



Centers for Medicare & Medicaid Services

**Center for Consumer Information and
Insurance Oversight (CCIIO)**

EDGE Server Operations and Maintenance Manual (O&MM)

Version 3.0

October 29, 2018

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.

Document Version History

Version Number	Date	Section	Description of Change
3.0	October 2018	1 Introduction	Added information regarding addition of the High Cost Risk Pool (HCRP) program.
3.0	October 2018	1.2 Additional Resources	Added link to the High Cost Risk Pool Reference Guide.
3.0	October 2018	2.1 Functional System Overview	Added background about High Cost Risk Pool reports.
3.0	October 2018	3.4.2 Server Registration	Consolidated section by deleting repeated steps for tracking server status. Added call-out box for issuers to email CMS_FEPS team when servers show 'Pending CMS Approval' status.
3.0	October 2018	3.6 Migration	Added additional guidance regarding migration approval, timeline, and concurrent steps.
3.0	October 2018	4.1.8 Troubleshooting Help for Claim Rejected as Duplicates	Added pharmacy duplicate claim queries.
3.0	October 2018	4.2.1 Local Commands	Added HCRP commands. Updated RACSD, RACSS, RARSD, RARSS, HCRPSR, and HCRPDE to include pharmacy claims.
3.0	October 2018	4.2.2 Remote Commands	Added RIAR command to Table 4-2: CMS Staged Remote Commands.
3.0	October 2018	5.1. Back-up and Data Retention Policy	Added information about the data retention policy.
3.0	October 2018	5.3 Annual Archive Process	Updated Pre-Archive and Archive steps based on BY 2017 Job Aid. Added call-out box advising use of the 'page down' button to view the 200 success code message in the edge.log. Updated note in Step 8. Note: YYYY = is the current year. Example: In July of 2018, this value should say 2018.
3.0	October 2018	5.4 Truncation Requests	Added information from BY2018 EDGE Server Truncation Web Form Guide.
3.0	October 2018	6.1 Global Reference Data	Added EDGE 27.0 update that reference data process will occur independently of maintenance release.
3.0	October 2018	6.2 Plan Data Source & Integration	Added clarification for reusing plan IDs.
3.0	October 2018	6.4 Plan Data Records on Server	Created subsections 6.4.1 Identifying Missing Plans and 6.4.2 Small Group Rollover.
3.0	October 2018	Appendix I	Added Appendix I: Data Validation Queries Before Archive Command.
3.0	October 2018	Appendix H: EDGE Server Reports and Local Commands	Updated RACSD, RACSS, RARSD, RARSS, HCRPSR, and HCRPDE to include pharmacy claims. Added HCRP command.

The current revision has been updated to reflect changes to this version of the document. Please note that past versions are not updated in the Revision History and reflect the updates made at the time of that revision.

Table of Contents

Section 1 - Introduction	12
1.1 Conventions	13
1.2 Additional Resources	14
1.3 Technical Assistance	15
Section 2 - System Overview	17
2.1 Functional System Overview	17
2.1.1 Issuer Responsibilities and Infrastructure Overview	18
2.1.2 Architecture	20
2.1.3 System Software Specifications	22
2.1.4 Application Users	23
2.1.5 Application Directories	23
2.1.6 Application Binary Files	24
2.2 Data Model & Dictionary	26
Section 3 - Provisioning & Set Up	29
3.1 EDGE Server Options	29
3.2 EDGE Server Management Console	29
3.2.1 Accessing the ESM Website	30
3.2.2 ESM Roles	34
3.3 EDGE Server Contacts	41
3.4 Server Set Up - On-Premise	42
3.4.1 Server Setup	42
3.4.2 Server Registration	47
3.4.3 On-Premise EDGE Server Provisioning	72
3.5 Server Set-Up - AWS	94
3.5.1 AWS Account Setup	94
3.5.2 Request an AWS EDGE Server Instance	99
3.5.3 Server Registration	106
3.5.4 AWS EDGE Server Provisioning	106
3.6 Migration	123
Section 4 - Operations	125
4.1 File Processing	125
4.1.1 EDGE Server Business Rules	125
4.1.2 Interface Control Document	125
4.1.3 File Ingest Overview	125
4.1.4 Submitting Files for Processing - AWS EDGE Servers	127
4.1.5 Submitting Files for Processing - On-Premise EDGE Servers	138
4.1.6 File Ingest Validation Errors	145
4.1.7 Missing Detail Report Troubleshooting Steps	146
4.1.8 Troubleshooting Help for Claims Rejected as Duplicates	151
4.2 Commands	162
4.2.1 Local Commands	164
4.2.2 Remote Commands	166
4.2.3 Prod to Test and Prod to Validation Copy Command	170
4.2.4 Command Performance Configuration	174
4.2.5 Common Command Errors	175
4.3 Configuration	175
4.3.1 edge.properties	175
4.3.2 my.cnf	176

4.3.3 Directory Ownership	177
4.3.4 Storage Requirements	177
4.3.5 Automated Job Scheduling	184
4.4 Application Error Logging	185
4.4.1 Application Debug Level	185
4.4.2 Common Application Errors	185
Section 5 - Backup and Maintenance Procedures	187
5.1 Backup and Data Retention Policy	187
5.1.1 Backup Command	189
5.1.2 Pre-Step Checklist	190
5.1.3 Executing the Backup Command - AWS Server	190
5.1.4 Executing the Backup Command - On-Premise Server	196
5.1.5 Restoring from Backup Files	198
5.2 Disaster Recovery	199
5.2.1 Inform CMS of the Disaster Recovery Event	200
5.2.2 Recreate Server	200
5.2.3 Backup Restoration	201
5.2.4 Backup Verification	201
5.3 Annual Archive Process	201
5.3.1 Pre-Archive Steps	202
5.3.2 Archive Steps	209
5.4 Truncation Requests	213
5.4.1 Truncation Request Approval	213
5.4.2 New EDGE Server Production Zone Truncation Request	216
5.4.3 New EDGE Server Test/Validation Truncation Request Page	223
5.4.4 EDGE Server Truncation Summary and Confirmation Pages	226
5.4.5 EDGE Server Truncation Extension Request	228
5.4.6 Executing a Truncation Script	236
5.5 EDGE Server Application and Software Stack Version Updates	236
Section 6 - Reference Data	238
6.1 Global Reference Data	238
6.2 Plan Data Source & Integration	238
6.3 Plan Data Public Sources	239
6.4 Plan Data Records on Server	240
6.5 Plan Data Small Group Rollover	241
6.6 Updating Plan Data	241
Section 7 - Appendices	244

List of Appendices

Appendix A: Enrollee File Ingest Job Error Messages.....	244
Appendix B: Medical File Ingest Informational and Error Messages.....	245
Appendix C: Supplemental File Ingest Informational and Error Messages	247
Appendix D: Pharmacy File Ingest Error Messages	249
Appendix E: Common Errors	251
Appendix F: Installer Policy Data	262
Appendix G: Tables in Prod/Test/Validation Schemas	268
Appendix H: EDGE Server Reports and Local Commands	270
Appendix I: Data Validation Queries Before Archive Command	285
Appendix J: Referenced Documents	286

List of Figures

Figure 1-1: REGTAP.....	14
Figure 2-1: AWS EDGE Server Data Flow	21
Figure 2-2: On-Premise EDGE Data Flow	22
Figure 3-1: CMS Enterprise Portal Homepage, Login, and Terms and Conditions.....	31
Figure 3-2: MFA Security Code	31
Figure 3-3a: HIOS Button	32
Figure 3-3b: HIOS Button (Expanded Menu).....	32
Figure 3-4: Access Plan Management & Market Wide Functions Link	32
Figure 3-5: Terms of Use	33
Figure 3-6: EDGE Server Management.....	33
Figure 3-7: Launch This Module on ESM	33
Figure 3-8: Access the EDGE Server Management Application	34
Figure 3-9: EDGE Server Home	34
Figure 3-10: Manage Roles	36
Figure 3-11: Request Role Tab	36
Figure 3-12: Request Issuer EDGE Registration Request Approver Role	37
Figure 3-13: Enter Issuer ID	37
Figure 3-14: Review/Continue Button	38
Figure 3-15: Submit Request.....	38
Figure 3-16: Confirmation Page.....	38
Figure 3-17: View Roles	39
Figure 3-18: Manage EDGE Server Button	40
Figure 3-19: Open Provisioned Request.....	40
Figure 3-20: EDGE View/Update Screen.....	40
Figure 3-21: Submit Updates.....	41
Figure 3-22: Submit Request Button.....	41
Figure 3-23: OP Server Set Up.....	42
Figure 3-24: Oracle Java Download Page	44
Figure 3-25: Search Requests Button.....	49
Figure 3-26: EDGE Server Request Search Screen.....	50
Figure 3-27: Create EDGE Server Request Button	50
Figure 3-28: EDGE Server Request POC Page	51
Figure 3-29: TPA Information	51
Figure 3-30: Select Server Type	52
Figure 3-31: EDGE Server Name	52
Figure 3-32: On-Premise Server Details.....	52
Figure 3-33: AWS Details	53
Figure 3-34: Download Attestation Agreement Template	53
Figure 3-35: Save Request.....	54
Figure 3-36: Upload Attestation Agreement.....	54
Figure 3-37: Attach and Upload Attestation Agreement.....	54
Figure 3-38: Successfully Uploaded the File Message	55
Figure 3-39: Submit Request.....	55
Figure 3-40: Homepage.....	55
Figure 3-41: Create EDGE Server Request Button	56
Figure 3-42: EDGE Server Request POC Page	56
Figure 3-43: Select TPA	57

Figure 3-44: EDGE Server Details.....	57
Figure 3-45: Download Attestation Agreement Template	58
Figure 3-46: Save Request.....	58
Figure 3-47: Upload Attestation Agreement.....	58
Figure 3-48: Attach and Upload Attestation Agreement.....	59
Figure 3-49: Successfully Uploaded the File Message	59
Figure 3-50: Submit Request.....	59
Figure 3-51: Rejected Requests in Issuer EDGE Registration Request Submitter's Inbox.....	60
Figure 3-52: Open Request	60
Figure 3-53: TPA EDGE Registration Submitter Homepage	62
Figure 3-54: Download TPA Attestation Agreement Template	62
Figure 3-55: Upload Signed TPA Attestation Agreement.....	63
Figure 3-56: Upload Attestation Agreement.....	63
Figure 3-57: Uploaded Attestations Agreement.....	63
Figure 3-58 Select to View Request	64
Figure 3-59: TPA EDGE Registration Submitters Request.....	64
Figure 3-60: Select Server Type	65
Figure 3-61: EDGE Server Name	65
Figure 3-62: AWS Server Details.....	65
Figure 3-63: AWS Details	66
Figure 3-64: Submit Button.....	66
Figure 3-65: Rejected Requests in Submitter's Inbox.....	67
Figure 3-66: Open Request	67
Figure 3-67: Issuer EDGE Registration Request Approver Homepage	69
Figure 3-68: Open Request	69
Figure 3-69: Request Approval	70
Figure 3-70: Reject Request.....	71
Figure 3-71: Approve Request.....	71
Figure 3-72: Pending Provisioning.....	72
Figure 3-73: Search Requests Button.....	73
Figure 3-74: Search Request Screen	73
Figure 3-75: Provisioning in Progress.....	74
Figure 3-76: Download Provisioning Installation Scripts.....	74
Figure 3-77: Go to Download Page Link.....	75
Figure 3-78: Download WinSCP	75
Figure 3-79: Download Installation Package	76
Figure 3-80: WinSCP Login Screen.....	76
Figure 3-81: WinSCP Login Information	77
Figure 3-82: WinSCP Files and Folders	77
Figure 3-83: PuTTY Home Page	78
Figure 3-84: PuTTY Download Page	78
Figure 3-85: PuTTY Configuration Window	79
Figure 3-86: PuTTY Configuration - Add IP Address.....	79
Figure 3-87: Enter Username for PuTTY	80
Figure 3-88: Enter Password for PuTTY.....	80
Figure 3-89: Create EDGE folder and Open Files	81
Figure 3-90 Open EDGE Folder	81
Figure 3-91: Unzip On-Premise Installation Information File	82
Figure 3-92 Open Config Folder	82

Figure 3-93: Open Deployment Script and Property File	83
Figure 3-94: Open Properties File in Editable Format.....	84
Figure 3-95: Enter New Password for Database	85
Figure 3-96: edgeserver_size field.....	86
Figure 3-97: Add/Modify EDGE Properties	86
Figure 3-98: Save File and Exit	87
Figure 3-99: Open Install Folder	87
Figure 3-100: Install EDGE Application	88
Figure 3-101: Confirm Successful Provisioning	89
Figure 3-102: MySQL Data Dump Commands	89
Figure 3-103: Create Databases	90
Figure 3-104: Create New Database User.....	91
Figure 3-105: Load Data to New Tables	91
Figure 3-106: Enter CRON Command.....	92
Figure 3-107: Configure Cron Timing	92
Figure 3-108: Save and Exit Cron	93
Figure 3-109: Confirm Provisioned Request.....	93
Figure 3-110: AWS Setup Flow	94
Figure 3-111: Amazon Web Services	95
Figure 3-112: AWS Create Account Screen	95
Figure 3-113: Create a New AWS Account	96
Figure 3-114: Enter in Contact Information.....	96
Figure 3-115: Enter in Payment Information	97
Figure 3-116: Provide a Telephone Number.....	97
Figure 3-117: Identity Verification PIN	98
Figure 3-118: Click Continue to Complete Identity Verification.....	98
Figure 3-119: Select your AWS Support Plan.....	98
Figure 3-120: AWS Account Set-Up Complete	99
Figure 3-121 : AWS My Account.....	100
Figure 3-122: Account Settings	100
Figure 3-123: AWS Homepage with Services Dropdown	100
Figure 3-124: Select Roles	101
Figure 3-125: Create New Role Button.....	101
Figure 3-126: Configure Role Window.....	101
Figure 3-127: Select Role Type	102
Figure 3-128: Enter Account IDs.....	102
Figure 3-129: Set Permissions - Custom Policy	103
Figure 3-130: EdgeInstallerPolicy- Custom Permissions	103
Figure 3-131: Final Review Page.....	104
Figure 3-132: Services Dropdown with All AWS Services Selected	105
Figure 3-133: EC2 Dashboard Options.....	105
Figure 3-134: Create Key Pair	105
Figure 3-135: Create Key Pair Name.....	106
Figure 3-136: Pending Provisioning.....	107
Figure 3-137: Search Requests Button.....	107
Figure 3-138: Search Request Screen	108
Figure 3-139: Provisioning in Progress.....	108
Figure 3-140: Server Provisioned Status	109
Figure 3-141: Pending Provisioning.....	109

Figure 3-142: PuTTY Home Page	110
Figure 3-143: PuTTY Download Page	110
Figure 3-144: PuTTYgen Program Screen	111
Figure 3-145: PuTTYgen Notice	111
Figure 3-146: Save Private Key	112
Figure 3-147: Services and All AWS Services Dropdowns	113
Figure 3-148: EC2 Options	113
Figure 3-149: All Instances List	114
Figure 3-150: Public IP Address	114
Figure 3-151: PuTTY Configuration Window	115
Figure 3-152: PuTTY Configuration - Add IP Address	115
Figure 3-153: Category List on PuTTY Configuration Window	116
Figure 3-154: PuTTY Authentication Options	116
Figure 3-155: Browsing for PuTTY Private Key	117
Figure 3-156: Save Session	117
Figure 3-157: Completing PuTTY Configuration	118
Figure 3-158: PuTTY Security Alert	118
Figure 3-159: Enter Password	119
Figure 3-160: Enter NEW Password	119
Figure 3-161: EDGE Version Command	120
Figure 3-162: Select Change Termination Protection	120
Figure 3-163: Enable Termination Protection	121
Figure 3-164: Terminate Instances Message	121
Figure 3-165: Select EC2	122
Figure 3-166: Stop Server Instance	122
Figure 3-167: Confirm Stop Instance	123
Figure 4-1: AWS S3 Bucket Structure	128
Figure 4-2: Amazon Web Services - Login Screen	128
Figure 4-3: Select EC2	129
Figure 4-4: Select Server Instance	130
Figure 4-5: Start Server Instance	130
Figure 4-6: Confirm Start	130
Figure 4-7: AWS Home Screen - Select S3	131
Figure 4-8: Select S3 Buckets Inbox	131
Figure 4-9: Select Issuer ID	132
Figure 4-10: Select Upload	132
Figure 4-11: Upload - Select Files and Folder	133
Figure 4-12: Choose File to Upload	133
Figure 4-13: Attached File in Select Files	134
Figure 4-14: Set Details and Upload	134
Figure 4-15: File Upload Error	135
Figure 4-16: Upload Complete	135
Figure 4-17: File Picked Up for Processing	136
Figure 4-18: Refresh Inbox	136
Figure 4-19: Select Outbox	136
Figure 4-20: Select Issuer ID	137
Figure 4-21: Locate and Download Report	137
Figure 4-22: Save Downloaded Report	138
Figure 4-23: WinSCP Login Screen	139

Figure 4-24: Edge Folder	140
Figure 4-25: Ingest Folder	140
Figure 4-26: Inbox Folder	140
Figure 4-27: Drag and Drop Upload Files to Server.....	141
Figure 4-28: PuTTY Login Screen	141
Figure 4-29: Enter Username and Password.....	141
Figure 4-30: Open OPT Folder	141
Figure 4-31: Run EDGE Ingest Command to Process Files	142
Figure 4-32: Files Processing Complete.....	142
Figure 4-33: Refresh Inbox	142
Figure 4-34: Navigate to Ingest Folder	143
Figure 4-35: Open Outbox Folder.....	143
Figure 4-36: Open Issuer Folder.....	143
Figure 4-37: Outbound Reports Folder.....	144
Figure 4-38: Locate Report to Download	145
Figure 4-39: Download and Save Report.....	145
Figure 4-40: Example EDGE_ERROR_LOG table	146
Figure 4-41: Job Still Being Processed.....	147
Figure 4-42: No Process Running.....	147
Figure 4-43: XML File Header - 'fileIdentifier'	148
Figure 4-44: Medical Claims Accepted Records Query Results	149
Figure 4-45: Medical Claims Rejected Records Query Results	150
Figure 4-46: Pharmacy Claims Accepted Records Query Results	150
Figure 4-47: Example Rejected Claim in Detail Output.....	152
Figure 4-48: Example Inbound Claim	153
Figure 4-49: Example Query Output for Overlapping Query to Identify the Active Claim.....	154
Figure 4-50: Example Rejected Claim in Detail Output.....	155
Figure 4-51: Example Rejected Claim Record in Inbound Claim	155
Figure 4-52: Example Query Output for Potential Duplicate Claims: Institutional Outpatient Claims.....	156
Figure 4-53: Example Query Output for Service Code Modifiers: Institutional Outpatient Claims	157
Figure 4-54: Example Rejected Claim in Detail Output.....	158
Figure 4-55: Example Rejected Claim Record in Inbound Claim	159
Figure 4-56: Example Query Output for Potential Duplicate Claims: Professional Claims.....	160
Figure 4-57: Example Query Output for Service Code Modifiers: Professional Claim Lines.....	161
Figure 4-58: Example Query Output for Service Code Modifiers: Duplicate Inclusive Service Claim Line.....	162
Figure 4-59: EDGE Queue Command Results	167
Figure 4-60: EDGE Queue Command Results	168
Figure 4-61: EDGE Server Home	171
Figure 4-62: EDGE Server Worklist and List of Servers	171
Figure 4-63: Copy Prod Data to Validation/Test Buttons	172
Figure 4-64: Prod to Test Success Message.....	172
Figure 4-65: Prod to Test Failure Message	173
Figure 4-66: Prod to Test Informational Message.....	173
Figure 4-67: Execute Copy Command.....	174
Figure 4-68: EDGE Schemas	174
Figure 4-69: edge.properties file	176

Figure 4-70: Sample: my.cnf File	177
Figure 4-71: Sample: Ownership of Directories (Image1 of 2).....	177
Figure 4-72: Sample: Ownership of Directories (Image 2 of 2).....	177
Figure 4-73: Edge.properties - DB User (Image 1 of 2)	178
Figure 4-74: Edge.properties - DB User (Image 2 of 2)	178
Figure 4-75: Schemas Check	178
Figure 4-76: MySQL - DB User Login	179
Figure 4-77: Schema Storage Space.....	179
Figure 4-78: DB Mount Points	180
Figure 4-79: DB Backup - Space Check.....	180
Figure 4-80: Help Dropdown Location	181
Figure 4-81: Expanded Help Dropdown.....	181
Figure 4-82: AWS Support Center.....	182
Figure 4-83: "Open a new case" Screen.....	182
Figure 4-84: AWS Service Limit Request - Call Me or Web Choice.....	184
Figure 5-1: AWS Account - EC2	191
Figure 5-2: AWS Account - Running Instances	191
Figure 5-3: AWS Account - Instance State	191
Figure 5-4: AWS Account - Public IP Address	191
Figure 5-5: Logging into PuTTY.....	192
Figure 5-6: DB Schemas	192
Figure 5-7: Backup Command Prompt for AWS Server	193
Figure 5-8: AWS S3 Folder.....	193
Figure 5-9: S3 Backup Folder.....	193
Figure 5-10: Verify Creation of Backup Files	194
Figure 5-11: S3 Folder Page	194
Figure 5-12: Backup Folder Link.....	195
Figure 5-13: Selecting Backup File (Image 1 of 3).....	195
Figure 5-14: Selecting Backup File (Image 2 of 3).....	195
Figure 5-15: Selecting Backup File (Image 3 of 3).....	196
Figure 5-16: Saving the Backup File.....	196
Figure 5-17: Navigate to opt/edge/bin folder.....	196
Figure 5-18: OP Backup Command Prompt	196
Figure 5-19: Ingest Backup Command	197
Figure 5-20: Confirming Creation of Backup File for OP Extraction.....	197
Figure 5-21: Log in to WinSCP	198
Figure 5-22: Ingest Folder	198
Figure 5-23: Edge.properties - DB User (Image 1 of 2)	203
Figure 5-24: Edge.properties - DB User (Image 2 of 2)	203
Figure 5-25: Schemas Check	203
Figure 5-26: MySQL - DB User Login	205
Figure 5-27: Schema Storage Space.....	205
Figure 5-28: DB Mount Points	206
Figure 5-29: DB Backup - Space Check.....	206
Figure 5-30: Obtain root password	207
Figure 5-31: MySQL Login for Remote Command Execution.....	207
Figure 5-32: Grant Privileges.....	208
Figure 5-33: Show Grants.....	208
Figure 5-34: Local Edge Commands to Execute the Remote Command	209

Figure 5-35: Command Execution Confirmation	210
Figure 5-36: Command Execution Confirmation	211
Figure 5-37: Backup Completion Confirmation	212
Figure 5-38: Welcome Page of Truncation Request Web Form	215
Figure 5-39: EDGE Server Truncation Request Type.....	216
Figure 5-40: New EDGE Server Truncation Production Zone Request Radio Buttons.....	217
Figure 5-41: Truncation Request Category Selection	218
Figure 5-42: Truncation Request Reason.....	219
Figure 5-43: Planned Truncation Date.....	219
Figure 5-44: Planned Re-load Date Selection	220
Figure 5-45: Files Ready for Submission Selection	220
Figure 5-46: Data Test Selection	221
Figure 5-47: Data Back-up Selection	221
Figure 5-48: HIOS ID Selection	222
Figure 5-49: FMCC Number Input	222
Figure 5-50: Continue Button.....	222
Figure 5-51: New EDGE Server Truncation Test/Validation Zone Request Radio Buttons	223
Figure 5-52: New EDGE Server Validation Zone Truncation Request Page	224
Figure 5-53: HIOS ID Selection	225
Figure 5-54: FMCC Number Input	225
Figure 5-55: Continue Button.....	226
Figure 5-56: EDGE Server Truncation Request(s) Summary Table	226
Figure 5-57: Contact Information Summary.....	227
Figure 5-58: Confirmation Page.....	228
Figure 5-59: Exit Button	228
Figure 5-60: EDGE Server Truncation Extension Request Radio Button	229
Figure 5-61: Truncation Request ID.....	230
Figure 5-62: Truncation Extension Request Reason	230
Figure 5-63: Planned Truncation Date.....	231
Figure 5-64: Planned Re-load Date Selection	231
Figure 5-65: Files Ready for Submission Selection	232
Figure 5-66: Data Test Selection	232
Figure 5-67: Data Back-up Selection	233
Figure 5-68: FMCC Number Input	233
Figure 5-69: Continue Button.....	233
Figure 5-70: EDGE Server Truncation Request(s) Summary Table	234
Figure 5-71: Contact Information Summary.....	234
Figure 5-72: Confirmation Page.....	235
Figure 5-73: Exit Button	235
Figure 6-1: Refresh Plan Data button on ESM	241
Figure 6-2: Refresh Plan Data Success Message	242

List of Tables

Table 1-1: Conventions Table.....	13
Table 1-2: Key Documents	14
Table 1-3: Technical Assistance Table	16
Table 2-1: EDGE Server Schemas	20
Table 2-2: Software Stack Components	22
Table 2-3: EDGE Server Application Users	23
Table 2-4: Application Directories	23
Table 2-5: Binary Files	24
Table 2-6: Data Model & Dictionary	27
Table 3-1: AWS & OP Considerations	29
Table 3-2: Server Configuration Based on INTEL CPUs	43
Table 3-3: AWS S3 Endpoints	45
Table 3-4: Self-Hosted Path	61
Table 3-5: TPA-Hosted Path.....	61
Table 3-6: TPA-Hosted Path.....	67
Table 4-1: List of EDGE Local Commands	164
Table 4-2: CMS Staged Remote Commands	168
Table 4-3: Server Size Estimation	183
Table 4-4: CRON Jobs	184
Table 4-5: Application Debug Level	185
Table 5-1: Disaster Recovery Responsibilities	199
Table 5-2: Summary Page Navigation	227
Table 5-3: Test Results Selection	232
Table 5-4: Summary Page Navigation	235
Table 6-1: Public Documents Containing Plan Data	239
Table 7-1: Additional Resources for Troubleshooting Enrollee Ingest Validation Errors.....	244
Table 7-2: Additional Resources for Troubleshooting Medical Ingest Validation Errors.....	245
Table 7-3: Additional Resources for Troubleshooting Supplemental Ingest Validation Errors..	247
Table 7-4: Additional Resources for Troubleshooting PHARMACY Ingest Validation Errors....	249
Table 7-5: Common Error for Remote Commands	251
Table 7-6: EDGE Server Reports	270
Table 7-7: Supporting Documents for O&MM	286

Section 1 - Introduction

As part of the Patient Protection and Affordable Care Act (PPACA), two (2) programs, Risk Adjustment (RA) and High Cost Risk Pool (HCRP) mitigate the impact of adverse selection of plans and provide stability for issuers. States have the option to operate the RA and HCRP programs 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 for Benefit Year (BY) 2018, the RA program was expanded to include the HCRP, which 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](#), reinsurance payments are based on a coinsurance rate or proportion of an issuer's claims costs that are above an AP and below a reinsurance cap for the applicable BY. The AP is the threshold dollar amount after which the issuer is eligible for reinsurance 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 reinsurance 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 reinsurance amounts, occurs on the issuer owned EDGE server.

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

1.1 Conventions

The following documentation conventions will be used:

Table 1-1: Conventions Table

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



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

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

Technical Assistance

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

1.2 Additional Resources

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



Figure 1-1: REGTAP

Issuers can sign up for training events, such as the EDGE Server Webinar Series, to receive updates about the EDGE server and ask questions to CMS representatives. In addition, issuers can access the Program Area Page and review the DDC for RI and RA/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 that a new document is created annually.

Document	Summary
EDGE Server Maintenance Release Notes	Provides EDGE Server version numbers, date and time of releases and updates to the functionality of the new EDGE server versions.
EDGE Server Timeline	Provides important deadlines for maintenance releases, command deployments, submission, etc.
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.
Interface Control Document - Risk Adjustment and Reinsurance (RARI) Addendum	An addendum to the ICD that provides file layouts and data element definitions/formats for the RA, RI and analytic XML reports generated by the EDGE server.
EDGE Server Business Rules (ESBR)	Supplements the EDGE Server ICD by providing the EDGE server file processing business rules issuers are required to follow when submitting enrollment, pharmacy claims, medical claims and supplemental diagnosis code files.
High Cost Risk Pool (HCRP) Reference Guide	Provides issuers with an overview of the HCRP calculations and associated EDGE reporting for BY2018. 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.

