directory. Issuers will need to setup a scheduler for automated processing of files. Detailed data never leaves the issuer environment. Within an OP file directory, issuers should have the following folders:

- Back-up
- Inbox
- Outbox

OP EDGE server issuers can configure additional folders in their file directory as necessary.

Distribution of outbound data files

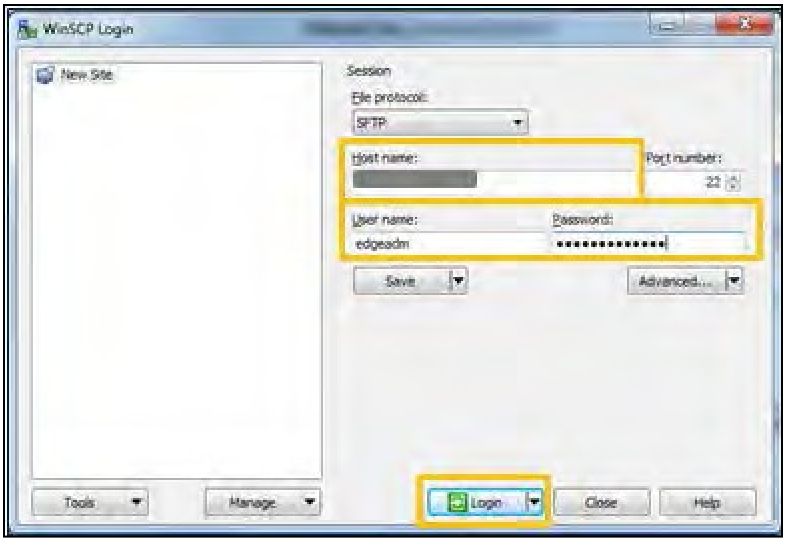
- OP EDGE server issuer reports will be delivered to the outbound file directory.
- Summary reports for OP EDGE servers will be pushed to the CMS AWS S3 bucket.

File Ingest Steps

The following steps provide issuers and TPAs using an OP EDGE server guidance on how to access their file directory, upload files to their inbox, and generate outbound reports to their outbox. WinSCP is a commonly used application for these purposes and, for sample purposes, the step-by-step instructions that follow reference use of WinSCP. However, issuers or TPAs may use their secure file transfer protocol (SFTP) client of choice for this purpose and will need to adapt the instructions that follow if they choose to use a different SFTP client.

1. To begin uploading files to your OP EDGE server, first open WinSCP program and login. Enter the **IP Address, Username** and **Password** for your server and click **Login**.

The username and password were configured as part of setting up your OP server as described in Section 3.3.1: Server Setup in the EDGE Server Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning.



Session
File protocol: SFTP
Host name: [redacted]
Port number: 22
User name: edgeadm
Password: ••••••••••••••

Figure 3-23: WinSCP Login Screen

2. From WinSCP main page, navigate to the server side (right side) and locate the **“edge”** folder created during the provisioning process. Click the **edge** folder link.

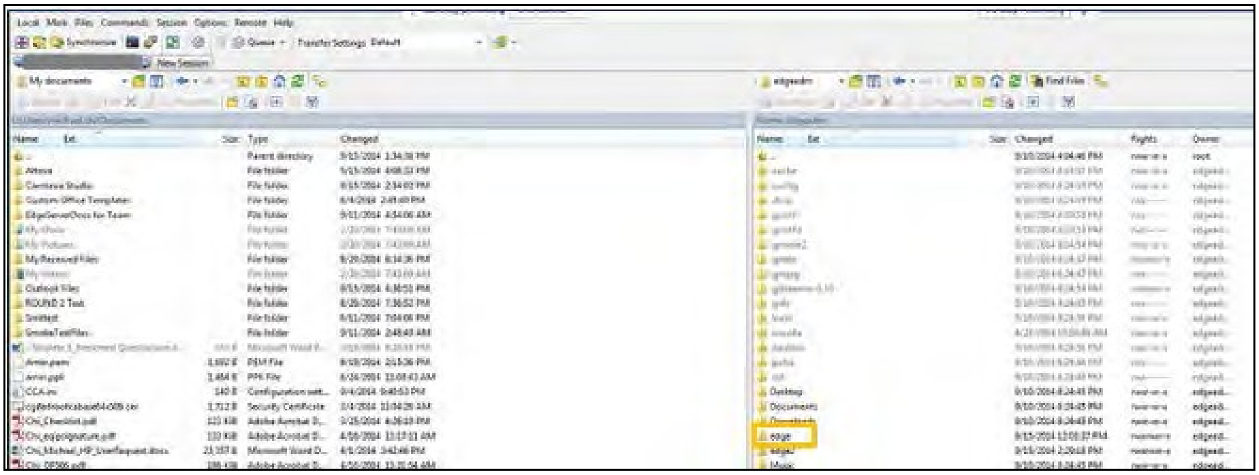

Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
New Session
My documents
edgeadm
Find Files
Name Ext Size Type Changed
Name Ext Size Changed Rights Owner
Desktop
Documents
edge
Music

Figure 3-24: Edge Folder

3. Once inside the **edge** folder, click the **ingest** folder.

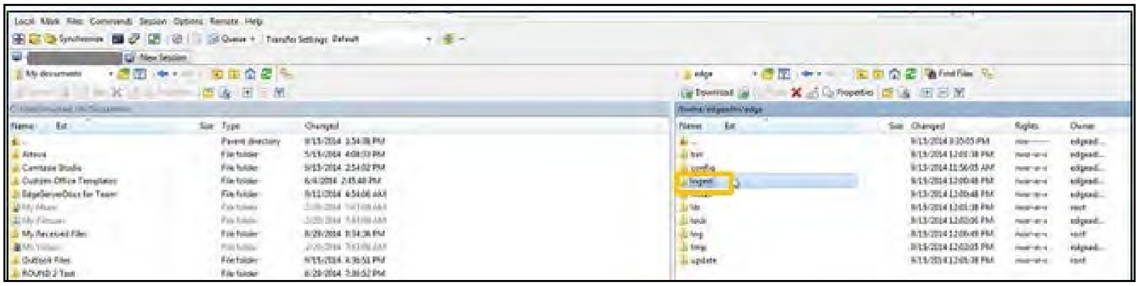

Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
New Session
My documents
edge
Find Files
Download
Properties
/home/edgeadm/edge
Name Ext Size Type Changed
Name Ext Size Changed Rights Owner
config
ingest
update

Figure 3-25: Ingest Folder

4. From within the **ingest** folder, next click **Inbox** to open your OP Inbox where you can upload files.

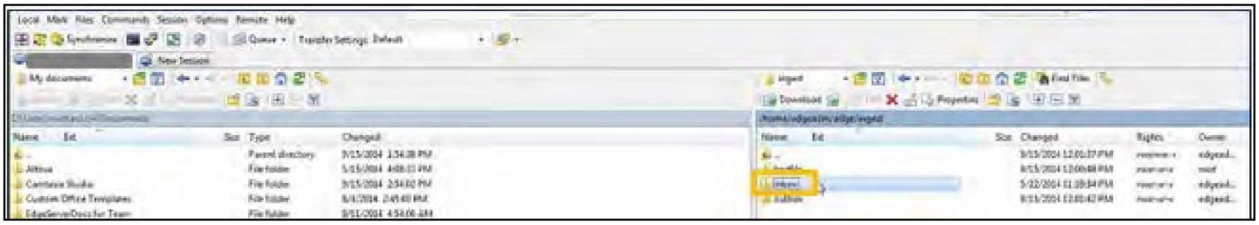

Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
[redacted]
New Session
My documents
ingest
Download
Properties
Find Files
Name Ext Size Type Changed
Name Ext Size Changed Rights Owner
Parent directory
File folder
Inbox
Outbox

Figure 3-26: Inbox Folder

5. Next, locate your enrollee and claims files saved to your local computer by navigating back to the left side of WinSCP to your local computer files. Once located, drag and drop those files from your local computer to your server in the **Inbox** folder.

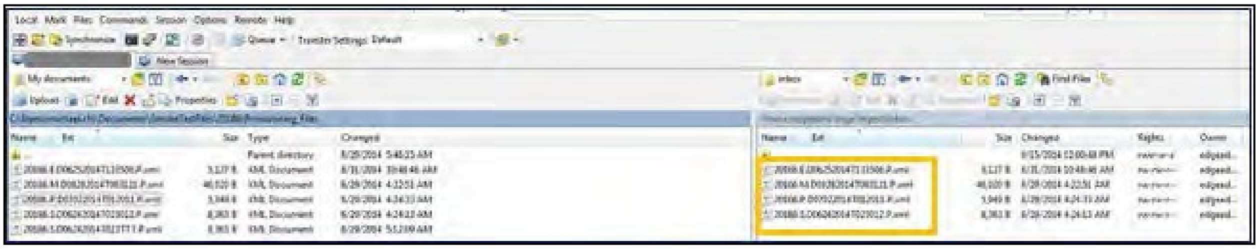
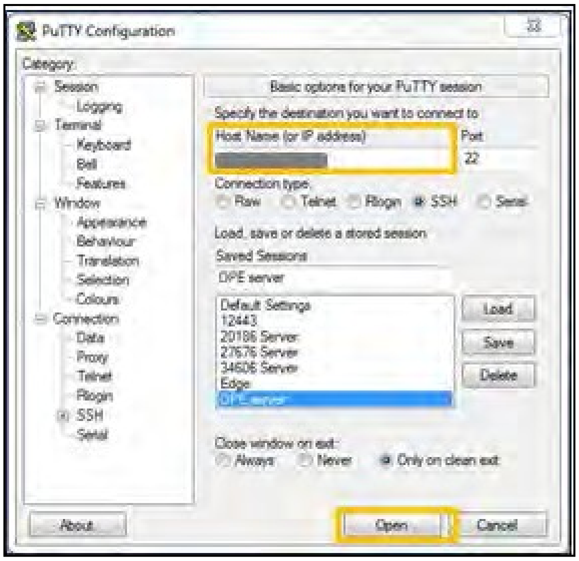

Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
[redacted]
New Session
My documents
Upload
Edit
Properties
inbox
Find Files
Name Ext Size Type Changed
Name Ext Size Changed Rights Owner
Parent directory
XML Document

Figure 3-27: Drag and Drop Upload Files to Server

6. Next, open your PuTTY program (or other SSH client of choice) and enter your server's IP address in the Host Name (or IP Address) field and then click **Open**.



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): [redacted]

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

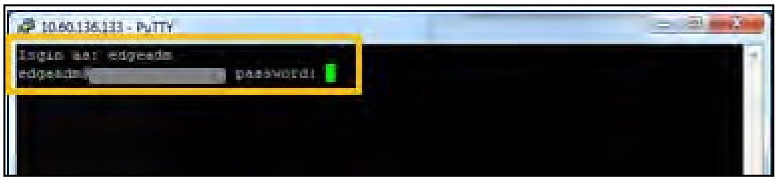
Saved Sessions: OPE server

Default Settings
12443
20186 Server
27676 Server
34606 Server
Edge
OPE server

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 3-28: PuTTY Login Screen

7. When PuTTY opens, enter your username and password and click **Enter.**

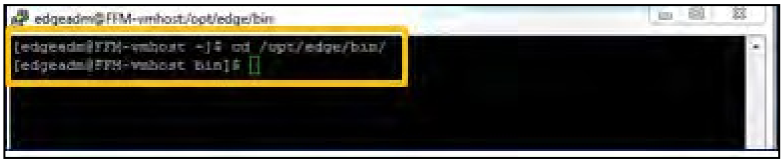


10.60.136.133 - PuTTY

```
login as: edgeadm
edgeadm@[redacted] password:
```

Figure 3-29: Enter Username and Password

8. In PuTTY, first enter command: cd /opt/edge/bin/ (all lowercase with a space between “cd” and “/opt”) and click **Enter**. This will open the OPT folder.

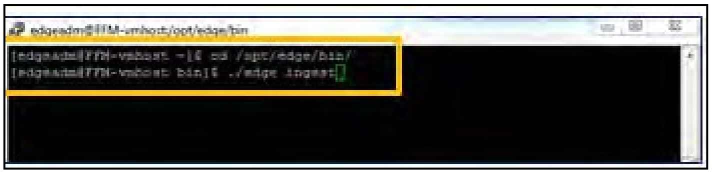


edgeadm@FFM-vmhost:/opt/edge/bin

```
[edgeadm@FFM-vmhost ~]$ cd /opt/edge/bin/
[edgeadm@FFM-vmhost bin]$
```

Figure 3-30: Open OPT Folder

9. Next, enter the following command. This command will pick up the files from the **Inbox** folder, process them, and generate the outbound reports:
   - ./edge ingest

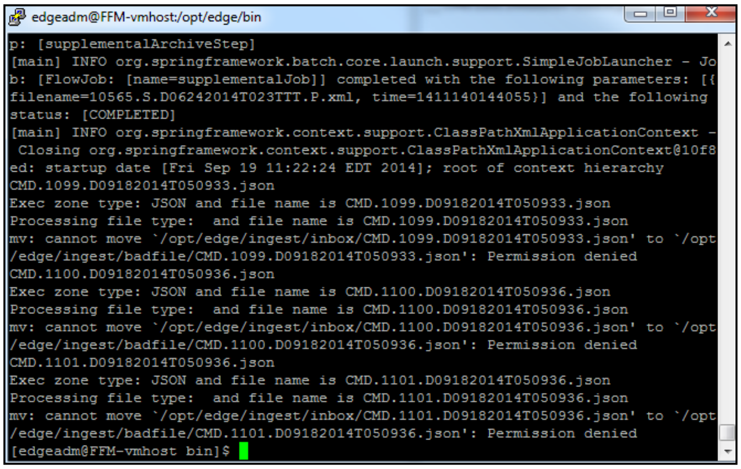


edgeadm@FFM-vmhost:/opt/edge/bin

```
[edgeadm@FFM-vmhost ~]$ cd /opt/edge/bin/
[edgeadm@FFM-vmhost bin]$ ./edge ingest
```

Figure 3-31: Run EDGE Ingest Command to Process Files

10. After running the command in the previous step, the script will run for about one (1) minute. When the script finishes, file processing is complete.

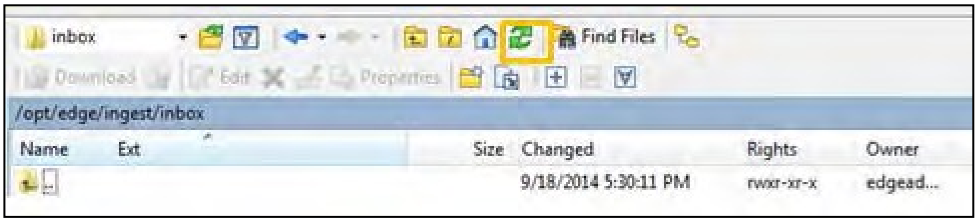


edgeadm@FFM-vmhost:/opt/edge/bin

```
p: [supplementalArchiveStep]
[main] INFO org.springframework.batch.core.launch.support.SimpleJobLauncher - Jo
b: [FlowJob: [name=supplementalJob]] completed with the following parameters: [{
filename=10565.S.D06242014T023TTT.P.xml, time=1411140144055}] and the following
status: [COMPLETED]
[main] INFO org.springframework.context.support.ClassPathXmlApplicationContext -
 Closing org.springframework.context.support.ClassPathXmlApplicationContext@10f8
ed: startup date [Fri Sep 19 11:22:24 EDT 2014]; root of context hierarchy
CMD.1099.D09182014T050933.json
Exec zone type: JSON and file name is CMD.1099.D09182014T050933.json
Processing file type:  and file name is CMD.1099.D09182014T050933.json
mv: cannot move `/opt/edge/ingest/inbox/CMD.1099.D09182014T050933.json' to `/opt
/edge/ingest/badfile/CMD.1099.D09182014T050933.json': Permission denied
CMD.1100.D09182014T050936.json
Exec zone type: JSON and file name is CMD.1100.D09182014T050936.json
Processing file type:  and file name is CMD.1100.D09182014T050936.json
mv: cannot move `/opt/edge/ingest/inbox/CMD.1100.D09182014T050936.json' to `/opt
/edge/ingest/badfile/CMD.1100.D09182014T050936.json': Permission denied
CMD.1101.D09182014T050936.json
Exec zone type: JSON and file name is CMD.1101.D09182014T050936.json
Processing file type:  and file name is CMD.1101.D09182014T050936.json
mv: cannot move `/opt/edge/ingest/inbox/CMD.1101.D09182014T050936.json' to `/opt
/edge/ingest/badfile/CMD.1101.D09182014T050936.json': Permission denied
[edgeadm@FFM-vmhost bin]$
```

Figure 3-32: Files Processing Complete

11. Once the upload completes, go back to your WinSCP program in your Inbox and click the **Refresh** icon at the top of the page and the files should clear from your inbox. This will indicate that the upload is complete.



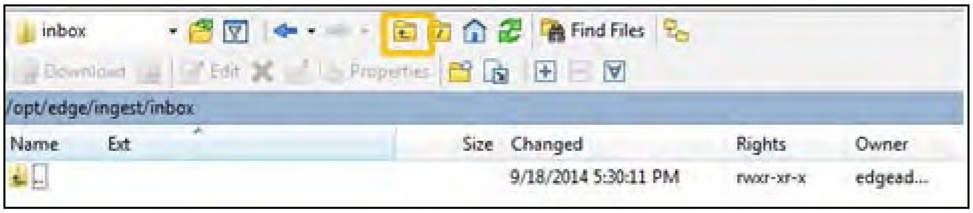
/opt/edge/ingest/inbox

Name	Ext	Size	Changed	Rights	Owner
..			9/18/2014 5:30:11 PM	rwxr-xr-x	edgead...

Figure 3-33: Refresh Inbox

Locate Outbound Reports

12. After refreshing your Inbox, click the folder icon at the top right to go back one (1) directory to your **ingest** folder.

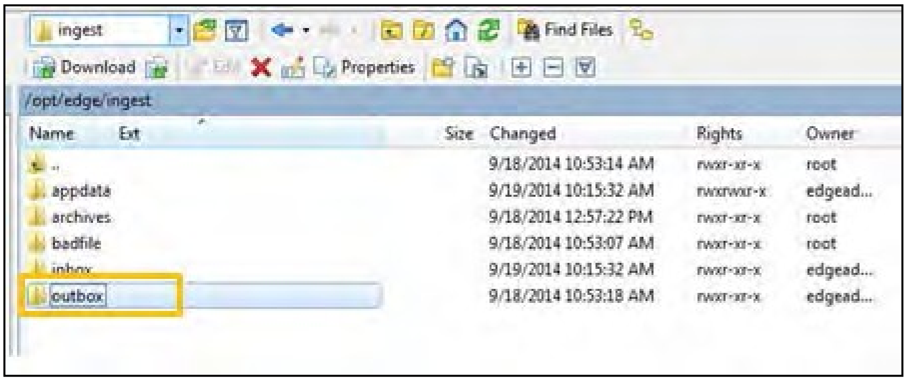


/opt/edge/ingest/inbox

Name	Ext	Size	Changed	Rights	Owner
..			9/18/2014 5:30:11 PM	rwxr-xr-x	edgead...

Figure 3-34: Navigate to Ingest Folder

13. From the **ingest** folder, click the **Outbox** folder to find your outbound reports.

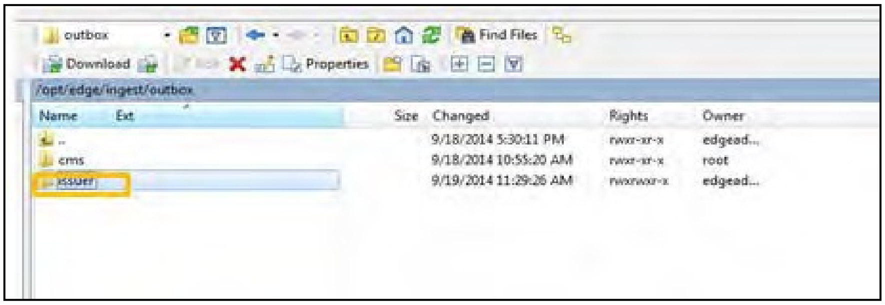


/opt/edge/ingest

Name	Ext	Size	Changed	Rights	Owner
..			9/18/2014 10:53:14 AM	rwxr-xr-x	root
appdata			9/19/2014 10:15:32 AM	rwxrwxr-x	edgead...
archives			9/18/2014 12:57:22 PM	rwxr-xr-x	root
badfile			9/18/2014 10:53:07 AM	rwxr-xr-x	root
inbox			9/19/2014 10:15:32 AM	rwxr-xr-x	edgead...
outbox			9/18/2014 10:53:18 AM	rwxr-xr-x	edgead...

Figure 3-35: Open Outbox Folder

14. Within your Outbox folder, you will find two (2) folders: one (1) for CMS and one (1) for theissuer. Click the **Issuer** folder to view the reports.



/opt/edge/ingest/outbox

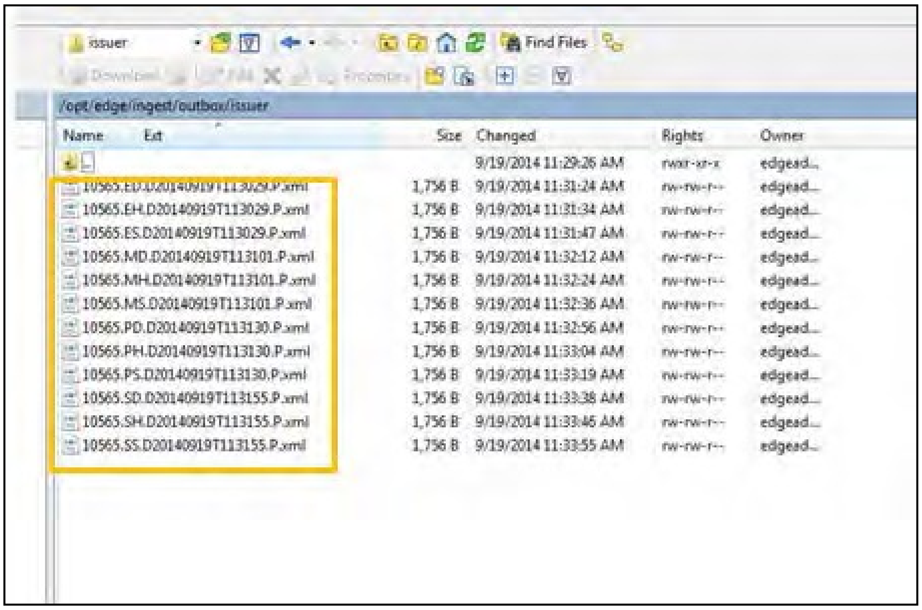
Name	Ext	Size	Changed	Rights	Owner
..			9/18/2014 5:30:11 PM	rwxr-xr-x	edgead...
cms			9/18/2014 10:55:20 AM	rwxr-xr-x	root
issuer			9/19/2014 11:29:26 AM	rwxrwxr-x	edgead...

Figure 3-36: Open Issuer Folder

15. In the **Issuer** folder, you will need to identify the outbound report that corresponds to the uploaded file by the **time/date** stamp and the file naming convention as

described. You can identify the type of outbound file produced by the two (2)-letter code provided in [Section 3.1.3 File Ingest overview](). The list below provides the two (2)-letter code and the corresponding file type:

- 'EH' - EDGE Server File Accept - Reject Report for Enrollment
- 'MH' - EDGE Server File Accept - Reject Report for Medical Claims
- 'PH' - EDGE Server File Accept - Reject Report for Pharmacy Claims
- 'SH' - EDGE Server File Accept - Reject Report for Supplemental Files
- 'ES' - EDGE Server Enrollment Summary Accept - Reject Report
- 'MS' - EDGE Server Medical Claim (MC) Summary Accept - Reject Report
- 'PS' - EDGE Server Pharmacy (RxC) Summary Accept - Reject Report
- 'SS' - EDGE Server Supplemental Diagnosis Summary Accept - Reject Report
- 'MD' - EDGE Server Medical Claim (MC) Detail Error Report
- 'PD' - EDGE Server Pharmacy Claim (RxC) Detail Error Report
- 'ED' - EDGE Server Enrollment Detail Error Report
- 'SD' - EDGE Server Supplemental Diagnosis Detail Error Report

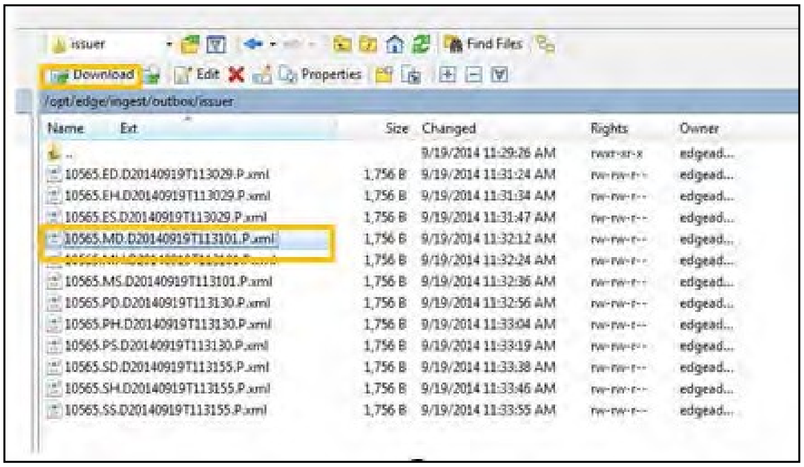


/opt/edge/ingest/outbox/issuer

Name	Ext	Size	Changed	Rights	Owner
			9/19/2014 11:29:26 AM	rwxr-xr-x	edgead...
10565.ED.D20140919T113029.P.xml		1,756 B	9/19/2014 11:31:24 AM	rw-rw-r--	edgead...
10565.EH.D20140919T113029.P.xml		1,756 B	9/19/2014 11:31:34 AM	rw-rw-r--	edgead...
10565.ES.D20140919T113029.P.xml		1,756 B	9/19/2014 11:31:47 AM	rw-rw-r--	edgead...
10565.MD.D20140919T113101.P.xml		1,756 B	9/19/2014 11:32:12 AM	rw-rw-r--	edgead...
10565.MH.D20140919T113101.P.xml		1,756 B	9/19/2014 11:32:24 AM	rw-rw-r--	edgead...
10565.MS.D20140919T113101.P.xml		1,756 B	9/19/2014 11:32:36 AM	rw-rw-r--	edgead...
10565.PD.D20140919T113130.P.xml		1,756 B	9/19/2014 11:32:56 AM	rw-rw-r--	edgead...
10565.PH.D20140919T113130.P.xml		1,756 B	9/19/2014 11:33:04 AM	rw-rw-r--	edgead...
10565.PS.D20140919T113130.P.xml		1,756 B	9/19/2014 11:33:19 AM	rw-rw-r--	edgead...
10565.SD.D20140919T113155.P.xml		1,756 B	9/19/2014 11:33:38 AM	rw-rw-r--	edgead...
10565.SH.D20140919T113155.P.xml		1,756 B	9/19/2014 11:33:46 AM	rw-rw-r--	edgead...
10565.SS.D20140919T113155.P.xml		1,756 B	9/19/2014 11:33:55 AM	rw-rw-r--	edgead...

Figure 3-37: Outbound Reports Folder

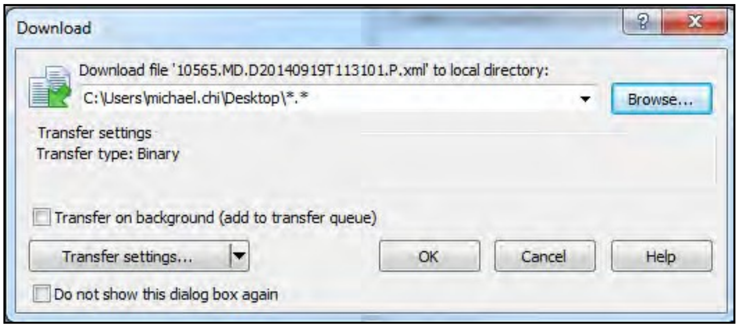
16. To match an outbound report to the inbound report, issuers will need to download the file produced, open the file and look for the Inbound File Identifier. To download a report, highlight the desired report you want to open from your server and then click the **Download** button at the top. In this example, the **EDGE Server Medical Claim (MC) Detail Error Report** is selected by identifying the **MD** code.



```
/opt/edge/ingest/outbox/issuer
Name    Ext                              Size    Changed                  Rights       Owner
..                                               9/19/2014 11:29:26 AM    rwxr-sr-x    edgead...
10565.ED.D20140919T113029.P.xml          1,756 B 9/19/2014 11:31:24 AM    rw-rw-r--    edgead...
10565.EH.D20140919T113029.P.xml          1,756 B 9/19/2014 11:31:34 AM    rw-rw-r--    edgead...
10565.ES.D20140919T113029.P.xml          1,756 B 9/19/2014 11:31:47 AM    rw-rw-r--    edgead...
10565.MD.D20140919T113101.P.xml          1,756 B 9/19/2014 11:32:12 AM    rw-rw-r--    edgead...
[illegible]                              1,756 B 9/19/2014 11:32:24 AM    rw-rw-r--    edgead...
10565.MS.D20140919T113101.P.xml          1,756 B 9/19/2014 11:32:36 AM    rw-rw-r--    edgead...
10565.PD.D20140919T113130.P.xml          1,756 B 9/19/2014 11:32:56 AM    rw-rw-r--    edgead...
10565.PH.D20140919T113130.P.xml          1,756 B 9/19/2014 11:33:04 AM    rw-rw-r--    edgead...
10565.PS.D20140919T113130.P.xml          1,756 B 9/19/2014 11:33:19 AM    rw-rw-r--    edgead...
10565.SD.D20140919T113155.P.xml          1,756 B 9/19/2014 11:33:38 AM    rw-rw-r--    edgead...
10565.SH.D20140919T113155.P.xml          1,756 B 9/19/2014 11:33:46 AM    rw-rw-r--    edgead...
10565.SS.D20140919T113155.P.xml          1,756 B 9/19/2014 11:33:55 AM    rw-rw-r--    edgead...
```

Figure 3-38: Locate Report to Download

17. From the **Download** window, choose a file location to save your report. Click the **Ok** button when finished to save the report.



Download file '10565.MD.D20140919T113101.P.xml' to local directory:

C:\Users\michael.chi\Desktop\*.*

Transfer settings

Transfer type: Binary

□ Transfer on background (add to transfer queue)

□ Do not show this dialog box again

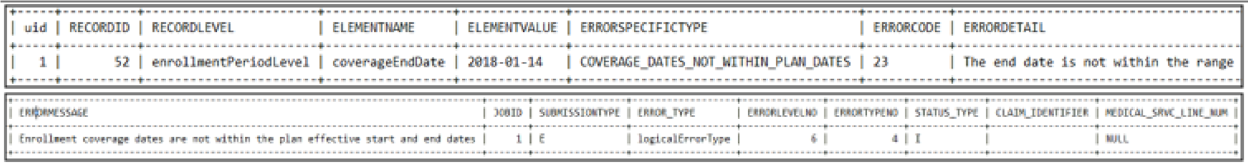
Figure 3-39: Download and Save Report

Once saved, you will be able to open and review the outbound report results to validate that submitted data was processed successfully and does not contain any deficiencies.

3.1.6 File Ingest Validation Errors

In addition to generating the summary and detail outbound reports, the EDGE Server application also logs file ingest validation errors in the MySQL database in the EDGE_ERROR_LOG table. The table logs business validation error and inline validation errors into this table to generate the outbound reports. More information on the fields can be found in the EDGE Server Production Schema Data Dictionary.

The below figure shows the fields associated with the EDGE_ERROR_LOG table. Issuers can use the table to troubleshoot and correct the errors of their inbound file. In this example, the error is caused by the coverageEndDate (elementname) because the enrollment coverage dates are not within the plan effective start and end dates (errormessage).



```
+-----+----------+-----------------------+-----------------+--------------+-----------------------------------+-----------+------------------------------------
| uid | RECORDID | RECORDLEVEL           | ELEMENTNAME     | ELEMENTVALUE | ERRORSPECIFICTYPE                 | ERRORCODE | ERRORDETAIL
+-----+----------+-----------------------+-----------------+--------------+-----------------------------------+-----------+------------------------------------
|   1 |       52 | enrollmentPeriodLevel | coverageEndDate | 2018-01-14   | COVERAGE_DATES_NOT_WITHIN_PLAN_DATES | 23     | The end date is not within the range
+-----+----------+-----------------------+-----------------+--------------+-----------------------------------+-----------+------------------------------------
```

```
+----------------------------------------------------------------+-------+----------------+------------------+--------------+-------------+-------------+------------------+-----------------------+
| ERRORMESSAGE                                                   | JOBID | SUBMISSIONTYPE | ERROR_TYPE       | ERRORLEVELNO | ERRORTYPENO | STATUS_TYPE | CLAIM_IDENTIFIER | MEDICAL_SRVC_LINE_NUM |
+----------------------------------------------------------------+-------+----------------+------------------+--------------+-------------+-------------+------------------+-----------------------+
| Enrollment coverage dates are not within the plan effective start and end dates |     1 | E | logicalErrorType |            6 |           4 | I           |                  | NULL                  |
+----------------------------------------------------------------+-------+----------------+------------------+--------------+-------------+-------------+------------------+-----------------------+
```

Figure 3-40: Example EDGE_ERROR_LOG table

In addition, the EDGE Server Job Aid: EDGE Server File Ingest Error Codes Excel file includes a complete list of file validation error codes, their description and next steps to resolve the error.

Refer to these appendices, which provide_more information about common ingest job error messages for each type of file, for further troubleshooting:

Appendix A: Enrollee File Ingest Job Error Messages
Appendix B: Medical File Ingest Informational and Error Messages
Appendix C: Supplemental File Ingest Informational and Error Messages
and Appendix D: Pharmacy File Ingest Error Messages
If a file was submitted for processing and a detailed report, including any errors, was not generated a new report cannot be regenerated. The next section provides troubleshooting steps to identify if a file is in progress or has completed processing.

3.1.7 Missing Detail Report Troubleshooting Steps

This section provides instructions on how to identify if a file is in progress or has completed processing, and whether records included in the file were accepted or rejected.

Note: This process is only necessary for medical and pharmacy file submissions that do not return a detail report. Issuers may resubmit enrollment and supplemental files but must change the File ID to avoid a rejection for duplicate file submission.

Under normal conditions, detail and summary medical and pharmacy reports are produced shortly after file processing has completed. If no detail medical or pharmacy claim report is produced, issuers should complete the following steps:

1. Determine whether the file has finished processing,
2. Query the tables to obtain a list of records that were accepted and stored and a list of records that were rejected.

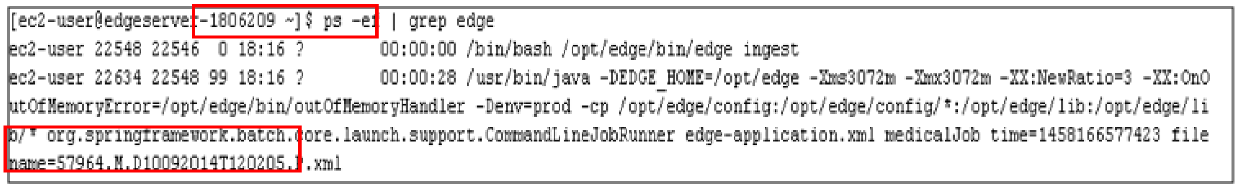
I. *Confirm if File Processing Completed*

An issuer who has not received a detail report can determine if the file has finished processing by checking the status of the file. The file processing can be monitored by inputting the following command at the EDGE Server Command Line:

- ps -ef | grep edge

1. Job Still in Process

If the job is still being processed, a row will be returned that includes the XML ingest file name as shown in the below screenshot:

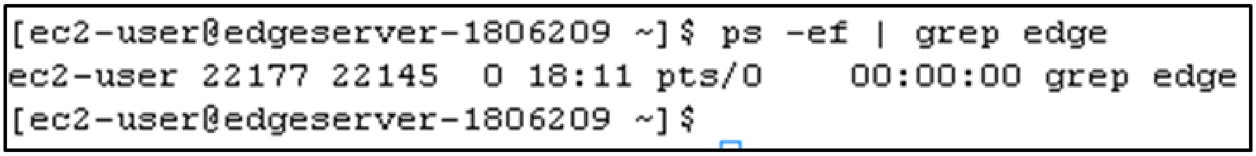


```
[ec2-user@edgeserver-1806209 ~]$ ps -ef | grep edge
ec2-user 22548 22546  0 18:16 ?        00:00:00 /bin/bash /opt/edge/bin/edge ingest
ec2-user 22634 22548 99 18:16 ?        00:00:28 /usr/bin/java -DEDGE_HOME=/opt/edge -Xms3072m -Xmx3072m -XX:NewRatio=3 -XX:OnO
utOfMemoryError=/opt/edge/bin/outOfMemoryHandler -Denv=prod -cp /opt/edge/config:/opt/edge/config/*:/opt/edge/lib:/opt/edge/li
b/* org.springframework.batch.core.launch.support.CommandLineJobRunner edge-application.xml medicalJob time=1458166577423 file
name=57964.M.D10092014T120205.P.xml
```

Figure 3-41: Job Still Being Processed

2. Job Not in Process

If a row indicating the job is still in process is not returned then the job has completed, either successfully or in error. Below is a screenshot of what it looks like when there is no process running:



```
[ec2-user@edgeserver-1806209 ~]$ ps -ef | grep edge
ec2-user 22177 22145  0 18:11 pts/0    00:00:00 grep edge
[ec2-user@edgeserver-1806209 ~]$
```

Figure 3-42: No Process Running

If the job process is no longer running the outbound reports should have been generated. If no reports were produced, the report generation has failed and must be investigated.

II. *Enrollment/Supplemental File Fails to Produce Detail Report*

Issuers should resubmit the enrollment or supplemental file again. If no detail report is produced a second time, issuers should notify their FM Service Representative at EDGE_Server_Data@cms.hhs.gov for further research.

III. *Minimum Record Count Required to Commit to Database*

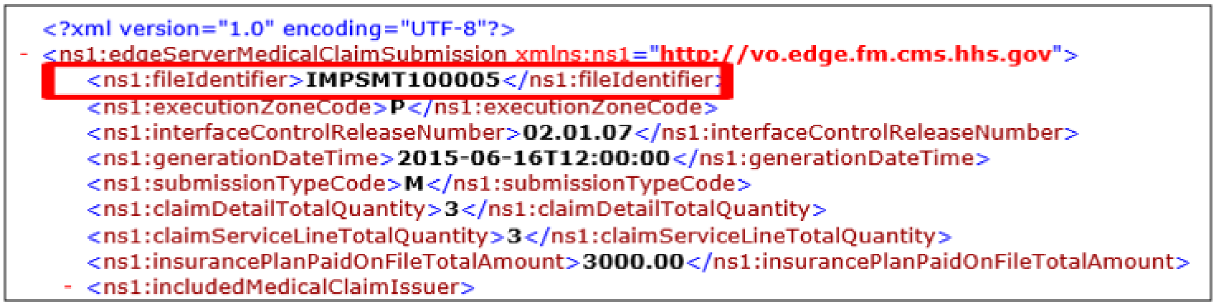
The number of records that must be processed before any records are committed to the database is 2,500. Therefore, if the file crashes before 2,500 are processed, no records will be committed to the database and the file that failed to produce an outbound report can be resubmitted in its entirety with a new File ID. Since accepted and rejected records are committed to the database in increments of 2,500, issuers should query the production tables to identify any records committed.

Note: Inbound file records submitted will be reordered and processed in date/time order. Do not assume if more than 2,500 records are processed that the records match records 1 - 2,500 in your submission file unless you have created a file that orders your records by date and time.

IV. *Queries for Accepted/Rejected Records*

If you did not receive a detail report and have confirmed the file has finished processing, you can use a query to identify whether any records in the submission file were accepted or rejected. The detail record queries identify accepted or rejected records for medical and pharmacy claims only.

The File ID in the submitted XML file header (fileIdentifier in the screenshot below) will be needed to determine if any records from the file were committed to the database as accepted records (in the MEDICAL_CLAIM or PHARMACY_CLAIM tables) or rejected records with an Error Message (in the EDGE_ERROR_LOG table):



```
  <?xml version="1.0" encoding="UTF-8"?>
- <ns1:edgeServerMedicalClaimSubmission xmlns:ns1="http://vo.edge.fm.cms.hhs.gov">
     <ns1:fileIdentifier>IMPSMT100005</ns1:fileIdentifier>
     <ns1:executionZoneCode>P</ns1:executionZoneCode>
     <ns1:interfaceControlReleaseNumber>02.01.07</ns1:interfaceControlReleaseNumber>
     <ns1:generationDateTime>2015-06-16T12:00:00</ns1:generationDateTime>
     <ns1:submissionTypeCode>M</ns1:submissionTypeCode>
     <ns1:claimDetailTotalQuantity>3</ns1:claimDetailTotalQuantity>
     <ns1:claimServiceLineTotalQuantity>3</ns1:claimServiceLineTotalQuantity>
     <ns1:insurancePlanPaidOnFileTotalAmount>3000.00</ns1:insurancePlanPaidOnFileTotalAmount>
   - <ns1:includedMedicalClaimIssuer>
```

Figure 3-43: XML File Header - 'fileIdentifier'

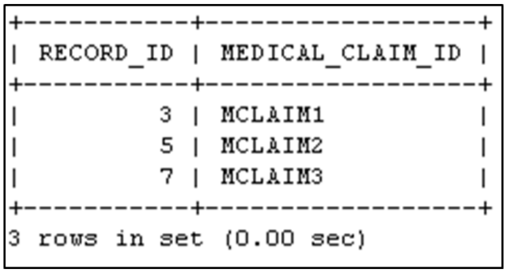
V. *Medical Claims Accepted Records Query*

The query below returns the Medical Claim ID and corresponding Record ID from the ingest file for all claims accepted and committed to the database.

Note: While Informational messages (reported on the detail reports as 'I') are accepted, they will not be returned in this query. An Informational status means the record was accepted but there was an identified discrepancy that should be reviewed. Only records that have been accepted without any discrepancies (Status 'A') will show up in accepted record queries.

- SELECT RECORD_ID, MEDICAL_CLAIM_ID FROM MEDICAL_CLAIM WHERE JOB_ID = (SELECT RCVD_SUBMSN_ID FROM PRM_STBLZTN_SUBMSN_STUS WHERE FIL_ID = '<FILE ID FROM INGEST FILE>');

While running the query, you will receive an output that includes the Record ID and the corresponding Medical Claim ID. The following is a sample output:



```
+-----------+------------------+
| RECORD_ID | MEDICAL_CLAIM_ID |
+-----------+------------------+
|         3 | MCLAIM1          |
|         5 | MCLAIM2          |
|         7 | MCLAIM3          |
+-----------+------------------+
3 rows in set (0.00 sec)
```

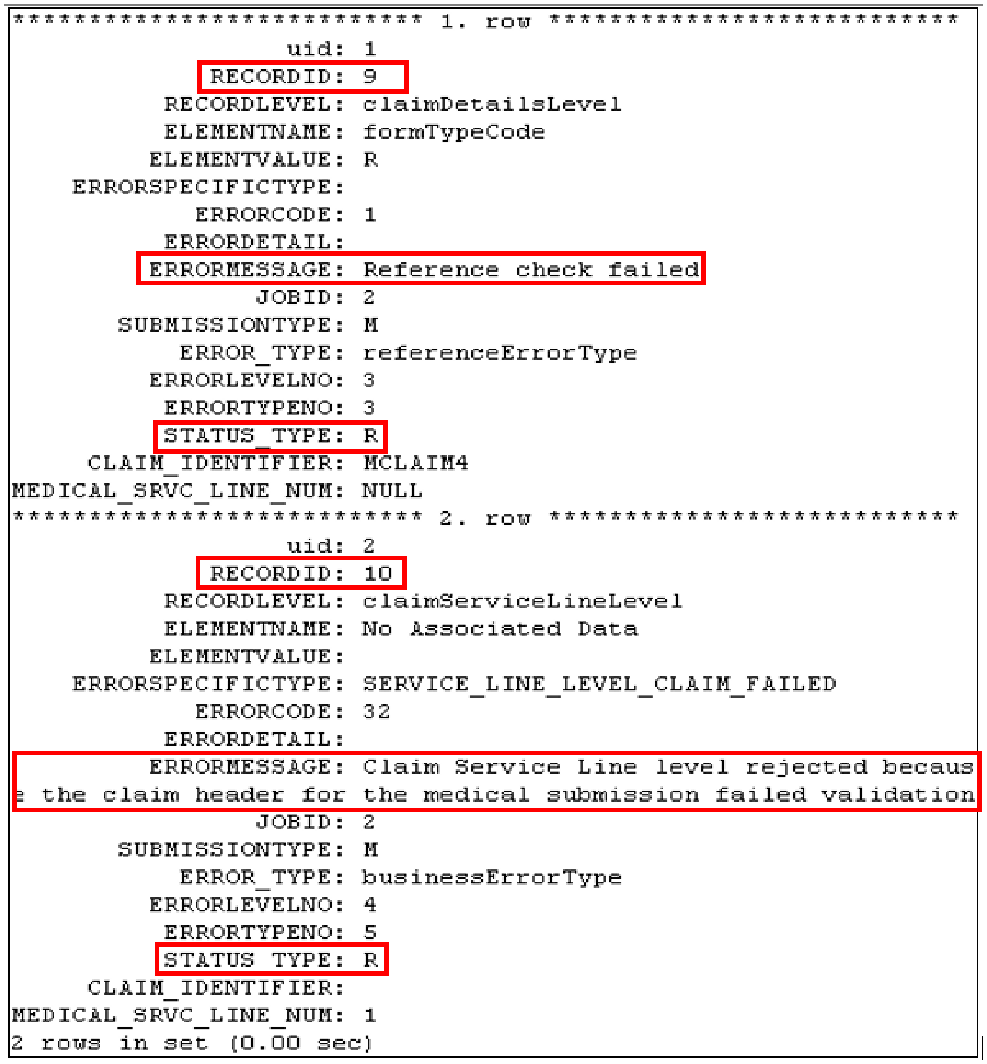
Figure 3-44: Medical Claims Accepted Records Query Results

VI. *Medical Claims Rejected Records Query*

The query below will return all records with the Error Codes, including rejected records (Status 'R') and records accepted with an Informational message (Status 'I'). While an Informational status means the record was accepted, the records appear because an error code was produced. Refer to Section 3.1.6 File Ingest Validation Errors and the EDGE Server Job Aid: EDGE Server File Ingest Error Codes for instructions on how to evaluate Informational error codes.