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
Technical assistance for EDGE server data submission/processing, EDGE reports, EDGE calculations	EDGE_Server_Data@cms.hhs.gov
Chief Executive Officer (CEO) Designation updates	https://acapaymentoperations.secure.force.com/EdgeContactDatabase
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 DIY, SAS software model questions	hhshccraops@cms.hhs.gov
Risk Adjustment Data Validation (RADV)	CCIIIOACARADatavalidation@cms.hhs.gov

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 Section 4.1.2: Interface Control Document) and the business validation rules outlined in the ESBR document (See Section 4.1.1: EDGE Server Business Rules). 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 7 - 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 4.3.5: Automated Job Scheduling. For each update processed, the update type (OS, DB, application, reference data), date, completion status (successful/error), and issuer for which the update was made will be logged on the EDGE Server Management console database, which is further explained in Section 3.2: EDGE Server Management Console.

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

2.1.1 Issuer Responsibilities and Infrastructure Overview

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

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

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

Issuer Roles and Responsibilities

Issuers are responsible for the following:

- Procuring dedicated server and Red Hat enterprise evaluation license
- Providing physical security and installation and maintenance of anti-virus and anti-intrusion software
- Developing the extract, transform and load (ETL) to extract data from issuer processing system and submit to the EDGE Server
- Loading claim, enrollment and supplemental diagnosis code information to the dedicated server

- Masking enrollee identities on claims and enrollment files
- Reviewing and resolving processing errors identified on outbound files
- Evaluating accuracy of program calculations as provided on outbound reports
- Contacting CMS to report problems



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 BY and supplemental records associated with claims for the new BY.
 - 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 BY 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_COMM ON
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_VALIDA TION
EDGE Server Common Validation Schema	Contains reference data used in the validation zone.	EDGE_SRVR_COMM ON_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.

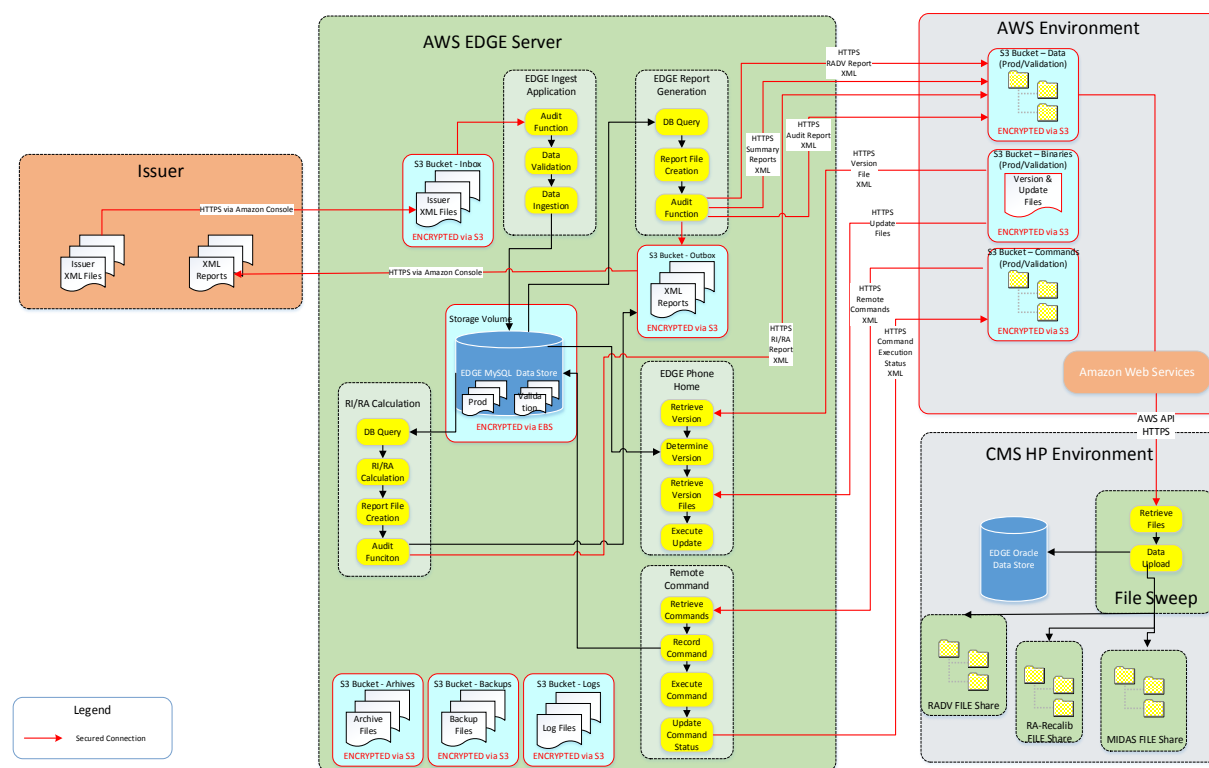


Figure 2-1: AWS EDGE Server Data Flow

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.

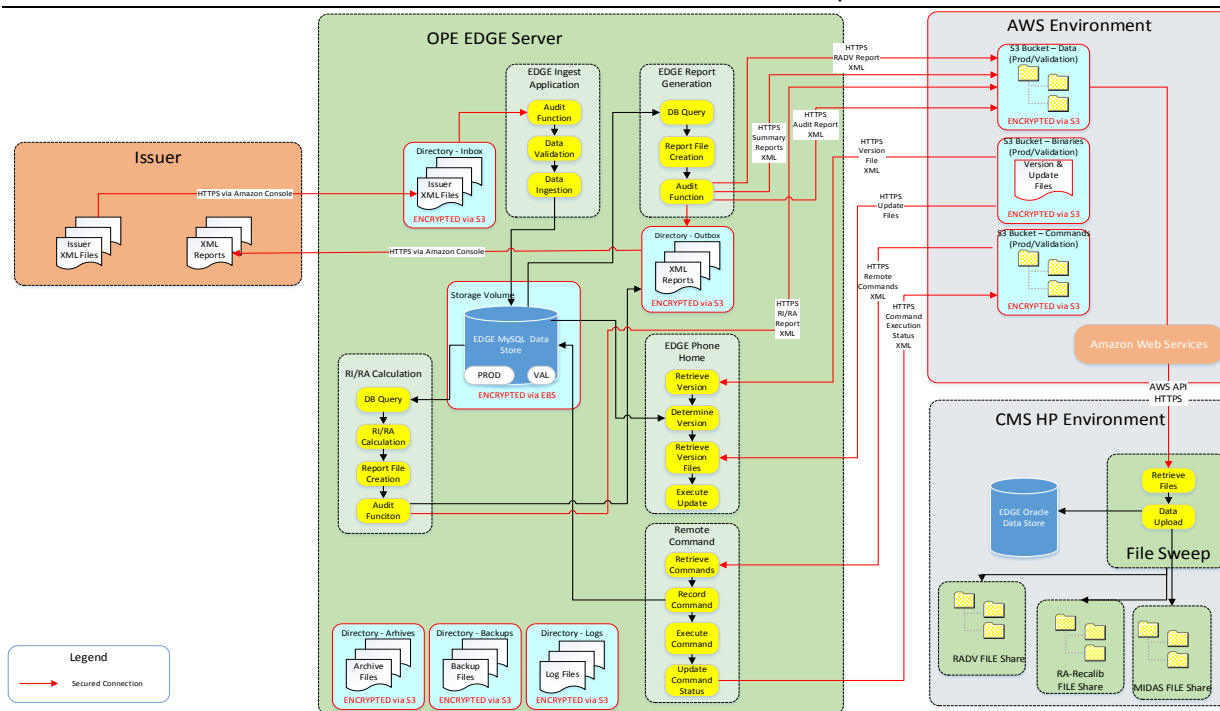


Figure 2-2: On-Premise EDGE Data Flow

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

Area	Vendor	Product
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 application utilizes.

Table 2-3: EDGE Server Application Users

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

2.1.5 Application Directories

The following directories are used by the EDGE Server application.

Table 2-4: Application Directories

Directory	Description
/opt/edge	Parent EDGE Server application directory
/opt/edge/bin	Contains the EDGE Server binaries
/opt/edge/config	Contains the EDGE Server application configuration files
/opt/edge/ingest	Parent directory for the ingest application
/opt/edge/ingest/appdata	Contains EDGE Server application data
/opt/edge/ingest/archives	Contains EDGE Server archival files
/opt/edge/ingest/archives/accepted	Contains the issuer data files that have been processed
/opt/edge/ingest/archives/rejected	Contains the issuer data files that have been rejected due to data issues
/opt/edge/ingest/inbox	Directory that issuers post their Enrollment, Medical, Pharmacy, and Supplemental data files
/opt/edge/ingest/logs	Contains the EDGE Server application log files
/opt/edge/ingest/outbox/cms	Contains summary report files that will be sent to CMS
/opt/edge/ingest/outbox/issuer	Contains the detailed and summary report files for the issuers
/opt/edge/update	Parent directory for EDGE Server application update files
/opt/edge/update/app	Contains the EDGE Server application update files
/opt/edge/update/config	Contains the EDGE Server configuration files
/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

Directory	Description
/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.



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 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

Binary Name	Description
commons-logging-1.1.1.jar	Java common logging framework
commons-pool-1.5.4.jar	Java common connection pool classes
edge-server-application.jar	Edge application binaries, contains edge batch processes
gson-2.2.4.jar	Google library to parse JSON objects
guava-17.0.jar	Guava library contain google collection, caching and concurrency. Used by gson library.
hamcrest-core-1.3.jar	Library of match objects used by other frameworks
hibernate-validator-5.1.0.Final.jar	Hibernate validator library
hibernate-validator-cdi-5.1.0.Final.jar	Hibernate validator library
hsqldb-1.8.0.7.jar	Hyper SQL library, used for execute queries against relational database
httpclient-4.2.jar	Java HTTP client library
httpcore-4.2.jar	Java HTTP core library
jackson-annotations-2.1.1.jar	Jackson library for XML parsing
jackson-core-2.1.1.jar	Jackson library for XML parsing
jackson-databind-2.1.1.jar	Jackson XML library, to build XML to java objects
javassist-3.18.1-GA.jar	Java assist provides basic java class objects
javax.el-2.2.4.jar	Java extension for Expression Language, supports for JSP and JSF
javax.el-api-2.2.4.jar	Java extension for Expression Language, supports for JSP and JSF
jaxb2-basics-0.6.3.jar	XML Schema compiler
jaxb2-basics-annotate-0.6.3.jar	XML Schema compiler using annotations
jaxb2-basics-runtime-0.6.3.jar	XML Schema compiler runtime
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

Binary Name	Description
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
spring-test-4.0.3.RELEASE.jar	Spring testing framework
spring-tx-4.0.3.RELEASE.jar	Spring framework transaction management classes
testng-6.8.7.jar	Testing framework for unit testing
tomcat-jdbc-7.0.53.jar	Tomcat framework for jdbc operations
tomcat-juli-7.0.53.jar	Tomcat framework objects
validation-api-1.1.0.Final.jar	Validation framework for XML
xpp3_min-1.1.4c.jar	XML publish library
xstream-1.3.jar	XML streaming library

2.2 Data Model & Dictionary

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

- Enrollment File

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

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

Table 2-6: Data Model & Dictionary

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

EDGE Server File Reports

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

- Summary and detail reports are generated each time an ingest file is processed.

- RA, HCRP, RI and analytic reports are generated by remote commands sent out by CMS and run by issuers.
 - Issuers can generate select RA, HCRP, RI and analytic reports through local commands. Please see Appendix H: 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 - Provisioning & Set Up

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

3.1 EDGE Server Options

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

Table 3-1: AWS & OP Considerations

Considerations	AWS	OP
Server Set-up	Automated	Manual
Hardware Requirements	None	Server
Software Requirements	Operating System included in Amazon server purchase	Issuer purchases Operating System license, see Section 3.4.1: Server Setup for more details
Security	Shared Responsibility between Amazon and issuers	Issuer-Owned
Infrastructure	Leverages Amazon's existing infrastructure	Issuer provided based on CMS specifications
Scalability	Additional capacity available	Dependent on issuer capability
HIPAA	Amazon offers HIPAA compliance programs	Issuer is responsible for complying with HIPAA requirements
Costs	Vary based on size of server	Vary based on needs of issuer. Issuers also need to purchase necessary operating system and other software.

3.2 EDGE Server Management Console

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

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

3.2.1 Accessing the ESM Website

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

Pre-Requisites for Registration: Setup Considerations

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

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

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

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

Accessing the EDGE Server Registration Site

The following steps will provide issuers and TPAs guidance on how to initially access the EDGE Registration Site. All issuers and TPAs will need to first access the HIOS portal through the CMS Enterprise Portal and then access the EDGE Registration site.

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

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

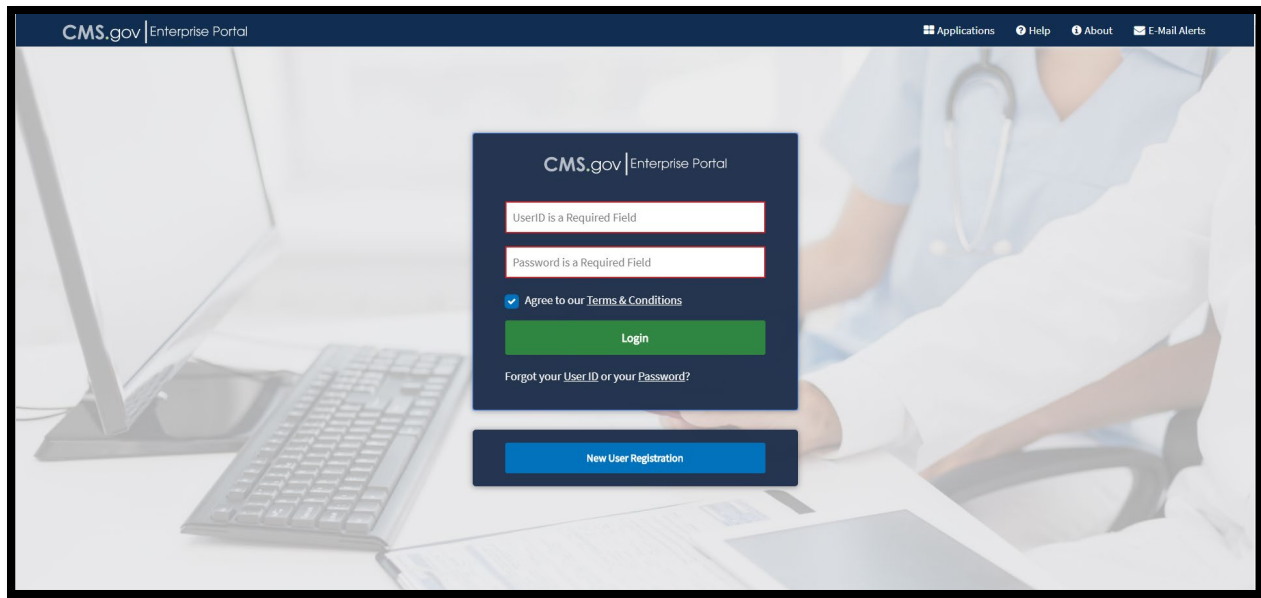


Figure 3-1: CMS Enterprise Portal Homepage, Login, and Terms and Conditions

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

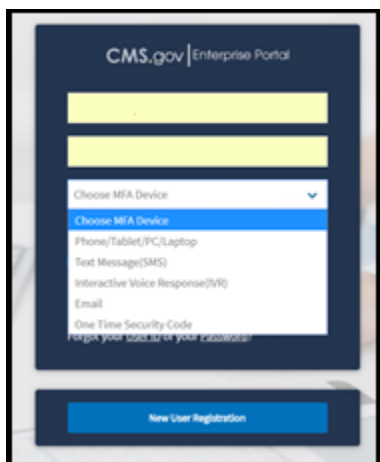


Figure 3-2: MFA Security Code

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

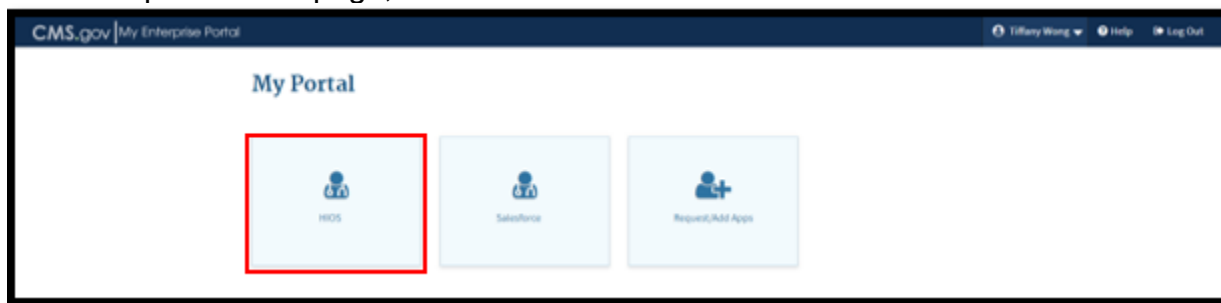


Figure 3-3a: HIOS Button

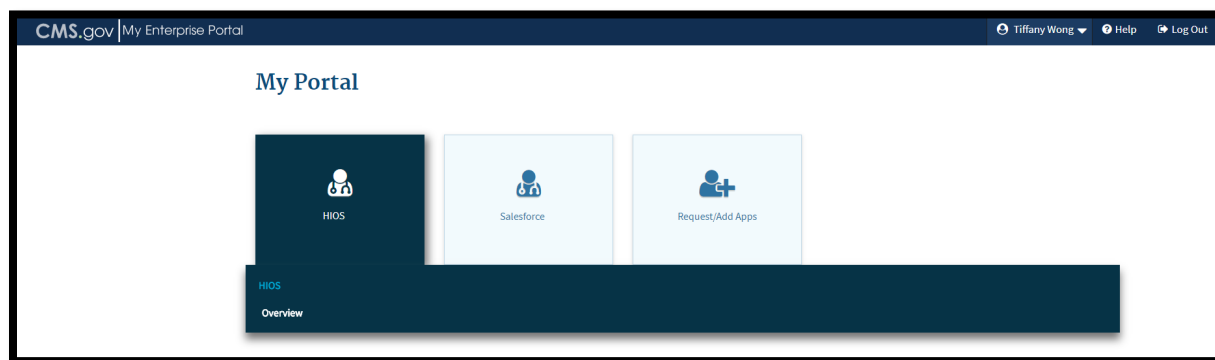


Figure 3-3b: HIOS Button (Expanded Menu)

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

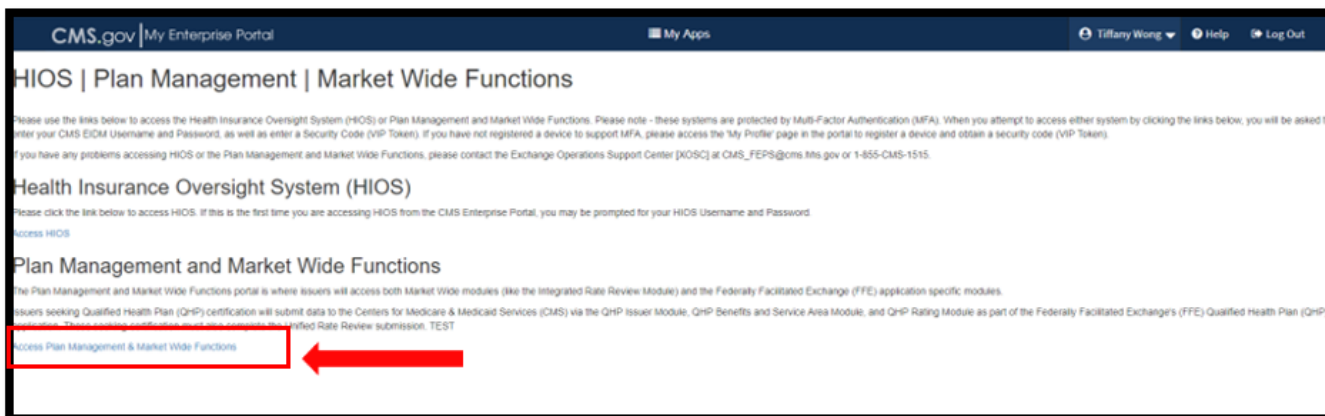


Figure 3-4: Access Plan Management & Market Wide Functions Link

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

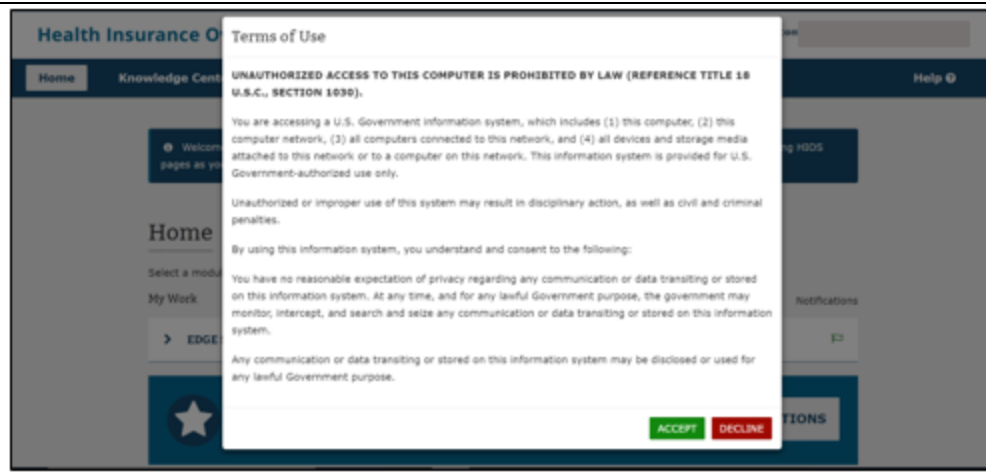


Figure 3-5: Terms of Use

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

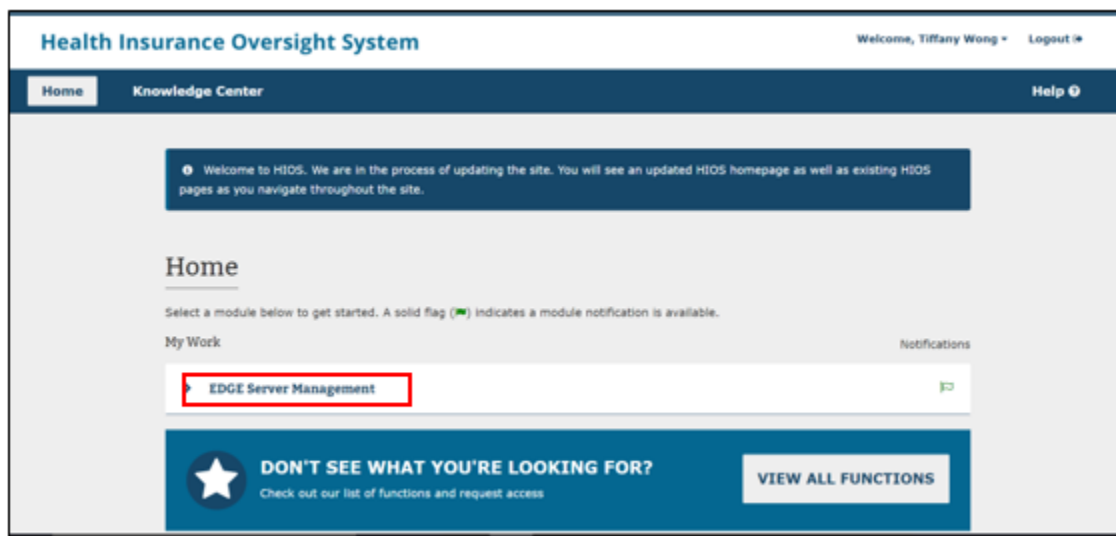


Figure 3-6: EDGE Server Management

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

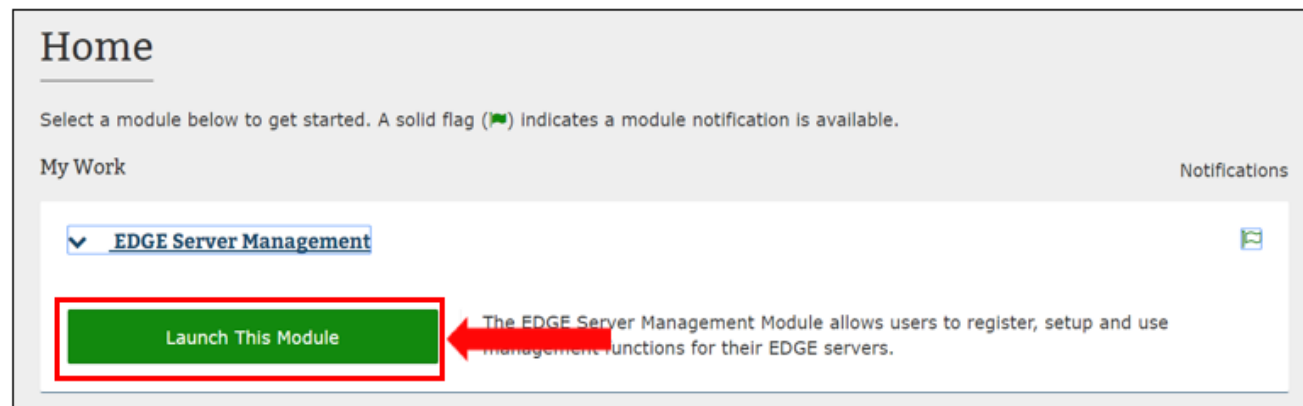


Figure 3-7: Launch This Module on ESM

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



Figure 3-8: Access the EDGE Server Management Application

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

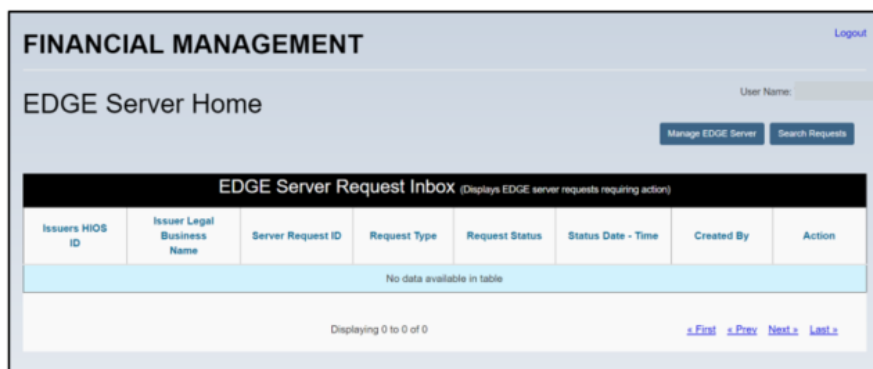


Figure 3-9: EDGE Server Home

3.2.2 ESM Roles

All users must register for a HIOS Issuer ID and/or a Company. Once registered, the user must assign two (2) ESM roles for two (2) different individuals in order to access the ESM via HIOS. The user's role will dictate the level of access in the ESM. Please note, a user may not register for issuer and TPA roles at the same time.

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



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

Issuer EDGE Registration Request Submitter

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

Issuer EDGE Registration Request Approver

- a. Approves EDGE server registration and provisioning requests
- b. Responsible for viewing the RA and RI payment reports

TPA EDGE Registration Request Submitter

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



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

All TPAs:

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

Amazon EDGE Server Issuers/TPAs:

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

OP EDGE Server Issuers/TPAs:

- Obtain and configure OP server:
 1. Choose physical or virtual server
 2. Install and configure software.
 - a. OP server provisioning steps can be found in Section 3.4.1: Server Setup. Latest software requirements for Red Hat Enterprise Linux, MySQL, and Oracle Java can be found in Section 5.5: EDGE Server Application and Software Stack Version Updates.
 3. Configure firewall rules
 4. Set up file directories

HIOS Role Management General Guidelines:

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



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

Assigning an EDGE Server Role to HIOS User

1. After logging in, click on your user name and then click the **Manage Roles** tab.

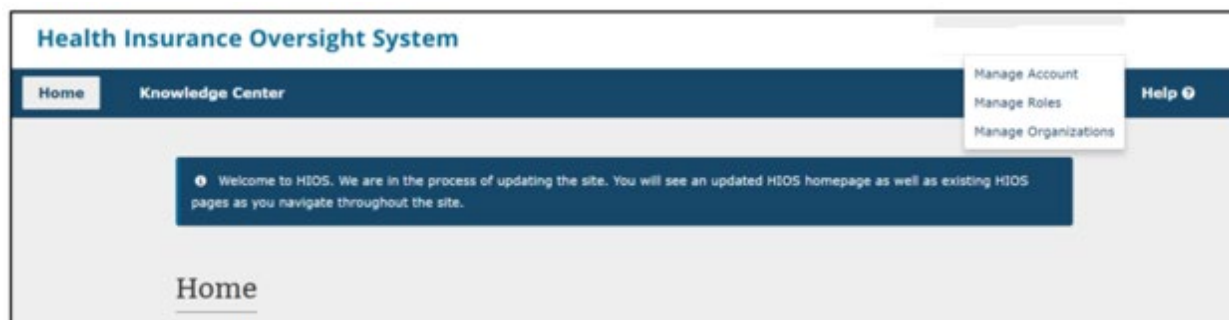


Figure 3-10: Manage Roles

2. Click the **Request Role** tab at the top of the page.

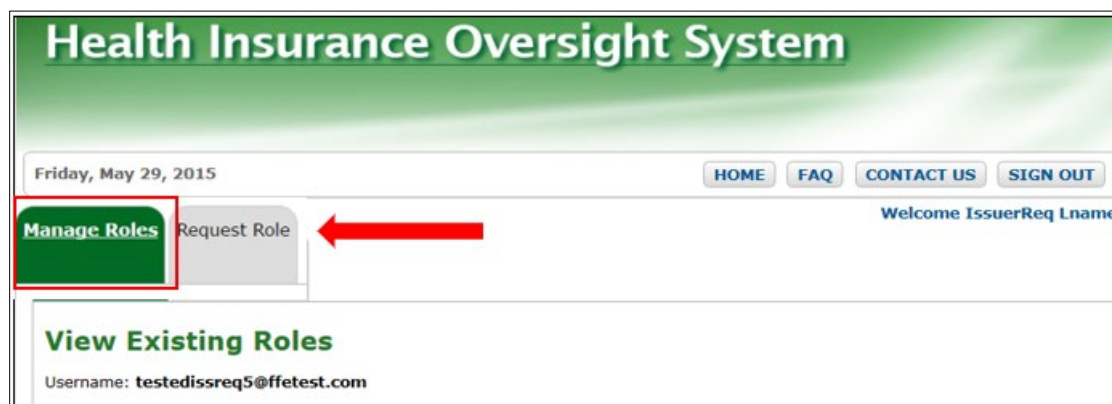
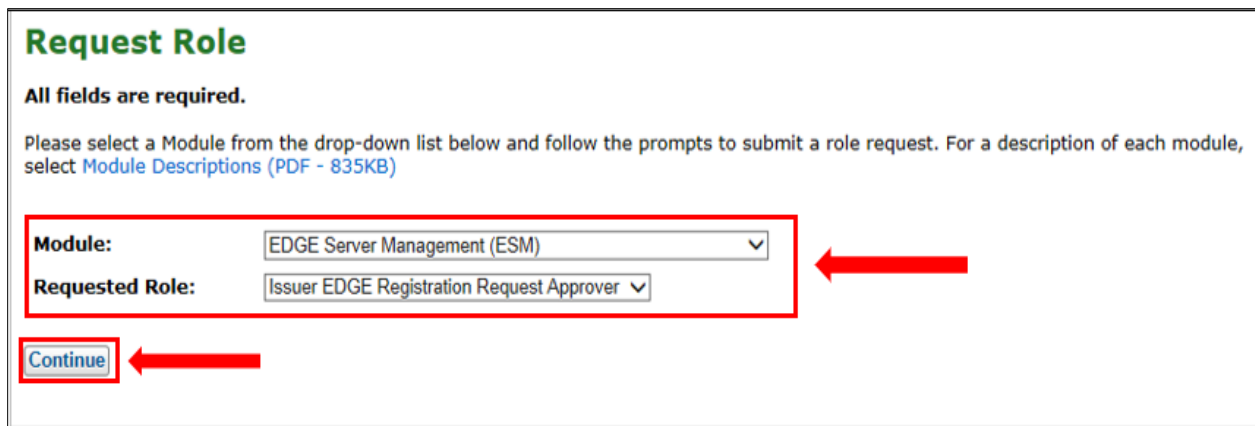


Figure 3-11: Request Role Tab

3. Click the **Select Module** dropdown menu and select **EDGE Server Management (ESM)**.

The **Requested Role** dropdown menu will appear.

Select **Issuer EDGE Registration Request Approver** role from the menu and **Continue**.



Request Role

All fields are required.

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

Module: EDGE Server Management (ESM) ▼

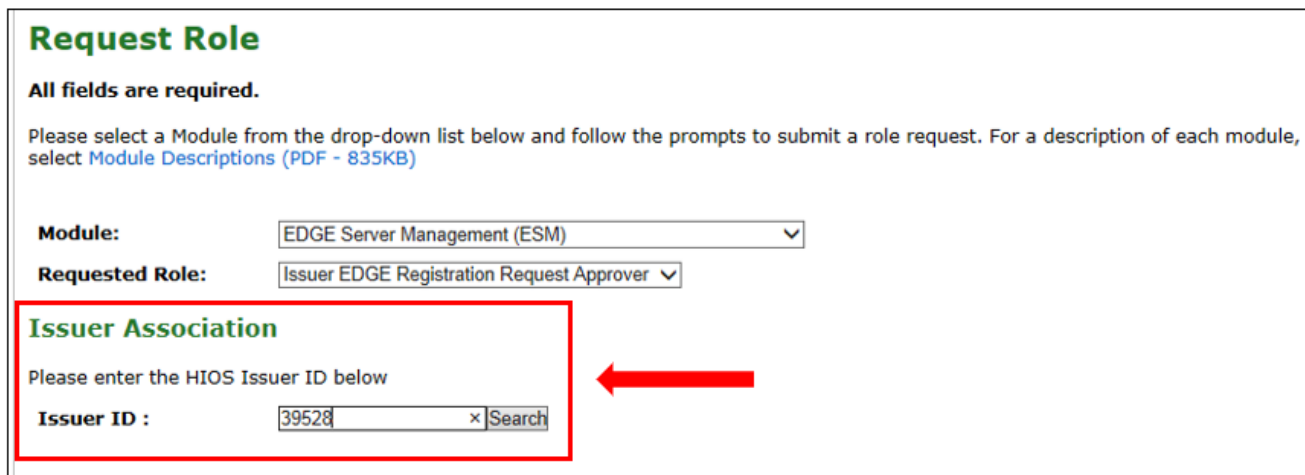
Requested Role: Issuer EDGE Registration Request Approver ▼

Continue

Figure 3-12: Request Issuer EDGE Registration Request Approver Role

After clicking **Continue**, the **Issuer Association** section will display at the bottom of the page.

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



Request Role

All fields are required.

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

Module: EDGE Server Management (ESM) ▼

Requested Role: Issuer EDGE Registration Request Approver ▼

Issuer Association

Please enter the HIOS Issuer ID below

Issuer ID : 39528 × Search

Figure 3-13: Enter Issuer ID

5. If all the information entered is correct, click the **Review/Continue** button to process the request.

Issuer Association

Please enter the HIOS Issuer ID below

Issuer ID :

Search Result: 39528 - Kilroys - MN

Figure 3-14: Review/Continue Button

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

Request Role

Please review your selections below, and select 'Submit' to submit the new role request for approval, or select 'Back' to make changes.

Module: **EDGE Server Management (ESM)**
Requested Role: **Issuer EDGE Registration Request Approver**
Selected Issuer: **39528 - Kilroys - MN**

Figure 3-15: Submit Request

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

Request Role

Confirm

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

All fields are required.

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

Module:

Figure 3-16: Confirmation Page



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

Users will need to log back into HIOS and access the **View Existing Role** tab in the **EDGE Server Management (ESM)** module to confirm approval.

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

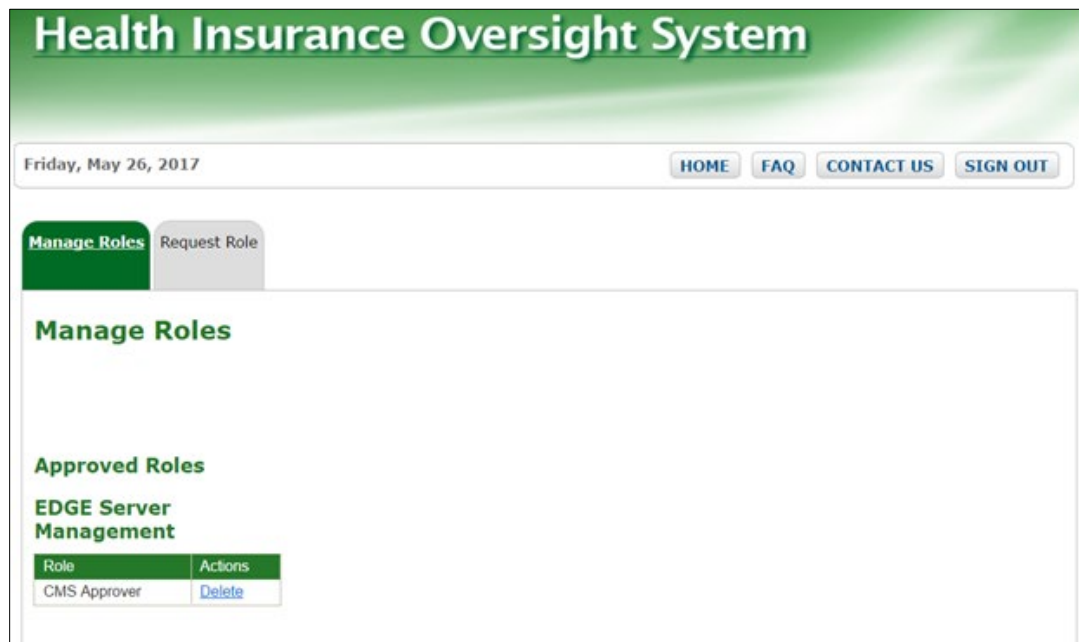


Figure 3-17: View Roles



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

Manage EDGE Server

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

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

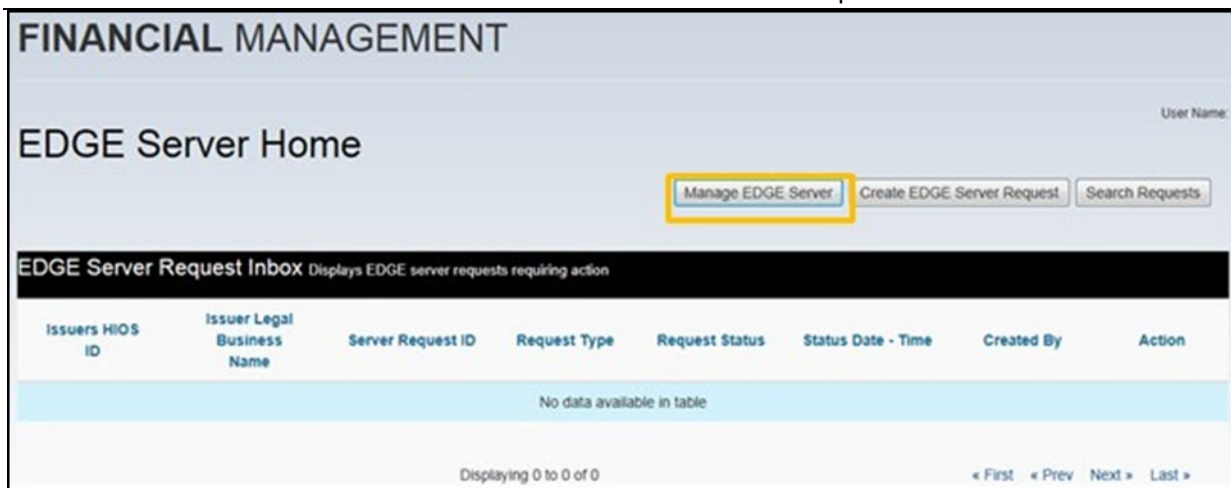


Figure 3-18: Manage EDGE Server Button

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



Figure 3-19: Open Provisioned Request

From the EDGE Request screen, you can update any Points of Contact (POC) or TPA-related information as applicable to your EDGE server.

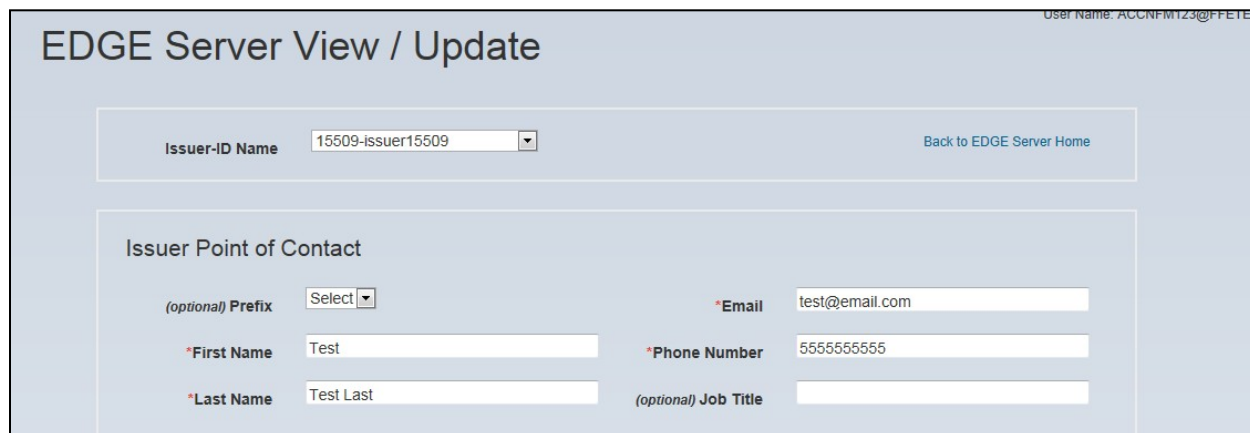


Figure 3-20: EDGE View/Update Screen

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

The screenshot shows the 'Issuer Attestation' page. On the left, there are two buttons: 'Download Attestation Template' and 'Upload Signed Attestation'. In the center, there is a table with two columns: 'Uploaded' and 'File Name'. The table contains two rows of data. At the bottom right, there are two buttons: 'Back' and 'Submit', with the 'Submit' button highlighted by a yellow box.

Uploaded	File Name
09-08-2014	Edge_Reg_Data_Agreement_Template (1).pdf
09-05-2014	Edge_Reg_Data_Agreement_Template.pdf

Figure 3-21: Submit Updates

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

The screenshot shows a dialog box titled 'Initiate EDGE Server Update Request'. The text inside says: 'Select SUBMIT REQUEST to save the updates entered and initiate the approval process or CANCEL to return to the previous page without saving.' At the bottom right, there are two buttons: 'Submit Request' and 'Cancel', with the 'Submit Request' button highlighted by a yellow box.

Figure 3-22: Submit Request Button

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

- POC Update ONLY: If only POC information was updated, the request will only require issuer approval (org approval).

3.3 EDGE Server Contacts

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

CMS requests that issuers maintain an accurate list of contacts for each company through an alternate web form. The EDGE Server Contact Database web page allows CEO designates and Alternate CEO designates to add, edit and replace EDGE server contacts. The [EDGE Server Contact Database User Guide](#) provides a link to the database and is a step-by-step guide to completing the web form.

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

3.4 Server Set Up - On-Premise

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



Figure 3-23: OP Server Set Up

3.4.1 Server Setup

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



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



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

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

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

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

Table 3-2: Server Configuration Based on INTEL CPUs

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

Refer to the table above for recommended volume storage allocation. Depending on the server size, it is recommended to have 100 Giga-Byte (GB) allocated for the operating system. The remaining storage can be allocated to the EDGE home directory (/opt) and MySQL data storage.

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

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

OP EDGE Environment Setup & Configuration

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



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

- Red Hat Enterprise Linux (RHEL) version 7.3 (64 bit)

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

Refer to Section 5.5: EDGE Server Application and Software Stack Version Updates for additional information

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

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

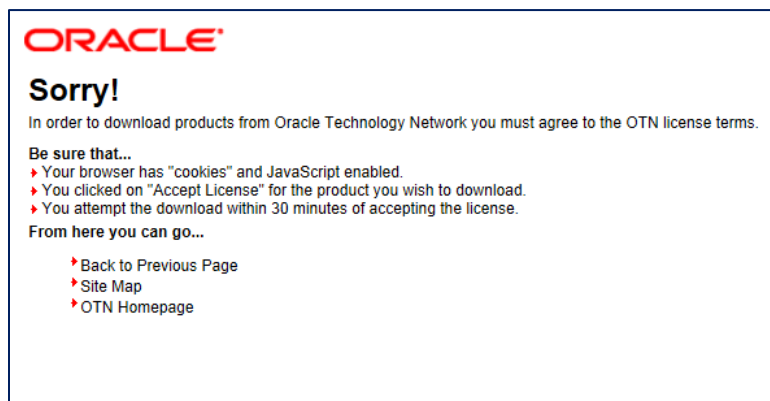


Figure 3-24: Oracle Java Download Page

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

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

Oracle Java should download after executing this command.

4. Issuers may choose to install additional software (monitoring, antivirus, IDS/IPS, etc.) as required by your company's policies.

5. The environment variable, JAVA_HOME, should be configured to point to the directory where Java is installed.
6. Configure users
 - a. Login as **root** and create user “**edgeadm**”.
 - b. Login as system admin and run command:
 - `useradd edgeadm`
 - c. Enter username **edgeadm**
 - d. Enter command
 - `passwd edgeadm`
 - e. Then enter a password
 - f. Ensure the “**edgeadm**” user have read/write/execute access for “**/opt/edge**”. The next steps will configure user “**edgeadm**” to have sudo access.
 - g. Connect to EDGE server as user who has sudo access or as root
 - h. Run the following command to open up **/etc/sudoer** file, which contains the user ID and groups that have sudo access
 - `sudo visudo`
 - i. Navigate to the end of the file
 - j. Insert line
 - `"edgeadm ALL=(ALL) ALL"`
 - k. Save and exit out of vi by pressing the ESC key then the command
 - `:wq`
 - l. For more information, please access the [Red Hat Customer Portal](#).

OP EDGE Server Connectivity

Enable AWS Connectivity

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

Table 3-3: AWS S3 Endpoints

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

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

Please execute the following command to test connectivity:

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

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

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

- **403 - Access Denied:** this could happen if the proxy server has missing credentials.
Resolution: Provide proxy credentials as the URL parameter (refer to curl documentation for proxy parameters: `curl -x PROXY-SERVER:PORT -U USER:PASS URL`)
- **404 - URL not found:** this could happen if your Dominion Name System (DNS) server is unable to resolve the host name to IP address for AWS services.
Resolution: Work with your DNS administrator or service provider to resolve.

Verify MySQL Connectivity

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

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

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

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

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

a. `sudo mysql`

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

3. Run command:

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

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

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

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

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

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

File Directories

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

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

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

Server Hardening

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



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

3.4.2 Server Registration

This section details the steps required to access the CMS EDGE server registration site and submit a request to provision an EDGE server.



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

EDGE Server Registration Overview

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

1. Issuer EDGE Registration Request Submitter
 - a. Create Self-Hosted Server Requests
 - b. Create TPA-Hosted Server Requests
2. TPA EDGE Registration Submitter

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

All issuers and TPAs will need to log into the EDGE Server Registration Site, as detailed in Section 3.2.1: Accessing the ESM Website, to complete a request to provision an EDGE server.

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

- Enter details for two (2) POC (typically server administrators) for the EDGE server they are registering.
- Indicate whether the server is self-hosted or TPA hosted.
- Signed Data Attestation Agreement.

ATTENTION TPAs:



Uploading a TPA Agreement through the EDGE Server Registration Site: Once TPAs have access to the EDGE Server Registration site, please remember to log in and upload your signed TPA Agreement through your EDGE server home page. Before issuers can select their TPA for managing their EDGE server, a signed agreement for the corresponding TPA must be uploaded through the EDGE Server Registration site. If the agreement is not uploaded, the TPA name and HIOS ID will not be available for selection when issuers create EDGE server requests. This document is separate from the data agreement uploaded by the issuer.

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



Issuers setting up an Amazon EDGE server will need to add the following additional AWS specific information. Please refer to Section 3.5.1: AWS Account Setup to obtain the following information, necessary.

- **AWS Account Number** - This is the issuer's AWS account number provided by AWS. This is NOT the CMS Account Number.

- **Key Name** - The name of the SSH key pair that is associated with the issuer's AWS account that will be used to connect to the provisioned EDGE server instance. The Key Pair Name was created when executing Section 3.5.2: Request an AWS EDGE Server Instance. The issuer should have this Key Pair file and name saved to their computer.



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

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

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

- **EDGE Server Size** - The size of the EDGE server. This defines the computing power of the provisioned instance. Please see Section 3.5.1: AWS Account Setup for additional information about size.
 - Small
 - Medium
 - Large

EDGE Server Management Console Server Status Tracking

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

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

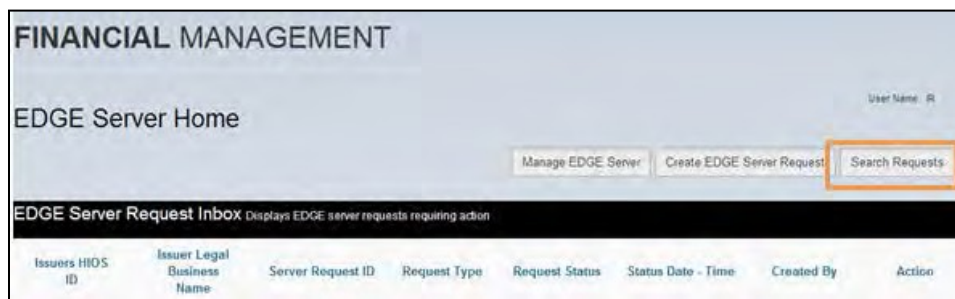


Figure 3-25: Search Requests Button

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

Issuer Legal Business Name	Issuer HIOS ID	TPA ID - Name	EDGE Server Name	AWS Account Number	Request ID	Request Status	Request Type	Last Updated By (HIOS User ID)	Last Updated Date	Action
	39774	42226	AWS39774		7210	Provisioning Failed	New AWS Server	ACCNFM134@FFETEST.COM	8/22/14 5:10:18 PM	view
ABC	99527	42226	Amin2		56060	Provisioned	New AWS Server	CMS	8/25/14 10:40:13 AM	view
	15040	42226			56064	Pending Hosted Server Details	New AWS Server	EDTEST2@FFETEST.COM	8/25/14 11:42:44 AM	view
ABC	99926	42226	Test		106103	CMS Rejected	New AWS Server	CMS	8/26/14 4:50:19 PM	view

Figure 3-26: EDGE Server Request Search Screen

Issuer EDGE Registration Request Submitter (aka: Issuer Submitters)

I. *Create a New EDGE Server Request - SELF-HOSTED*

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

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

Figure 3-27: Create EDGE Server Request Button



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

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

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



During the registration and set-up process in the ESM module, issuers are required to enter contact information. The ESM is no longer the repository used by CMS for contacting issuers with EDGE servers, therefore, the information in the ESM does not need to be maintained or updated after provisioning has been completed. Please see Section 3.3: EDGE Server Contacts for more information.

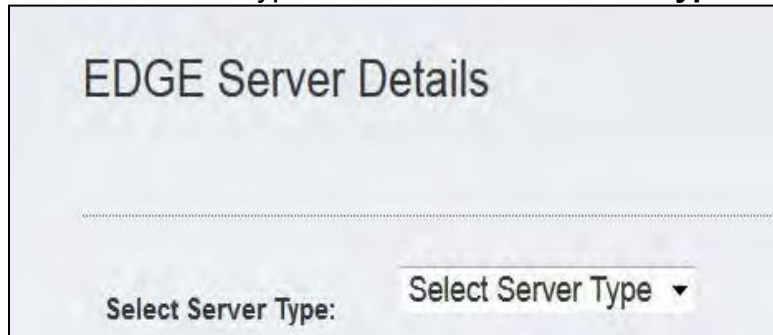
Figure 3-28: EDGE Server Request POC Page

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

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

Figure 3-29: TPA Information

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



The screenshot shows the 'EDGE Server Details' form. At the bottom, there is a label 'Select Server Type:' followed by a dropdown menu that currently displays 'Select Server Type' with a downward arrow.

Figure 3-30: Select Server Type

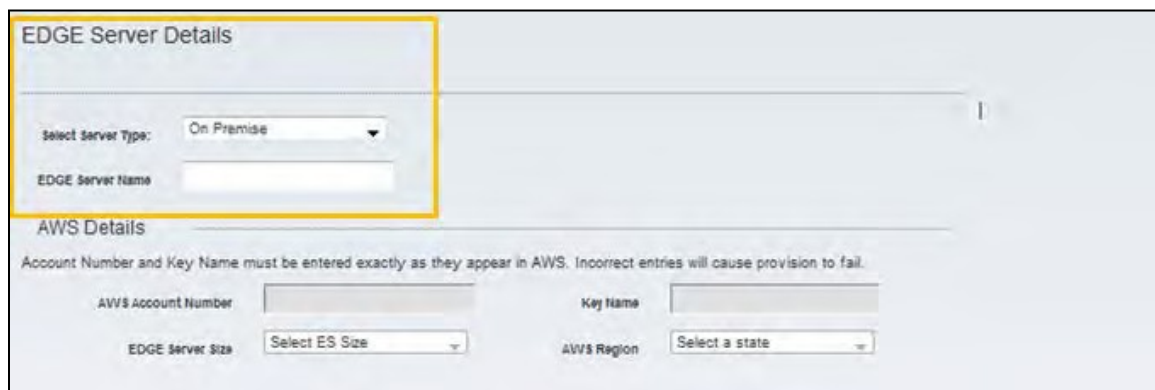
5. Enter a name for their EDGE server in the **EDGE Server Name** field. There is no specific guidance on what to name your server.



The screenshot shows the 'EDGE Server Details' form. The 'Select Server Type' dropdown is set to 'AWS'. Below it, the 'EDGE Server Name' text field contains the text 'AWS Server' and is highlighted with a yellow border.

Figure 3-31: EDGE Server Name

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



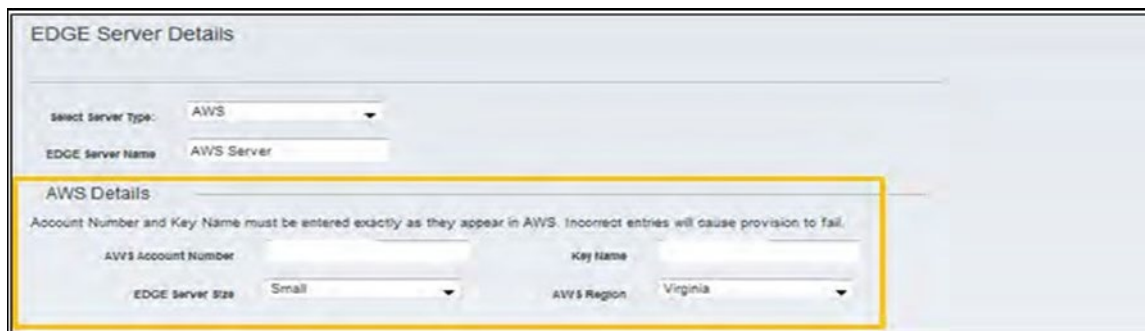
The screenshot shows the 'EDGE Server Details' form. The 'Select Server Type' dropdown is set to 'On Premise'. Below it, the 'EDGE Server Name' text field is empty. A yellow box highlights the 'Select Server Type' dropdown and the 'EDGE Server Name' field. Below this, the 'AWS Details' section is visible, which includes a warning message: 'Account Number and Key Name must be entered exactly as they appear in AWS. Incorrect entries will cause provision to fail.' This section contains four fields: 'AWS Account Number', 'Key Name', 'EDGE Server Size' (with a dropdown menu), and 'AWS Region' (with a dropdown menu).