- SELECT * FROM EDGE_ERROR_LOG WHERE JOBID = (SELECT RCVD_SUBMSN_ID FROM PRM_STBLZTN_SUBMSN_STUS WHERE FIL_ID = '<FILE ID FROM INGEST FILE>')\G;

The output below displays an example of the Medical Claims Rejected Records Query. This example includes: the record ID number, error message and the status type. This information can be used to identify the claim submitted on the inbound file and the reason for the rejection.

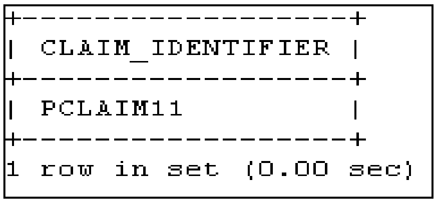


```
*************************** 1. row ***************************
                  uid: 1
             RECORDID: 9
          RECORDLEVEL: claimDetailsLevel
          ELEMENTNAME: formTypeCode
         ELEMENTVALUE: R
    ERRORSPECIFICTYPE:
            ERRORCODE: 1
          ERRORDETAIL:
         ERRORMESSAGE: Reference check failed
                JOBID: 2
       SUBMISSIONTYPE: M
           ERROR_TYPE: referenceErrorType
         ERRORLEVELNO: 3
          ERRORTYPENO: 3
          STATUS_TYPE: R
     CLAIM_IDENTIFIER: MCLAIM4
MEDICAL_SRVC_LINE_NUM: NULL
*************************** 2. row ***************************
                  uid: 2
             RECORDID: 10
          RECORDLEVEL: claimServiceLineLevel
          ELEMENTNAME: No Associated Data
         ELEMENTVALUE:
    ERRORSPECIFICTYPE: SERVICE_LINE_LEVEL_CLAIM_FAILED
            ERRORCODE: 32
          ERRORDETAIL:
         ERRORMESSAGE: Claim Service Line level rejected becaus
e the claim header for the medical submission failed validation
                JOBID: 2
       SUBMISSIONTYPE: M
           ERROR_TYPE: businessErrorType
         ERRORLEVELNO: 4
          ERRORTYPENO: 5
          STATUS_TYPE: R
     CLAIM_IDENTIFIER:
MEDICAL_SRVC_LINE_NUM: 1
2 rows in set (0.00 sec)
```

Figure 3-45: Medical Claims Rejected Records Query Results

VII. *Pharmacy Claim Accepted Record Query*

The query below returns the pharmacy Claim ID of any record that was accepted and committed to the database:



```
+-------------------+
| CLAIM_IDENTIFIER |
+-------------------+
| PCLAIM11         |
+-------------------+
1 row in set (0.00 sec)
```

Figure 3-46: Pharmacy Claims Accepted Records Query Results

Note: This query will not contain claims that were accepted with an informational message. An Informational status means the record was accepted but there was an identified discrepancy that should be reviewed. Only records that have been accepted without any discrepancies (Status ‘A’) will show up in accepted record queries. The Record ID does not exist in the pharmacy claim table, so the Claim ID must be used to link the accepted record to the record in the ingest file.

- SELECT CLAIM_IDENTIFIER FROM PHARMACY_CLAIM WHERE JOBID = (SELECT RCVD_SUBMSN_ID FROM PRM_STBLZTN_SUBMSN_STUS WHERE FIL_ID = ‘<FILE ID FROM INGEST FILE>’);

VIII. *Pharmacy Claim Rejected Record Query*

The query below will return all records with Error Codes, including rejected records (Status ‘R’) and records accepted with an Informational message (Status ‘I’). While an Informational status means the record was accepted, the records appear because there was an error code produced. Refer to Section 3.1.6: File Ingest Validation Errors and the EDGE Server Job Aid: EDGE Server File Ingest Error Codes for instructions on how to evaluate Informational error codes.

- SELECT * FROM EDGE_ERROR_LOG WHERE JOBID = (SELECT RCVD_SUBMSN_ID FROM PRM_STBLZTN_SUBMSN_STUS WHERE FIL_ID = ‘<FILE ID FROM INGEST FILE>’);

The Record ID produced from the query can be used to link the error back to the corresponding record in the ingest file.

3.1.8 Troubleshooting Help for Claims Rejected as Duplicates

The ESBR outlines the rules used to identify duplicate claims. This section will provide instructions for identifying the stored active claim that caused a newly submitted claim to be rejected as a duplicate.

The instructions are specific to the type of claim being rejected:

- Inpatient Institutional Medical Claims
- Outpatient Institutional Medical Claims
- Professional Medical Claims

In the case of outpatient institutional and professional claims, duplicates may or may not be identical in the service line modifier value. Details regarding inclusive services that are not permitted on the same day are outlined in the ESBR.

Duplicate Rejection of an Inpatient Institutional Medical Claim

Duplicate inpatient institutional claims are rejected with error code 3.5.49 - Claim header level rejected because the Statement-covers-from and Statement-covers-to dates are overlapping within the file or database.

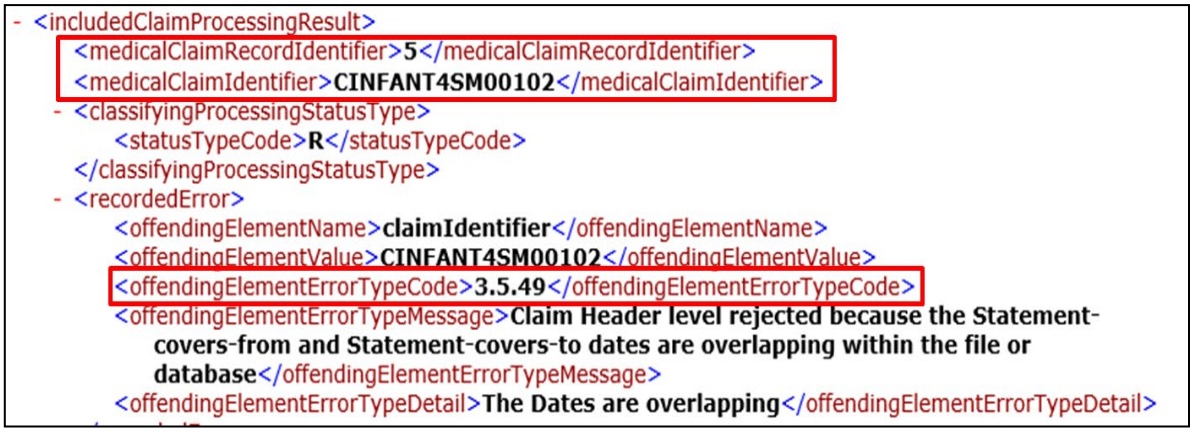
Follow the steps below to identify the existing claim that caused the inbound claim to be rejected due to the overlapping claim error:

1. Identify the rejected claim in the medical detail output XML file.
2. Locate the corresponding claim record in the inbound medical claim XML file.
3. Execute the overlapping stay query provided to determine which existing claim on the EDGE server caused the rejection.

In the outbound medical detail report, issuers need to identify which claim has been rejected due to the overlapping inpatient claim error code 3.5.49. Issuers should note the Record ID and Claim ID associated with the error.

Step 1 - Identify the Rejected Claim in the Detail Output XML File

In looking at the Medical Claim Detail Report, issuers can obtain the Claim ID that was rejected for error code 3.5.49 as shown below.



```
- <includedClaimProcessingResult>
    <medicalClaimRecordIdentifier>5</medicalClaimRecordIdentifier>
    <medicalClaimIdentifier>CINFANT4SM00102</medicalClaimIdentifier>
  - <classifyingProcessingStatusType>
      <statusTypeCode>R</statusTypeCode>
    </classifyingProcessingStatusType>
  - <recordedError>
      <offendingElementName>claimIdentifier</offendingElementName>
      <offendingElementValue>CINFANT4SM00102</offendingElementValue>
      <offendingElementErrorTypeCode>3.5.49</offendingElementErrorTypeCode>
      <offendingElementErrorTypeMessage>Claim Header level rejected because the Statement-
         covers-from and Statement-covers-to dates are overlapping within the file or
         database</offendingElementErrorTypeMessage>
      <offendingElementErrorTypeDetail>The Dates are overlapping</offendingElementErrorTypeDetail>
```

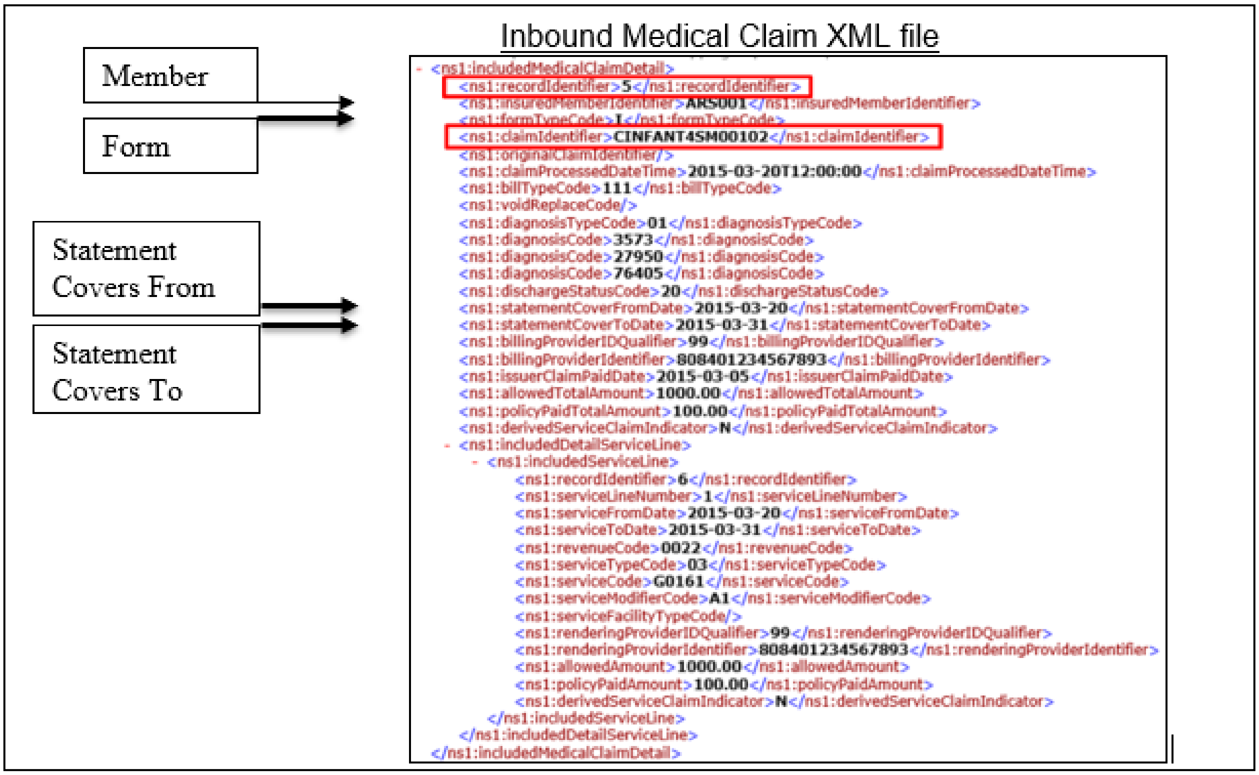
Figure 3-47: Example Rejected Claim in Detail Output

The Record ID and Claim ID is needed to obtain specific data elements from the claim that was submitted and rejected. These data elements will be identified in the next step and used to populate the query.

Step 2 - Locate Rejected Claim Record in the Inbound Medical Claim XML File

Locate the medical claim XML file that was submitted and search for the Record ID and Claim ID that was identified as rejected in the Medical Claim Detail Report (indicated in the red boxes below) and gather the data elements necessary to identify the claim that caused the rejection (indicated by the arrows below).

In addition to the elements below, issuers will also need the Plan ID associated with the claim.



```
- <ns1:includedMedicalClaimDetail>
    <ns1:recordIdentifier>5</ns1:recordIdentifier>
    <ns1:insuredMemberIdentifier>ARS001</ns1:insuredMemberIdentifier>
    <ns1:formTypeCode>I</ns1:formTypeCode>
    <ns1:claimIdentifier>CINFANT4SM00102</ns1:claimIdentifier>
    <ns1:originalClaimIdentifier/>
    <ns1:claimProcessedDateTime>2015-03-20T12:00:00</ns1:claimProcessedDateTime>
    <ns1:billTypeCode>111</ns1:billTypeCode>
    <ns1:voidReplaceCode/>
    <ns1:diagnosisTypeCode>01</ns1:diagnosisTypeCode>
    <ns1:diagnosisCode>3573</ns1:diagnosisCode>
    <ns1:diagnosisCode>27950</ns1:diagnosisCode>
    <ns1:diagnosisCode>76405</ns1:diagnosisCode>
    <ns1:dischargeStatusCode>20</ns1:dischargeStatusCode>
    <ns1:statementCoverFromDate>2015-03-20</ns1:statementCoverFromDate>
    <ns1:statementCoverToDate>2015-03-31</ns1:statementCoverToDate>
    <ns1:billingProviderIDQualifier>99</ns1:billingProviderIDQualifier>
    <ns1:billingProviderIdentifier>808401234567893</ns1:billingProviderIdentifier>
    <ns1:issuerClaimPaidDate>2015-03-05</ns1:issuerClaimPaidDate>
    <ns1:allowedTotalAmount>1000.00</ns1:allowedTotalAmount>
    <ns1:policyPaidTotalAmount>100.00</ns1:policyPaidTotalAmount>
    <ns1:derivedServiceClaimIndicator>N</ns1:derivedServiceClaimIndicator>
  - <ns1:includedDetailServiceLine>
    - <ns1:includedServiceLine>
        <ns1:recordIdentifier>6</ns1:recordIdentifier>
        <ns1:serviceLineNumber>1</ns1:serviceLineNumber>
        <ns1:serviceFromDate>2015-03-20</ns1:serviceFromDate>
        <ns1:serviceToDate>2015-03-31</ns1:serviceToDate>
        <ns1:revenueCode>0022</ns1:revenueCode>
        <ns1:serviceTypeCode>03</ns1:serviceTypeCode>
        <ns1:serviceCode>G0161</ns1:serviceCode>
        <ns1:serviceModifierCode>A1</ns1:serviceModifierCode>
        <ns1:serviceFacilityTypeCode/>
        <ns1:renderingProviderIDQualifier>99</ns1:renderingProviderIDQualifier>
        <ns1:renderingProviderIdentifier>808401234567893</ns1:renderingProviderIdentifier>
        <ns1:allowedAmount>1000.00</ns1:allowedAmount>
        <ns1:policyPaidAmount>100.00</ns1:policyPaidAmount>
        <ns1:derivedServiceClaimIndicator>N</ns1:derivedServiceClaimIndicator>
      </ns1:includedServiceLine>
    </ns1:includedDetailServiceLine>
  </ns1:includedMedicalClaimDetail>
```

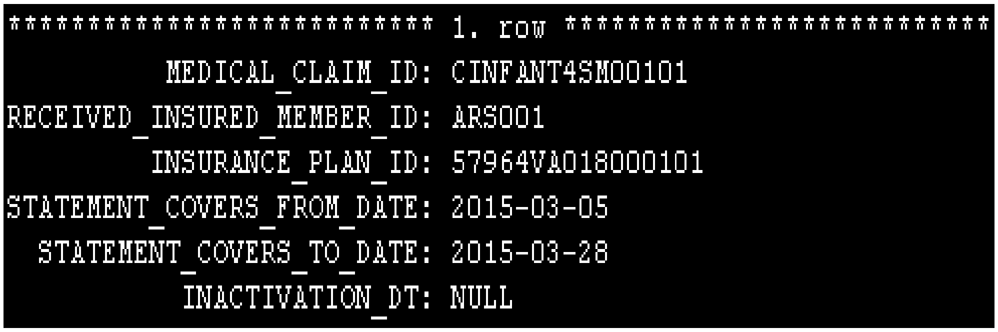
Figure 3-48: Example Inbound Claim

Step 3 - Execute the Overlapping Stay Query

Populate the below query using the data values for the rejected claim and identified in the inbound XML file.

```
•    SELECT
*
•    FROM
EDGE SRVR PROD MEDICAL_CLAIM mc,
EDGE_SRVR_COMMON.CLAIM_BILL_TYPE cbt
•    WHERE
cbt.CLM_TYPE_CD = 'I'
AND CLAIM_FORM_TYPE = 'I'
AND mc.CLAIM_BILL_TYPE = cbt.CLM_BILL_TYPE_CD
AND mc.INACTIVATION_DT IS NULL
AND RECEIVED_INSURED_MEMBER_ID = '<Insured Member ID>'
AND INSURANCE_PLAN_ID = '<Plan ID>'
AND STATEMENT_COVERS_TO_DATE > '<Statement Covers to Date>'
AND STATEMENT_COVERS_FROM_DATE < '<Statement Covers From Date>'\G;
```

Example Output (select fields only):



```
*************************** 1. row ***************************
          MEDICAL_CLAIM_ID: CINFANT4SM00101
RECEIVED_INSURED_MEMBER_ID: ARS001
         INSURANCE_PLAN_ID: 57964VA018000101
STATEMENT_COVERS_FROM_DATE: 2015-03-05
  STATEMENT_COVERS_TO_DATE: 2015-03-28
           INACTIVATION_DT: NULL
```

Figure 3-49: Example Query Output for Overlapping Query to Identify the Active Claim

The query result indicates the Claim ID already exists as an active claim in the medical claim table, which caused the submitted inpatient institutional claim to reject.

If the query did not return a result, recheck the accuracy of the query and the data values populated. If the information in the query is accurate, please contact the FMCC at EDGE_Server_Data@cms.hhs.gov and provide a copy of the query that was performed, and the results received. The FMCC will contact you with instructions on how to proceed.

Duplicate Rejection of an Outpatient Institutional Claim

Outpatient institutional claims are rejected with error code 4.5.36 - Claim Service Line level rejected because the claim service line already exists in the database.

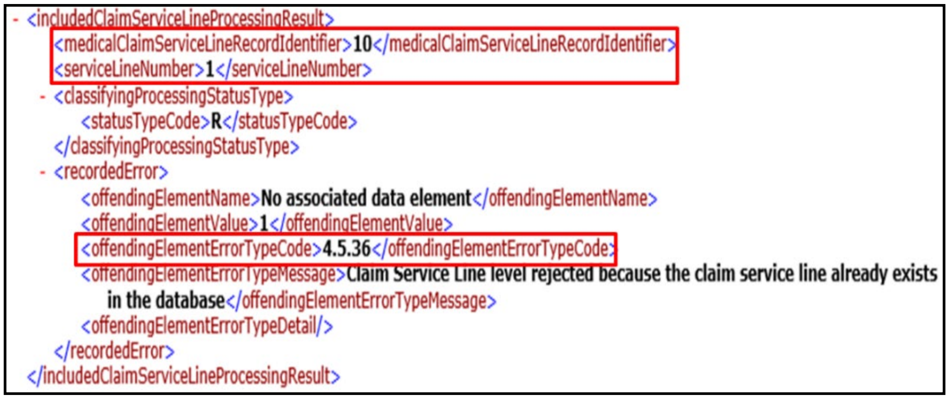
Follow the steps below to identify the existing claim that caused the inbound claim to be rejected due to the duplicate logic:

1. Identify the rejected claim in the medical detail output XML file.
2. Locate the corresponding claim record in the inbound medical claim XML file.
3. Execute the duplicate claim query provided to determine which existing claim on the EDGE server caused the rejection.

In the outbound medical detail report, issuers need to identify which claim has been rejected with error code 4.5.36. Issuers should note the Record ID and Claim ID associated with the error.

Step 1 - Identify the Rejected Claim in the Medical Detail Output XML file

In looking at the medical claim detail report, issuers can obtain the claim ID that was rejected for error code 4.5.36 as shown below.



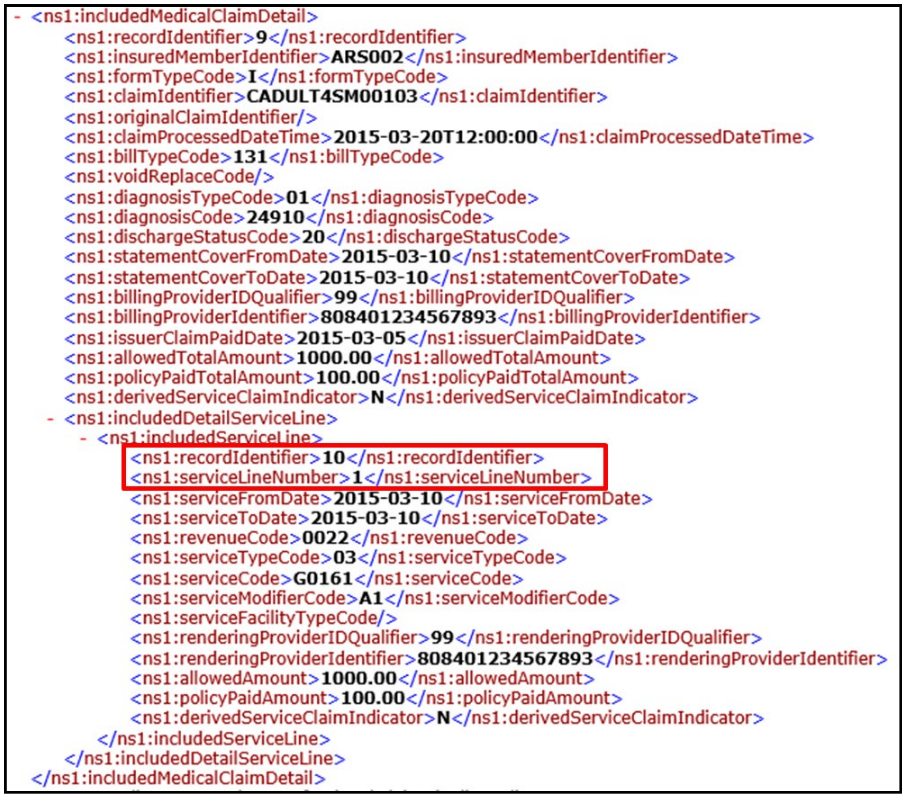
```
- <includedClaimServiceLineProcessingResult>
    <medicalClaimServiceLineRecordIdentifier>10</medicalClaimServiceLineRecordIdentifier>
    <serviceLineNumber>1</serviceLineNumber>
  - <classifyingProcessingStatusType>
      <statusTypeCode>R</statusTypeCode>
    </classifyingProcessingStatusType>
  - <recordedError>
      <offendingElementName>No associated data element</offendingElementName>
      <offendingElementValue>1</offendingElementValue>
      <offendingElementErrorTypeCode>4.5.36</offendingElementErrorTypeCode>
      <offendingElementErrorTypeMessage>Claim Service Line level rejected because the claim service line already exists
        in the database</offendingElementErrorTypeMessage>
      <offendingElementErrorTypeDetail/>
    </recordedError>
  </includedClaimServiceLineProcessingResult>
```

Figure 3-50: Example Rejected Claim in Detail Output

The Record ID and Claim ID is needed to obtain specific data elements from the claim that was submitted and rejected. These data elements will be identified in the next step and used to populate the query.