Figure 3-32: On-Premise Server Details

Issuers setting up an Amazon EDGE server will need to add the following additional AWS specific information.

- AWS Account Number
- Key Name
- AWS Region
- EDGE Server Size

Please refer to the EDGE Server Registration Overview in the beginning of this section, Section 3.4.1: Server Setup to obtain the following information, if necessary.



EDGE Server Details

Select Server Type: AWS

EDGE Server Name: AWS Server

AWS Details

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

AWS Account Number: [Text Field] Key Name: [Text Field]

EDGE Server Size: Small AWS Region: Virginia

Figure 3-33: AWS Details

6. After entering all EDGE Server details, upload the **Issuer Attestation Agreement** for the request. This agreement must be uploaded for every EDGE Server Request submitted.

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



Issuer Attestation

Download Attestation Template Upload Attestation Download Signed Data Attestation

Back Save Submit Request

Comments History

Comment	User	Date - Time
---------	------	-------------

Figure 3-34: Download Attestation Agreement Template

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

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



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

Figure 3-35: Save Request

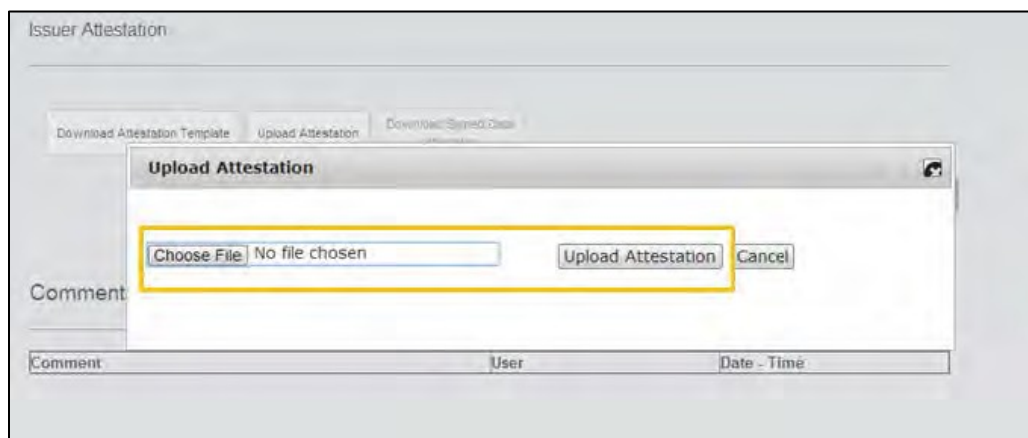
8. Scroll down to the bottom of the request screen and click the **Upload Attestation** button.



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

Figure 3-36: Upload Attestation Agreement

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



The screenshot shows the 'Upload Attestation' dialog box. It has a title bar with a close button. Inside, there is a 'Choose File' button, a text field displaying 'No file chosen', an 'Upload Attestation' button, and a 'Cancel' button. The 'Choose File' button is highlighted with a yellow border. The background shows the 'Issuer Attestation' interface with the 'Upload Attestation' button highlighted.

Figure 3-37: Attach and Upload Attestation Agreement

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

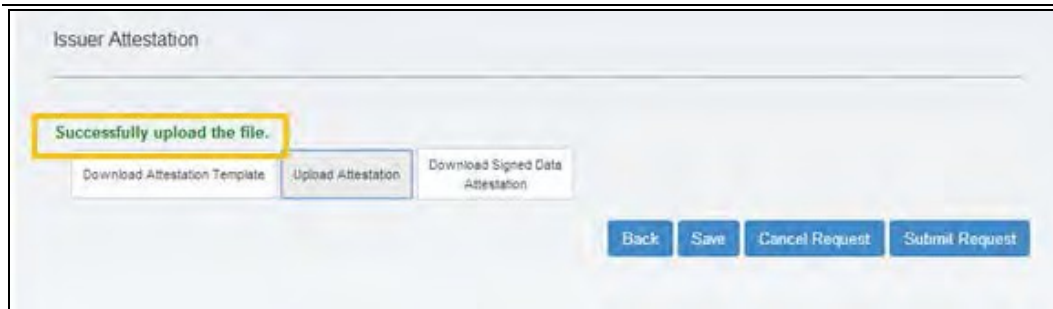


Figure 3-38: Successfully Uploaded the File Message

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

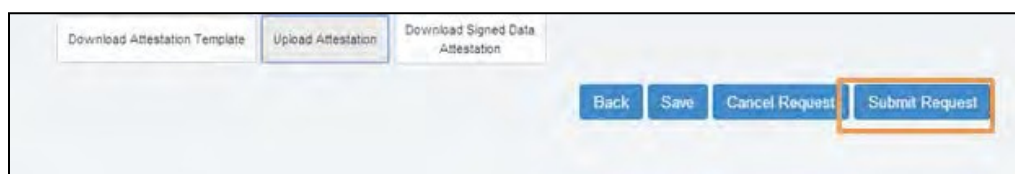


Figure 3-39: Submit Request

11. Once submitted, Issuer Submitters will be taken back to their homepage.

The request is now sent to the Issuer Approver for review and approval. Issuer Submitters can track the status of their request using the **Search Requests** function. Refer to the IV **Track Request Status** section for how to search for requests.



Figure 3-40: Homepage

II. *Create a New EDGE Server Request - TPA-HOSTED*

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



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

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

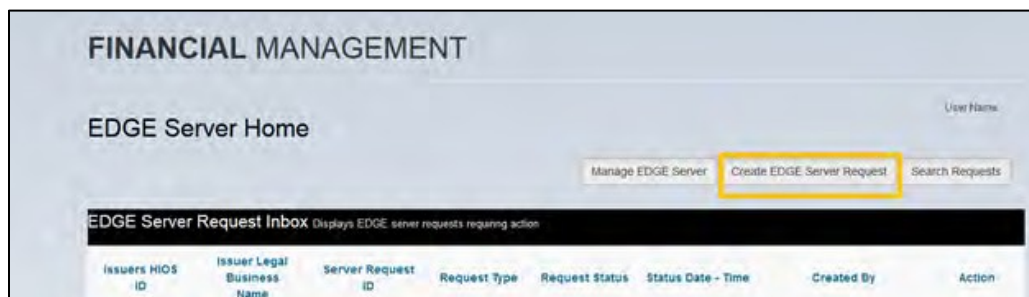


Figure 3-41: Create EDGE Server Request Button

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



During the registration and set-up process in the ESM module, issuers are required to enter contact information. The ESM is no longer the repository used by CMS for contacting issuers with EDGE servers, therefore, the information in the ESM does not need to be maintained or updated after provisioning has been completed. Please see Section 3.3: EDGE Server Contacts for more information.

Figure 3-42: EDGE Server Request POC Page

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

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



Figure 3-43: Select TPA



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

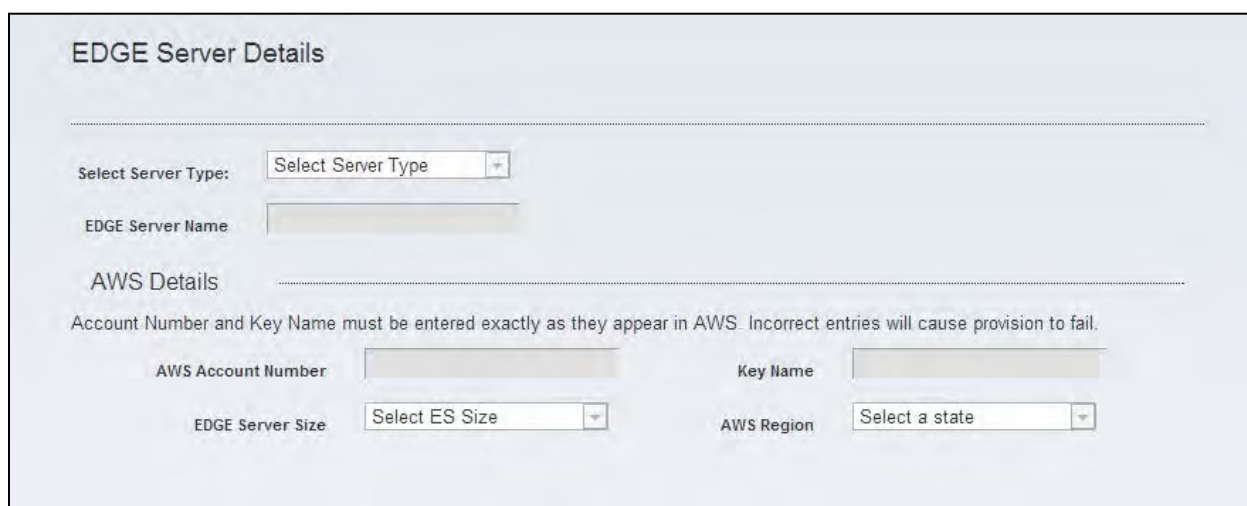


Figure 3-44: EDGE Server Details

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

4. After indicating the EDGE server will be TPA hosted, upload the **Issuer Attestation Agreement** for the request.
 - a. Download the template by selecting the **Download Attestation Template** button



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

Figure 3-45: Download Attestation Agreement Template

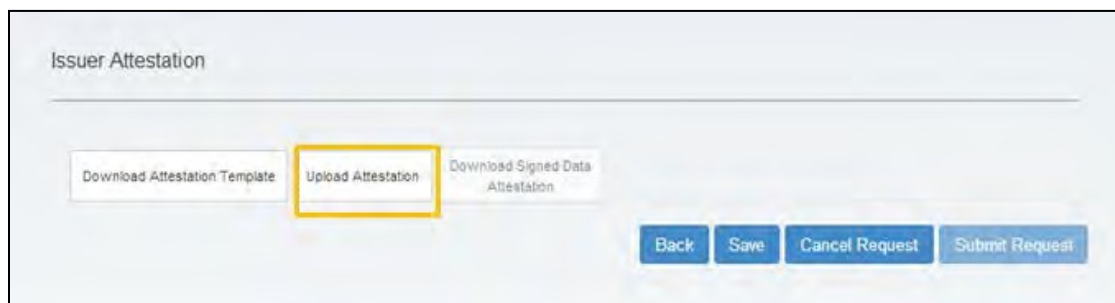
- b. A pop-up window will appear asking to download a PDF document. Download the template, review and sign the agreement and save the document for uploading.
- c. Before uploading the **Issuer Attestation Agreement**, click the **Save** button to save enable the **Upload Attestation** button.



The screenshot shows the 'Issuer Attestation' interface. The buttons 'Download Attestation Template', 'Upload Attestation', and 'Download Signed Data Attestation' are visible. The 'Save' button (highlighted with a yellow box) is now active and highlighted in blue, while 'Back' and 'Submit Request' are also blue. The 'Comments History' table is at the bottom.

Figure 3-46: Save Request

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



The screenshot shows the 'Issuer Attestation' interface. The 'Upload Attestation' button (highlighted with a yellow box) is now active and highlighted in blue. The 'Back', 'Save', 'Cancel Request', and 'Submit Request' buttons are also visible at the bottom right.

Figure 3-47: Upload Attestation Agreement

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

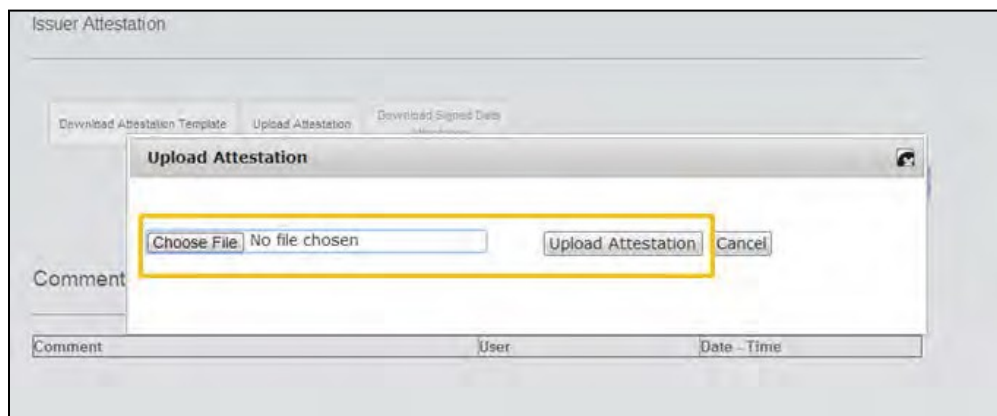


Figure 3-48: Attach and Upload Attestation Agreement

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

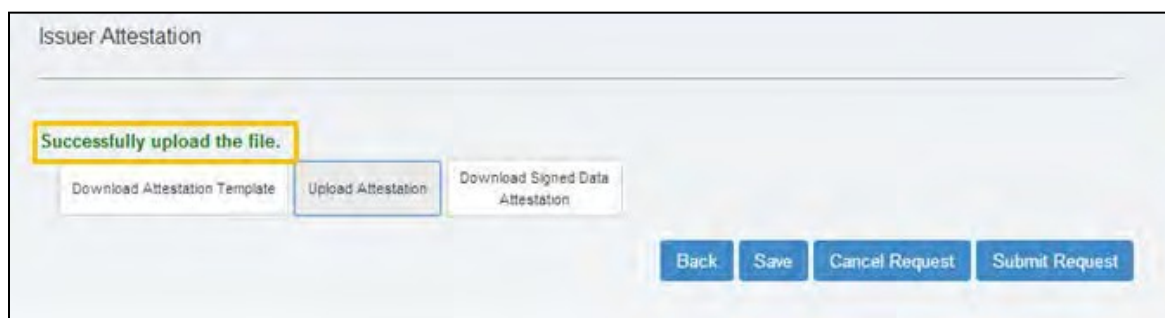


Figure 3-49: Successfully Uploaded the File Message

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



Figure 3-50: Submit Request

Issuer Submitters will be taken back to their homepage.

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

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

III. *Updating a Rejected Request*

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



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

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

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

Showing 1 to 3 of 3 entries

Figure 3-51: Rejected Requests in Issuer EDGE Registration Request Submitter's Inbox

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

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

Figure 3-52: Open Request

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

IV. *Track Request Status*

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

- Self-Hosted
- TPA-Hosted

Table 3-4: Self-Hosted Path

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

Table 3-5: TPA-Hosted Path

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

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

TPA EDGE Registration Submitter

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



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

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

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

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

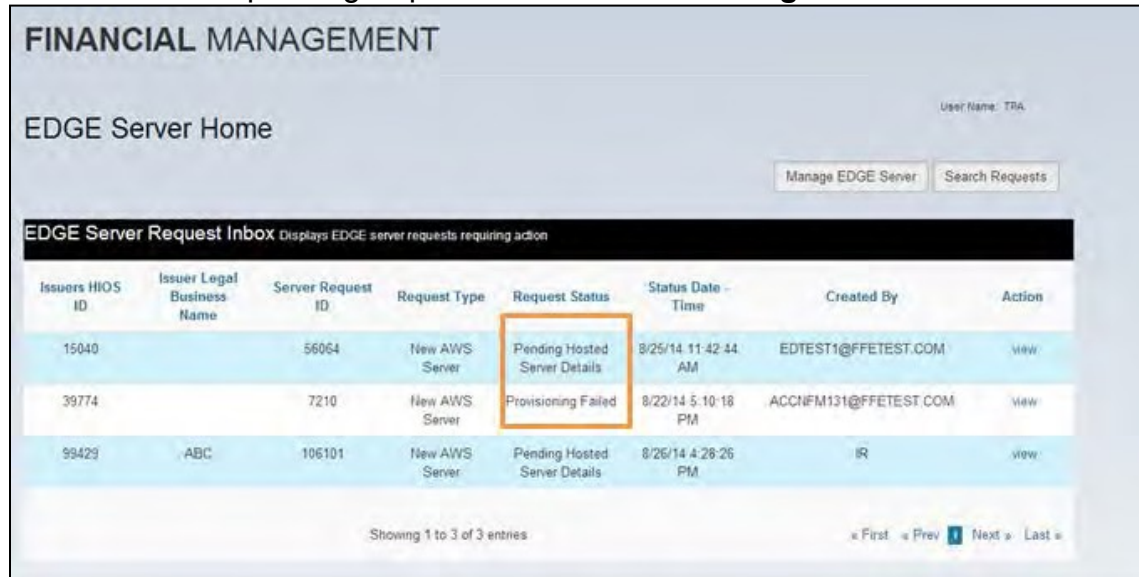


Figure 3-53: TPA EDGE Registration Submitter Homepage

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



TPA EDGE Registration Submitters will need to upload a TPA Attestation Agreement for every issuer they are hosting.

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



Figure 3-54: Download TPA Attestation Agreement Template

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

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

Manage TPA Agreement

Select TPA

TPA ID - Name
42226

Download Signed TPA Agreement

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

Download TPA Attestation Template Upload Signed TPA Attestation

Figure 3-55: Upload Signed TPA Attestation Agreement

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

Data Agreement

Choose File No file chosen Upload Attestation Cancel

Figure 3-56: Upload Attestation Agreement



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

Download Signed TPA Agreement

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

Download TPA Attestation Template Upload Signed TPA Attestation

Figure 3-57: Uploaded Attestations Agreement

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

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



Figure 3-58 Select to View Request

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

The screenshot shows a form titled 'TPA Information' with the following sections:

- TPA Information:**
 - Will this be a TPA hosted EDGE Server: ☒ yes ☐ no
 - Select TPA: By Name and HIOS ID
 - TPA Name - Paul Test Email TST (dropdown menu)
- EDGE Server Details:**
 - Select Server Type: Select Server Type (dropdown menu)
 - EDGE Server Name: (text input field)
- AWS Details:**
 - Account Number and Key Name must be entered exactly as they appear in AWS. Incorrect entries will cause provision to fail.
 - AWS Account Number: (text input field)
 - Key Name: (text input field)
 - EDGE Server Size: Select ES Size (dropdown menu)
 - AWS Region: Select a state (dropdown menu)

Figure 3-59: TPA EDGE Registration Submitters Request

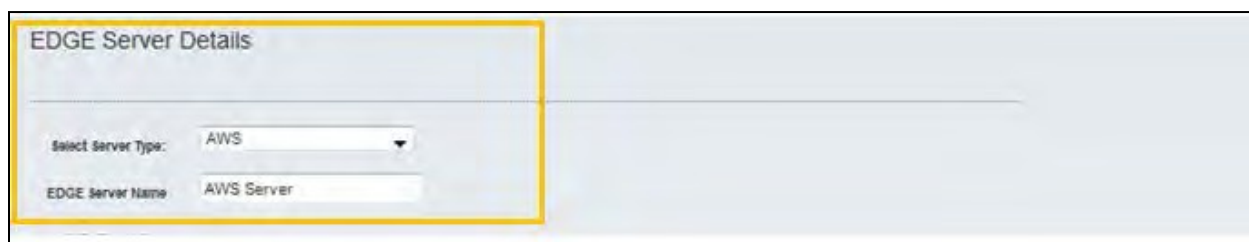


EDGE Server Details

Select Server Type:

Figure 3-60: Select Server Type

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



EDGE Server Details

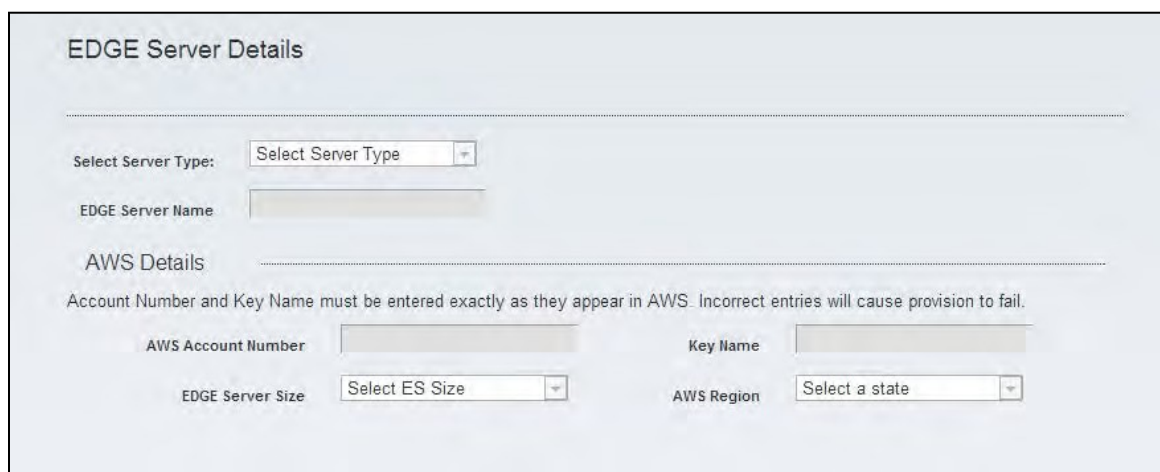
Select Server Type:

EDGE Server Name:

Figure 3-61: EDGE Server Name

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

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



EDGE Server Details

Select Server Type:

EDGE Server Name:

AWS Details

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

AWS Account Number: Key Name:

EDGE Server Size: AWS Region:

Figure 3-62: AWS Server Details

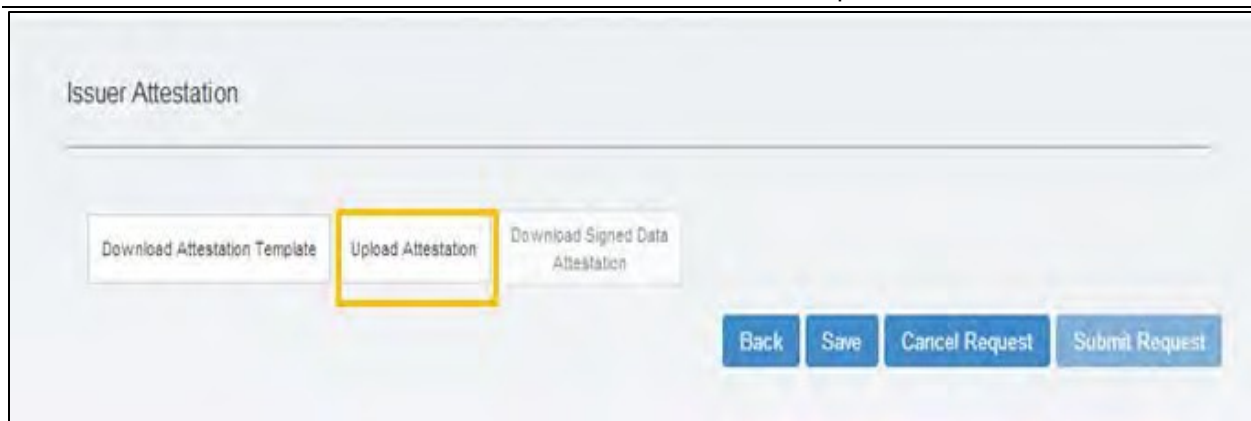


Figure 3-63: AWS Details

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

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

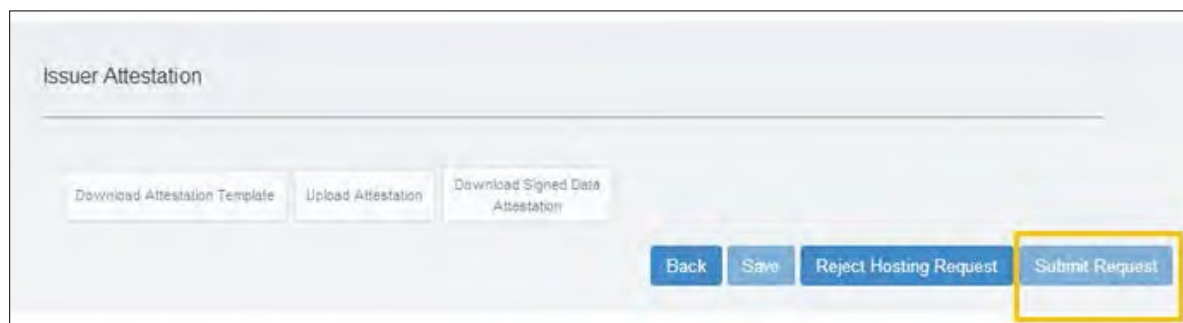


Figure 3-64: Submit Button

V. *Updating a Rejected Request*

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

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

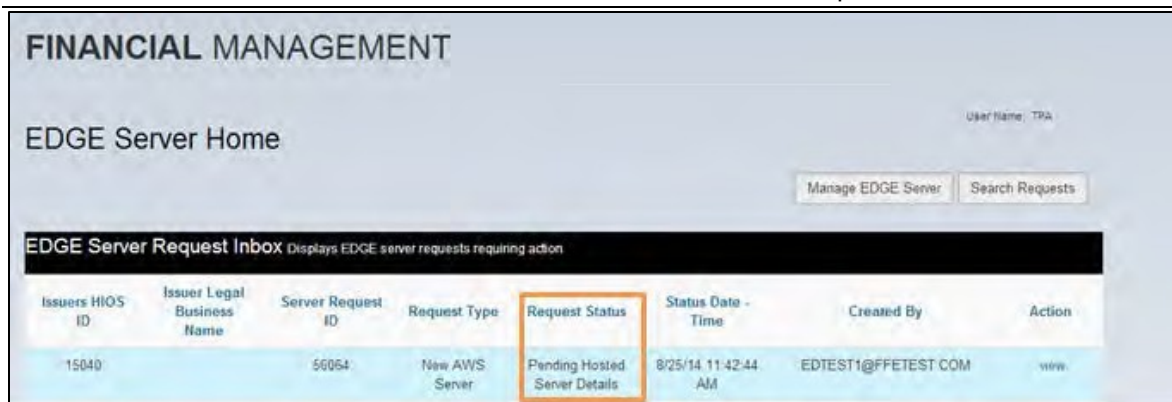


Figure 3-65: Rejected Requests in Submitter's Inbox

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



Figure 3-66: Open Request

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

VI. Track Request Status

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

Table 3-6: TPA-Hosted Path

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

Step	Request Status
4. Approved by CMS and provisioning pending	Pending Provisioning



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

TPA Submitters can track the status of their request using the **Search Requests** button to open the search request screen.

Confirm the request has a status of “Pending Provisioning” and continue to Section 3.4.3: On-Premise EDGE Server Provisioning for On Premise servers or Section 3.5.4: AWS EDGE Server Provisioning for AWS servers.

Issuer EDGE Registration Request Approver

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



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

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

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

FINANCIAL MANAGEMENT

EDGE Server Home

User Name: JA

Manage EDGE Server Search Requests

EDGE Server Request Inbox Displays EDGE server requests requiring action

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

Showing 1 to 3 of 3 entries

« First « Prev 1 Next » Last »

Figure 3-67: Issuer EDGE Registration Request Approver Homepage

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

FINANCIAL MANAGEMENT

EDGE Server Home

User Name: JA

Manage EDGE Server Search Requests

EDGE Server Request Inbox Displays EDGE server requests requiring action

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

Figure 3-68: Open Request

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

The screenshot shows a web form titled "FINANCIAL MANAGEMENT" with a sub-header "EDGE Server Request Approval". In the top right corner, it says "User Name: VA". Below the header, there is a "Back to EDGE Server Home" link. The form contains several input fields: "Issuer ID Name" with a dropdown menu showing "99427-issuer99427", "Request ID" with a text box containing "106100", and "Request Status" with a text box containing "PENDING_ORG_APPROVAL". Below these fields is a section titled "Issuer Point of Contact" with a note: "All fields marked with an asterisk[*] are required." This section is divided into two parts: "Primary Point of Contact" and "Secondary Point of Contact". Each part has fields for "Prefix" (dropdown menu), "First Name", "Last Name", "Email", "Phone Number", and "Job Title". The "Primary Point of Contact" fields are filled with "Mr", "TestFirst", "TestLast", "email@tst.com", "3017402313", and "Manager". The "Secondary Point of Contact" fields are filled with "Mr", "SecondFirst", "SecondLast", "dsa@yahoo.com", "2402348241", and "PM". At the bottom left of the form, there is a link labeled "Additional POCs".

Figure 3-69: Request Approval

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

Comment	User	Date - Time
---------	------	-------------

New Comments:
Rejecting this request

Back Download Signed Issuer Attestation Approve Request **Reject Request**

Status History

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

Figure 3-70: Reject Request

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

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

Back Download Signed Issuer Attestation **Approve Request** Reject Request

Status History

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

Figure 3-71: Approve Request

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

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



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

- TPA-Hosted: Request will move to TPA Submitter's inbox for processing.
- Issuer Approvers can track the status of their request, using the **Search Requests** button to open the search request screen.

3.4.3 On-Premise EDGE Server Provisioning

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

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

OP EDGE Server Provisioning

I. *Download Installation Scripts*

Once an OP EDGE server request has been approved by CMS, the request will return to the Issuer Submitter's inbox with a status of **Pending Provisioning**. This indicates servers may begin the provisioning process. The following steps explain how to access the installation scripts to complete the provisioning process.

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

FINANCIAL MANAGEMENT							
EDGE Server Home							
Manage EDGE Server Create EDGE Server Request Search Requests							
EDGE Server Request Inbox displays EDGE server requests requiring action							
Issuers HIOS ID	Issuer Legal Business Name	Server Request ID	Request Type	Request Status	Status Date - Time	Created By	Action
10297		106183	New Server Request	Pending Provisioning	9/15/14 10:05:04 AM	ZFMLOADTEST1991	view

Figure 3-72: Pending Provisioning

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

Issuer Submitter's inbox. The Issuer Submitter will need to Search for the request at this point to see the status of Provisioning in Progress.

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



Figure 3-73: Search Requests Button

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

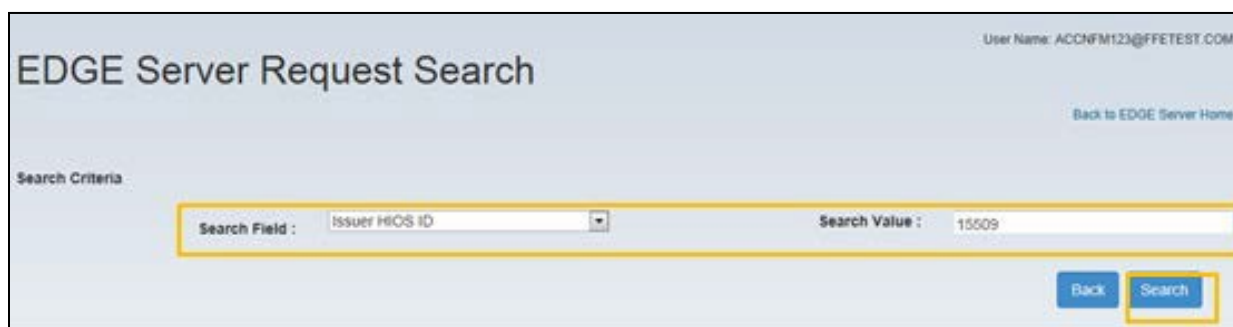


Figure 3-74: Search Request Screen

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

FINANCIAL MANAGEMENT

User Name: ZFMLOADTEST1991

EDGE Server Request Search

Back to EDGE Server Home

Search Criteria

Search Field: Issuer HROS ID Search Value: 10297

Back Search

Issuer Legal Business Name	Issuer HROS ID	TPA Name	EDGE Server Name	AWS Account Number	Request ID	Request Status	Request Type	Last Updated By (HROS User ID)	Last Updated Date	Action
	10297		Test1		106183	Provisioning In Progress	New Server Request	ZFMLOADTEST6236	9/15/14 11:05:54 AM	View

Figure 3-75: Provisioning in Progress

4. Download links for the three (3) files for OP EDGE server installation:

- Installation Information
- Deployment Script
- Property File

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

FINANCIAL MANAGEMENT

User Name: ZFMLOADTEST1991

EDGE Server Request

Back to EDGE Server Home

Issuer ID Name: 10297 Request ID: 106183

Request Status: PROVISIONING IN PROGRESS

The EDGE server request has been approved. Use the links below to download provisioning script and property file required to provision the server. Refer to www.regap.info for installation and setup instructions.

Download On-Premise Installation Information

Deployment Script: Download On-Premise Deployment Script

Property File: Download On-Premise Property File

Figure 3-76: Download Provisioning Installation Scripts

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

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

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

I. Download WinSCP

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

1. Go to www.winscp.net.
2. Click the **Go to Download Page** link.

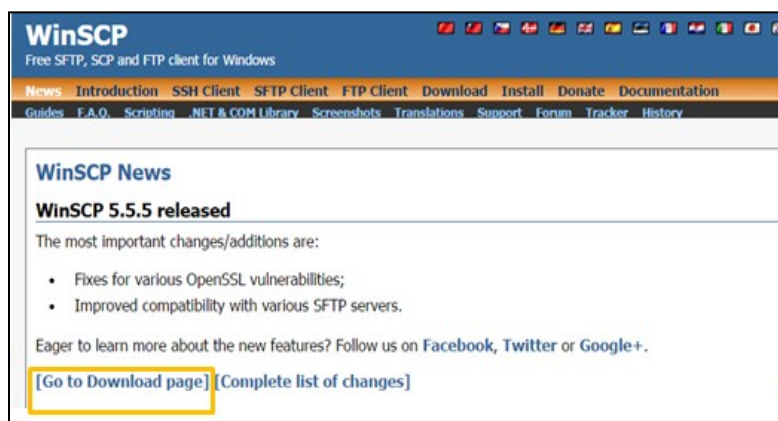


Figure 3-77: Go to Download Page Link

3. Click the **Download WinSCP** link at the top.



Figure 3-78: Download WinSCP

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

Download WinSCP	
WinSCP 5.5.5	
Installation package (4.4 MiB; 247,655 downloads to date)	Released: 2014-08-21
Portable executables (4.2 MiB; 52,630 downloads to date)	
.NET assembly / COM library (0.1 MiB; 2,370 downloads to date)	
Source code (9.6 MiB; 1,566 downloads to date)	
[Release Notes, Checksums] [What's New] [Release Notifications]	

Figure 3-79: Download Installation Package

II. Run WinSCP

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

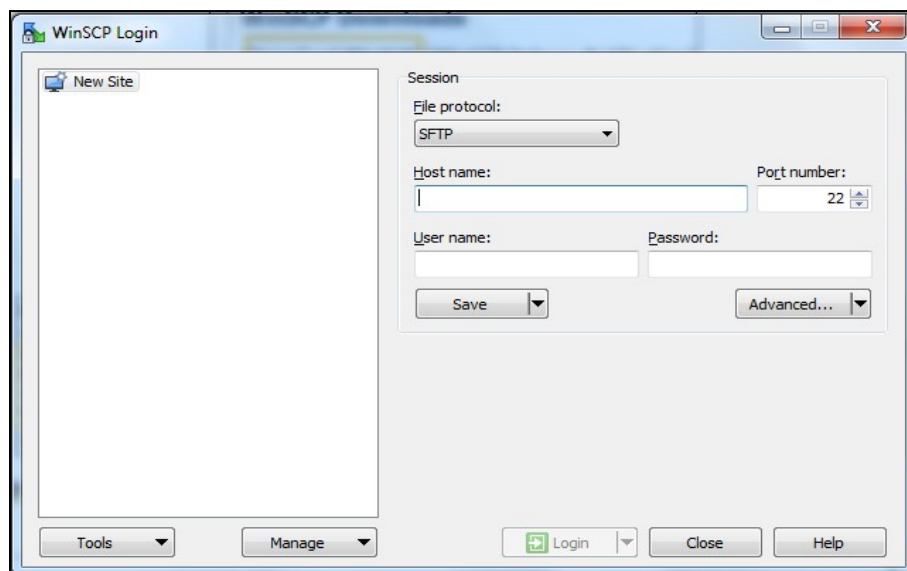


Figure 3-80: WinSCP Login Screen

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

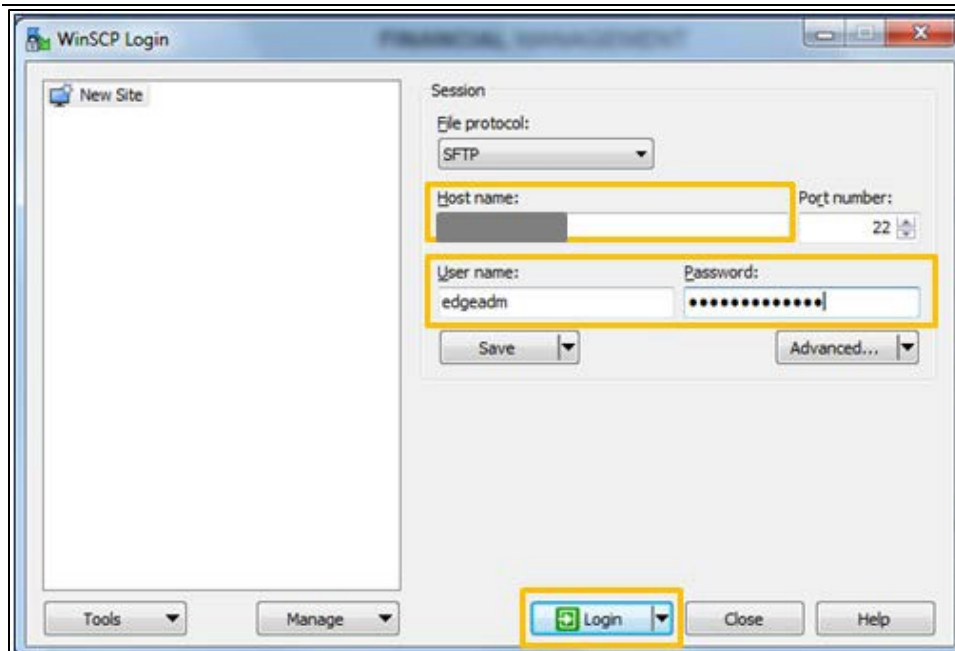


Figure 3-81: WinSCP Login Information

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

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

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

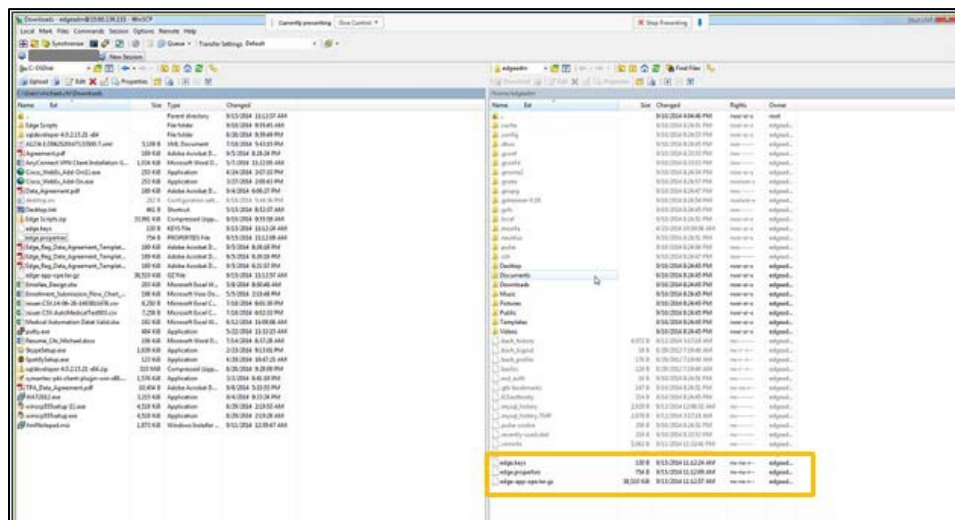


Figure 3-82: WinSCP Files and Folders

III. Download PuTTY

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

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

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

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

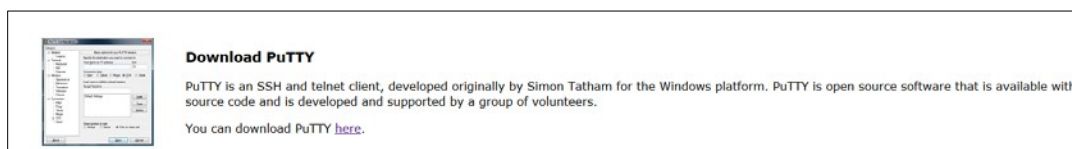


Figure 3-83: PuTTY Home Page

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



Figure 3-84: PuTTY Download Page

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

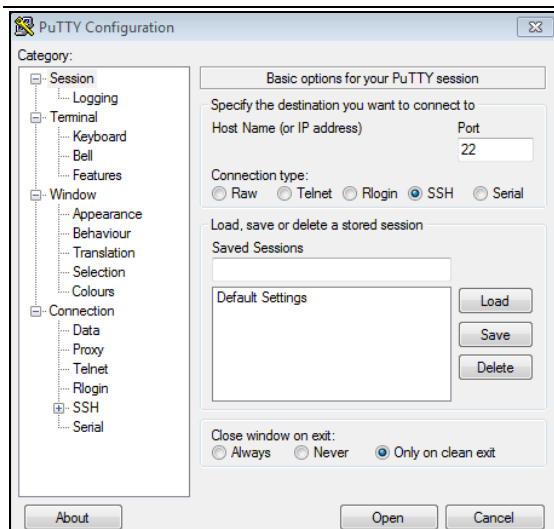


Figure 3-85: PuTTY Configuration Window

Run PuTTY.exe

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

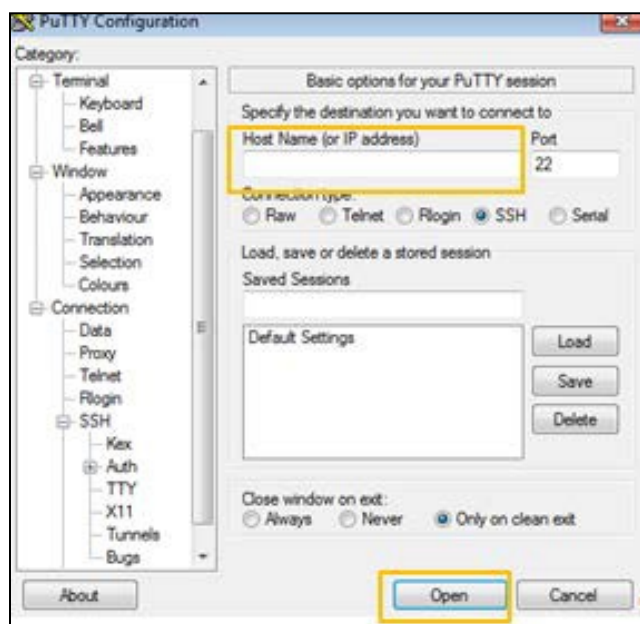


Figure 3-86: PuTTY Configuration - Add IP Address

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

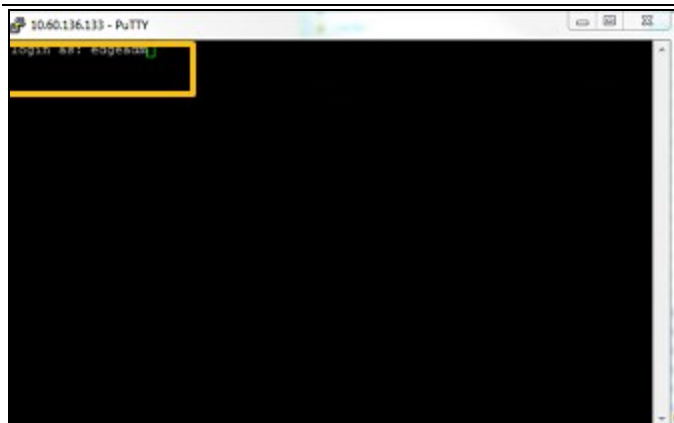


Figure 3-87: Enter Username for PuTTY

Enter your password and then click enter.

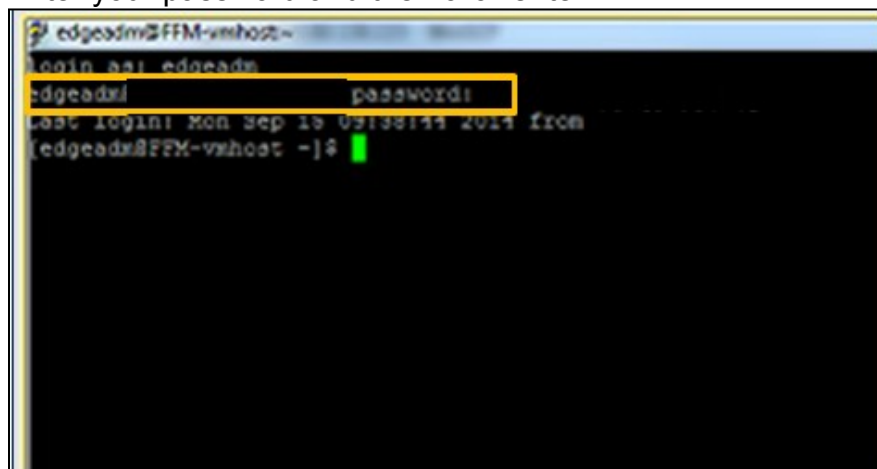


Figure 3-88: Enter Password for PuTTY

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



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

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

- mkdir edge

and click **Enter**.

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

- ls -l

and click **Enter**.

```

[edgeadm@FFM-vrhost ~]$ mkdir edge
[edgeadm@FFM-vrhost ~]$ ls -l
total 38536
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Desktop
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Documents
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Downloads
drwxrwxr-x 2 edgeadm edgeadm 4096 Sep 15 11:36 edge
-rw-rw-r-- 1 edgeadm edgeadm 39434240 Sep 15 11:12 edge-app-opc.tar.gz
-rw-rw-r-- 1 edgeadm edgeadm 130 Sep 15 11:12 edge.keys
-rw-rw-r-- 1 edgeadm edgeadm 754 Sep 15 11:12 edge.properties
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Music
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Pictures
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Public
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Templates
drwxr-xr-x 2 edgeadm edgeadm 4096 Sep 10 20:24 Videos
[edgeadm@FFM-vrhost ~]$
  
```

Figure 3-89: Create EDGE folder and Open Files

- Enter command:

- cd edge

and then click **Enter**.

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

```

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

Figure 3-90 Open EDGE Folder

- Enter command:

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

and click **Enter**.

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

```

edge@edge-RTM-vmhost edge]$ jar xvf ~/edge-app-cpe.tar.gz
...
bin/edge
config/
config/logback.xml
ingest/
  ingest/inbox/
  ingest/outbox/
install/
  install/1.CREATE_DATABASE_OBJECTS.sql
  install/hosts
  install/installApplication.sh
  install/issuer
  install/network
lib/
  lib/afp-common-4.5.0.jar
  lib/annex-0.5.0.jar
  lib/aspelliance-1.0.jar
  lib/aws-java-sdk-1.7.11.jar
  lib/bah-2.0b4.jar
  lib/cglib-nodep-2.2.2.jar
  lib/classmate-1.0.0.jar
  lib/commons-beanutils-1.9.1.jar
  lib/commons-codec-1.3.jar
  lib/commons-collections-3.2.1.jar
  lib/commons-configuration-1.7.jar
  lib/commons-dbcp-1.4.jar
  lib/commons-digester-1.8.1.jar
  lib/commons-io-2.4.jar
  lib/commons-lang-2.3.jar
  lib/commons-logging-1.1.1.jar
  lib/commons-pool-1.5.4.jar
  lib/easyMock-3.2.jar
  lib/edge-application.jar

```

Figure 3-91: Unzip On-Premise Installation Information File

6. Next, enter command:

- `cd config/`

and click **Enter**.

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

```

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

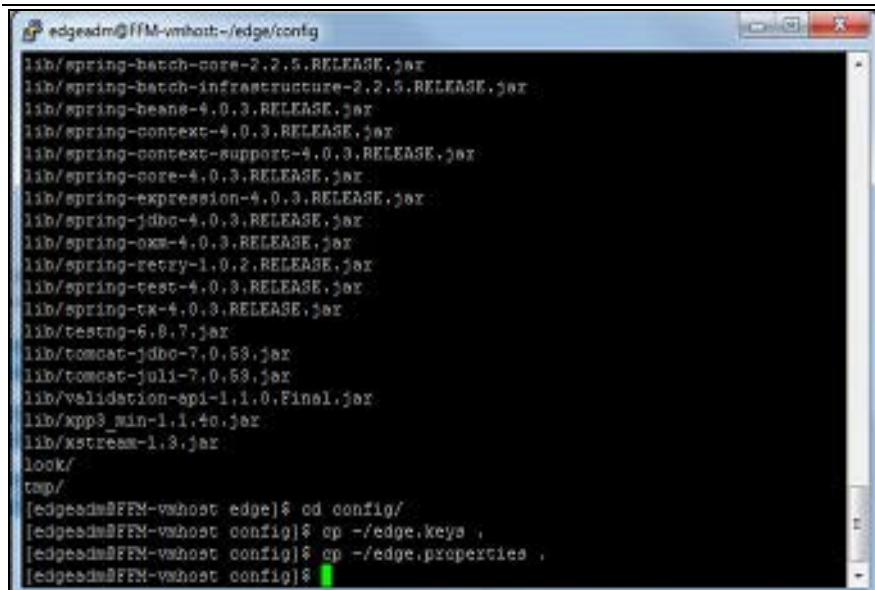
```

Figure 3-92 Open Config Folder

7. Enter commands:

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

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



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

Figure 3-93: Open Deployment Script and Property File

8. Next, enter command:

- vi edge.properties

then click **Enter**.

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

```

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

```

Figure 3-94: Open Properties File in Editable Format

9. Enter

- i

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

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

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



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

```

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

```

Figure 3-95: Enter New Password for Database

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

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

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

1. Execute the following command:

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

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

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

Figure 3-96: edgeserver_size field

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

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

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

- a. Run the following command:

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

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

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

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

Figure 3-97: Add/Modify EDGE Properties

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

- `:wq`

and click **Enter**.

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

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

Figure 3-98: Save File and Exit

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

Enter command:

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

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

- `cd ../install/`

and click **Enter**.

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

Figure 3-99: Open Install Folder



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

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

15. Enter command:

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

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

The EDGE Application will now install and create the following:

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



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

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

Figure 3-100: Install EDGE Application

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

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

```

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

```

Figure 3-101: Confirm Successful Provisioning

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

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

```

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

```

```

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

```

Figure 3-102: MySQL Data Dump Commands

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

- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_COMMON
- CREATE DATABASE EDGE_SRVR_<ISSUER ID>_TEST

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

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

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

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

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

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

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

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

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

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

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

Figure 3-103: Create Databases

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

- edgeapp_<ISSUER ID>

```

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

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

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

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

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

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

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

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

```

Figure 3-104: Create New Database User

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

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