Step 2 - Locate Rejected Claim Record in the Inbound Medical Claim XML File

Locate the medical claim XML file that was submitted and search for the Record ID and Claim ID that was identified as rejected in the medical claim detail report (indicated in the red boxes below) and gather the data elements necessary to identify the claim that caused the rejection (indicated by the arrows below).



```
- <ns1:includedMedicalClaimDetail>
      <ns1:recordIdentifier>9</ns1:recordIdentifier>
      <ns1:insuredMemberIdentifier>ARS002</ns1:insuredMemberIdentifier>
      <ns1:formTypeCode>I</ns1:formTypeCode>
      <ns1:claimIdentifier>CADULT4SM00103</ns1:claimIdentifier>
      <ns1:originalClaimIdentifier/>
      <ns1:claimProcessedDateTime>2015-03-20T12:00:00</ns1:claimProcessedDateTime>
      <ns1:billTypeCode>131</ns1:billTypeCode>
      <ns1:voidReplaceCode/>
      <ns1:diagnosisTypeCode>01</ns1:diagnosisTypeCode>
      <ns1:diagnosisCode>24910</ns1:diagnosisCode>
      <ns1:dischargeStatusCode>20</ns1:dischargeStatusCode>
      <ns1:statementCoverFromDate>2015-03-10</ns1:statementCoverFromDate>
      <ns1:statementCoverToDate>2015-03-10</ns1:statementCoverToDate>
      <ns1:billingProviderIDQualifier>99</ns1:billingProviderIDQualifier>
      <ns1:billingProviderIdentifier>808401234567893</ns1:billingProviderIdentifier>
      <ns1:issuerClaimPaidDate>2015-03-05</ns1:issuerClaimPaidDate>
      <ns1:allowedTotalAmount>1000.00</ns1:allowedTotalAmount>
      <ns1:policyPaidTotalAmount>100.00</ns1:policyPaidTotalAmount>
      <ns1:derivedServiceClaimIndicator>N</ns1:derivedServiceClaimIndicator>
    - <ns1:includedDetailServiceLine>
        - <ns1:includedServiceLine>
              <ns1:recordIdentifier>10</ns1:recordIdentifier>
              <ns1:serviceLineNumber>1</ns1:serviceLineNumber>
              <ns1:serviceFromDate>2015-03-10</ns1:serviceFromDate>
              <ns1:serviceToDate>2015-03-10</ns1:serviceToDate>
              <ns1:revenueCode>0022</ns1:revenueCode>
              <ns1:serviceTypeCode>03</ns1:serviceTypeCode>
              <ns1:serviceCode>G0161</ns1:serviceCode>
              <ns1:serviceModifierCode>A1</ns1:serviceModifierCode>
              <ns1:serviceFacilityTypeCode/>
              <ns1:renderingProviderIDQualifier>99</ns1:renderingProviderIDQualifier>
              <ns1:renderingProviderIdentifier>808401234567893</ns1:renderingProviderIdentifier>
              <ns1:allowedAmount>1000.00</ns1:allowedAmount>
              <ns1:policyPaidAmount>100.00</ns1:policyPaidAmount>
              <ns1:derivedServiceClaimIndicator>N</ns1:derivedServiceClaimIndicator>
          </ns1:includedServiceLine>
      </ns1:includedDetailServiceLine>
  </ns1:includedMedicalClaimDetail>
```

Figure 3-51: Example Rejected Claim Record in Inbound Claim

Step 3 - Execute the Duplicate Claim Query

The following query will identify the claim that caused a duplicate rejection for an institutional outpatient claim only.

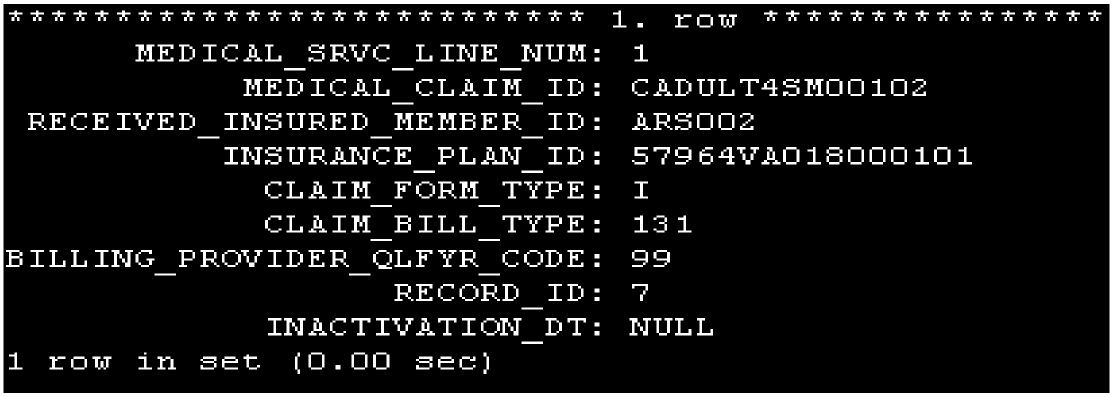
Note: This query does not include a comparison of modifiers. If the claim returned by this query does not appear to be a duplicate, please execute the query to Compare Service Code Modifiers provided.

Issuers should populate the following query using the appropriate fields from the rejected medical claim to identify potential claims that may have caused the inbound claim to be rejected.

```
•   SELECT
ml.MEDICAL_SRVC_LINE_NUM,
mc.*
•   FROM
MEDICAL_CLAIM mc
```

```
JOIN
MEDICAL_CLAIM_SRVC_LINE ml ON mc.UID = ml.MEDICAL_CLAIM_UID_FK
JOIN
EDGE_SRVR_COMMON.CLAIM_BILL_TYPE cbt on mc.CLAIM_BILL_TYPE = cbt.CLM_BILL_TYPE_CD
•    WHERE
mc.INACTIVATION_DT IS NULL
AND mc.CLAIM_FORM_TYPE ='I'
AND cbt.CLM_TYPE_CD = 'O'
AND mc.RECEIVED_INSURED_MEMBER_ID = '<Insured Member ID>'
AND mc.CLAIM_BILL_TYPE = '<Bill Type Code>'
AND mc.INSURANCE_PLAN_ID = '<Plan ID>'
AND ml.RNDRNG_PRVDR_QLFYR_CD = '<Rendering Provider ID Qualifier>'
AND ml.RNDRNG_PRVDR_ID = '<Rendering Provider ID>'
AND ml.REV_CD = '<Revenue Code>'
AND ml.SRVC_CD = '<Service Code>'\G;
```

Example Output (select fields only):



```
*************************** 1. row ****************
      MEDICAL_SRVC_LINE_NUM: 1
           MEDICAL_CLAIM_ID: CADULT4SM00102
 RECEIVED_INSURED_MEMBER_ID: ARS002
          INSURANCE_PLAN_ID: 57964VA018000101
            CLAIM_FORM_TYPE: I
            CLAIM_BILL_TYPE: 131
BILLING_PROVIDER_QLFYR_CODE: 99
                  RECORD_ID: 7
            INACTIVATION_DT: NULL
1 row in set (0.00 sec)
```

Figure 3-52: Example Query Output for Potential Duplicate Claims: Institutional Outpatient Claims

The query result indicates the Claim ID already exists as an active claim in the medical claim table, which caused the submitted outpatient claim to reject.

If the claim returned does not appear to be a duplicate an additional query can be performed to compare the Service Code Modifiers as described in the following section.

If the query did not return a result, recheck the accuracy of the query and the data values populated. If no claim is returned, please contact the FMCC at EDGE_Server_Data@cms.hhs.gov for further assistance, and provide a copy of the query that was performed and the results received. The FMCC will contact you with instructions on how to proceed.

Compare Service Code Modifiers: Institutional Outpatient Claims

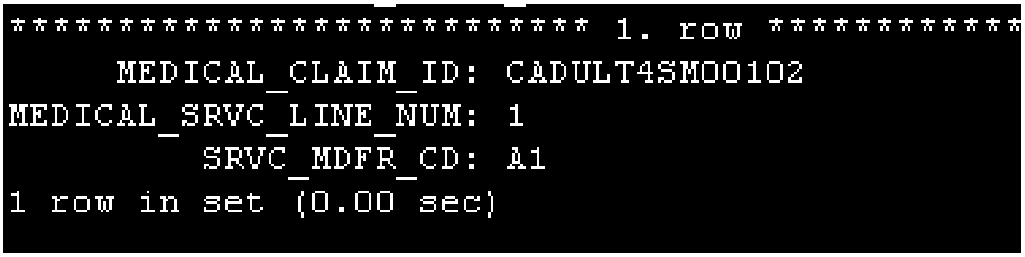
Issuers who have executed the query in the previous section and identified the claim that caused a duplicate rejection may need to run a second query to identify the modifier(s) associated with the claim to confirm it is a true duplicate.

As a reminder, duplicate claims are not always identical as outlined in the EDGE Server Business Rules (ESBR).

Issuers should populate the below query with each Claim ID returned in the previous query to identify the serviceModifierCode.

```
•    SELECT
mc.MEDICAL_CLAIM_ID,
mcsl.MEDICAL_SRVC_LINE_NUM,
mcsma.SRVC_MDFR_CD
•    FROM
MEDICAL_CLAIM mc
LEFT OUTER JOIN MEDICAL_CLAIM_SRVC_LINE mcsl on mc.UID mcsl.MEDICAL_CLAIM_UID_FK
LEFT OUTER JOIN MEDICAL_CLAIM_SRVC_MDFR_ASCTN mcsma on mcsl.UID =
mcsma.MEDICAL_CLAIM_SRVC_LINE_UID_FK
●    WHERE
mc.MEDICAL_CLAIM_ID = '<Medical Claim ID>'\G;
```

Example Output:



```
*************************** 1. row ************
     MEDICAL_CLAIM_ID: CADULT4SM00102
MEDICAL_SRVC_LINE_NUM: 1
         SRVC_MDFR_CD: A1
1 row in set (0.00 sec)
```

Figure 3-53: Example Query Output for Service Code Modifiers: Institutional Outpatient Claims

Note: In this example, claim line 1 identified in the previous query returned the same serviceModifierCode (A1) as the rejected claim and is the claim line that caused the duplicate error.

If you believe the claim is not a duplicate and have reviewed the duplicate logic in the EDGE Server Business Rules (ESBR) please contact the FMCC for further assistance.

Inclusive Services

In some instances, duplicate claims will not be identical but will have differences in the service code modifiers. The EDGE Server Business Rules (ESBR) lists the modifiers that would be considered duplicate for the same service on the same day. These modifiers are usually “inclusive services” such as professional, technical and global services billed for radiology services.

A second query, to identify the modifiers on both claims, is included at the end of the next section.

Duplicate Rejection of a Professional Medical Claim

Duplicate professional claims are rejected with error code 4.5.36 - Claim Service Line level rejected because the claim service line already exists in the database.

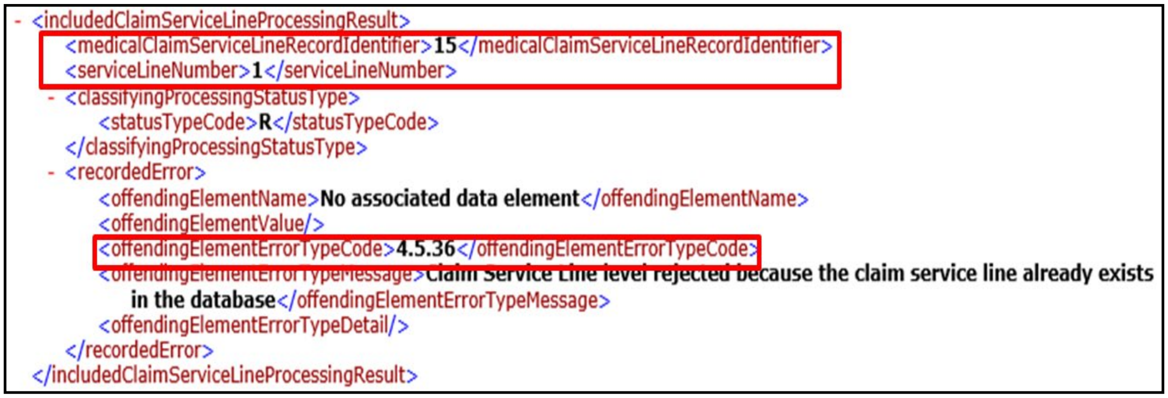
Follow the steps below to identify the existing claim that caused the inbound claim to be rejected due to the duplicate logic:

1. Identify the rejected claim in the medical detail output XML file.
2. Locate the corresponding claim record in the inbound medical claim XML file.
3. Execute the duplicate claim query provided to determine which existing claim on the EDGE server caused the rejection.

In the outbound medical detail report, issuers need to identify which claim has been rejected with error code 4.5.36. Issuers should note the Record ID and Claim ID associated with the error.

Step 1 - Identify the Rejected Claim in the Medical Detail output XML file

In looking at the medical claim detail report, issuers can obtain the claim ID that was rejected for error code 4.5.36 as shown below.



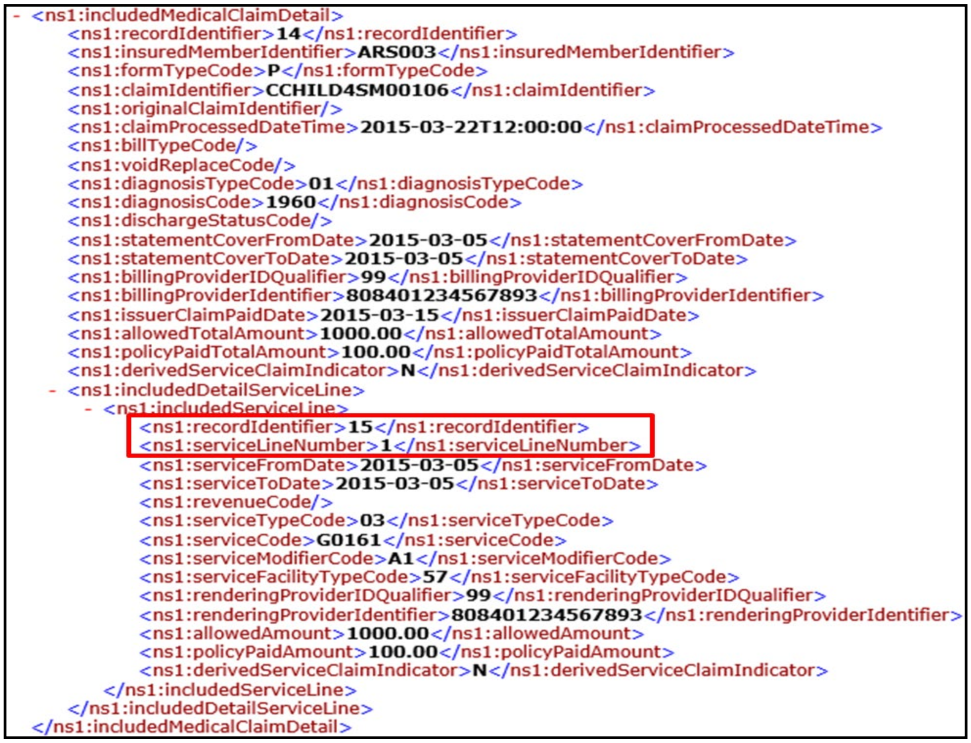
```
- <includedClaimServiceLineProcessingResult>
    <medicalClaimServiceLineRecordIdentifier>15</medicalClaimServiceLineRecordIdentifier>
    <serviceLineNumber>1</serviceLineNumber>
  - <classifyingProcessingStatusType>
      <statusTypeCode>R</statusTypeCode>
    </classifyingProcessingStatusType>
  - <recordedError>
      <offendingElementName>No associated data element</offendingElementName>
      <offendingElementValue/>
      <offendingElementErrorTypeCode>4.5.36</offendingElementErrorTypeCode>
      <offendingElementErrorTypeMessage>Claim Service Line level rejected because the claim service line already exists
        in the database</offendingElementErrorTypeMessage>
      <offendingElementErrorTypeDetail/>
    </recordedError>
  </includedClaimServiceLineProcessingResult>
```

Figure 3-54: Example Rejected Claim in Detail Output

The Record ID and Claim ID is needed to obtain specific data elements from the claim that was submitted and rejected. These data elements will be identified in the next step and used to populate the query.

Step 2 - Locate Rejected Claim Record in the Inbound Medical Claim XML File

Locate the medical claim XML file that was submitted and search for the Record ID and Claim ID that was identified as rejected in the medical claim detail report (indicated in the red boxes below), and gather the data elements necessary to identify the claim that caused the rejection (indicated by the arrows below).



```
- <ns1:includedMedicalClaimDetail>
    <ns1:recordIdentifier>14</ns1:recordIdentifier>
    <ns1:insuredMemberIdentifier>ARS003</ns1:insuredMemberIdentifier>
    <ns1:formTypeCode>P</ns1:formTypeCode>
    <ns1:claimIdentifier>CCHILD4SM00106</ns1:claimIdentifier>
    <ns1:originalClaimIdentifier/>
    <ns1:claimProcessedDateTime>2015-03-22T12:00:00</ns1:claimProcessedDateTime>
    <ns1:billTypeCode/>
    <ns1:voidReplaceCode/>
    <ns1:diagnosisTypeCode>01</ns1:diagnosisTypeCode>
    <ns1:diagnosisCode>1960</ns1:diagnosisCode>
    <ns1:dischargeStatusCode/>
    <ns1:statementCoverFromDate>2015-03-05</ns1:statementCoverFromDate>
    <ns1:statementCoverToDate>2015-03-05</ns1:statementCoverToDate>
    <ns1:billingProviderIDQualifier>99</ns1:billingProviderIDQualifier>
    <ns1:billingProviderIdentifier>808401234567893</ns1:billingProviderIdentifier>
    <ns1:issuerClaimPaidDate>2015-03-15</ns1:issuerClaimPaidDate>
    <ns1:allowedTotalAmount>1000.00</ns1:allowedTotalAmount>
    <ns1:policyPaidTotalAmount>100.00</ns1:policyPaidTotalAmount>
    <ns1:derivedServiceClaimIndicator>N</ns1:derivedServiceClaimIndicator>
  - <ns1:includedDetailServiceLine>
    - <ns1:includedServiceLine>
        <ns1:recordIdentifier>15</ns1:recordIdentifier>
        <ns1:serviceLineNumber>1</ns1:serviceLineNumber>
        <ns1:serviceFromDate>2015-03-05</ns1:serviceFromDate>
        <ns1:serviceToDate>2015-03-05</ns1:serviceToDate>
        <ns1:revenueCode/>
        <ns1:serviceTypeCode>03</ns1:serviceTypeCode>
        <ns1:serviceCode>G0161</ns1:serviceCode>
        <ns1:serviceModifierCode>A1</ns1:serviceModifierCode>
        <ns1:serviceFacilityTypeCode>57</ns1:serviceFacilityTypeCode>
        <ns1:renderingProviderIDQualifier>99</ns1:renderingProviderIDQualifier>
        <ns1:renderingProviderIdentifier>808401234567893</ns1:renderingProviderIdentifier>
        <ns1:allowedAmount>1000.00</ns1:allowedAmount>
        <ns1:policyPaidAmount>100.00</ns1:policyPaidAmount>
        <ns1:derivedServiceClaimIndicator>N</ns1:derivedServiceClaimIndicator>
      </ns1:includedServiceLine>
    </ns1:includedDetailServiceLine>
  </ns1:includedMedicalClaimDetail>
```

Figure 3-55: Example Rejected Claim Record in Inbound Claim

Step 3 - Execute the Duplicate Claim Query

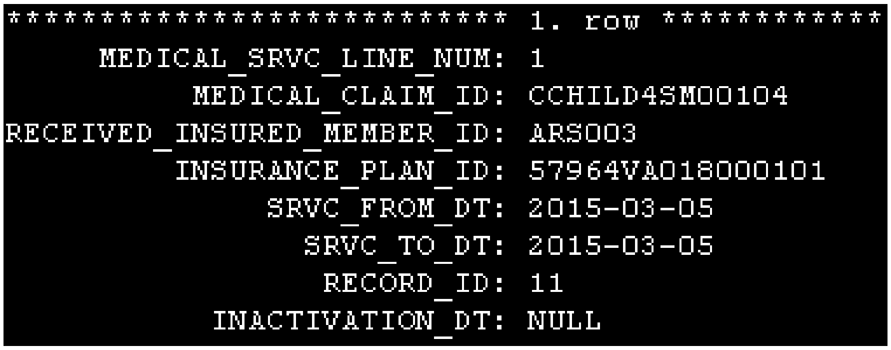
The following query will identify the claim that caused a duplicate rejection for a professional claim only.

Note: This query does not include a comparison of modifiers. If the claim returned by this query does not appear to be a duplicate, please execute the query to Compare Service Code Modifiers provided.

Issuers should populate the below query using the appropriate fields from the rejected medical claim to identify potential claims that may have caused the inbound claim to be rejected.

```
•    SELECT
ml.MEDICAL_SRVC_LINE_NUM,
mc.*
•    FROM
MEDICAL_CLAIM mc
•    JOIN
MEDICAL_CLAIM_SRVC_LINE ml ON mc.UID = ml.MEDICAL_CLAIM_UID_FK
•    WHERE
mc.INACTIVATION_DT IS NULL
AND mc.CLAIM_FORM_TYPE = 'P'
AND mc.RECEIVED_INSURED_MEMBER_ID = '<Insured Member ID>'
AND mc.INSURANCE_PLAN_ID = '<Plan ID>'
AND ml.RNDRNG_PRVDR_QLFYR_CD = '<Rendering Provider ID Qualifier>'
AND ml.RNDRNG_PRVDR_ID = '<Rendering Provider ID>'
AND ml.SRVC_CD = '<Service Code>'
AND ml.SRVC_FROM_DT = '<Service From Date>'
AND ml.SRVC_TO_DT = '<Service To Date>'
AND ml.SRVC_PLACE_CD = '<Facility Type Code>'\G;
```

Example Output (select fields only):



```
*************************** 1. row ************
     MEDICAL_SRVC_LINE_NUM: 1
          MEDICAL_CLAIM_ID: CCHILD4SM00104
RECEIVED_INSURED_MEMBER_ID: ARS003
         INSURANCE_PLAN_ID: 57964VA018000101
              SRVC_FROM_DT: 2015-03-05
                SRVC_TO_DT: 2015-03-05
                 RECORD_ID: 11
           INACTIVATION_DT: NULL
```

Figure 3-56: Example Query Output for Potential Duplicate Claims: Professional Claims

The query result indicates the Claim ID already exists as an active claim in the medical claim table,which caused the submitted outpatient claim to reject.

If the claim returned does not appear to be a duplicate an additional query can be performed to compare the Service Code Modifiers as described in the following section.