```

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

```

Figure 3-105: Load Data to New Tables

IV. Configure CRON

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

In PuTTY, enter command:

- `crontab -e`

and press **Enter**.

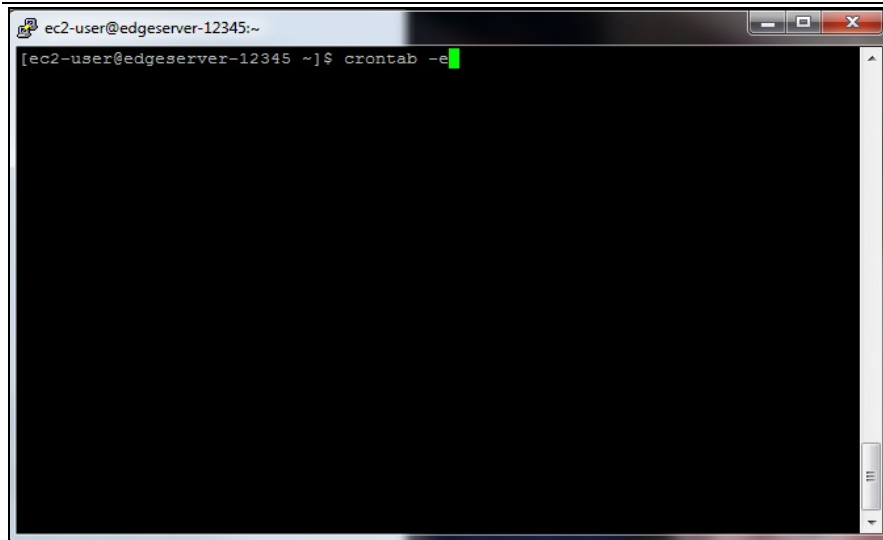


Figure 3-106: Enter CRON Command

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

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

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

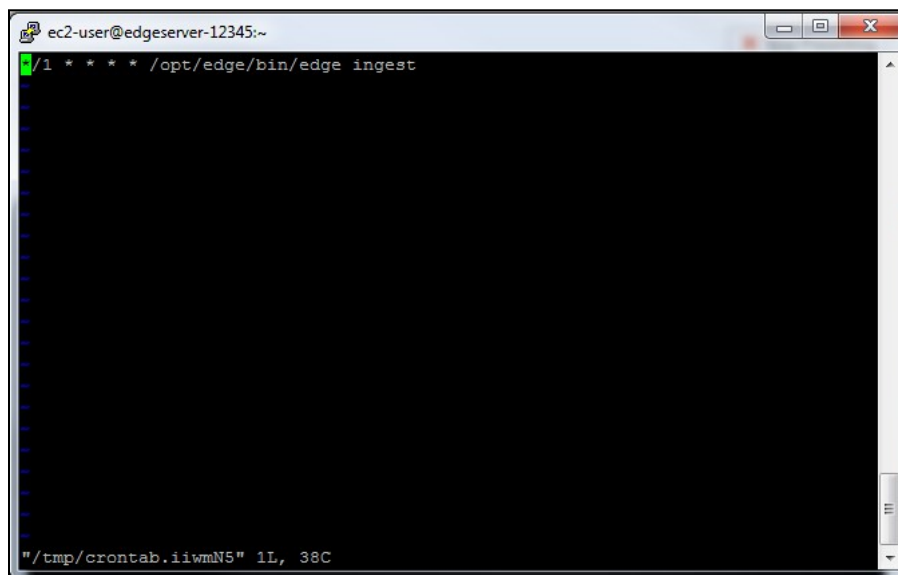


Figure 3-107: Configure Cron Timing

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

- :wq

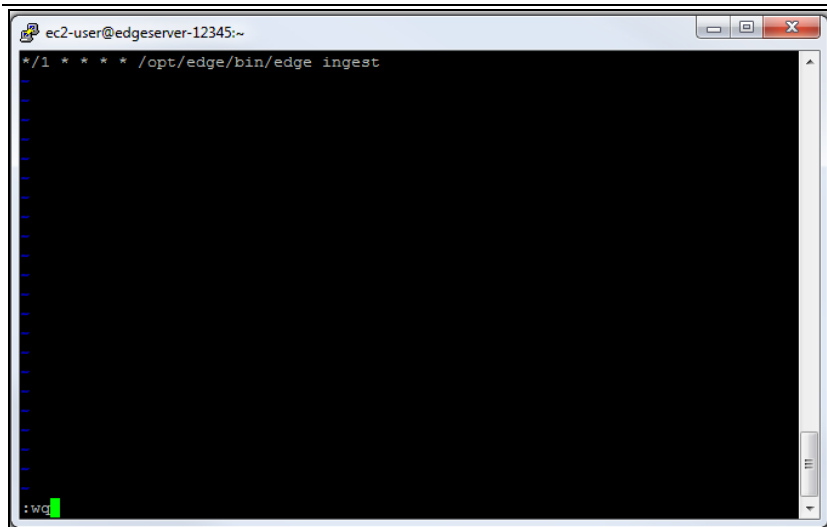


Figure 3-108: Save and Exit Cron

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



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

FINANCIAL MANAGEMENT

EDGE Server Request Search

User Name: ZFMLOADTEST1991

Back to EDGE Server Home

Search Criteria

Search Field : Issuer HIOS ID

Search Value : 10297

Back Search

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

Figure 3-109: Confirm Provisioned Request

V. Provisioning Failed

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



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

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

3.5 Server Set-Up - AWS

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



Figure 3-110: AWS Setup Flow

3.5.1 AWS Account Setup

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



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

In addition to the instructions in this section, an Amazon developed YouTube video on “Creating an Amazon Web Services Account” is accessible via the following link:
<https://www.youtube.com/watch?v=WviHsoz8yHk>



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

In addition, in the event an issuer must transfer hosting to or from a TPA, ownership of the AWS account must be transferred as well. The steps to complete a server migration is provided in more detail in Section 3.6: Migration.

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

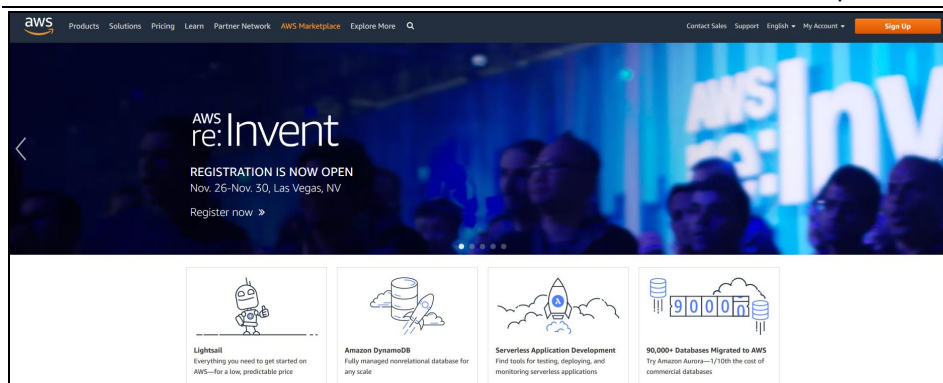


Figure 3-41: Amazon Web Services

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

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

Figure 3-52: AWS Create Account Screen

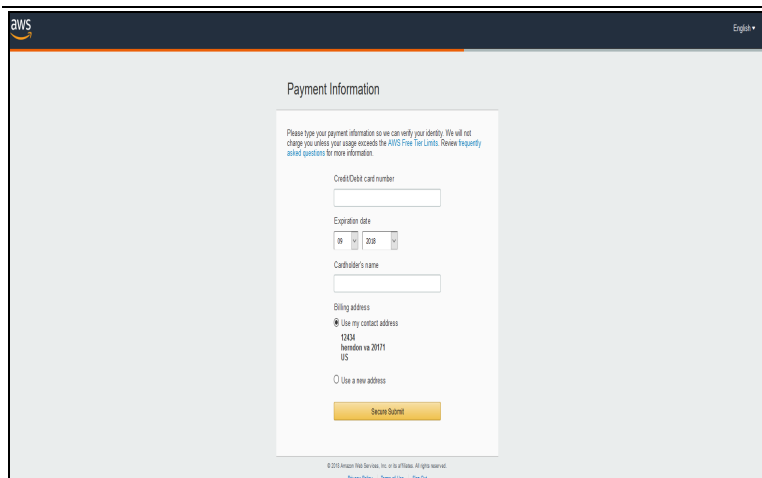
3. At the “**Login Credentials**” screen, click on “Create a new AWS account.”

Figure 3-113: Create a New AWS Account

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

Figure 3-114: Enter in Contact Information

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



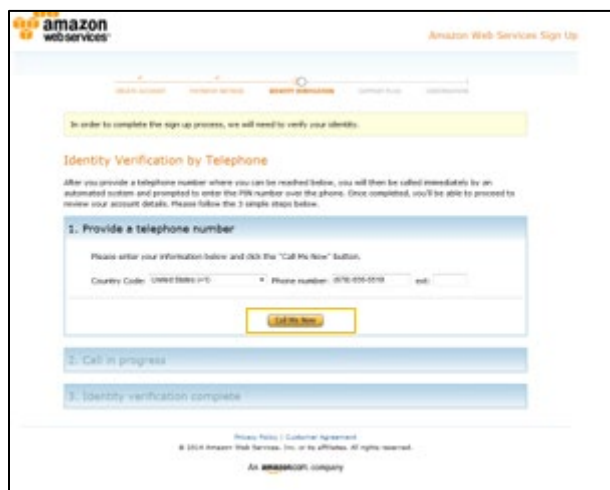
The screenshot shows the AWS 'Payment Information' form. At the top, it says 'Payment Information' and includes a disclaimer: 'Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the AWS Free Tier Limits. Review frequently asked questions for more information.' The form contains the following fields: 'Credit/Debit card number' (a text input), 'Expiration date' (two dropdown menus for month and year, with '08' and '2018' selected), and 'Cardholder's name' (a text input). Below these is the 'Billing address' section with two radio buttons: 'Use my contact address' (which is selected) and 'Use a new address'. Under the selected radio button, the address is listed as '1234 London rd 2017 US'. At the bottom of the form is a yellow 'Secure Submit' button. The footer of the page includes the copyright notice '© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy', 'Terms of Use', and 'Sign Out'.

Figure 3-115: Enter in Payment Information



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

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



The screenshot shows the 'Amazon Web Services Sign Up' page, specifically the 'Identity Verification by Telephone' step. At the top, there is a progress bar with four steps: 'CREATE AN ACCOUNT', 'CHOOSE A SERVICE', 'VERIFY YOUR IDENTITY' (which is the current step), and 'CONFIRM YOUR ACCOUNT'. Below the progress bar, a yellow box states: 'In order to complete the sign up process, we will need to verify your identity.' The main heading is 'Identity Verification by Telephone'. The text below explains: 'After you provide a telephone number where you can be reached below, you will then be called immediately by an automated system and prompted to enter the PIN number over the phone. Once completed, you'll be able to proceed to review your account details. Please follow the 3 simple steps below.' The first step is '1. Provide a telephone number'. It asks the user to 'Please enter your information below and click the "Call Me Now" button.' There are two input fields: 'Country Code' (with a dropdown menu showing 'United States (+1)') and 'Phone number' (with a dropdown menu showing '(876) 825-0518'). Below these fields is a yellow 'Call Me Now' button. The second step is '2. Call in progress' and the third is '3. Identity verification complete'. The footer includes links for 'Privacy Policy' and 'Customer Agreement', the copyright notice '© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.', and the text 'An Amazon.com company'.

Figure 3-116: Provide a Telephone Number

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

Figure 3-117: Identity Verification PIN

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

Figure 3-118: Click Continue to Complete Identity Verification

8. Select a support plan and then click Continue.



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

Figure 3-119: Select your AWS Support Plan

9. You are now registered for an AWS Account!

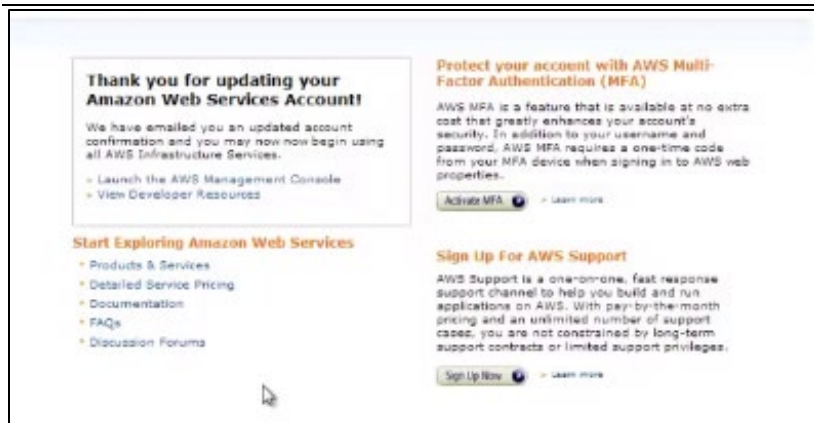


Figure 3-120: AWS Account Set-Up Complete



Issuers who require more than 20 servers must request a service limit increase from AWS so that their server can be provisioned by CMS at the desired size. Please see Section 4.3.4: Storage Requirements for more information. Since it typically takes AWS 48 hours to process these requests, issuers will need to complete this step prior to requesting an AWS EDGE server. For issuers who need more than 20 EDGE servers, it is highly recommended that the service increase request be submitted to AWS when you are at 18 instances, in order to allow a few extra instances without hitting the 20 instances limit.

3.5.2 Request an AWS EDGE Server Instance

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

Locate Account Number

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

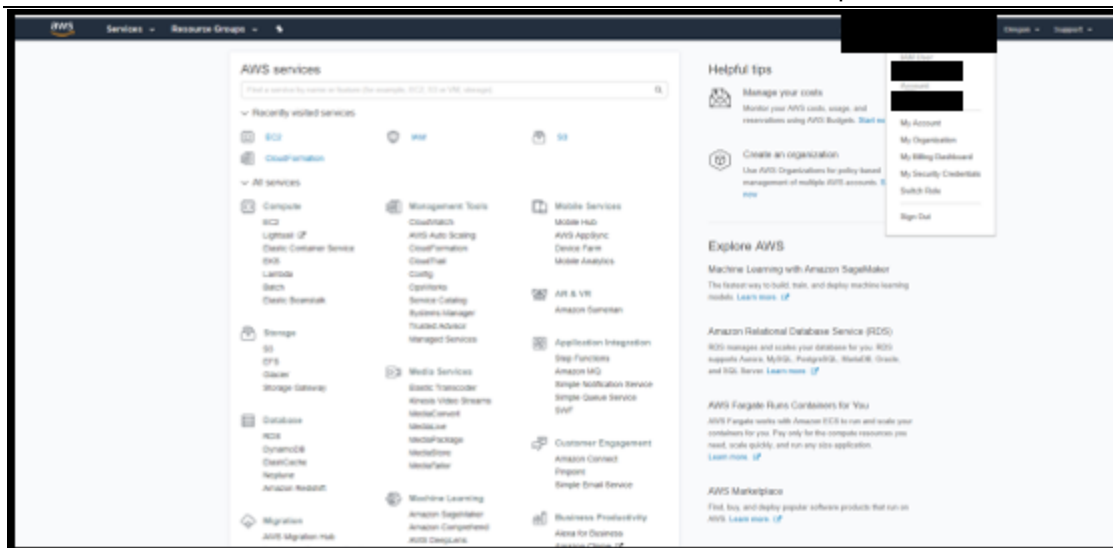


Figure 61 : AWS My Account

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

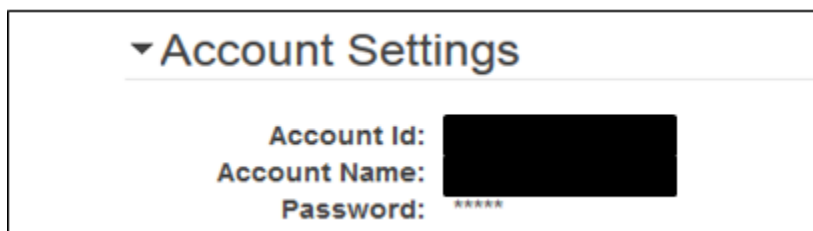


Figure 3-122: Account Settings

Create EDGE Installer Role

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

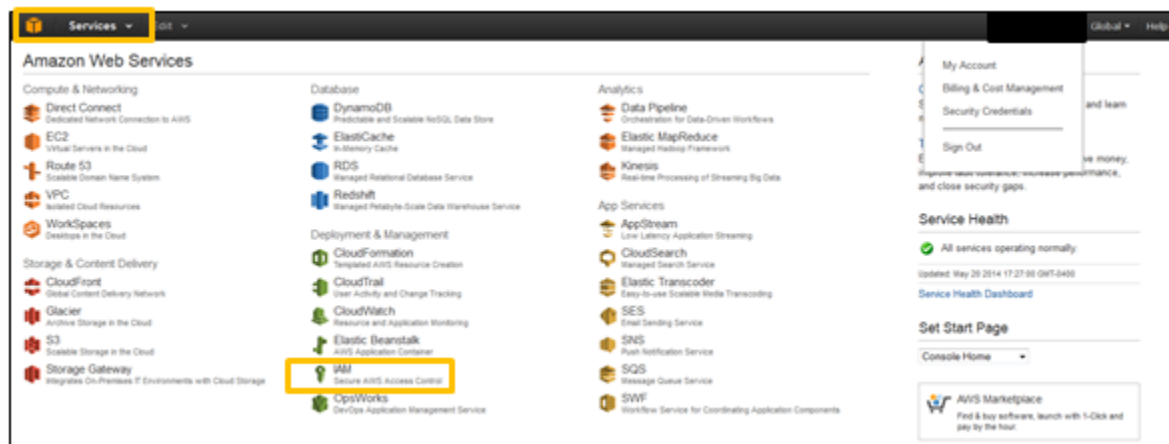


Figure 3-123: AWS Homepage with Services Dropdown

5. Select Roles from left navigation bar

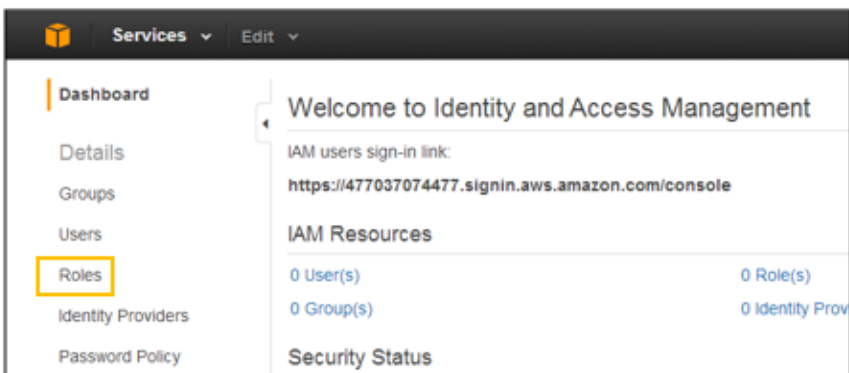


Figure 3-124: Select Roles

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

Figure 3-125: Create New Role Button

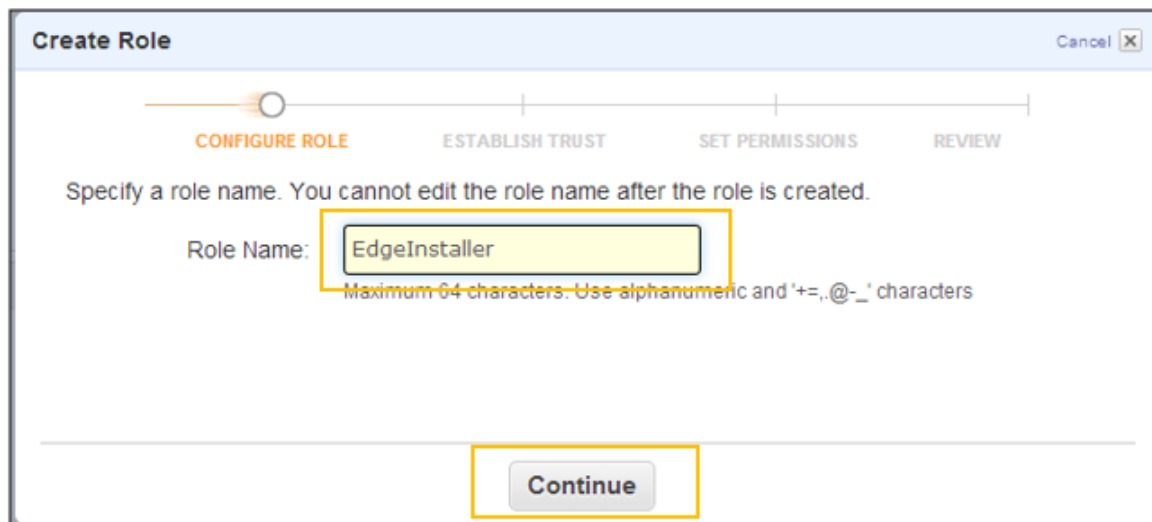
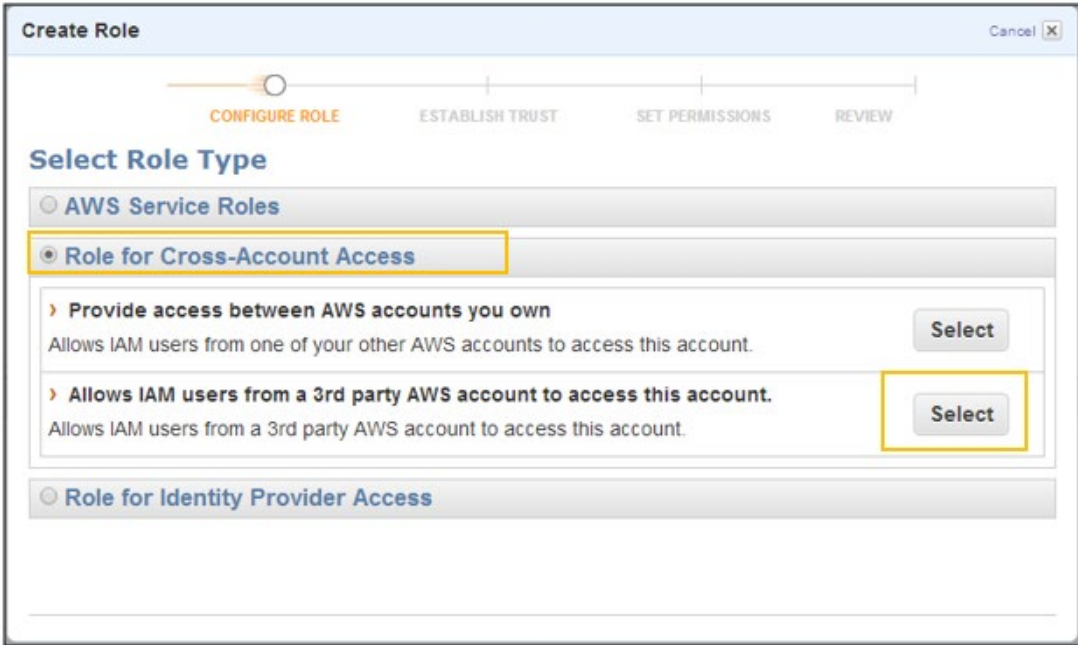
7. Enter **"EdgeInstaller"** in the text box and select **Continue** button.

Figure 3-126: Configure Role Window

8. In the next window select, **Role for Cross-Account Access** option.

9. Click the **Select** button for the option: **Allows IAM users from a 3rd party AWS account to access this account.**



Create Role Cancel X

CONFIGURE ROLE ESTABLISH TRUST SET PERMISSIONS REVIEW

Select Role Type

☐ AWS Service Roles

☒ **Role for Cross-Account Access**

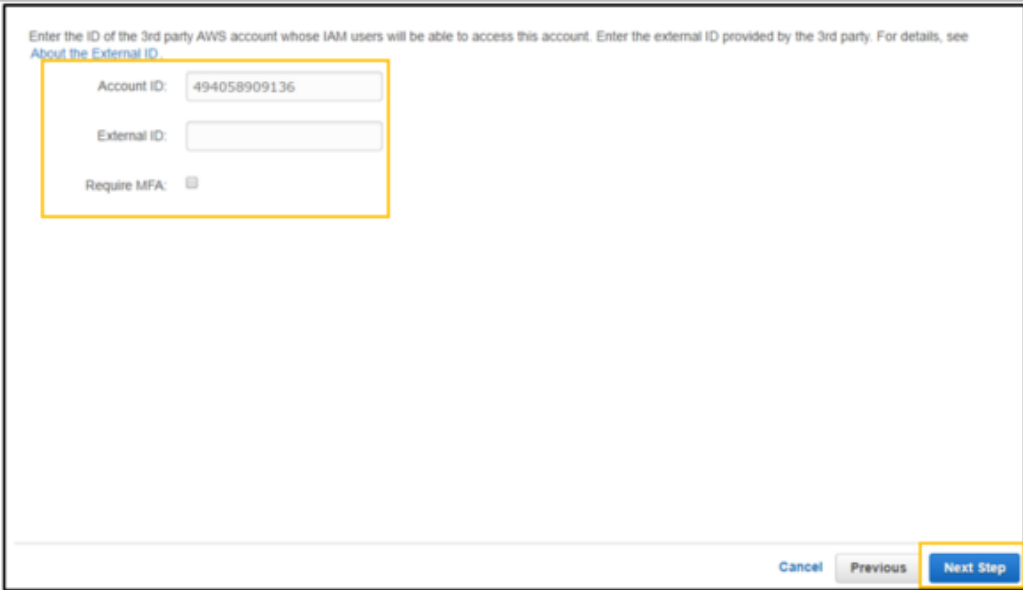
› **Provide access between AWS accounts you own**
Allows IAM users from one of your other AWS accounts to access this account. Select

› **Allows IAM users from a 3rd party AWS account to access this account.**
Allows IAM users from a 3rd party AWS account to access this account. Select

☐ Role for Identity Provider Access

Figure 3-127: Select Role Type

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



Enter the ID of the 3rd party AWS account whose IAM users will be able to access this account. Enter the external ID provided by the 3rd party. For details, see [About the External ID](#).

Account ID:

External ID:

Require MFA: ☐

Cancel Previous Next Step

Figure 3-128: Enter Account IDs

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

Create Role [Cancel X]

CONFIGURE ROLE ESTABLISH TRUST SET PERMISSIONS REVIEW

Set Permissions

Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.

☐ Select Policy Template

☐ Policy Generator

☒ Custom Policy

Use the policy editor to customize your own set of permissions.

Select

☐ No Permissions

Figure 3-129: Set Permissions - Custom Policy

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

The EDGE Installer Policy Data is posted in Appendix F: Installer Policy Data.

Create Role [Cancel X]

CONFIGURE ROLE ESTABLISH TRUST SET PERMISSIONS REVIEW

Set Permissions

You can customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies](#) in Using IAM. To test the effects of your policies before committing them into production, you can use the [IAM Policy Simulator](#).

Policy Name

EdgeInstallerPolicy

Policy Document