If the query did not return a result, recheck the accuracy of the query and the data values populated. If no claim is returned, please contact the FMCC at EDGE_Server_Data@cms.hhs.gov for further assistance and provide a copy of the query that was performed, and the results received. The FMCC will contact you with instructions on how to proceed.

Compare Service Code Modifiers: Professional Claim Lines

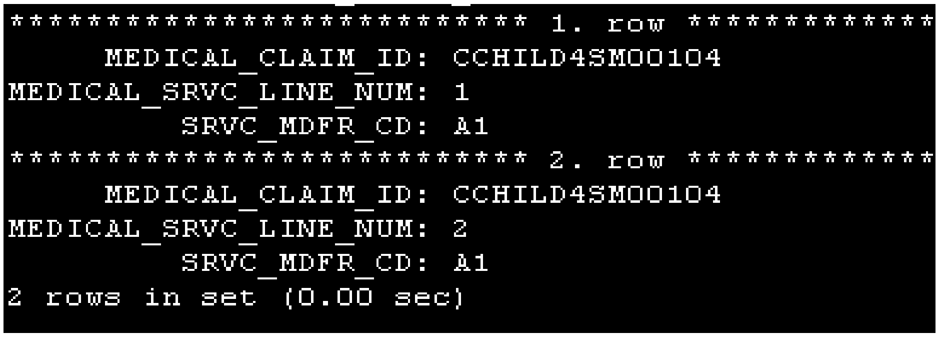
Issuers who have executed the query in the previous section and identified the claim that caused a duplicate rejection will need to run a second query to identify the modifier(s) associated with the claim to confirm it is a true duplicate.

As a reminder, duplicate claims are not always identical as outlined in the EDGE Server Business Rules (ESBR).

Issuers should populate the below query with each Claim ID returned in the previous query to identify the serviceModifierCode. For steps to identify the overlapping claims, to identify the rejected claim in the detail output XML file, and to locate the rejected claim record in the inbound medical claim XML file, please refer to the beginning of Section 3.1.8 Troubleshooting Help for Claims Rejected as Duplicates.

```
●  SELECT
mc.MEDICAL_CLAIM_ID,
mcsl.MEDICAL_SRVC_LINE_NUM,
mcsma.SRVC_MDFR_CD
●  FROM
MEDICAL_CLAIM mc
LEFT OUTER JOIN MEDICAL_CLAIM_SRVC_LINE mcsl on mc.UID = mcsl.MEDICAL_CLAIM_UID_FK
LEFT OUTER JOIN MEDICAL_CLAIM_SRVC_MDFR_ASCTN mcsma on mcsl.UID =
mcsma.MEDICAL_CLAIM_SRVC_LINE_UID_FK
●  WHERE
mc.MEDICAL_CLAIM_ID = '<Medical Claim ID>'\G;
```

Example Output:



```
*************************** 1. row *************
     MEDICAL_CLAIM_ID: CCHILD4SM00104
MEDICAL_SRVC_LINE_NUM: 1
         SRVC_MDFR_CD: A1
*************************** 2. row *************
     MEDICAL_CLAIM_ID: CCHILD4SM00104
MEDICAL_SRVC_LINE_NUM: 2
         SRVC_MDFR_CD: A1
2 rows in set (0.00 sec)
```

Figure 3-57: Example Query Output for Service Code Modifiers: Professional Claim Lines

Note: In this example, claim line 1 identified in the previous query returned the same serviceModifierCode (A1) as the rejected claim and is the claim line that caused the duplicate error.

Duplicate Inclusive Services Query

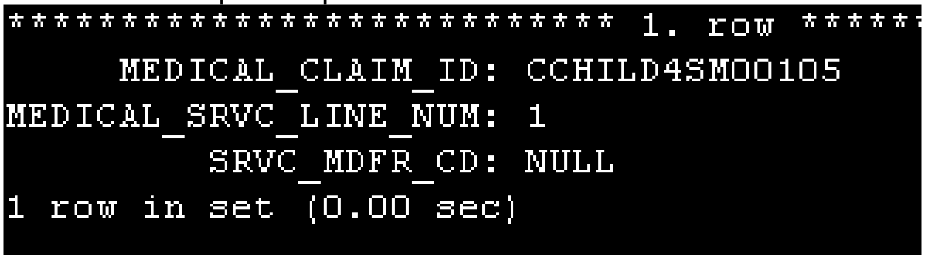
Compare Service Code Modifiers: Duplicate Inclusive Service Claim Line

Issuers who have executed the query in the outpatient institutional claims or professional claims sections and identified the claim that caused a duplicate rejection may need to run a second query to identify the modifiers associated with both claims to determine if the services would be considered inclusive of each other.

Issuers should populate the below query with each Claim ID returned in the previous query to identify the serviceModifierCode.

```
●    SELECT
mc.MEDICAL_CLAIM_ID,
mcsl.MEDICAL_SRVC_LINE_NUM,
mcsma.SRVC_MDFR_CD
●    FROM
MEDICAL_CLAIM mc
LEFT OUTER JOIN MEDICAL_CLAIM_SRVC_LINE mcsl on mc.UID = mcsl.MEDICAL_CLAIM_UID_FK
LEFT OUTER JOIN MEDICAL_CLAIM_SRVC_MDFR_ASCTN mcsma on mcsl.UID =
mcsma.MEDICAL_CLAIM_SRVC_LINE_UID_FK
●    WHERE
mc.MEDICAL_CLAIM_ID = '<Medical Claim ID>'\G;
```

Example Output:



```
*************************** 1. row *****
     MEDICAL_CLAIM_ID: CCHILD4SM00105
MEDICAL_SRVC_LINE_NUM: 1
          SRVC_MDFR_CD: NULL
1 row in set (0.00 sec)
```

Figure 3-58: Example Query Output for Service Code Modifiers: Duplicate Inclusive Service Claim Line

In this example, the query result shows claim line 1 was submitted with a NULL serviceModifierCode. Since the rejected claim had a modifier code of ‘TC’, the claim line qualified as a duplicate under the inclusive services logic.

Duplicate Rejection of a Pharmacy Claim

Duplicate pharmacy claims are rejected with either error code 3.5.6 - Claim rejected because claim Identifier already exist in the database) or 3.5.11 (Claim level rejected because the claim did not successfully pass duplicate check validation) depending on the validation error. Issuers can use the two (2) queries below to identify the existing claim that caused the inbound claim to be rejected due to the duplicate logic. Issuers should populate the queries using the appropriate fields from the rejected pharmacy claim to identify potential claims that may have caused the inbound claim to be rejected. As mentioned in the ESBR, the dispensing status for the new claim depends on the status of the active stored claim. The claim may be accepted or rejected as a duplicate based on the guidance in that document.

```
•    SELECT * FROM EDGE_SRVR_PROD.PHARMACY_CLAIM WHERE
             CLAIM_IDENTIFIER = '<Unique Claim ID>' AND
             INSURANCE_PLAN_IDENTIFIER = '<Unique Plan ID>';
•    SELECT * FROM EDGE_SRVR_PROD.PHARMACY_CLAIM WHERE
     INSURANCE_PLAN_IDENTIFIER = '<Plan ID>' AND
     DISPENSING_PROVIDER_ID_QUALIFIER = '<Dispensing Provider ID Qualifier>' AND
     DISPENSING_PROVIDER_IDENTIFIER = '<Dispensing Provider ID>' AND
     PRESCRIPTION_FILL_DATE = '<Fill Date>' AND
     PRESCRIPTION_SERVICE_REFERENCE_NUMBER = '<Prescription/Service Reference Number>' AND
     PRESCRIPTION_FILL_NUMBER = '<Fill Number>' AND
     DISPENSING_STATUS_CODE = '<Dispensing Status>';
```

The query result indicates the Claim ID already exists as an active claim in the pharmacy claim table, which caused the submitted outpatient claim to reject.

If the query did not return a result, recheck the accuracy of the query and the data values populated. If no claim is returned, please contact the FMCC at

EDGE_Server_Data@cms.hhs.gov for further assistance and provide a copy of the query that was performed and the results received. The FMCC will contact you with instructions on how to proceed.

3.2 Commands

All activities on the EDGE server are initiated through an “edge” command. CMS stages and deploys “remote commands” that must be executed by the issuer at a frequency determined by CMS. Remote commands are picked up by the EDGE Talk Phone Home request that is executed each time an “edge” command is run on the EDGE server.

In addition to the remote commands, there are “local commands” that issuers can execute independently at any time. The local commands, and any reports produced as a result, are not official CMS reports and will not be used for program calculations. Only reports generated as the result of CMS-deployed remote commands will be used for program calculations.

With local commands and remote commands, the order of operations on the EDGE server is important. Every invocation of an “edge” command on the EDGE server starts with a “Phone Home” command prior to executing any of the local commands that are specified in the “edge” command.

EDGE Talk Phone Home

Phone Home verifies that the local version of the EDGE software is the same version as the version that is available on the CMS software site. If it is not, it downloads the latest software version and installs it. (**Note:** all software versions are cumulative). If one (1) or more software versions have not been downloaded due to non-operation of the EDGE server, the latest software version will be downloaded, including all prior database updates. Database updates are applied in order originally released. Upon completion of the software upgrade, the EDGE software will restart in order to continue operations.

In addition to the software version verification and update, the Phone Home command also downloads any remote commands that CMS staged for a particular EDGE server. These commands are stored in the **REMOTE_CMD_QUEUE** table in the EDGE_SRVR_COMMON schema in MySQL.

> **Note:** Remote commands are not stored as files or retrieved from the inbox folder. Placing CMD files in the inbox folder will NOT result in those remote command files being captured and executed. Some of these remote commands may also be “Cancel” commands to cancel execution of remote commands that had been staged earlier but not yet executed by the EDGE server.

After the Phone Home command is complete, the EDGE application checks to see if there are any remote commands in the REMOTE_CMD_QUEUE table that have a future effective date and have not been cancelled.

Remote commands can be created and sent with a future effective date and will not be executed until that time. Remote commands are executed by CMS in the order that they were received in the queue for any that are currently scheduled to execute on or prior to the current date.

After these have completed, any local commands will execute (EDGE Ingest, for example). A common practice is to set up a CRON job to perform “edge ingest.” Doing this will result in the EDGE server automatically receiving EDGE software updates, executing remote commands staged by CMS, and picking up any data files that issuers have provided for processing - in that order.

3.2.1 Local Commands

In order for EDGE servers to process each CMS remote command, a local command must be executed by the issuer on the EDGE server.

Issuers will be unable to execute the Risk Score Local Remote Command (RA_RS_Transfer_Prelim YYYY prod) in the production zone during the blackout period. An error will be returned if issuers attempt to execute the Risk Score remote command during the blackout period in the production zone.

The below table contains a list of local commands and a description of what will occur upon execution.

Table 3-1: List of EDGE Local Commands

Command	Result
• edge ingest	Initiates the processing of any properly named data files in your inbox, producing reports in your outbox folder.
• edge version	Interrogates the local software to determine the software version and displays it on the screen.

Command	Result
• edge truncate TEST ALL • edge truncate TEST E • edge truncate TEST P • edge truncate TEST M	This command requires issuers to submit a one (1)-time permission request to CMS for a complete truncation of the test zone. Issuers submit truncation requests through the EDGE Server Truncation Web form. The web form is only available through FM Community in Salesforce. To access the truncation web form, please log into FM Community via the following link: ccrms-rari.force.com/financialmanagement **Note:** Issuers should not request truncations through the CMS FEPS mailbox. All requests to the CMS FEPS mailbox will be returned with instructions to use the web form. ⚠ **Note**: CMS will provide approval for one (1) of the four (4) scripts at a time. 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. Each command will delete data from the test schema data tables based on command executed. The command ending with “ALL” = ALL data, “E” = Enrollment only, “P” = Pharmacy only, “M” = Medical and Supplemental only. The production schema and common tables will be unaffected. Refer to Section 3.4.1: Truncation Requests in the EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures.

Command	Result
- edge truncate VALIDATION ALL - edge truncate VALIDATION E - edge truncate VALIDATION P - edge truncate VALIDATION M	This command requires issuers to submit a one (1)-time per benefit year permission request to CMS for a complete truncation of the validation zone. Issuers submit truncation requests through the EDGE Server Truncation Web form. The web form is only available through FM Community in Salesforce. To access the truncation web form, please log into FM Community via the following link: ccrms-rari.force.com/financialmanagement ⚠ **Note**: CMS will provide approval for one (1) of four (4) scripts at a time. 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 web form 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. Each command will delete data from the validation schema data tables based on the command executed. The command ending with “ALL” = ALL data, “E” = Enrollment only, “P” = Pharmacy only, “M” = Medical and Supplemental only. The production schema and common tables will be unaffected. Refer to Section 3.4.1: Truncation Requests in the EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures.

Command	Result
• edge truncate PROD ALL • edge truncate PROD E • edge truncate PROD P • edge truncate PROD M	This command requires permission from CMS each time it is performed. Issuers must submit truncation requests through the EDGE Server Truncation Web form. The web form is only available through FM Community in Salesforce. To access the truncation web form, please log into FM Community via the following link: ccrms-rari.force.com/financialmanagement **Note:** Issuers should not request truncations through the CMS FEPS mailbox. All requests to the CMS FEPS mailbox will be returned with instructions to use the web form. ⚠ CMS will provide approval for one of the four (4) scripts at a time. The applicable script that must be executed in the agreed upon timeframe. 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 a time, issuers must notify CMS when the first truncation is complete by replying to the truncation approval request for CMS to stage the second truncation. These scripts can only be used once. Issuers must submit and receive approval to truncate in PROD for each request. If the user is unable to execute the command in the given timeframe, the user must request an extension. Each command will delete data from the PROD schema data tables based on the command executed. The command ending with “ALL” = ALL data. This command will delete all data from the production schema data tables in the EDGE server. The command ending with “E” = Enrollment only, “P” = Pharmacy only, and “M” = Medical and Supplemental only. The test schema and common tables will be unaffected. Refer to Section 3.4.1: Truncation Requests in the EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures.
• edge queue list	Provides a list of all EDGE remote commands received by the EDGE server and their status.
• edge update	Typically used only by the EDGE software but can be executed manually. The command checks the CMS site for the latest version of software and updates the local EDGE software as necessary. This command also sends a message back to CMS that the software update has been successfully completed by issuers and provides the current version number of the software on your EDGE server.

Command	Result
- edge queue execute	Executes any commands in the REMOTE_CMD_QUEUE table. This command should not be required for use as this is built into the sequencing as described earlier in this document.
- edge provisioned	Provides a status update to CMS that the EDGE server has completed the provisioning process. The command is typically executed automatically during the initial provisioning process.
- edge dbbackup	Triggers database back up of the test, common and prod schemas. Issuers are encouraged to back up their servers often and to retain the backups in a different location in the event of disaster. See Section 3.2: Disaster Recovery in the EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures.
- edge report OrphanClaimEnrollee YYYY test - edge report OrphanClaimEnrollee YYYY prod - edge report OrphanClaimEnrollee YYYY validation	Initiates the Enrollee Claims Detail (ECD) and Enrollee Claims Summary (ECS) Reports. Descriptions of all reports can be found in Appendix G: EDGE Server Reports and Local Commands and the RARI ICD Addendum found in Interface Control Document (ICD).
- edge report RI_prelim YYYY test - edge report RI_prelim YYYY prod - edge report RI_prelim YYYY validation	Initiates RI calculations and produces the RI Detail Enrollee (RIDE) Report and the RI Summary Report (RISR). Descriptions of all reports can be found in Appendix G: EDGE Server Reports and Local Commands and in the RARI ICD Addendum found in Interface Control Document (ICD).
- edge report RA_RS_Transfer_Prelim YYYY test - edge report RA_RS_Transfer_Prelim YYYY prod - edge report RA_RS_Transfer_Prelim YYYY validation	Initiates all RA calculations and reports including: - RA Claims Selection Detail (RACSD) and RA Claims Selection Summary (RASSD) Reports - RA Risk Score Detail (RARSD) and RA Risk Score Summary (RARSS) Reports - RA Transfer Elements Extract (RATEE) Report - RADV Population Summary Statistics (RADVPS) Report Descriptions of all reports can be found in Appendix G: EDGE Server Reports and Local Commands and in the RARI ICD Addendum found in Interface Control Document (ICD).

Command	Result
• edge report HCRP_NATIONAL_PRELIM YYYY test • edge report HCRP_NATIONAL_PRELIM YYYY prod • edge report HCRP_NATIONAL_PRELIM YYYY validation	Initiates both HCRP calculations and reports including: • HCRP Summary Report (HCRPSR) • HCRP Detailed Enrollee (HCRPDE) Report Descriptions of all reports can be found in Appendix G: EDGE Server Reports and Local Commands and in the RARI ICD Addendum found in Interface Control Document (ICD).
• edge report SRI_ PRELIM YYYY test I • edge report SRI_ PRELIM YYYY prod I • edge report SRI_ PRELIM YYYY validation I • edge report SRI_ PRELIM YYYY test SG • edge report SRI_ PRELIM YYYY prod SG • edge report SRI_ PRELIM YYYY validation SG • edge report SRI_ PRELIM YYYY test ALL • edge report SRI_ PRELIM YYYY prod ALL edge report SRI_ PRELIM YYYY validation ALL	⚠ **Note:** This is only applicable for issuers who are in a state where CMS is operating a State-based Reinsurance (SRI) program on behalf of the state under the Section 1332 Waiver (i.e. Maryland issuers for BY2019). Initiates both SRI detail and summary reports including: • EDGE Server State-based Reinsurance Summary (SRISR) • EDGE Server State-based Reinsurance Detail Enrollee (SRIDE) Descriptions of all reports can be found in Appendix G: EDGE Server Reports and Local Commands Market Values: • I – Individual Market • SG – Small Group • ALL – Individual and Small Group Markets

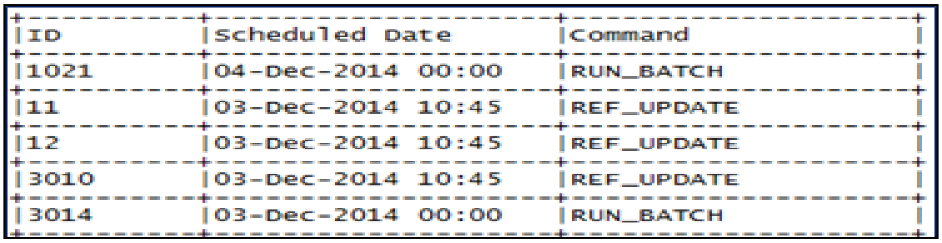
3.2.2 Remote Commands

CMS schedules deployment of a variety of remote commands for issuers to execute on their EDGE servers, most frequently to execute RA, HCRP and analytic data reports on issuer EDGE servers. In addition to these analytic data reports, other remote commands are deployed that include REF_UPDATE, KEY_CHANGE and RUN_BATCH. When CMS issues a remote command, a remote command file is created and staged in the S3 bucket, which only the EDGE server can access. Access to this location is controlled using the keys that are present on the EDGE server.

Issuers are required to execute CMS deployed remote commands within 48 business hours. Typically, CMS deploys commands at 12:01 a.m. ET on Friday so issuers can execute the commands during Friday business hours. CMS publishes upcoming command deployments on the EDGE Server Timeline which is published weekly in the REGTAP Library. CMS also makes announcements of upcoming command deployments during the EDGE Server Webinar Series sessions. A full remote command schedule is published in the REGTAP Library by CMS for the entire benefit year.

The EDGE server maintains a record of remote commands along with the parameter and results in the REMOTE_CMD_QUEUE table, which issuers can find in the EDGE_SRVR_COMMON schema of MySQL. Please refer to the EDGE Server Common Schema Data Dictionary, published in the REGTAP Library, for the structure of this table.

Issuers can view a list of scheduled remote commands in the REMOTE_CMD_QUEUE table and execute them as needed (via any EDGE command). However, issuers do not have the option of selecting which specific remote commands they want to execute. To view the scheduled remote commands, issuers may run the "edge queue list" command, which produces the following output:



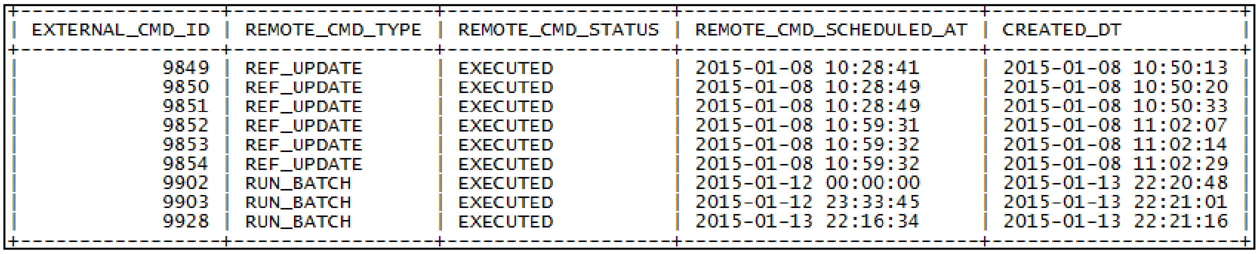
```
+-----------+----------------------+----------------------+
|ID         |Scheduled Date        |Command               |
+-----------+----------------------+----------------------+
|1021       |04-Dec-2014 00:00     |RUN_BATCH             |
+-----------+----------------------+----------------------+
|11         |03-Dec-2014 10:45     |REF_UPDATE            |
+-----------+----------------------+----------------------+
|12         |03-Dec-2014 10:45     |REF_UPDATE            |
+-----------+----------------------+----------------------+
|3010       |03-Dec-2014 10:45     |REF_UPDATE            |
+-----------+----------------------+----------------------+
|3014       |03-Dec-2014 00:00     |RUN_BATCH             |
+-----------+----------------------+----------------------+
```

Figure 3-59: EDGE Queue Command Results

The above table list only displays the remote commands that are staged and waiting to execute. When the commands are ready to execute, CMS issues the remote command ID and the remote command ID is cross-referenced against the EXTERNAL_CMD_ID on the REMOTE_CMD_QUEUE table to determine if a command is executed.

Issuers may connect to MySQL and run the following queries to get a list of remote commands executed by CMS that were already executed on their server, including the date and time they were executed.

- SELECT EXTERNAL_CMD_ID, REMOTE_CMD_TYPE, REMOTE_CMD_STATUS, REMOTE_CMD_SCHEDULED_AT, CREATED_DT FROM REMOTE_CMD_QUEUE;



```
+-----------------+-----------------+-------------------+-------------------------+---------------------+
| EXTERNAL_CMD_ID | REMOTE_CMD_TYPE | REMOTE_CMD_STATUS | REMOTE_CMD_SCHEDULED_AT | CREATED_DT          |
+-----------------+-----------------+-------------------+-------------------------+---------------------+
|            9849 | REF_UPDATE      | EXECUTED          | 2015-01-08 10:28:41     | 2015-01-08 10:50:13 |
|            9850 | REF_UPDATE      | EXECUTED          | 2015-01-08 10:28:49     | 2015-01-08 10:50:20 |
|            9851 | REF_UPDATE      | EXECUTED          | 2015-01-08 10:28:49     | 2015-01-08 10:50:33 |
|            9852 | REF_UPDATE      | EXECUTED          | 2015-01-08 10:59:31     | 2015-01-08 11:02:07 |
|            9853 | REF_UPDATE      | EXECUTED          | 2015-01-08 10:59:32     | 2015-01-08 11:02:14 |
|            9854 | REF_UPDATE      | EXECUTED          | 2015-01-08 10:59:32     | 2015-01-08 11:02:29 |
|            9902 | RUN_BATCH       | EXECUTED          | 2015-01-12 00:00:00     | 2015-01-13 22:20:48 |
|            9903 | RUN_BATCH       | EXECUTED          | 2015-01-12 23:33:45     | 2015-01-13 22:21:01 |
|            9928 | RUN_BATCH       | EXECUTED          | 2015-01-13 22:16:34     | 2015-01-13 22:21:16 |
+-----------------+-----------------+-------------------+-------------------------+---------------------+
```

Figure 3-60: EDGE Queue Command Results

The "edge queue execute" command will attempt to execute all remote commands when the time execute occurs. "Edge queue execute" is an implicit command embedded into all edge commands except for "edge update".