```
{
  "Statement": [
    {
      "Sid": "Stmt1404268724069",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ]
    }
  ]
}
```

[Back](#) **Continue**

Figure 3-130: EdgeInstallerPolicy- Custom Permissions

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

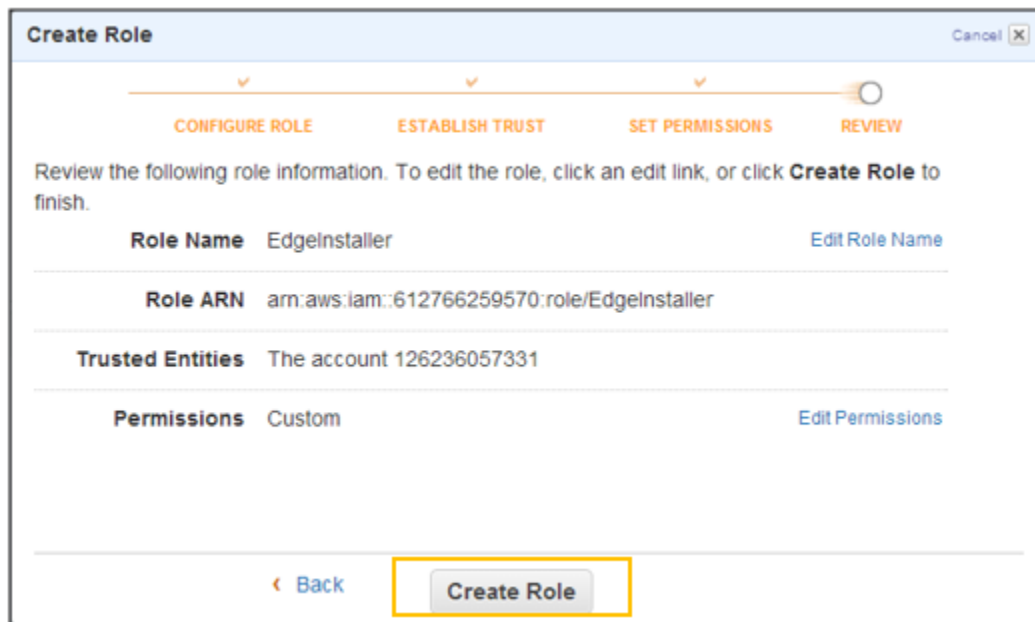


Figure 3-131: Final Review Page

Generate Key Pair

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

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



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

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

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

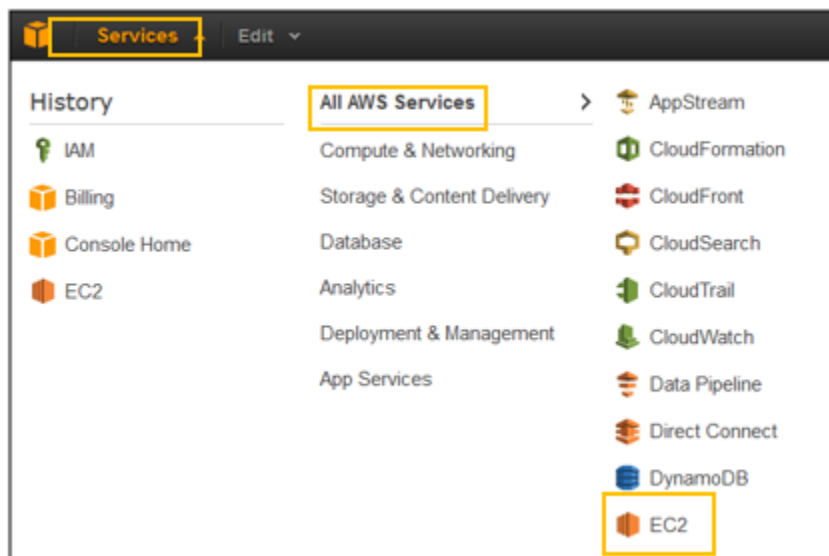


Figure 3-132: Services Dropdown with All AWS Services Selected

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

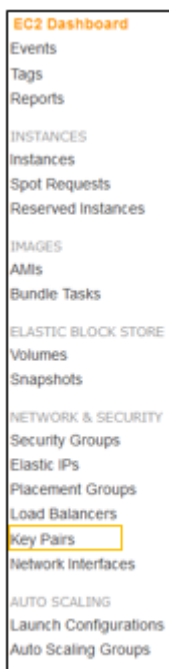


Figure 3-133: EC2 Dashboard Options

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



Figure 3-134: Create Key Pair

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



Figure 3-135: Create Key Pair Name

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

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

A Key Pair Name has been created.



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

3.5.3 Server Registration

Now that an AWS account and key pair has been established, you are ready to register your AWS EDGE server with CMS.

The AWS Server Registration uses the same steps as the OP Server Registration. Please refer to Section 3.4.2: Server Registration for steps to access the EDGE server registration site.

3.5.4 AWS EDGE Server Provisioning

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

Once an Amazon EDGE server request has been approved by CMS, the EDGE server is automatically provisioned in the AWS cloud using the details provided by the issuer or TPA during registration. The provisioning process itself is triggered by CMS approving the registration request through the EDGE Registration Site and requires no further action from the issuer. Once provisioning is completed, the request status is updated in the registration site and the user is able to log in to AWS and begin processing files.

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

I. *Provisioning Successful*

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

1. Log in and access the ESM using the steps in Section 3.2.1: Accessing the ESM Website.

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

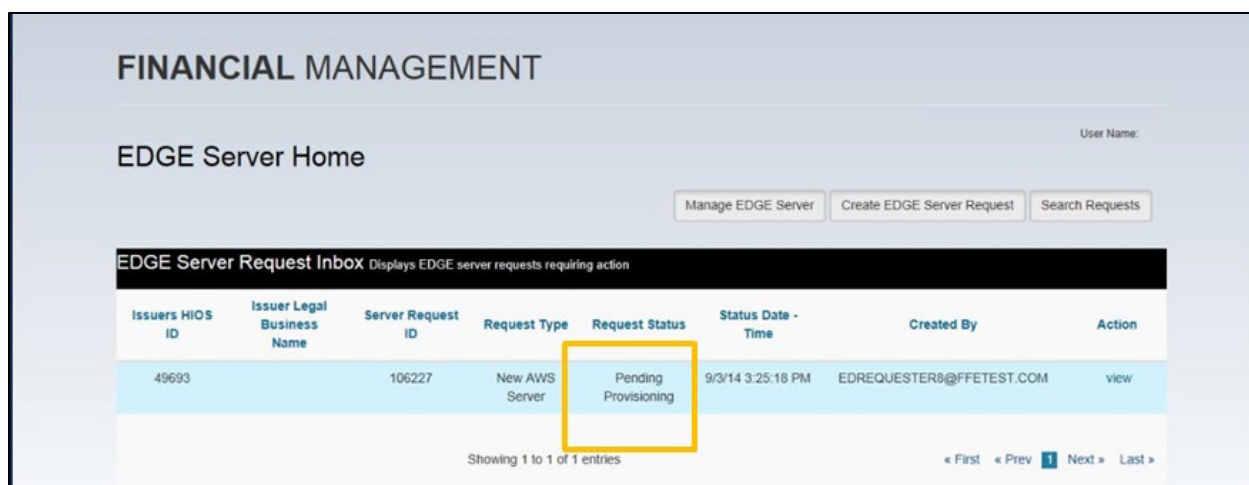


Figure 3-136: Pending Provisioning

2. The information provided during the submission of the registration request is automatically passed as parameters to the EDGE provisioning script. The script is executed to create the EDGE server with no further action required.

At this point, the request status will be updated to **Provisioning in Progress**. Once this occurs, the request will clear from the Issuer Submitter's inbox. The Issuer Submitter will need to search for the request to see the status of **Provisioning in Progress**.

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

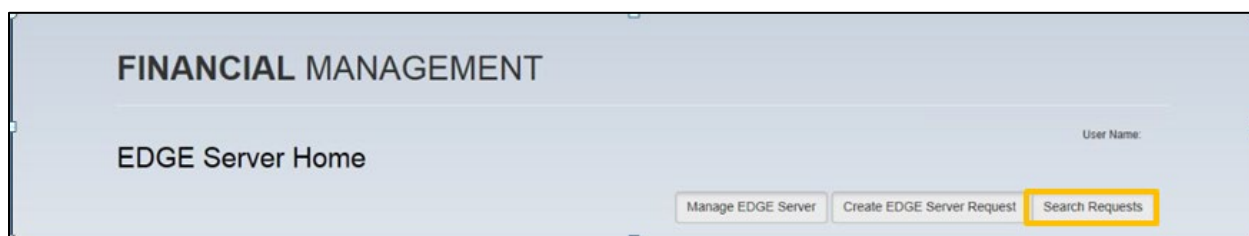


Figure 3-137: Search Requests Button

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

EDGE Server Request Search

User Name: ACCNFM123@FFETEST.COM

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Issuer HIOS ID Search Value : 15509

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

Figure 3-138: Search Request Screen

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



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

EDGE Server Request Search

User Name: EDCMTEST1@FFETEST.COM

[Back to EDGE Server Home](#)

Search Criteria

Search Field : Request ID Search Value : 106853

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

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

Figure 3-139: Provisioning in Progress

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

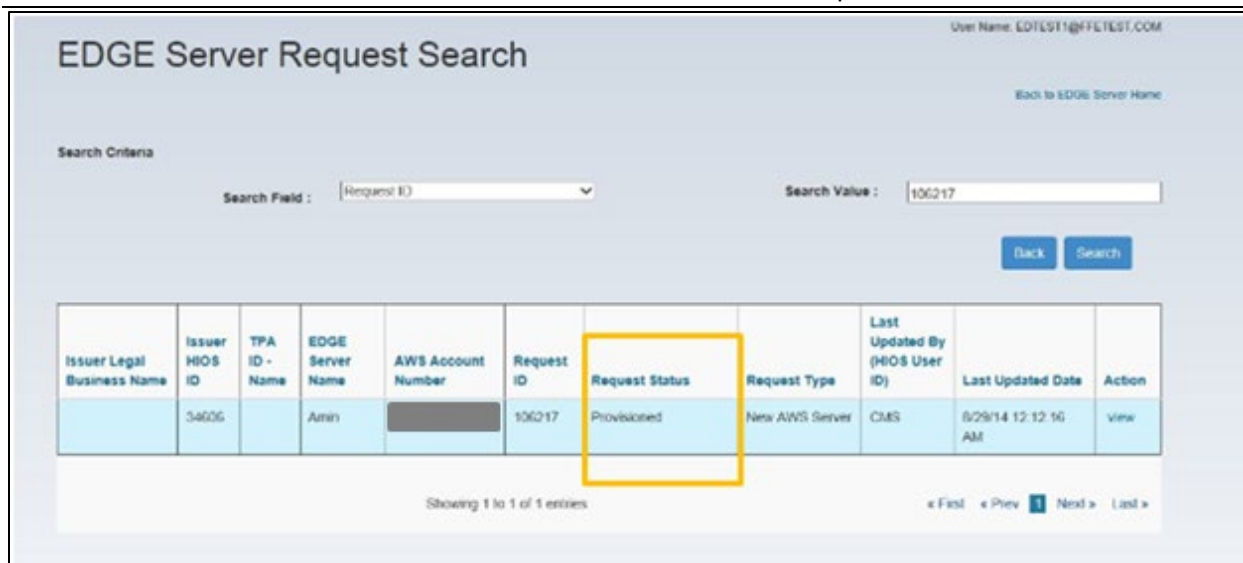


Figure 3-140: Server Provisioned Status

II. *Provisioning Failed*

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

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

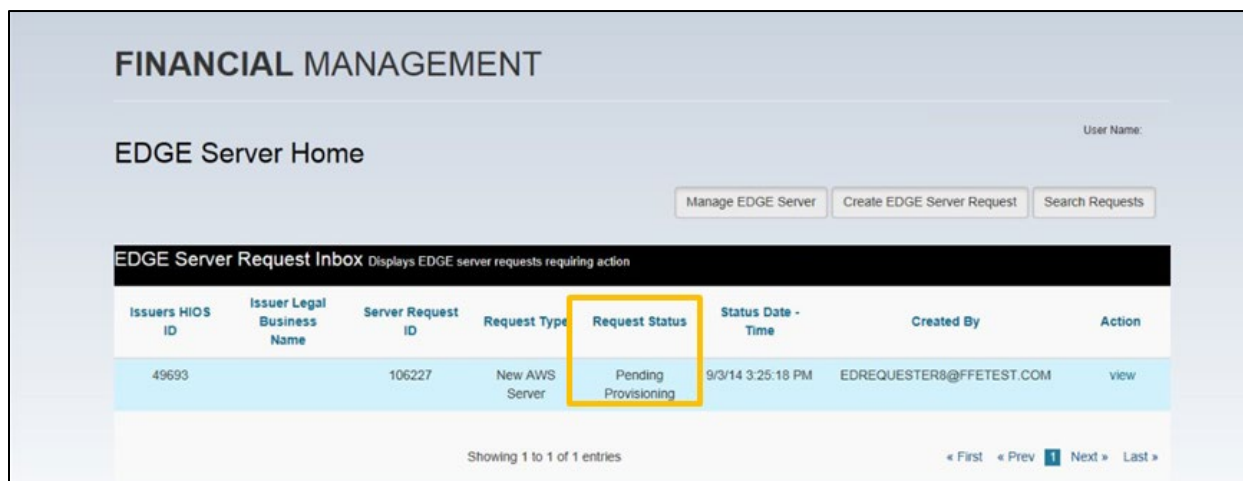


Figure 3-141: Pending Provisioning

When provisioning has failed, the Issuer Submitter will need to contact the FMCC Team at EDGE_server_data@cms.hhs.gov to determine the cause of the failure. Your representative will provide more details on the cause of the failure and the resolution process. Errors may be related to EDGE Server Storage, insufficient capacity issues for AWS, or incorrect AWS Region, and

the issuer may need to open up a ticket with AWS in order to assist in supporting solution. Please update your FMCC representative on the progress.

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

Confirming Successful AWS EDGE Server Provisioning and Connecting to the Server

I. Download PuTTY

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

To download PuTTY to connect to the provisioned server:

6. Go to www.putty.org.
7. Click **you can download PuTTY here**.

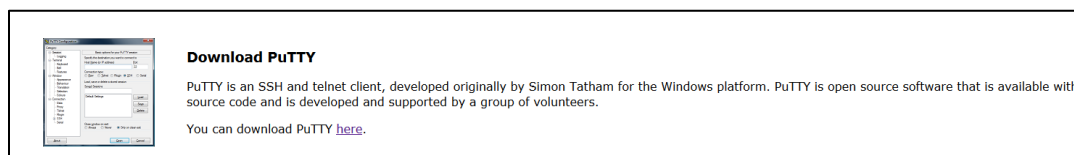


Figure 3-142: PuTTY Home Page

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

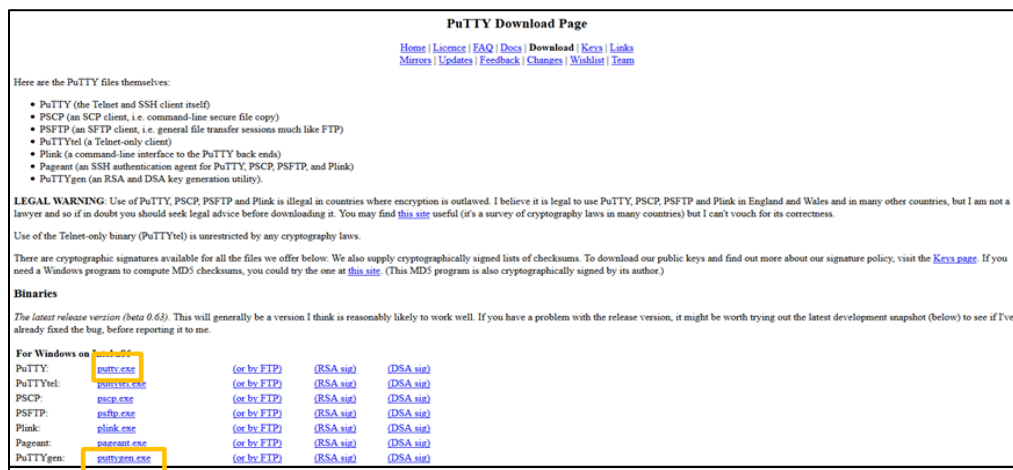


Figure 3-143: PuTTY Download Page

II. Configure Puttygen.exe

8. Open and run the puttygen.exe file. The window below will appear.
9. Click **Load** and then select the Key Pair file that was saved (.pem file) in Section 3.5.2: Request an AWS EDGE Server Instance.

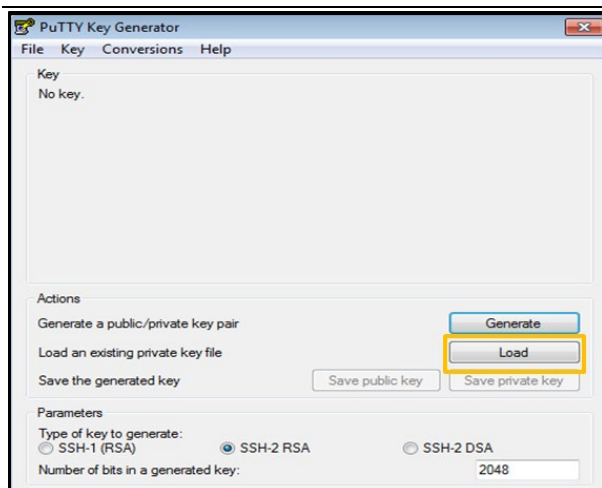


Figure 3-144: PuTTYgen Program Screen

After loading the Key Pair file from your computer, the following pop-out window will display.

Click **OK** to generate the file in .ppk format. This is the format you will need to utilize the Private key in later steps.

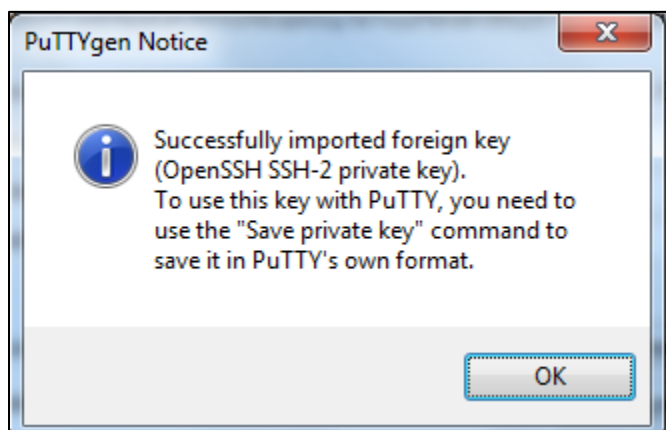


Figure 3-145: PuTTYgen Notice

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

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



Figure 3-146: Save Private Key

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



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

III. *Configure Putty.exe*



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

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

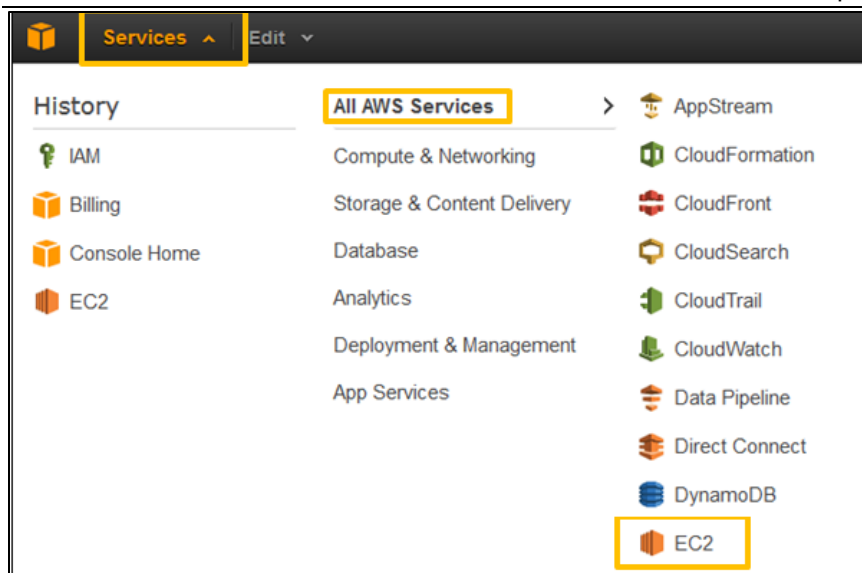


Figure 3-147: Services and All AWS Services Dropdowns

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

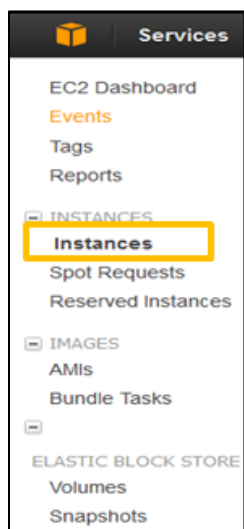


Figure 3-148: EC2 Options

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

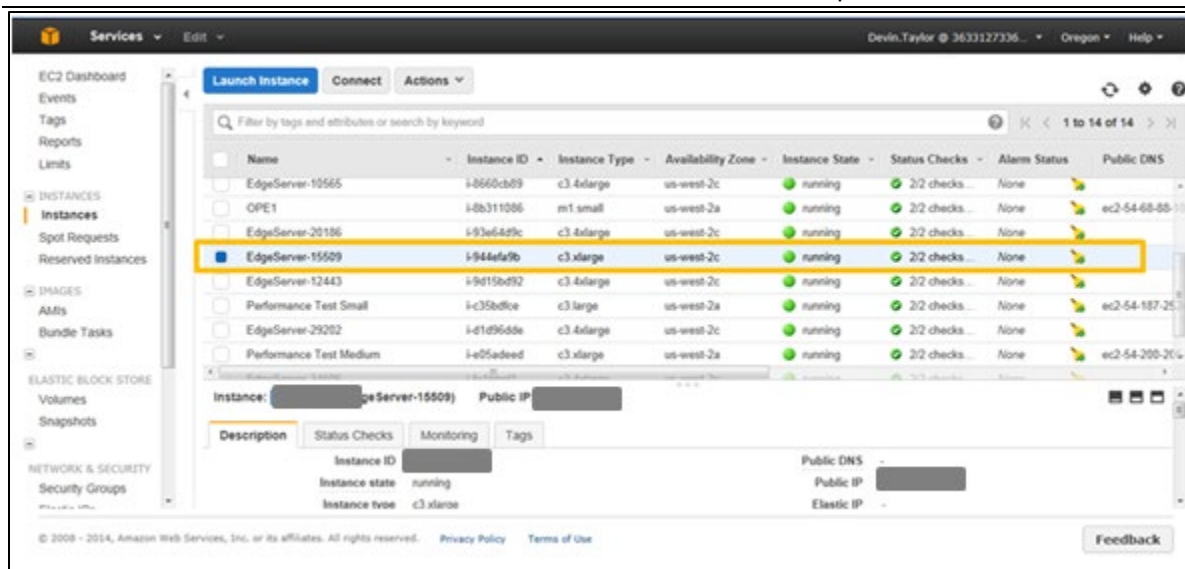


Figure 3-149: All Instances List

14. Select the **EDGE Server Instance**. You can find the public IP address in the bottom section of the page on the **Description** tab.



Remember to save this IP address number. You will need this public IP address for configuring PuTTY in the steps below. If the server ever crashes or is restarted for any reason, the public IP address will change to a new number. Issuers will need to remember to note this new IP address number when executing these steps again.

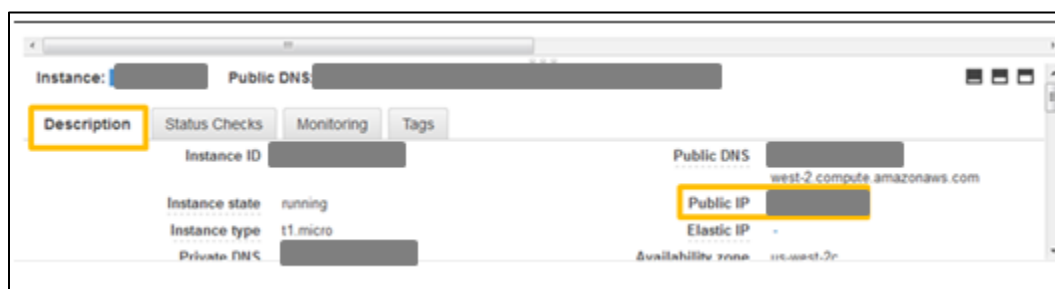
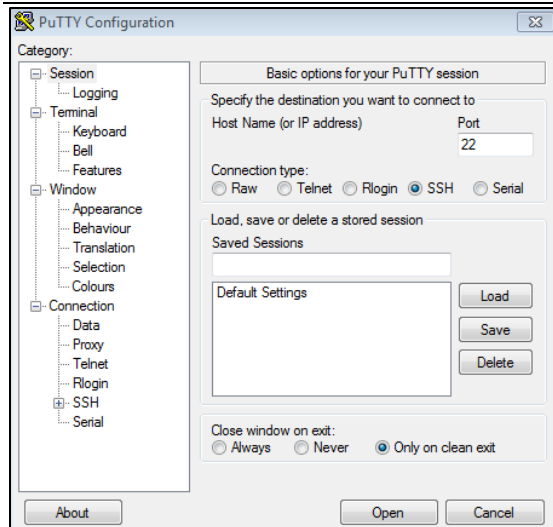


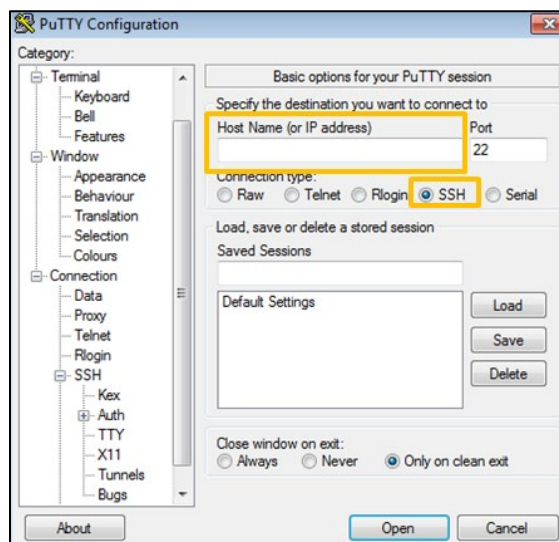
Figure 3-150: Public IP Address

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

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

**Figure 3-151: PuTTY Configuration Window**

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

**Figure 3-152: PuTTY Configuration - Add IP Address**

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

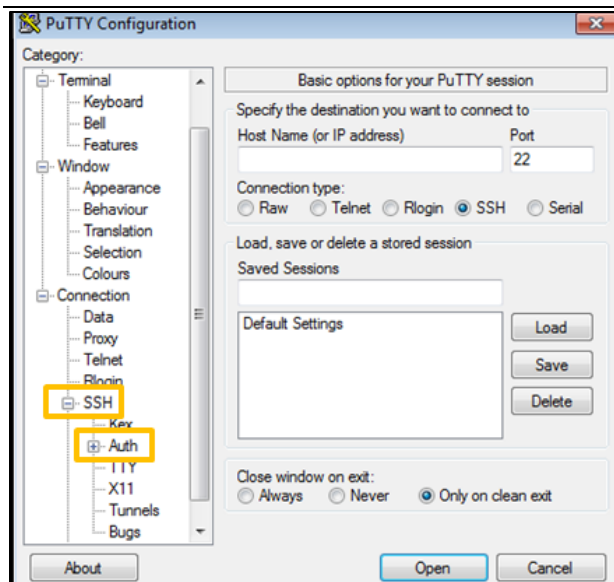


Figure 3-153: Category List on PuTTY Configuration Window

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

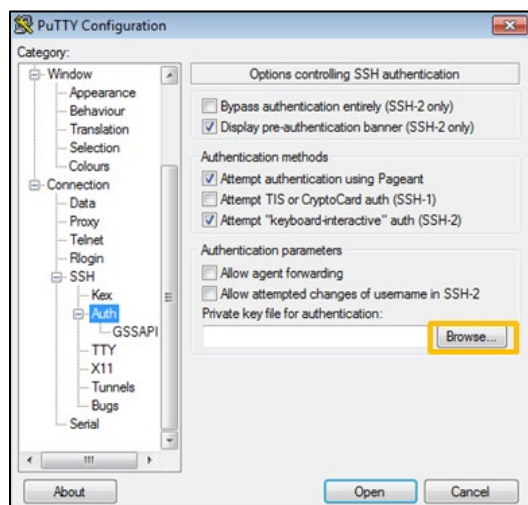


Figure 3-154: PuTTY Authentication Options

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

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

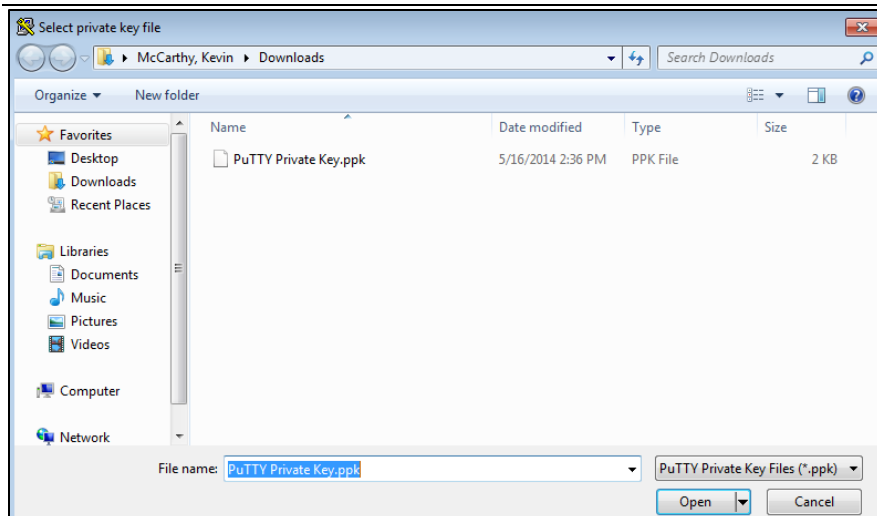


Figure 3-155: Browsing for PuTTY Private Key

20. After loading the Private Key file, save the session prior to executing.

When running PuTTY for the first time, a password reset is required that will close the program and require to execute the PuTTY configuration again. Saving the session will store the data you entered above.

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

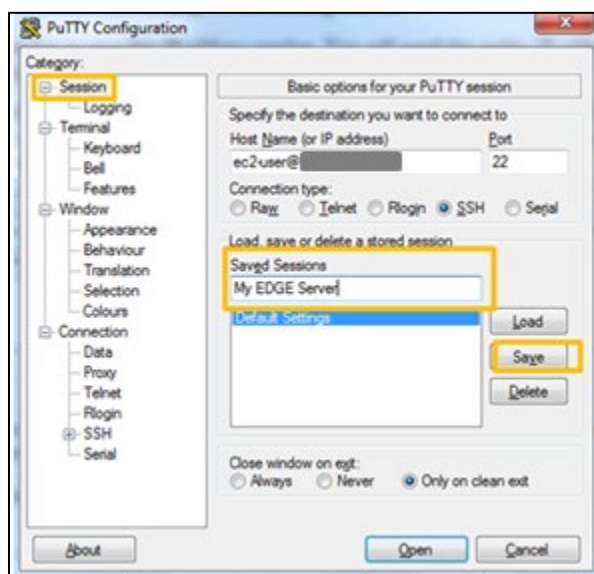


Figure 3-156: Save Session

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

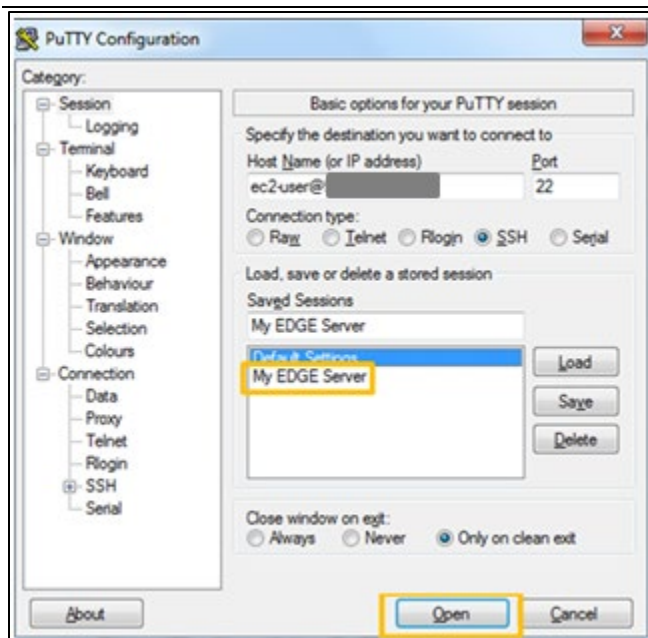


Figure 3-157: Completing PuTTY Configuration

23. The following security alert will appear verifying that you trust the host and that you want to add the key to PuTTY's cache and continue connecting. Click the **Yes** button to continue



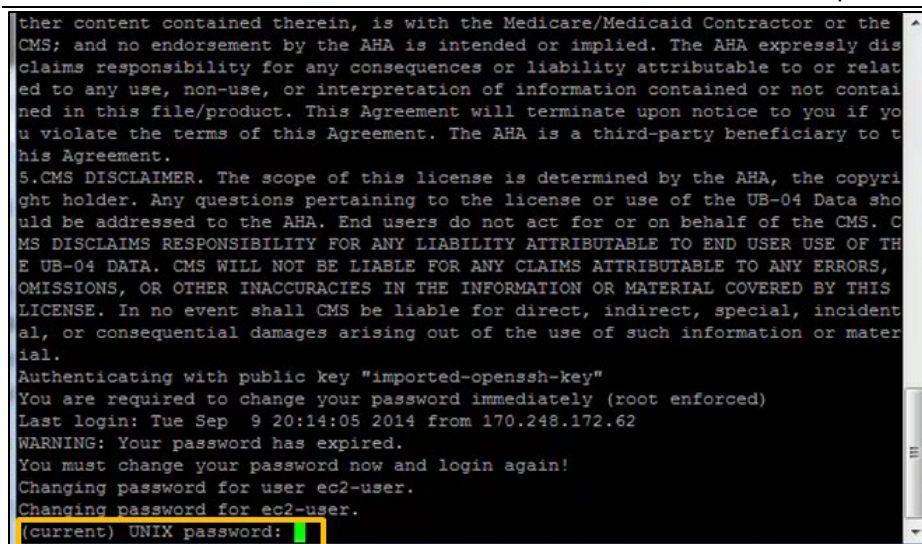
Figure 3-158: PuTTY Security Alert

IV. *Connect to EDGE Instance and confirm functionality*

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

Enter the following in the PuTTY window: **edgeserver (enter as one word with no spaces)**.

You will then need to enter a new password for your server for future logins. The cursor will not move when typing in password characters (passwords only). Remember to be precise when entering your password.



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

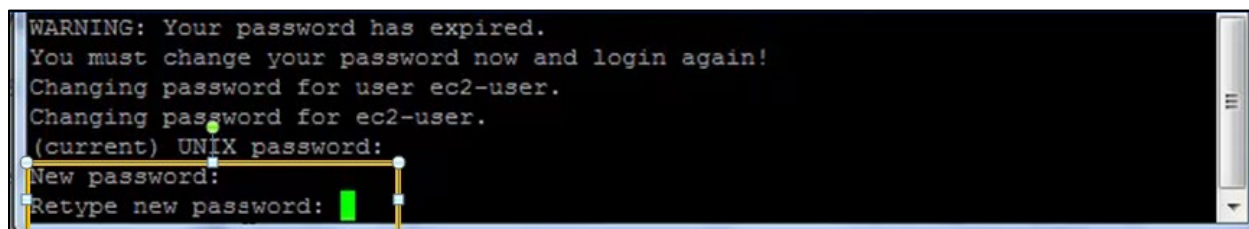
Figure 3-159: Enter Password

Enter and then re-type a new password for your server for future logins.

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

EDGE server password MUST:

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

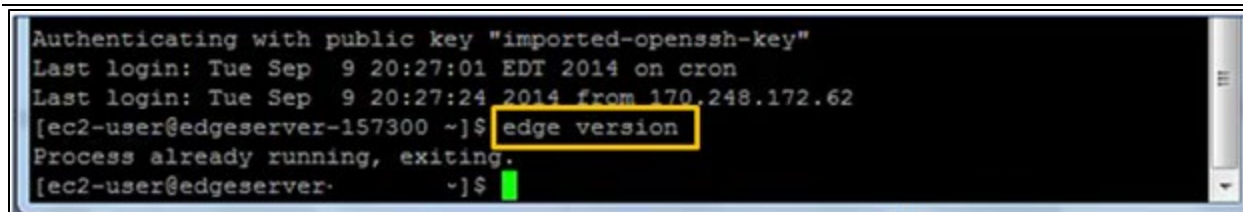