The table below includes a list of remote commands that CMS will stage at various intervals throughout a given benefit year along with the order in which they will be staged. For further details, refer to Appendix G: EDGE Server Reports and Local Commands.

Table 3-2: CMS Staged Remote Commands

CMS Staged Remote Commands	Description
• CLAIM_ENR_REP	ECS Report, produced by the ECS Command, provides basic counts to CMS and issuers about the issuer's current data loaded and accepted on the EDGE server. The primary data elements identified and used by CMS in quantity and quality analysis are number of unique enrollees in unique plans and number of claims, both orphan and non-orphan
• FREQUENCY_REP	The FREQ Command produces five (5) Frequency Distribution Reports, each of which contain various counts of data elements specific to a particular file submission. Data elements within the frequency reports are used in calculating EDGE data quality metrics, such as number of Diagnosis Codes per claim, percent of medical claims that are institutional and average number of pharmacy claims per enrollee, among others. Please refer to Appendix G: EDGE Server Reports and Local Commands for the detailed description of the different Frequency reports.
• RI_PRELIM • RI_FINAL	The RI command generates and sends the two (2) RI reports to CMS. There are two (2) separate commands that CMS can stage: The Prelim command is staged throughout the submission year as a way for CMS to analyze the data that was submitted. The Final command is staged at the end of the submission year only (typically in May). Please refer to Appendix G: EDGE Server Reports and Local Commands for the detailed description of each RI report.
• RA_RS_TRANSFER_PRELIM • RA_RS_TRANSFER_FINAL	The RA command generates and sends the five (5) RA reports to CMS. There are two (2) separate commands that CMS can stage: The Prelim command is staged throughout the submission year as a way for CMS to analyze the data that was submitted. The Final command is staged at the end of the submission year only (typically in May). Please refer to Appendix G: EDGE Server Reports and Local Commands for the detailed description of each RA report.

CMS Staged Remote Commands	Description
• RA_UF_PRELIM • RA_UF_FINAL	The RAUF command generates and send the RAUF report to CMS. There are two (2) separate commands that CMS may stage: The Prelim command can be staged only after the final RA command has been staged in May. The Final command is staged at the end of the submission year only (typically in May). Please refer to Appendix G: EDGE Server Reports and Local Commands for the detailed description of the RAUF report.
• RADV_PRELIM • RADV_FINAL	The RADV command generates and send the RADV reports to CMS. There are two (2) separate commands that CMS may stage: The Prelim command can be staged only after the final RA command has been staged in May. The Final command is staged at the end of the submission year only (typically in May). Please refer to Appendix G: EDGE Server Reports and Local Commands for the detailed description of the different RADV reports.
• RA_RECALIBRATION	The RA Recalibration job executes on issuers EDGE servers to provide CMS an extract of enrollee data, medical claims, pharmacy claims and supplemental claims to evaluate the current RA model. This job may only be initiated by CMS via a remote command and is queued on issuer's individual servers.
• ADHOC	The Adhoc command allows for the development, testing, and staging of non-standard remote commands to issuers' servers to query EDGE server data.
• YEAR_END_BACKUP_DB	The Year End Backup DB command creates archived schemas of PROD and Common for the specified year, where all the information in PROD is transferred to the archived schema, and all in the information in Common schema is copied to the archived schema.
• RI_ANALYTIC	The RI Analytic command produces the RI Analytic Report (RIAR) and sends it to CMS.

CMS Staged Remote Commands	Description
• HCPR_NATIONAL_PRELIM • HCRP_NATIONAL_FINAL	The HCRP report contains detailed information available to issuers based on market and plan (Claims and HCRP payment after coinsurance is applied), cross-year claims, and total premium for issuer.
• SRI_ PRELIM • SRI _ FINAL	⚠ **Note:** This is only applicable for issuers who are in a state where CMS is operating a SRI program on behalf of the state under the Section 1332 Waiver (i.e. Maryland issuers for BY2019). The CMS REMOTE SRI command produces the EDGE Server State-based Reinsurance Summary (SRISR) & EDGE Server State-based Reinsurance Detail Enrollee (SRIDE): • Both summary and detail reports are transmitted to the issuer. • The summary report is transmitted to CMS. Please refer to Appendix G: EDGE Server Reports and Local Commands for the detailed description of the SRISR & SRIDE reports.

3.2.3 Prod to Test and Prod to Validation Copy Command

Issuers can utilize the test zone to test data submissions, evaluate the results and make any necessary corrections before submitting them to the production zone. Based on issuer feedback, CMS recognized that maintaining identical data in the test and production zones may be difficult and a burden on issuer resources. Any issuer who truncated the test zone would have to submit multiple files, in the correct order, to achieve a data sync with the production zone. Resubmission of data files to the test zone also meant that submission to the production zone would be interrupted. Therefore, to address these challenges issuers face when attempting to synchronize data, CMS created a script that will allow issuers to copy data from the production zone.

The Prod to Test and Prod to Validation Copy Command feature is available on the ESM portal for users with any of the following roles: **Issuer Submitter, Issuer Approver** and/or **TPA Approver**. Users having any of the roles can use the feature to copy data from the production schema to either the test or validation schema(s). After retrieving the issuer-initiated copy action command from the ESM portal, a remote command is initiated to copy data and the data would be copied from the production schema to the test/validation schema(s).

The following sections will provide issuers with 1) the pre-steps necessary to successfully prepare their servers to execute the EDGE server remote command that will copy data from Prod to Test/Validation schema(s) and initiate the remote command through ESM Portal and 2) provide post-steps to be taken on the EDGE server to confirm that the Prod to Test/Validation copy command was successful.

Pre-Copy

Prior to initiating the copy command script, issuers must follow the three (3) pre-steps in Section 3.1.3: Storage Requirements in the EDGE Server Operations and Maintenance Manual (O&MM) – Configuration, Validation & Application Errors to successfully prepare their EDGE server for the Prod to Test/Validation copy command script. That section provides steps to add additional storage to the MySQL database mount point for insufficient space, which is needed to successfully execute the copy remote command.

> **Note:** The system capacity must be at least double the size of the EDGE_SRVR_PRODschema when only copying to one (1) zone. However, issuers could allocate at least three (3) times the space taken by EDGE_SRVR_PROD schema to accommodate copying to two (2) zones.

Copy Command

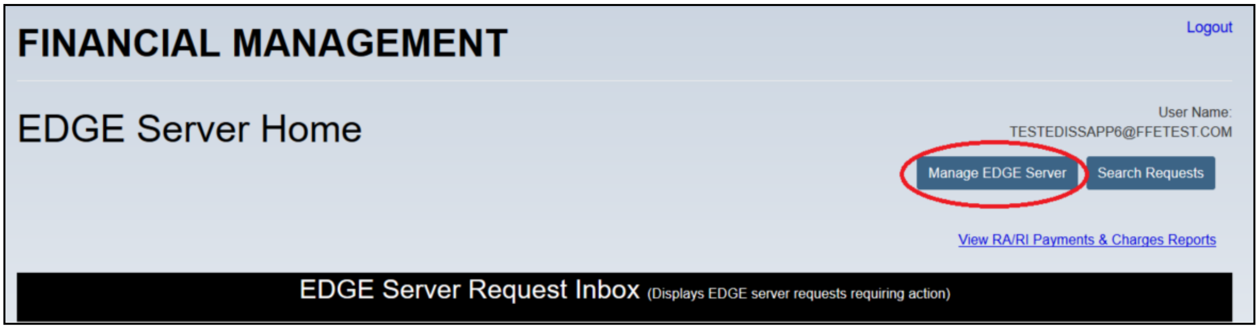
The Prod to Test and Prod to Validation copy feature is available on the ESM portal, to users having any of the following roles: **Issuer Submitter, Issuer Approver** and/or **TPA Approver**. Users having any of the aforementioned roles can log in and use this feature to copy data from the production schema to either the test or validation schema(s).

Log into the ESM portal in HIOS

Note: If there is a CRON job running, the command will be automatically picked up.

The following steps outline how to execute the 'Copy' remote command:

1. Log into ESM portal in HIOS and click on the **Manage EDGE Server** button. Refer to Section 3.6: Accessing the ESM Website in the EDGE Server Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning for additional steps.



FINANCIAL MANAGEMENT

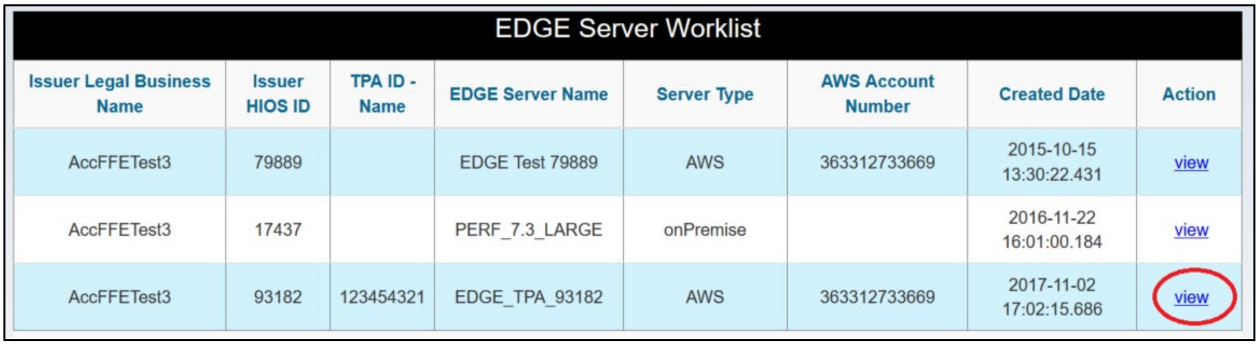
EDGE Server Home

User Name:
TESTEDISSAPP6@FFETEST.COM

EDGE Server Request Inbox (Displays EDGE server requests requiring action)

Figure 3-61: EDGE Server Home

2. Search for the five (5)-digit HIOS ID and click the **View** button for that HIOS ID:

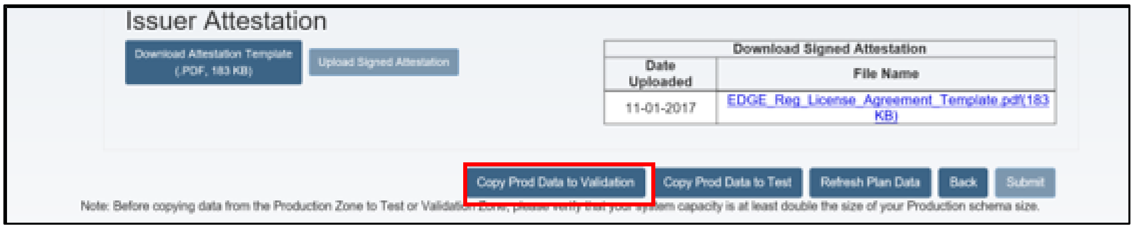


EDGE Server Worklist

Issuer Legal Business Name	Issuer HIOS ID	TPA ID - Name	EDGE Server Name	Server Type	AWS Account Number	Created Date	Action
AccFFETest3	79889		EDGE Test 79889	AWS	363312733669	2015-10-15 13:30:22.431	view
AccFFETest3	17437		PERF_7.3_LARGE	onPremise		2016-11-22 16:01:00.184	view
AccFFETest3	93182	123454321	EDGE_TPA_93182	AWS	363312733669	2017-11-02 17:02:15.686	view

Figure 3-62: EDGE Server Worklist and List of Servers

3. The next page is the EDGE Server View / Update. Scroll down towards the bottom of the page and click on the **Copy Prod Data to Test** or **Copy Prod Data to Validation** button.



Issuer Attestation

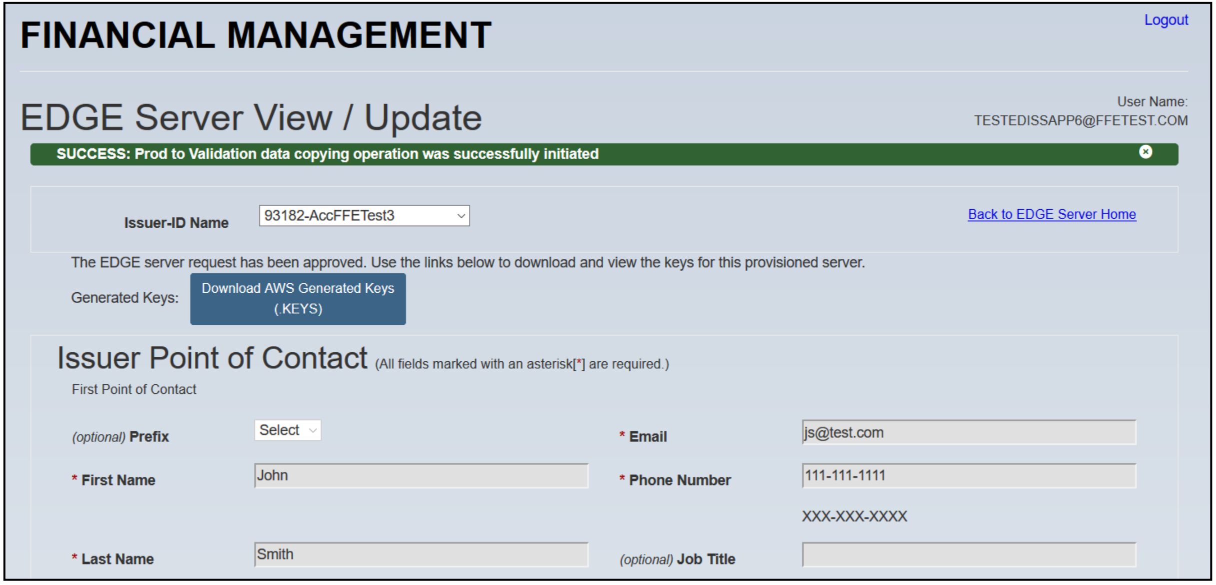
Download Attestation Template (.PDF, 183 KB)
Upload Signed Attestation
Copy Prod Data to Validation
Copy Prod Data to Test
Refresh Plan Data
Back
Submit

Download Signed Attestation	
Date Uploaded	File Name
11-01-2017	EDGE_Reg_License_Agreement_Template.pdf(183 KB)

Note: Before copying data from the Production Zone to Test or Validation Zone, please verify that your system capacity is at least double the size of your Production schema size.

Figure 3-63: Copy Prod Data to Validation/Test Buttons

4. If the initiation of the remote command for copy command is successful, a *Success Message* (**SUCCESS: Prod to Test data copying operation was successfully initiated**) will be displayed as shown below:



FINANCIAL MANAGEMENT

EDGE Server View / Update

User Name: TESTEDISSAPP6@FFETEST.COM

SUCCESS: Prod to Validation data copying operation was successfully initiated

Issuer-ID Name: 93182-AccFFETest3

The EDGE server request has been approved. Use the links below to download and view the keys for this provisioned server.

Generated Keys:

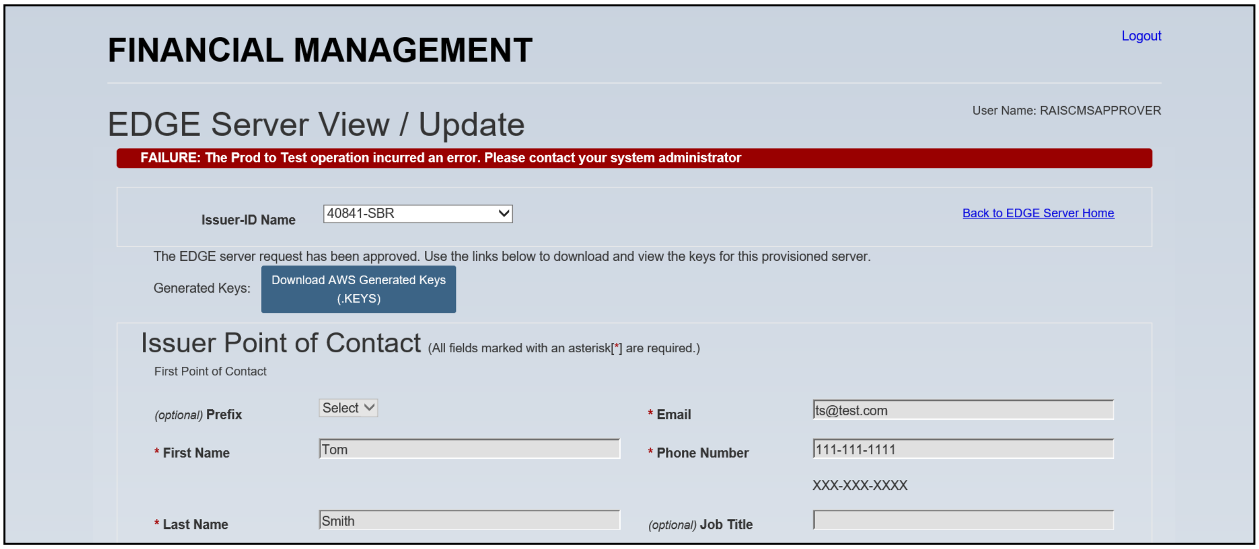
Issuer Point of Contact (All fields marked with an asterisk[*] are required.)

First Point of Contact

(optional) Prefix	Select	* Email	js@test.com
* First Name	John	* Phone Number	111-111-1111 XXX-XXX-XXXX
* Last Name	Smith	(optional) Job Title	

Figure 3-64: Prod to Test Success Message

5. If there is a failure with initiating the copy command, a *Failure Message* will be displayed as shown below. In such cases, contact a FMCC representative for technical assistance at EDGE_Server_Data@cms.hhs.gov.



FINANCIAL MANAGEMENT

Logout

EDGE Server View / Update

User Name: RAISCMSAPPROVER

FAILURE: The Prod to Test operation incurred an error. Please contact your system administrator

Issuer-ID Name: 40841-SBR

Back to EDGE Server Home

The EDGE server request has been approved. Use the links below to download and view the keys for this provisioned server.

Generated Keys: Download AWS Generated Keys (.KEYS)

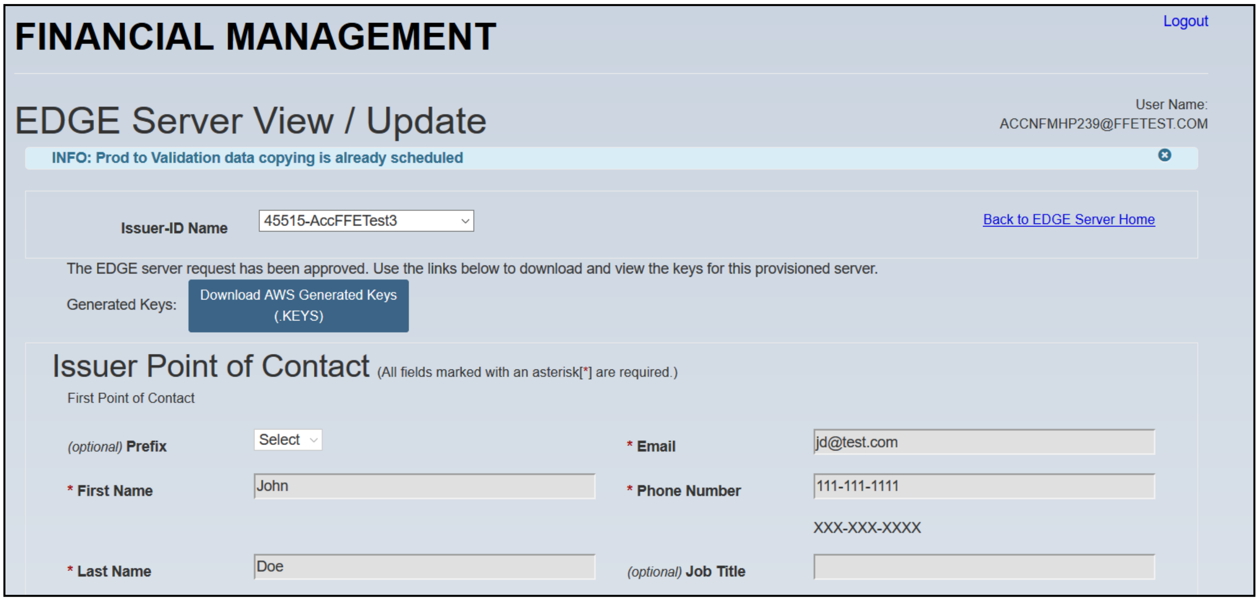
Issuer Point of Contact (All fields marked with an asterisk[*] are required.)

First Point of Contact

(optional) Prefix	Select	* Email	ts@test.com
* First Name	Tom	* Phone Number	111-111-1111 XXX-XXX-XXXX
* Last Name	Smith	(optional) Job Title	

Figure 3-65: Prod to Test Failure Message

6. If the copy command is already scheduled, an *Informational Message* will be displayed as shown below:



FINANCIAL MANAGEMENT

Logout

EDGE Server View / Update

User Name: ACCNFMHP239@FFETEST.COM

INFO: Prod to Validation data copying is already scheduled

Issuer-ID Name: 45515-AccFFETest3

Back to EDGE Server Home

The EDGE server request has been approved. Use the links below to download and view the keys for this provisioned server.

Generated Keys: Download AWS Generated Keys (.KEYS)

Issuer Point of Contact (All fields marked with an asterisk[*] are required.)

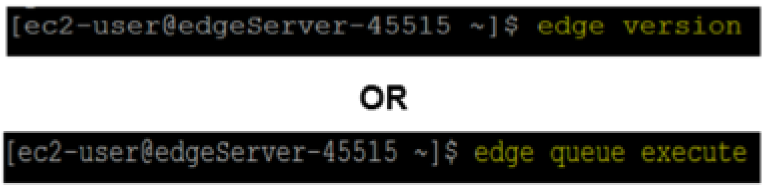
First Point of Contact

(optional) Prefix	Select	* Email	jd@test.com
* First Name	John	* Phone Number	111-111-1111 XXX-XXX-XXXX
* Last Name	Doe	(optional) Job Title	

Figure 3-66: Prod to Test Informational Message

7. After receiving the ‘Success Message’ in the ESM Portal, issuers may execute the copy command on the EDGE Server. Log into the EDGE server then enter one (1) of the two (2) commands in the command window to start the ‘Copy’ command process:

```
•   edge queue execute
•   edge version
```



```
[ec2-user@edgeServer-45515 ~]$ edge version
```

OR

```
[ec2-user@edgeServer-45515 ~]$ edge queue execute
```

Figure 3-67: Execute Copy Command

Note: Please be aware that it takes time in staging your PROD to VAL or PROD to TEST copy command from the ESM Console to your EDGE server. Please allow up to 15 minutes before running the ./edge version command on your server to copy your data. After running the ./edge version command, issuers can run the below query to confirm that the PROD to VAL or PROD to TEST command was executed on their EDGE Server.

Prod to Val

SELECT * FROM EDGE_SRVR_COMMON.REMOTE_CMD_QUEUE WHERE REMOTE_CMD_TYPE='RUN_BATCH' AND PARAMETERS LIKE '%PROD_COPY_V%' ORDER BY REMOTE_CMD_SCHEDULED_AT DESC LIMIT 1;

Prod to Test

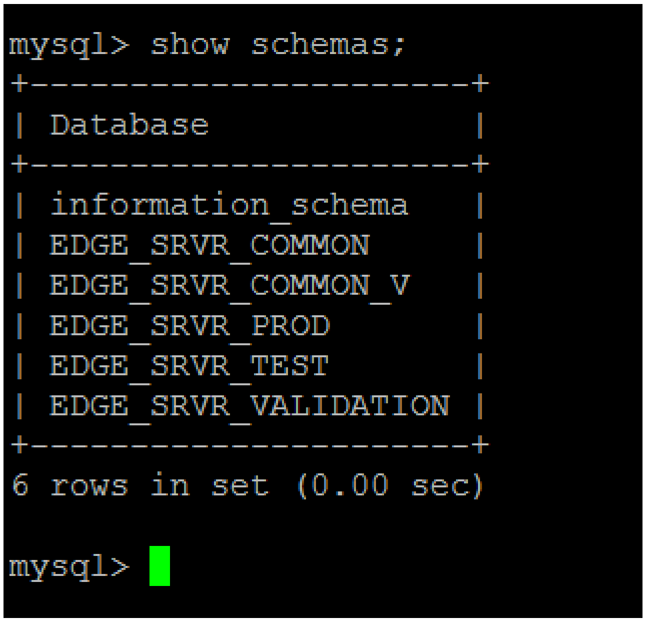
SELECT * FROM EDGE_SRVR_COMMON.REMOTE_CMD_QUEUE WHERE REMOTE_CMD_TYPE='RUN_BATCH' AND PARAMETERS LIKE '%PROD_COPY_T%' ORDER BY REMOTE_CMD_SCHEDULED_AT DESC LIMIT 1;

Post-Copy

The following steps outline how to confirm the PROD to test/validation schema copy command was successfully executed. The record counts of tables in PROD schema are taken and compared with record counts of test/validation schemas to validate copy command.

8. Execute the following command from MySQL shell to identify schemas:

- Show schemas;



```
mysql> show schemas;
+----------------------+
| Database             |
+----------------------+
| information_schema   |
| EDGE_SRVR_COMMON     |
| EDGE_SRVR_COMMON_V   |
| EDGE_SRVR_PROD       |
| EDGE_SRVR_TEST       |
| EDGE_SRVR_VALIDATION |
+----------------------+
6 rows in set (0.00 sec)

mysql> 
```

Figure 3-68: EDGE Schemas

9. Validate the data is copied from PROD schema to test/validation schema(s) by checking the record count(s) of each of the tables as specified in Appendix F: Tables in Prod/Test/Validation Schemas
10. for the EDGE_SRVR_PROD schema. Then compare the record count(s) of the corresponding tables from the EDGE_SRVR_TEST or EDGE_SRVR_VALIDATION schema(s). These record count(s) should match. For custom schemas, use custom schema names when validating the record counts.

3.2.4 Command Performance Configuration

To improve performance of the RA and RI command execution on the EDGE server, CMS strongly recommends that all issuers complete the following steps as needed:

Note: If issuers are using any type of virtualization software, then this directory may contain files from virtualization software. Issuers using this software will need to act accordingly.

1. If your server has not been rebooted for an extensive period of time, consider rebooting the server.
2. MySQL performance might degrade over time. Please run the following command to fix any corrupted table or index:
   - mysqlcheck --auto-repair --all-databases --user=xxxx --password=xxxx
3. Restart MySQL service by running:
   - sudo service mysqld restart

⚠ **Note:** The EDGE RI/RA process may fail for issuers who have enabled an automated process to monitor and move files out of the following path: /opt/edge/ingest/outbox/issuer. If you have a file utility set up, CMS recommends issuers disable the file utility on Fridays (usually when remote commands are deployed) until the remote commands complete in order to avoid remote command failures.

3.2.5 Common Command Errors

Please refer to Appendix E: Common Errors for a complete list of common errors and their resolution steps.

Section 4 - Appendices

Appendix A: Enrollee File Ingest Job Error Messages

Section 3.1.6: File Ingest Validation Errors. This table list additional resources for troubleshooting.

Table 4-1: Additional Resources for Troubleshooting Enrollee Ingest Validation Errors

Error Message	Error Description	Cause	Fix
Batch Current Version DO NOT MATCH with Latest Version, Aborting Enrollee JOB !!!	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Version in the version.json file should match latest version of the application
File name " + filename + " is not valid. Please correct the file name and resubmit	Invalid file name	Invalid file name	Fix the file name as per ICD
File " +filename + " does not exist	File does not exist in the specified Inbox	File does not exist in the specified Inbox	Put file in the specified Inbox
schema validation exception msg--------------->	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Fix the file to comply against schema
File failed header validation, invalid file id, rejecting file	File header failed validation, file rejected	File header failed validation, file rejected	Fix the file header to be in accordance with XSD/ICD
FileNotFound Exception from FileUtils...	File not found when uploading to CMS or Issuer	File not found when uploading to CMS or Issuer	Check outbox
Exception from Az S3...	AWS Exception	AWS Exception	Ops involvement required

Appendix B: Medical File Ingest Informational and Error Messages

Section 3.1.6: File Ingest Validation Errors. This table list additional resources for troubleshooting.

Table 4-2: Additional Resources for Troubleshooting Medical Ingest Validation Errors

Error Message	Error Description	Cause	Fix
Batch Current Version DO NOT MATCH with Latest Version, Aborting Enrollee JOB !!!!!	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Version in version.json should match latest version
File name " + filename + " is not valid. Please correct the file name and resubmit	Invalid file name	Invalid file name	Fix the file name as per ICD
File " +filename + " does not exist	File does not exist in the specified Inbox	File does not exist in the specified Inbox	Put file in the specified Inbox
schema validation exception msg---------------->	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Fix the file to comply against schema
File failed header validation, invalid file id, rejecting file	File header failed validation, file rejected	File header failed validation, file rejected	Fix the file header to be in accordance with XSD/ICD
Issuer is not valid	Issuer is not valid	Issuer is not valid	Provide valid issuer in file
RecordID Error	Error in record IDs	Error in record IDs	Fix the record IDs in the file
JOB ID is NULL---Aborting FAR REPORT generation step	Runtime error, no JOB ID, job aborted in this step	Runtime error, no JOB ID, job aborted in this step	Typically caused by missing file or header failure. Correct these.
every StngMdclSubmsn must be flagged a valid (1) or invalid (0)	The validation flag on this row in the staging table is invalid	System/Runtime error	Needs research by Ops team

Error Message	Error Description	Cause	Fix
No active claim found for claim family XXX	No active claim found when void/replace indicator is populated	No active claim found when void/replace indicator is populated	Examine file and provide the correct original claim ID
FileNotFoundException from FileUtils...	File not found when uploading to CMS or Issuer	File not found when uploading to CMS or Issuer	Check outbox
Exception from AWS S3...	AWS Exception	AWS Exception	Ops involvement required

Appendix C: Supplemental File Ingest Informational and Error Messages

Section 3.1.6: File Ingest Validation Errors. This table list additional resources for troubleshooting.

Table 4-3: Additional Resources for Troubleshooting Supplemental Ingest Validation Errors

Error Message	Error Description	Cause	Fix
Batch Current Version DO NOT MATCH with Latest Version, Aborting Enrollee JOB!!!!!	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Version in version.json should match latest version
File name " + filename + " is not valid. Please correct the file name and resubmit	Invalid file name	Invalid file name	Fix the file name as per ICD
File " +filename + " does not exist	File does not exist in the specified Inbox	File does not exist in the specified Inbox	Put file in the specified Inbox
schema validation exception msg--------------->	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Fix the file to comply against schema
File failed header validation, invalid file id, rejecting file	File header failed validation, file rejected	File header failed validation, file rejected	Fix the file header to be in accordance with XSD/ICD
Issuer is not valid	Issuer is not valid	Issuer is not valid	Provide valid issuer in file
JOB ID is NULL---Aborting FAR REPORT generation step	Runtime error, no JOB ID, job aborted in this step	Runtime error, no JOB ID, job aborted in this step	Typically caused by missing file or header failure. Correct these.

Error Message	Error Description	Cause	Fix
every StngSupplSubmsn must be flagged a valid (1) or invalid (0)	The validation flag on this row in the staging table is invalid	System/Runtime error	Needs research by Ops team
FileNotFoundException from FileUtils...	File not found when uploading to CMS or Issuer	File not found when uploading to CMS or Issuer	Check outbox
Exception from Az S3...	AWS Exception	AWS Exception	Ops involvement required

Appendix D: Pharmacy File Ingest Error Messages

Section 3.1.6: File Ingest Validation Errors. This table list additional resources for troubleshooting.

Table 4-4: Additional Resources for Troubleshooting PHARMACY Ingest Validation Errors

Error Message	Error Description	Cause	Fix
Batch Current Version DO NOT MATCH with Latest Version, Aborting Enrollee JOB!!!!!	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Logged and thrown If Remote Version does not match with the Latest Version available in S3, the Job aborts, with this message	Version in version.json should match latest version
File name " + filename + " is not valid. Please correct the file name and resubmit	Invalid file name	Invalid file name	Fix the file name as per ICD
File " +filename + " does not exist	File does not exist in the specified Inbox	File does not exist in the specified Inbox	Put file in the specified Inbox
schema validation exception msg--------------->	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Schema exception when inbound file fails schema validation. This msg is followed by the exception stack trace.	Fix the file to comply against schema
File failed header validation, invalid file id, rejecting file	File header failed validation, file rejected	File header failed validation, file rejected	Fix the file header to be in accordance with XSD/ICD
Issuer is not valid	Issuer is not valid	Issuer is not valid	Provide valid issuer in file
RecordID Error	Record ID error	Incorrect record ID in inbound file	Fix the record id and resubmit file
JOB ID is NULL---Aborting FAR REPORT generation step	Runtime error, no JOB ID, job aborted in this step	Runtime error, no JOB ID, job aborted in this step	Typically caused by missing file or header failure. Correct these.

Error Message	Error Description	Cause	Fix
every StngPhrmcySubmsn must be flagged a valid (1) or invalid (0)	The validation flag on this row in the staging table is invalid	System/Runtime error	Needs research by Ops team
FileNotFoundException from FileUtils...	File not found when uploading to CMS or Issuer	File not found when uploading to CMS or Issuer	Check outbox
Exception from Az S3...	AWS Exception	AWS Exception	Ops involvement required

Appendix E: Common Errors

Refer to the table below for common errors related to remote commands on the EDGE application and include invalid AWS Access Key ID issues, HTTP issues, Access Denied errors and other EDGE access issues that may affect the generation of summary and detail reports.

Table 4-5: Common Error for Remote Commands

Category	Error	Solution	Additional Steps
EDGE Server Settings	DEBUG Log Setting	1. Log into the server 2. Go to configuration directory (This could vary based on Issuer configuration) • cd /opt/edge/config 3. Edit the logback.xml • vi logback.xml 4. Edit this line • <logger level="WARN" name="gov.hhs.cms"/> 5. Change it to • <logger level="DEBUG" name="gov.hhs.cms"/> 6. Save the file and exit	Must revert back to WARN as part of the full process

Category	Error	Solution	Additional Steps
EDGE Server Settings	WARN Log Setting	1. Log into the server 2. Go to configuration directory (This could vary based on Issuer configuration) • cd /opt/edge/config 3. Edit the logback.xml • vi logback.xml 4. Edit this line • <logger level="DEBUG" name="gov.hhs.cms"/> 5. Change it to • <logger level="WARN" name="gov.hhs.cms"/> 6. Save the file and exit	Must revert back to WARN as part of the full process
EDGE Server Command	Error: Could not find or load main class gov.hhs.cms.ff.fm.edge.app.service.EdgeLauncherImpl	This might happen for the first time going into the validation zone; please contact FMCC with screenshots of following: • /opt/edge/bin • /opt/edge/lib • /opt/edge/lib-validation • /opt/edge/log	None
EDGE Server Command	ERROR g.h.c.f.f.e.a.c.i.TruncateCommandHandlerImpl - Error getting truncate allowed date for PROD zone com.amazonaws.services.s3.model.AmazonS3Exception: The specified key does not exist. (Service: Amazon S3; Status Code: 404; Error Code: NoSuchKey; Request ID: E1CDD24CDF259160)	Confirm through Helpdesk (CMS_FEPS@cms.hhs.gov) if you have truncation privilege. Check to ensure the truncate.PROD command is staged in the issuers S3 bucket and the date range is current. **Note:** Issuers are only given one (1) full week to execute this command or it will expire.	Contact FMCC and include: 1. edge.log

Category	Error	Solution	Additional Steps
EDGE Server Command	org.springframework.batch.item.ItemStreamException: Failed to initialize the reader	Please go to the edge.properties under/opt/edge/config directory and add the streaming properties below. • processor_reader_verifyCursorPosition=true • processor_reader_fetchSize=0	Attempt file ingest again. If error persists, contact FMCC and provide your 1. edge.log.
EDGE Server Access	ERROR g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception ...com.amazonaws.services.s3.model.AmazonS3Exception: The AWS Access Key Id you provided does not exist in our records. (Service: Amazon S3; Status Code: 403; Error Code: InvalidAccessKeyId;	To obtain new AWS Access Key ID: 1. Please log into the ESM portal and click "Manage EDGE Server." 2. Perform a search by your "Issuer HIOS ID" and then click "View" for this server. 3. Next you will need to generate a new key by clicking "Download AWS/OP Generated Keys." 4. Once you have generated the new key file, log into your EDGE server, go to /opt/edge/config and backup the existing key file (edge.keys). 5. Now copy the new key file you just generated from the ESM portal to /opt/edge/config.	None
EDGE Server Access	ERROR g.h.c.f.f.e.a.s.EdgeLauncherImpl - Error during processing command com.amazonaws.AmazonClientException: Unable to calculate MD5 hash: /opt/edge/ingest/outbox/issuer/28162.RAPHCCER.D20160222T112034.T.xml (Permission denied)	Confirm the output of the commands below. If edge application runs under user 'ec2-user': • chown -R ec2-user:ec2-user /opt/edge (For AWS $USER) • chmod -R 755 /opt/edge	Re-execute command and if there are still issues contact FMCC and provide the 1. edge.log

Category	Error	Solution	Additional Steps
EDGE Server Access	ERROR g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception ...com.amazonaws.AmazonClientException: Unable to execute HTTP request: peer not authenticated	1. Add the following proxy related properties in /opt/edge/config/edge.properties • proxy_host=xxx • proxy_port=xxxx • proxy_user=xxxx • proxy_password=xxxxx 2. Change log level to DEBUG for com.amazonaws and also in /opt/edge/config/logback.xml • <logger name="com.amazonaws" level="DEBUG" /> 3. Run the following command • ./edge version 4. Contact FMCC and provide the edge.log for review/next steps.	None
EDGE Server Access	ERROR g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Unable to load 34808.APP_UPDATE.D10272016T051036.json to edge.data.prod com.amazonaws.services.s3.model. AmazonS3Exception: Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied;	To obtain new AWS Access Key ID: 1. Please log into the ESM portal and click "Manage EDGE Server." 2. Perform a search by your "Issuer HIOS ID" and then click "View" for this server. 3. Next you will need to generate a new key by clicking "Download AWS/OP Generated Keys." 4. Once you have generated the new key file, log into your EDGE server, go to /opt/edge/config and backup the existing key file (edge.keys). 5. Now copy the new key file you just generated from the ESM portal to /opt/edge/config.	None

Category	Error	Solution	Additional Steps
EDGE Server Command	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step gov.hhs.cms.ff.fm.edge.app.command.exception.UnableToRunIngestException: Ingest operation is not allowed at this time, it could be a due to blackout period or edge not able to update due to connectivity.	Run the following command to fix this intermittent issue: • edge update	If error persists, contact FMCC and provide the 1. edge.log
EDGE Server Settings	Archive schemas error. Unable to create schemas	Lack of privileges is preventing the issuer from creating the schemas. You will need to grant privileges to $db_user using root access in order to be able to create the archive schemas. After you grant all privileges, you should then be able to create the (current year) schemas using edgeDBuser and then restore from the backup. Slides 12-14 in the EDGE Server 2015 Data Archive and Preparing for 2016 Data Submission presentation provide steps on how to grant all privileges using root access.	None
EDGE Server Storage	Insufficient capacity issue (AWS)	Open up a ticket with AWS and open a case with FMCC in order to assist in supporting solution. Please update your FMCC representative on the progress.	None
EDGE Server Access	403 - Access Denied:	Provide proxy credentials as the URL parameter. Refer to curl documentation for proxy parameters: • curl -x PROXY-SERVER:PORT -U USER:PASS URL	None

Category	Error	Solution	Additional Steps
EDGE Server Connection	404 - URL not found:	Work with your Domain Name System (DNS) administrator or service provider to resolve.	None
EDGE Server Connection	ERROR g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception ...com.amazonaws.AmazonClientException: Unable to execute HTTP request: edge.binaries.prod.s3.amazonaws.com	Contact the FMCC team and provide: 1. edge.log 2. edge.properties	None
EDGE Server Error	ERROR gov.hhs.cms.ff.fm.edge.util.FileUtil - Cannot create directory	Confirm the current EDGE version by executing the following command: • edge version The "Cannot create directory" message is a warning message that is part of the upgrade. The message can be ignored if the EDGE version is correct.	None
EDGE Server Access	Authentication token manipulation error	If the issuer forgot their current ec2-user password, then it requires re-provisioning.	None

Category	Error	Solution	Additional Steps
Remote Command Failure	ERROR g.h.c.f.f.e.a.s.PhoneHomeClientImpl - Unable to execute queue command. Incorrect result size: expected 1, actual 2 org.springframework.dao.IncorrectResultSizeDataAccessException: Incorrect result size: expected 1, actual 2	This error indicates the presence of a duplicate remote command. Contact the FMCC and include a dump of the remote command queue table to identify duplicate commands. Please send all these columns: • SELECT REMOTE_CMD_QUEUE_ID, REMOTE_CMD_STATUS, REMOTE_CMD_TYPE, EXTERNAL_CMD_ID, RESULTS, CREATED_DT, UPDATED_DT, REMOTE_CMD_EXPIRES_ON FROM EDGE_SRVR_COMMON.REMOTE_CMD_QUEUE;	None
EDGE Server Error	Exception in thread "main" java.lang.NoClassDefFoundError: java/time/LocalDate	Indicates incorrect Java Version. Download the latest version of Java as indicated in Section 3.5: Server Application and Software Stack in the EDGE Server Operations and Maintenance Manual (O&MM) – Backup & Maintenance Procedures.	Please download the latest Oracle Java version as detailed in Section 3.3.1: Server Setup in the EDGE Server Operations and Maintenance Manual (O&MM) – HIOS, ESM, & Provisioning.

Category	Error	Solution	Additional Steps
File Ingest Issue	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step org.springframework.dao.RecoverableDataAccessException: Attempt to process next row failed; ERROR g.h.c.f.f.e.j.m.MedicalInlineProcessor - File failed header validation, rejecting file ERROR g.h.c.f.f.e.r.FileAcceptRejectReportGenerator - REPPARAMS-------->File Header Validation Failed---Skipping Other Steps	One reason your file might get rejected, check if you've submitted a file with same 'fileIdentifier'. If you have different file names and this error persists, contact FMCC and provide: 1. edge.log 2. edge.properties	None
MySQL Error	The MySQL server is running with the --secure-file-priv option, so it cannot execute this statement	1. Open my.cnf 2. Add the field: • secure-file-priv="" 3. Restart MySQL	None
EDGE Server Command	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step org.springframework.batch.item.ItemStreamException: Failed to initialize the reader	Please go to the edge.properties under/opt/edge/config directory and add the streaming properties below. • processor_reader_verifyCursorPosition=true • processor_reader_fetchSize=0	Ask issuer to then attempt file ingest again. If error persists, contact FMCC
EDGE Server Update	ERROR g.h.c.f.f.e.d.i.SchemaBackupHelper - DataAccessException while re-creating target schema	Contact FMCC with your: 1. edge.log 2. screenshots of /var/lib/mysql	None

Category	Error	Solution	Additional Steps
EDGE Server Update	ERROR g.h.c.f.f.e.r.r.ReferenceServiceImpl - Problem loading plan Id to metal level reference lookup: Plan ID: 94248KS0140004::Metal Code: ::BenefitYear: 2015	Contact FMCC with your: 1. edge.log	None
Remote Command Failure	ERROR g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception ...com.amazonaws.services.s3.model.AmazonS3Exception: The specified key does not exist. (Service: Amazon S3; Status Code: 404; Error Code: NoSuchKey	Contact FMCC with your: 1. edge.log	None
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step java.lang.OutOfMemoryError: GC overhead limit exceeded	We would like to get the following information: 1. Edge.properties 2. Output of the following command including MySQL process - Top 3. edge.log	None
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step org.springframework.dao.RecoverableDataAccessException: Attempt to process next row failed;	Contact FMCC with your: 1. edge.log	None

Category	Error	Solution	Additional Steps
Remote Command Failure	Caused by: com.mysql.jdbc.exceptions.jdbc4.CommunicationsException: Communications link failure	Contact FMCC and provide: 1. Edge.properties 2. Output of the following command including MySQL process • Top 3. Edge.log 4. my.cnf	None
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step org.springframework.dao.DeadlockLoserDataAccessException: PreparedStatementCallback; SQL [UPDATE MEDICAL_CLAIM SET RA_FLAG='1', RA_REASON_CODE=NULL]; Deadlock found when trying to get lock; try restarting transaction; nested exception is com.mysql.jdbc.exceptions.jdbc4.MySQLTransactionRollbackException: Deadlock found when trying to get lock; try restarting transaction	1. Restart MySQL 2. Run a local command to the corresponding failure. 3. Confirm if worked, if not provide FMCC with your edge.log for review.	None

Category	Error	Solution	Additional Steps
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step org.springframework.jdbc.BadSqlGrammarException: StatementCallback; bad SQL grammar [TRUNCATE INFANTS_HCC_MATURITY_INFO]; nested exception is com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: Table 'EDGE_SRVR_PROD.INFANTS_HCC_MATURITY_INFO' doesn't exist	Contact FMCC with your: 1. edge.log	None
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Exception in afterStep callback java.lang.NullPointerException: null	Contact FMCC with your: 1. edge.log	None
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Encountered an error executing the step org.springframework.jdbc.BadSqlGrammarException: StatementCallback; bad SQL grammar [TRUNCATE INFANTS_HCC_MATURITY_INFO]; nested exception is com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: Table 'EDGE_SRVR_PROD.INFANTS_HCC_MATURITY_INFO' doesn't exist	Contact FMCC with your: 1. edge.log	None

Category	Error	Solution	Additional Steps
Remote Command Failure	ERROR o.s.batch.core.step.AbstractStep - Exception in afterStep callback java.lang.NullPointerException: null	Contact FMCC with your: 1. edge.log	None
Remote Command Failure	ERROR g.h.c.f.f.e.j.r.RiskScoreJobListener - Exception in afterJob::RiskScoreJobListener java.lang.NullPointerException: null	Contact FMCC with your: 1. edge.log	None
Remote Command Failure	Local Risk Score Job cannot be executed in the production zone during blackout.	Wait for Blackout to be lifted in the production zone to be able to run RA_RS_Transfer_Prelim YYYY prod	

Appendix F: Tables in Prod/Test/Validation Schemas

The following SQLs should be run from the MySQL shell to obtain the record counts of each of the tables from the PROD/test/validation schemas and the record counts of the tables from the PRODR schema would be compared with the record counts of tables from the test/validation schemas to validate the execution of the copy command. The record counts of tables from the PROD schema should match with the test/validation schema upon a successful run of the copy command.

USE **EDGE_SRVR_PROD/EDGE_SRVR_TEST/EDGE_SRVR_VALIDATION**:

```
SELECT COUNT(*) FROM EDGE_ERROR_LOG;
SELECT COUNT(*) FROM EDGE_EVENT_LOG;
SELECT COUNT(*) FROM HCRP_CLAIM;
SELECT COUNT(*) FROM HCRP_ENROLLEE;
SELECT COUNT(*) FROM HCRP_ INSURED_MEMBER_PLAN;
SELECT COUNT(*) FROM HCRP_PREMIUM;
SELECT COUNT(*) FROM HCRP_SUBPOLICY;
SELECT COUNT(*) FROM INFANTS_HCC_MATURITY_INFO;
SELECT COUNT(*) FROM INSRD_MMBR;
SELECT COUNT(*) FROM MDCL_CLM_DGNS_CD_ASCTN;
SELECT COUNT(*) FROM MEDICAL_CLAIM;
SELECT COUNT(*) FROM MEDICAL_CLAIM_SRVC_LINE;
SELECT COUNT(*) FROM MEDICAL_CLAIM_SRVC_MDFR_ASCTN;
SELECT COUNT(*) FROM MMBR_INSRNC_PLCY_CVRG;
SELECT COUNT(*) FROM MMBR_INSRNC_PLCY_CVRG_CRSS_YR_HSTY;
SELECT COUNT(*) FROM MMBR_INSRNC_PLCY_CVRG_PROFILE_ASCTN;
SELECT COUNT(*) FROM PHARMACY_CLAIM;
SELECT COUNT(*) FROM PRM_STBLZTN_SUBMSN_STUS;
SELECT COUNT(*) FROM RECORD_LEVEL_HIER;
SELECT COUNT(*) FROM RISKSCORE;
SELECT COUNT(*) FROM RISKSCORE_REMOTE;
SELECT COUNT(*) FROM STNG_BILLABLE_MMBR_MNTHS;
SELECT COUNT(*) FROM STNG_ENRCLAIMS_DETS;
SELECT COUNT(*) FROM STNG_ENRCLAIMS_PLAN_INFO;
SELECT COUNT(*) FROM STNG_ENRLMT_SUBMSN;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_CC_ASSOC;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_DGNS_ASSOC_ACCEP;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_DGNS_UTI_ASSOC;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_DROP_HCC_ASSOC;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_ENRLMNT_DURATION;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_HASH;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_HCC_ASSOC;
SELECT COUNT(*) FROM STNG_INSRD_MMBR_HCC_GROUP_ASSOC;
SELECT COUNT(*) FROM STNG_MDCL_SUBMSN;
SELECT COUNT(*) FROM STNG_MMBR_INSRNC_PLCY_CVRG_CRSS_YR;
SELECT COUNT(*) FROM STNG_MMBR_INSRNC_PLCY_CVRG_PROFILE_ASCTN;
SELECT COUNT(*) FROM STNG_PHRMCY_SUBMSN;
SELECT COUNT(*) FROM STNG_PRE_RA_ENRLMNT_PERIODS;
SELECT COUNT(*) FROM STNG_RADV_POPULATION;
SELECT COUNT(*) FROM STNG_RADV_SAMPLE;
SELECT COUNT(*) FROM STNG_RATEE;
SELECT COUNT(*) FROM STNG_RATEE_AGGREGATE;
SELECT COUNT(*) FROM STNG_REINSURANCE;
SELECT COUNT(*) FROM STNG_RIAR;
SELECT COUNT(*) FROM STNG_SPLMNTL_SUBMSN;
SELECT COUNT(*) FROM SUB_PLCY;
SELECT COUNT(*) FROM SUB_PLCY_CLM_ASSOC;
SELECT COUNT(*) FROM SUB_PLCY_CLM_ASSOC_RIAR;
SELECT COUNT(*) FROM SUB_PLCY_RIAR;
SELECT COUNT(*) FROM SUP_CLM_DGNS_CD_ASCTN;
SELECT COUNT(*) FROM SUPPLEMENTAL_CLAIM;
```

Appendix G: EDGE Server Reports and Local Commands

Describes each EDGE server report and informs issuers how and when each report is generated, as well as who receives each report. In many cases, issuers may execute local commands to generate certain EDGE server reports. In these cases, Table 4-6: EDGE Server Reports

Table 4-6: EDGE Server Reports

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server System Error (SE) Report	The outbound SE Report contains information on system-level errors that cause processing to abort on the EDGE server. The SE Report will generate independently when an error occurs displaying the Error Code and Error Message. For more information, reference the RARI ICD Addendum, located in the REGTAP Library.	At file submission, but only if the file fails before verifying the header elements.	N/A	Issuer: At file submission	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server File Accept - Reject Report for Enrollee (EH), Medical (MH), Pharmacy (PH), and Supplemental Diagnosis (SH)	The outbound ESFAR Report is produced for every inbound file submission and indicates if the file header of a submitted file was Accepted, Rejected or Informational (Accepted with a warning message. The ESFAR Report consists of a report header, status and Error Message.	Based on file submission.	N/A	Issuer: After file submission, if an SE Report was not produced	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server Detail Enrollment Error (ED) Report	The outbound ESDEE Report contains the acceptance and rejection information of all data levels within the enrollment submission. The ESDEE Report is generated for each enrollment submission that has been successfully validated at the file header level. Accepted (A) status: records passed all verifications. Rejected (R) status: records failed one (1) or more verifications. Informational (I) status: records have enrollment periods with enrollment coverage end dates that are later than the effective end date of the plan in the plan reference table.	Based on file submission.	N/A	Issuer: After file submission, if the ESFAR Report status indicates Accepted (A)	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server Summary Enrollment Accept - Reject (ES) Report	The outbound ESSEFE Report contains counts of accepted enrollee and enrollment period claims at the file header, issuer and plan levels. The ESSEFE Report is generated for each submitted enrollment file submission that has been successfully validated at the file header level.	Based on file submission.	N/A		Issuer: After file submission if the ESFAR status indicates Accepted (A) CMS
FILE PROCESSING	EDGE Server Detail Medical Claim Error Report (MD)	The outbound ESDMCE Report provides the processing results of all records submitted on an inbound medical claim file that passed all file header verifications. The ESDMCE Report contains the submitted value, error code and description of the error. ESDMCS records not validated or processed due to edit/validation failures of associated records are not reported.	Based on file submission.	N/A If the EDGE server fails to produce a claim detail report, please review the "Missing Detail Report Troubleshooting Steps" in Section 3.1.7: Missing Detail Report Troubleshooting Steps.		Issuer: At file submission if the ESFAR Report status indicates Accepted (A)

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server Summary Medical Claim File Accept - Reject Error Report (MS)	The outbound ESSMFE Report contains counts of accepted claims at the file header, issuer and plan levels. At the issuer and plan level, the counts are divided by year and month. The ESSMFE Report is generated for each medical claim file submission that has been successfully validated at the file header level.	Based on file submission.	N/A	Issuer: After file submission, if the ESFAR status indicates Accepted (A)	Issuer CMS
FILE PROCESSING	EDGE Server Detail Pharmacy Claim Error (PD) Report	The outbound ESDPCE Report contains the acceptance and rejection information of all pharmacy claim submission levels. The ESDPCE Report is generated for each pharmacy claim file submission that has been successfully validated at the file header level. ESPCS records that were not validated or processed due to edit or validation failures of the associated records are not reported.	Based on file submission.	N/A If the EDGE Server fails to produce a claim detail report, please review the "Missing Detail Report Troubleshooting Steps" in Section 3.1.7: Missing Detail Report Troubleshooting Steps.	Issuer: After file submission, if the ESFAR status indicates Accepted (A)	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server Summary Pharmacy Claim File Accept - Reject (PS) Report	The outbound ESSPFE Report contains counts of accepted claims at the file header, issuer and plan levels. The ESSPFE Report is generated for each pharmacy claim file submission that has been successfully validated at the file header level.	Based on file submission.	N/A	Issuer: After file submission, if the ESFAR status indicates Accepted (A)	Issuer CMS
FILE PROCESSING	EDGE Server Detail Supplemental Diagnosis File Error (SD) Report	The outbound ESDSFE Report contains the acceptance and rejection information of all record levels within the ESSFS. The ESDSFE Report is generated for each supplemental diagnosis file submission that has been successfully validated at the file header level. ESSFS records that were not validated or processed due to edit/validation failures of the associated parent level records are not reported.	Based on file submission.	N/A	Issuer: After file submission, if the ESFAR status indicates Accepted (A)	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FILE PROCESSING	EDGE Server Supplemental Diagnosis Summary Accept - Reject Error (SS) Report	The outbound ESSSFE Report contains counts of accepted claims at the file header, issuer and plan levels. The ESSSFE Report is generated for each supplemental diagnosis file submission that has been successfully validated at the file header level.	Based on file submission.	N/A	Issuer: After file submission, if the ESFAR status indicates Accepted (A)	Issuer CMS
ENROLEE WITHOUT CLAIMS REPORT	Enrollee (Without) Claims - Summary (ECS) Report	The outbound ECS Report contains information on enrollees without linked claims.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report OrphanClaimEnrollee YYYY test edge report OrphanClaimEnrollee YYYY prod edge report OrphanClaimEnrollee YYYY validation	Executed Monthly Command: ECS_REPORT	Issuer CMS
ENROLEE WITHOUT CLAIMS REPORT	Enrollee (Without) Claims - Detail (ECD) Report	The outbound ECD Report contains information on enrollees without linked claims.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report OrphanClaimEnrollee YYYY test edge report OrphanClaimEnrollee YYYY prod edge report OrphanClaimEnrollee YYYY validation	Issuer: At any time CMS: At least monthly	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FREQUENCY	Frequency by Data Element for Enrollment Accepted Files (FDEEAF) Report	The outbound FDEEAF Report contains frequency by data element for enrollment accepted files. The FDEEAF states the cumulative counts based on all records stored in the enrollment table, including the last file ingested.	CMS sends report specific remote command.	N/A	CMS: At least monthly	Issuer CMS
FREQUENCY	Frequency by Data Element for Pharmacy Accepted Files (FDEPAF) Report	The outbound FDEPAF Report contains frequency by data element for pharmacy accepted files. The FDEPAF states the cumulative counts based on all records stored in the pharmacy claim tables, including the last file ingested.	CMS sends report specific remote command.	N/A	CMS: At least monthly	Issuer CMS
FREQUENCY	Frequency by Data Element for Medical Accepted Files (FDEMAF) Report	The outbound FDEMAF Report contains frequency by data element for medical accepted files. The FDEMAF states the cumulative counts based on all records stored in the medical claim table, including the last file ingested.	CMS sends report specific remote command.	N/A	CMS: At least monthly	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
FREQUENCY	Frequency by Data Element for Supplemental Accepted Files (FDESAF) Report	The outbound FDESAF Report contains frequency by data element for supplemental accepted files. The FDESAF states the cumulative counts based on all records stored in the supplemental tables, including the last file ingested.	CMS sends report specific remote command.	N/A	CMS: At least monthly	Issuer CMS
FREQUENCY	Claims and Enrollment Frequency (CEFR) Report	The outbound CEFR report contains frequency data for claim and enrollee counts for each claim type.	CMS sends report specific remote command.	N/A	CMS: At least monthly	Issuer CMS
REINSURANCE(BY14 – BY16 only)	RI – Detail Enrollee (RIDE) Report	The outbound RIDE Report contains enrollee level details used for the RI calculation. The RIDE Report is generated with the RI batch Job.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RI_Prelim YYYY test edge report RI_Prelim YYYY prod edge report RI_Prelim YYYY validation	CMS: As of BY17, no longer run	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
REINSURANCE(BY14 – BY16 only)	RI – Summary Report (RISR)	The outbound RISR Report contains the issuer level calculated RI outputs that are used for payment processing. The RISR Report is generated after the RI plan batch job.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RI_Prelim YYYY test edge report RI_Prelim YYYY prod edge report RI_Prelim YYYY validation	CMS: As of BY17, no longer run	Issuer CMS
RISK ADJUSTMENT CLAIMS SELECTION	RA Claim Selection - Detail (RACSD) Report	The RACSD Report contains the included and excluded medical claims for RA, with details for each excluded claim. The RACSD Report will be generated with the risk score and transfer extract batch job.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RA_RS_Transfer_Prelim YYYY test edge report RA_RS_Transfer_Prelim YYYY prod edge report RA_RS_Transfer_Prelim YYYY validation	CMS: At least monthly	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
RISK ADJUSTMENT CLAIMS SELECTION	RA Claim Selection - Summary (RACSS) Report	The RACSS Report contains the included and excluded medical and pharmacy claim summary data. The RACSS Report is generated with the risk score and transfer extract batch job. Enrollee-specific information is not on this report.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RA_RS_Transfer_Prelim YYYY test edge report RA_RS_Transfer_Prelim YYYY prod edge report RA_RS_Transfer_Prelim YYYY validation	CMS: At least monthly Note: A complete report for all accepted medical files is generated based on remote command sent by CMS.	Issuer CMS
RISK ADJUSTMENT RISK SCORE & TRANSFER EXTRACT	RA Risk Score - Detail (RARSD) Report	The RARSD Report notifies the issuer regarding individual risk scores for the issuer, plan and enrollee based on medical and pharmacy claims. The RARSD Report is generated when the risk score and transfer extract batch job is initiated by CMS.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RA_RS_Transfer_Prelim YYYY test edge report RA_RS_Transfer_Prelim YYYY prod edge report RA_RS_Transfer_Prelim YYYY validation	CMS: At least monthly	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
RISK ADJUSTMENT RISK SCORE & TRANSFER EXTRACT	RA Risk Score - Summary (RARSS) Report	The RARSS Report notifies CMS about average/individual risk score and RA transfer inputs for the plan based on medical and pharmacy claims, and will not include orphan claims. Enrollee specific information is not on this report. The RARSS Report is generated with the risk score and transfer extract batch job initiated by CMS.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RA_RS_Transfer_Prelim YYYY test edge report RA_RS_Transfer_Prelim YYYY prod edge report RA_RS_Transfer_Prelim YYYY validation	CMS: At least monthly	Issuer CMS
RISK ADJUSTMENT RISK SCORE & TRANSFER EXTRACT	RA Transfer Elements Extract (RATEE) Report	The RATEE Report contains information relating to plan inputs to the payment transfers, which are aggregated and transmitted to CMS to be used to calculate the transfer payment amount. Enrollee specific information is not on this report. The RATEE Report is generated with the risk score and transfer extract batch job initiated by CMS. The information from this report is appended to the RARSS Report.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report RA_RS_Transfer_Prelim YYYY test edge report RA_RS_Transfer_Prelim YYYY prod edge report RA_RS_Transfer_Prelim YYYY validation	CMS: At least monthly	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
RISK ADJUSTMENT RISK SCORE & TRANSFER EXTRACT	RADV Population Summary Statistics (RADVPS) Report	The RADVPS Report contains population statistics calculated per stratum (High, Medium, Low - thirds based on population distribution) for the total population of the issuer. The RADVPS Report is generated with the risk score and transfer extract batch job initiated by CMS. Enrollee specific information is not on this report.	CMS sends report specific remote command.	edge report RA_RS_Transfer_Prelim YYYY test edge report RA_RS_Transfer_Prelim YYYY prod edge report RA_RS_Transfer_Prelim YYYY validation	CMS: At least monthly	Issuer CMS
RISK ADJUSTMENT RISK SCORE & TRANSFER EXTRACT	RADV Population Summary Statistics Final (RADVPSF) Report	The RADVPSF Report contains population statistics calculated per stratum (High, Medium, Low - thirds based on population distribution) for the enrollees in a risk pool market where a RA transfer occurs and excludes enrollees in a risk pool market if the issuer is the only issuer in that risk pool market. The RADVPSF Report will be generated with the RADV batch job initiated by CMS.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
RISK ADJUSTMENT USER FEE	RA User Fee (RAUF) Report	The RAUF Report contains information on RA User Fee amounts calculated on each issuer's EDGE server and is an input sent to the EDGE calculation module. The RAUF Report is generated with the RA User Fee batch job initiated by CMS. The RAUF Report contains the calculated RA User Fee amounts for each issuer's 16-digit Plan ID. Enrollee specific information is not on this report.	CMS sends report specific remote command.	N/A	CMS: At least yearly	Issuer CMS
Risk Adjustment Data Validation	RADV IVA Statistics (RADVIVAS) Report	The RADVIVAS Report contains sample statistics calculated per stratum for the RADV Initial Validation Audit (IVA) sample and is an output report available to CMS and the issuer. The RADVIVAS Report will be generated with the RADV batch job initiated by CMS.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS
Risk Adjustment Data Validation	RADV Detailed Enrollee (RADVDE) Report	The RADVDE Report contains enrollee level data for each enrollee included in the RADV IVA sample. The RADVDE Report will be generated with the RADV batch job initiated by CMS.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
Risk Adjustment Data Validation	RADV Enrollment Extract (RADVEE) Report	The RADVEE Report contains all enrollment periods for all enrollees in the RADV sample that was submitted by the issuer in the enrollment XML. The report also includes enrollment periods associated with plans in a risk pool market (RPM) that is excluded from RADV due to a single issuer scenario. The RADVEE Report will be generated with the RADV batch job initiated by CMS.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS
Risk Adjustment Data Validation	RADV Medical Claim Extract (RADVMCE) Report	The RADVMCE Report contains all active RA-eligible and/or RXC eligible medical claim data that was submitted by the issuer in the medical claim XML for each enrollee included in the RADV IVA sample. The RADVMCE Report will be generated with the RADV batch job initiated by CMS.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
Risk Adjustment Data Validation	RADV Pharmacy Claim Extract (RADVPCE) Report	The RADVPCE Report contains all active RA-eligible pharmacy claim data that was submitted by the issuer in the pharmacy claim XML for each enrollee included in the RADV IVA sample. The RADVPCE Report will be generated with the RADV batch job initiated by CMS.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS
Risk Adjustment Data Validation	RADV Supplemental Extract (RADVSE) Report	The RADVSE Report contains all active supplemental records for active RA-eligible medical claims that were submitted by the issuer in the supplemental XML for each enrollee included in the RADV IVA sample. The RADVSE Report will be generated with the RADV batch job.	CMS sends report specific remote command.	N/A	CMS: Annually	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
Risk Adjustment Recalibration	RA Recalibration Reports Enrollment Data Extract Medical Claims Extract Pharmacy Claims Extract Supplemental Claims Extract	The RA Recalibration job executes on issuers EDGE servers to provide CMS an extract of enrollee data, medical claims, pharmacy claims, and supplemental claims to evaluate the current RA model and provide data for recalibration. This job may only be initiated by CMS via a remote command and is queued on issuer's individual servers via the following remote command name: RA_RECALIBRATION.	CMS sends report specific remote command	N/A	Mid-June	CMS
High Cost Risk Pool (HCRP)	High Cost Risk Pool Summary Report (HCRPSR)	The outbound HCRP Summary Report contains issuer-, market-, and plan-level results of the HCRP payment calculation and data that will be used for the HCRP charge calculation. The HCRPSR is generated after the HCRP batch job.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report HCRP_NATIONAL_PRELIM YYYY test edge report HCRP_NATIONAL_PRELIM YYYY prod edge report HCRP_NATIONAL_PRELIM YYYY validation	CMS: At least monthly	Issuer CMS

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
High Cost Risk Pool (HCRP)	High Cost Risk Pool Detail Enrollee (HCRPDE) Report	The outbound HCRP Summary Report enrollee- and claim-level results of the HCRP payment calculation and data that will be used for the HCRP charge calculation. The HCRPSR is generated after the HCRP batch job.	Issuer initiates report specific EDGE command OR CMS sends report specific remote command.	edge report HCRP_NATIONAL_PRELIM YYYY test edge report HCRP_NATIONAL_PRELIM YYYY prod edge report HCRP_NATIONAL_PRELIM YYYY validation	CMS: at least monthly	Issuer CMS

State-based Re-Insurance (SRI)	Local SRI Command: State-based Reinsurance Summary (SRISR) State Based Re-Insurance Detail Enrollee (SRIDE) *Prelim command	The State-based Reinsurance job executes on issuers' EDGE servers to provide details and a summary of all claims and enrollees that meet the standard SRI claim/enrollee selection criteria for EDGE. Both summary and detail reports are transmitted to the Issuer. Neither report is transmitted to CMS.	Issuer initiates report specific EDGE command	edge report SRI_ PRELIM YYYY test I edge report SRI_ PRELIM YYYY prod I edge report SRI_ PRELIM YYYY validation I edge report SRI_ PRELIM YYYY test SG edge report SRI_ PRELIM YYYY prod SG edge report SRI_ PRELIM YYYY validation SG edge report SRI_ PRELIM YYYY test ALL edge report SRI_ PRELIM YYYY prod ALL edge report SRI_ PRELIM YYYY validation ALL	Annually	Issuer

EDGE Server Function	Report Name	Report Description	Generated During File Ingest?	Issuer Initiated Local Command	When is the Report Initiated?	Who Receives the Report?
State-based Re-Insurance (SRI)	CMS Remote SRI Command: State-based Reinsurance Summary (SRISR) State Based Re-Insurance Detail Enrollee (SRIDE) *Prelim & Final Command	The State-based Reinsurance job executes on issuers' EDGE servers to provide details and a summary of all claims and enrollees that meet the standard SRI claim/enrollee selection criteria for EDGE. SRI_PRELIM All summary reports are provided to CMS for review. SRI_FINAL Both summary and detail reports are transmitted to the Issuer. All summary reports from both the preliminary and final runs are provided to CMS for review.	CMS sends report specific remote command.	N/A	Annually	Issuer CMS

Appendix H: Data Validation Queries for Archive Command

- The following zip file contains the Archive Validation Queries to run **before** the archive command to ensure that the data counts are correct for the current benefit year.

ArchiveValidationQ
ueries_Before_05241

- The following zip file contains the Archive Validation Queries to run **after** the archive command to ensure that the data counts are correct for the current benefit year.

ArchiveValidationQ
ueries_After_201806