```
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user ec2-user.
Changing password for ec2-user.
(current) UNIX password:
New password:
Retype new password: 
```

Figure 3-160: Enter NEW Password

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

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



```

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

```

Figure 3-161: EDGE Version Command

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

V. Enable Termination Protection

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



Selecting **Terminate** will shut down the instance and you will no longer be able to connect to or restart the instance after you've terminated it. The root device volume will be deleted and the EIP is disassociated from the instance. **This will effectively destroy your server instance permanently.**

In order to prevent your server instance from accidentally being terminated, enable termination protection on the server instance.

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

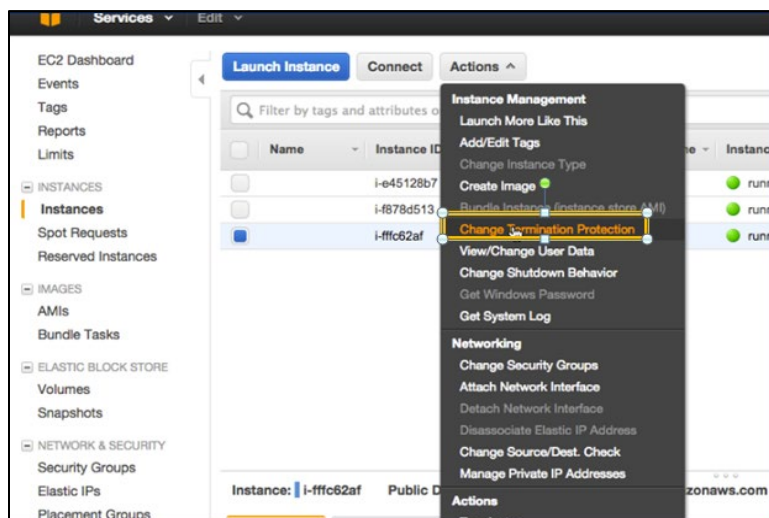


Figure 3-162: Select Change Termination Protection

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

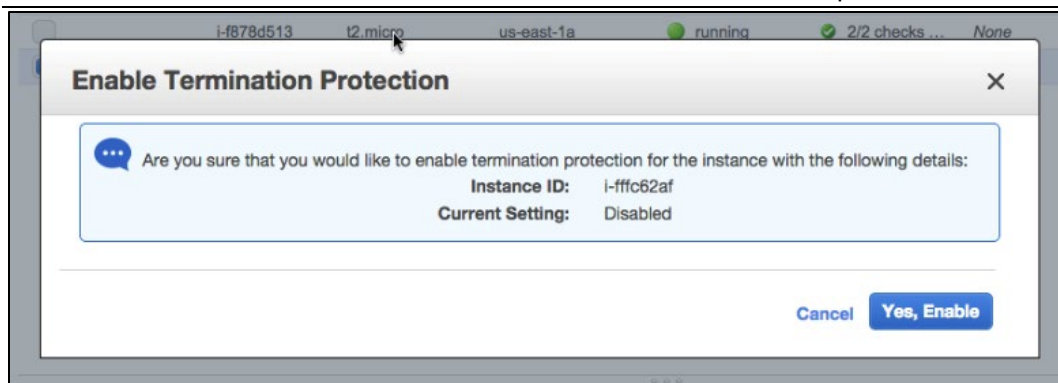


Figure 3-163: Enable Termination Protection

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

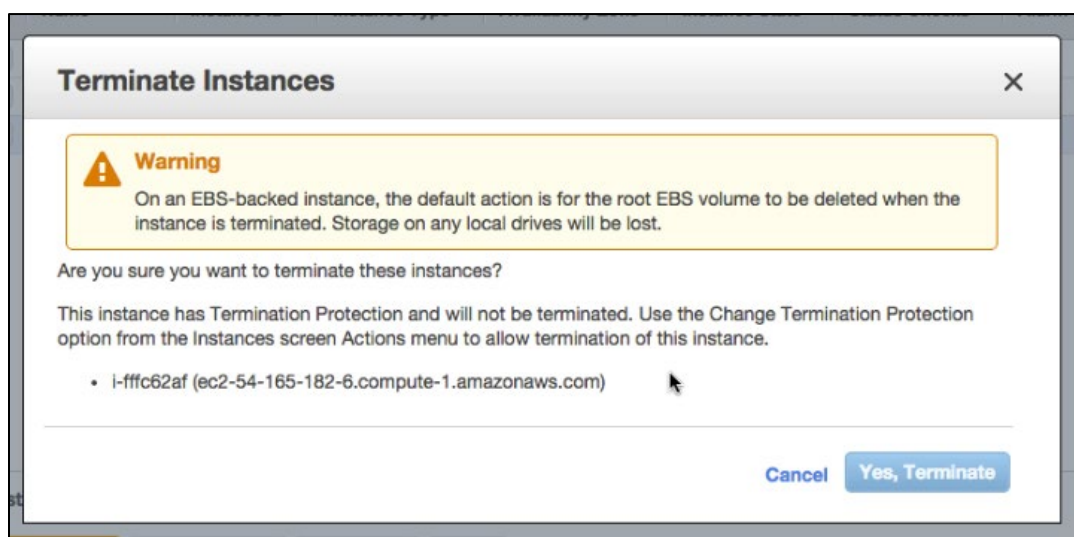


Figure 3-164: Terminate Instances Message

VI. Stop Server Instance

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

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

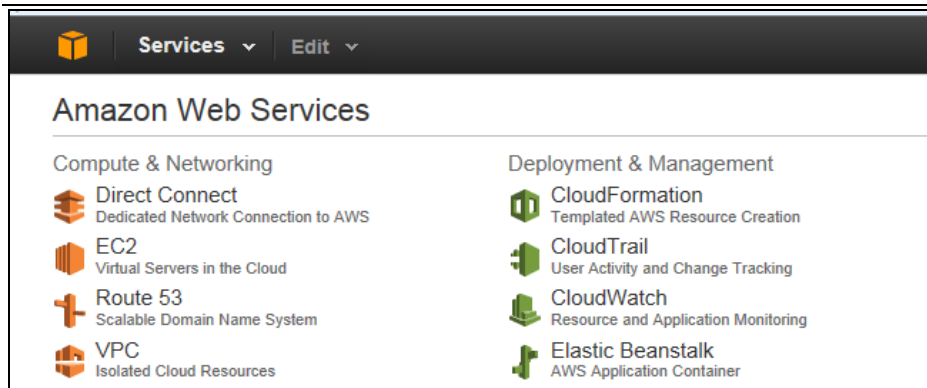


Figure 3-165: Select EC2

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

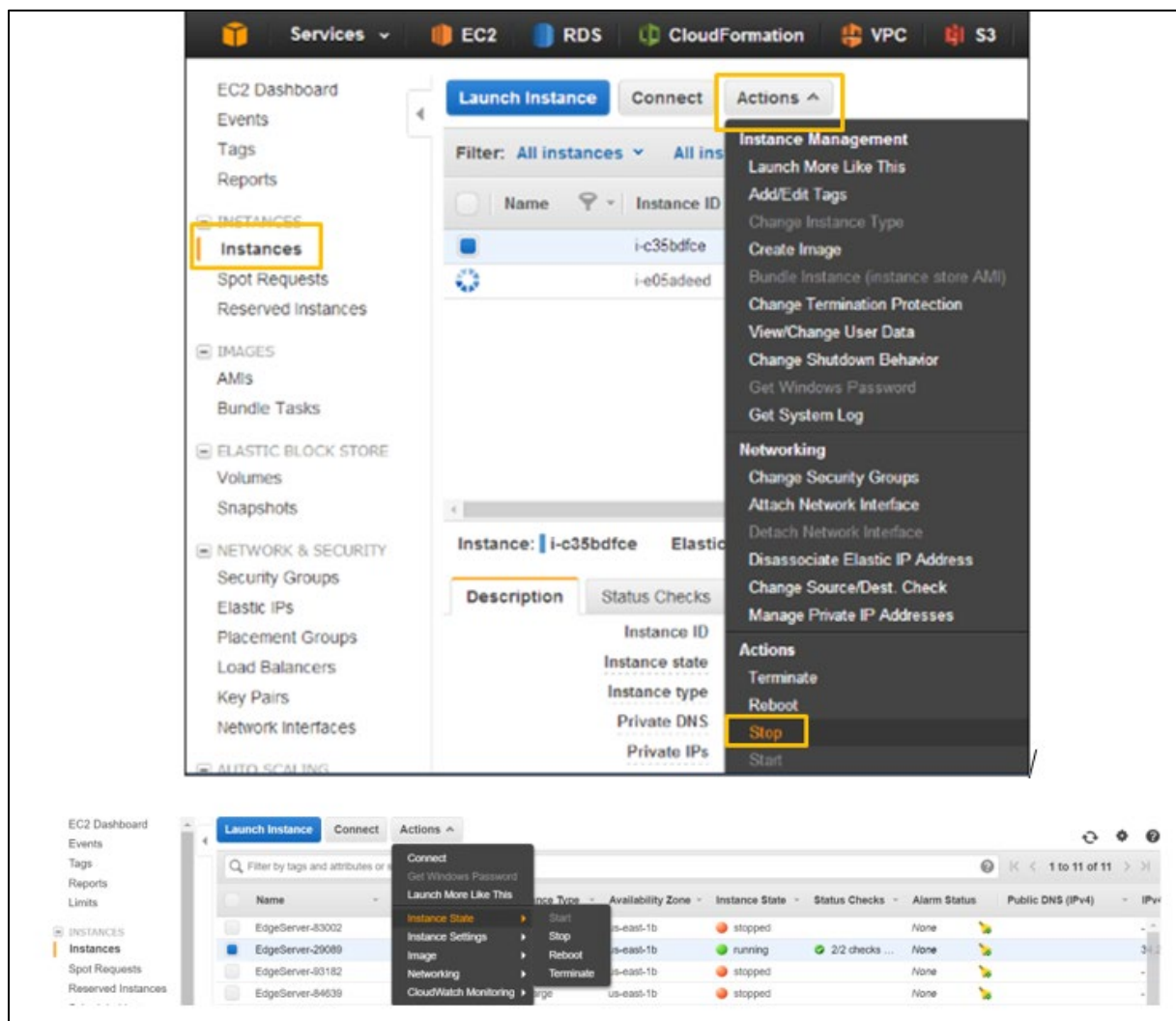


Figure 3-166: Stop Server Instance

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

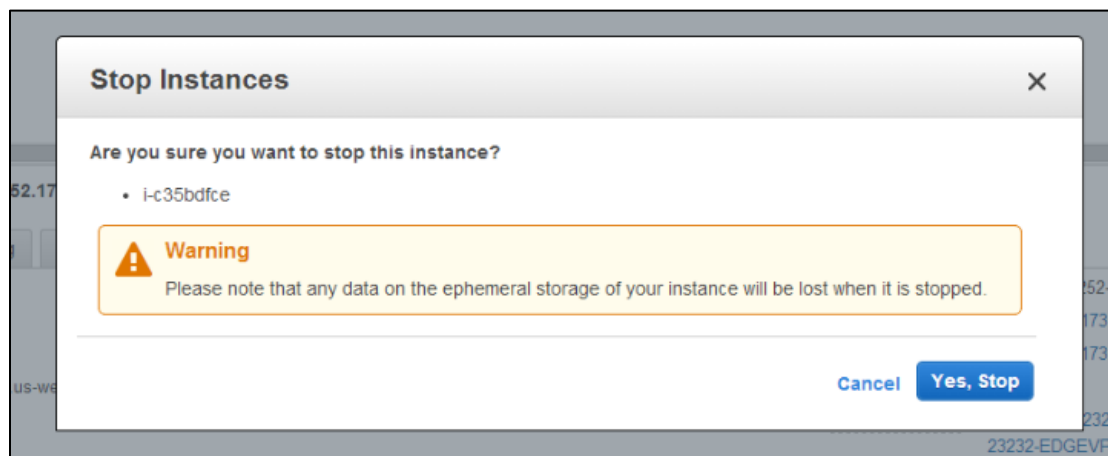


Figure 3-167: Confirm Stop Instance

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

3.6 Migration



Issuers **must** contact CMS by emailing the FMCC mailbox at Edge_Server_Data@cms.hhs.gov to create a migration ticket. This includes any self-hosted server or TPA changes. CMS must approve the migration request before the issuer performs any action. Migrating before CMS approval can have detrimental effects on remote commands or the data archival process.

This section will provide details involved in data migration for both OP and AWS server options. The [EDGE Server Migration Job Aids](#) located in the REGTAP Library are distinguished by the type of server that the issuer uses initially. Each document is then divided into subsections that provide pre-migration and migration steps for issuers who are self-hosted (SH) and for issuers who contract with TPAs.

- OP to OP
- OP to AWS
- AWS to OP
- AWS to AWS

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

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

Section 4 - 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.

4.1 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 7 - 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.

4.1.1 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.

4.1.2 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 [Interface Control Document - RARI Addendum](#) 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.

4.1.3 File Ingest Overview

Issuers upload enrollment, claims and supplemental diagnosis files. The EDGE server software applies the verification edits outlined in Sections 4.1.2 Interface Control Document (ICD) and 4.1.1 EDGE Server Business Rules. 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 Interface Control Document. File layouts and requirements related to data submission are outlined in the Interface Control Document and EDGE Server Business Rules 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 (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

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.

4.1.4 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 3.5.4: AWS EDGE Server 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

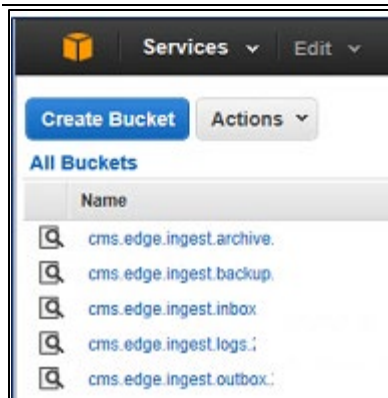


Figure 4-1: AWS S3 Bucket Structure

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.

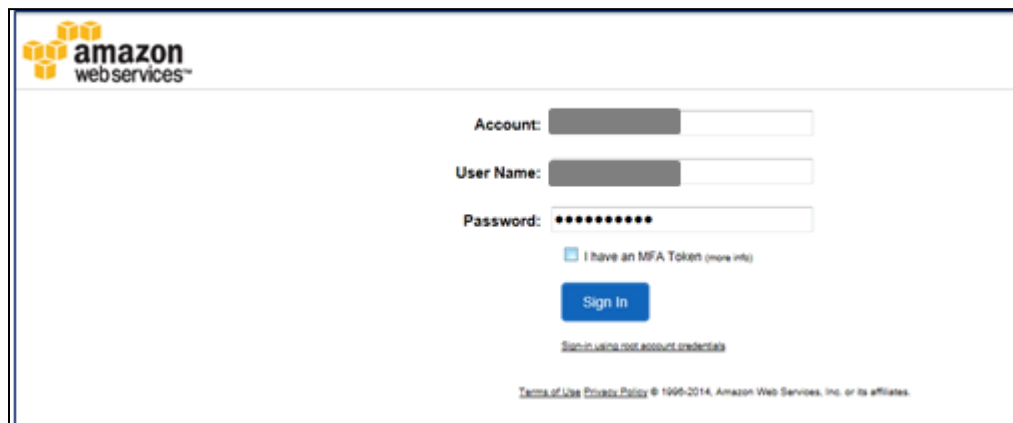


Figure 4-2: Amazon Web Services - Login Screen

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.

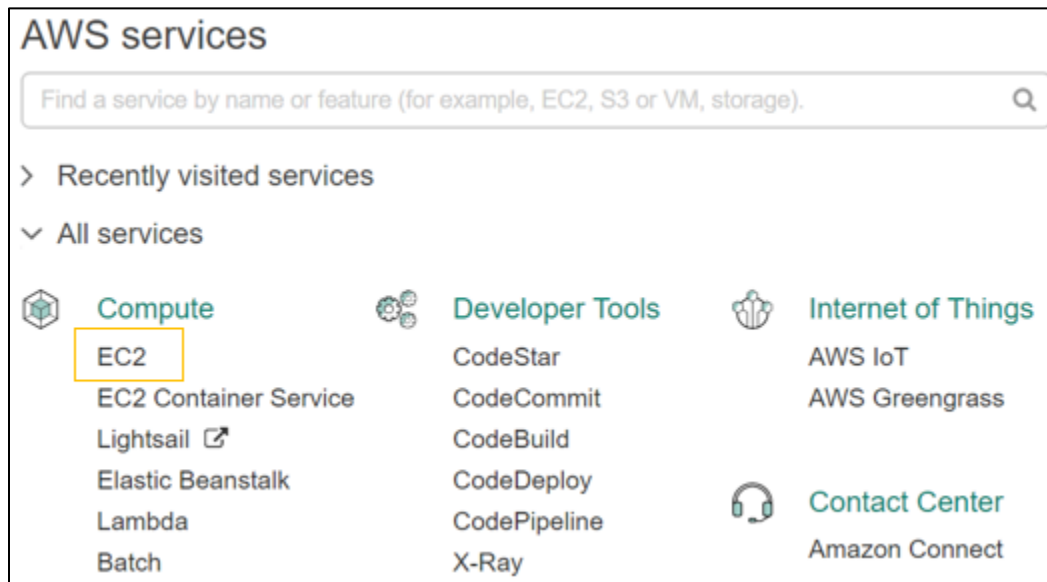


Figure 4-3: Select EC2

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.

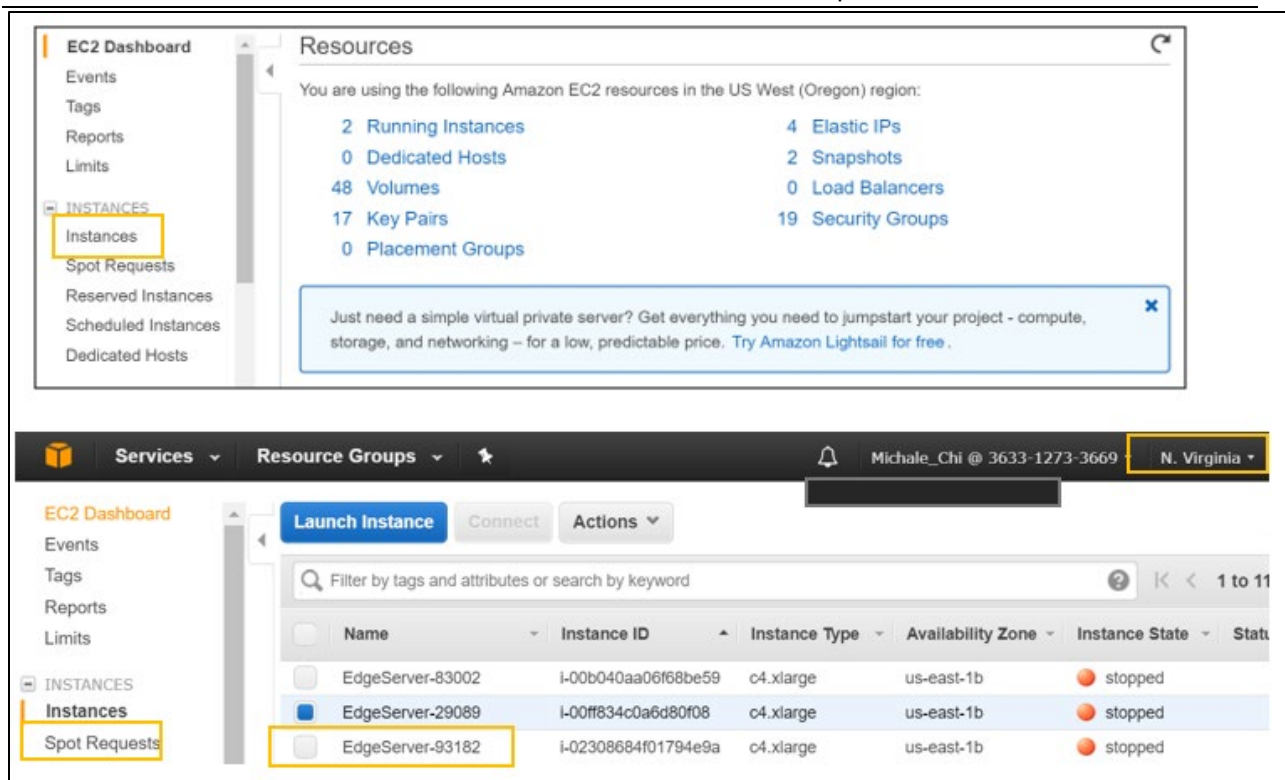


Figure 4-4: Select Server Instance

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

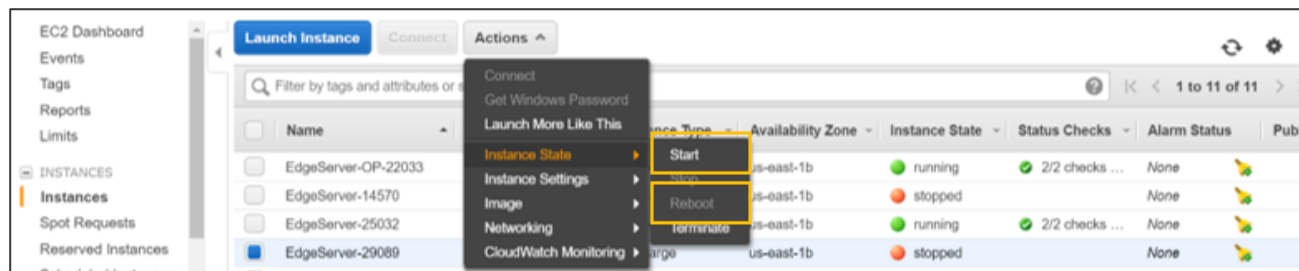


Figure 4-5: Start Server Instance

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

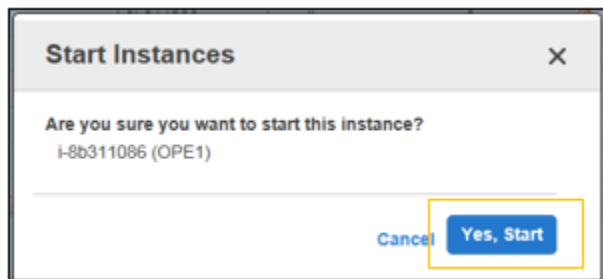


Figure 4-6: Confirm Start

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.

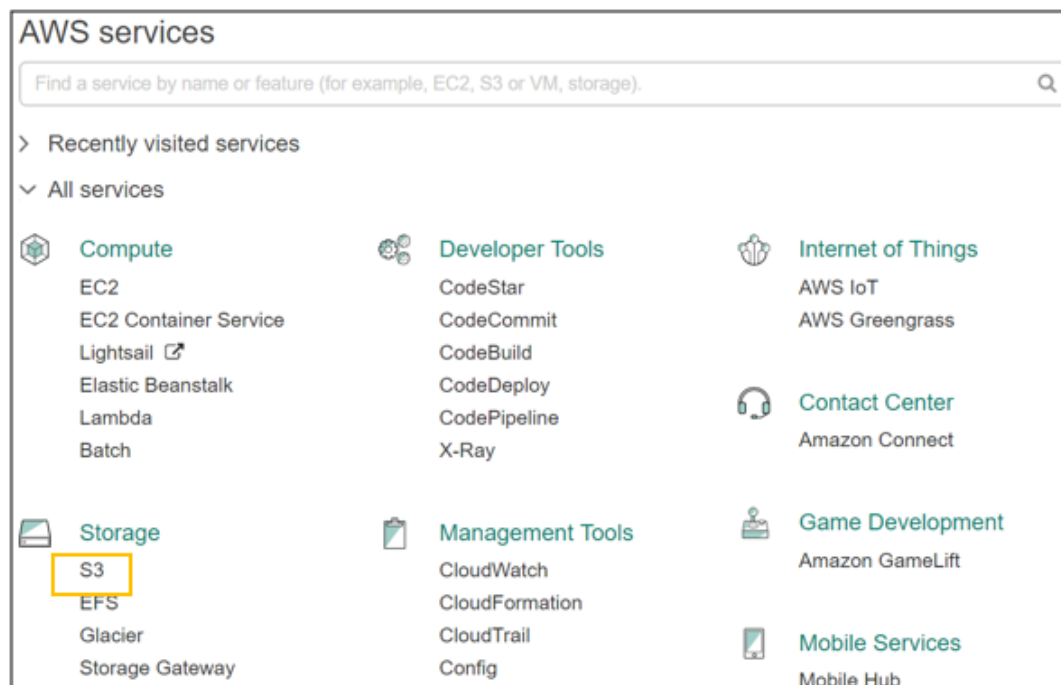


Figure 4-7: AWS Home Screen - Select S3

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

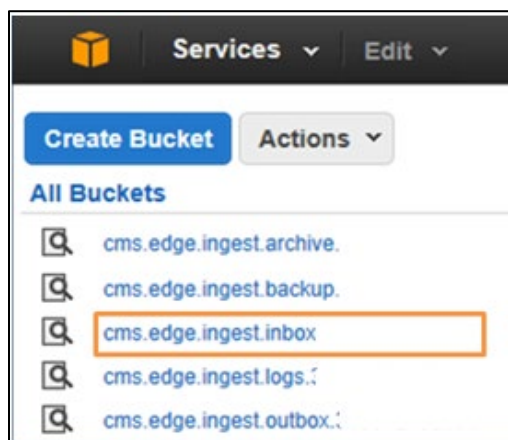


Figure 4-8: Select S3 Buckets Inbox

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

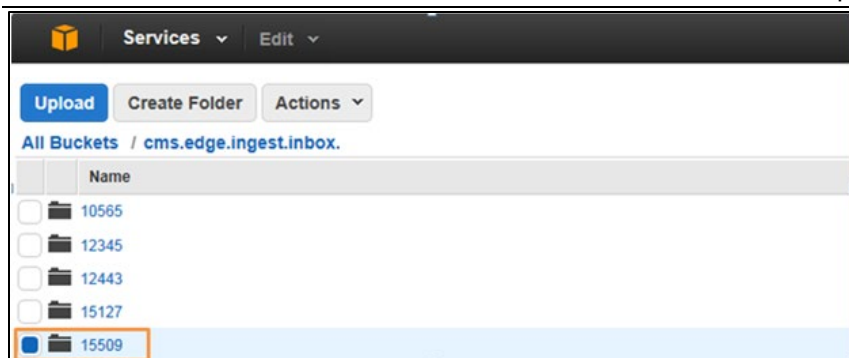


Figure 4-9: Select Issuer ID

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.

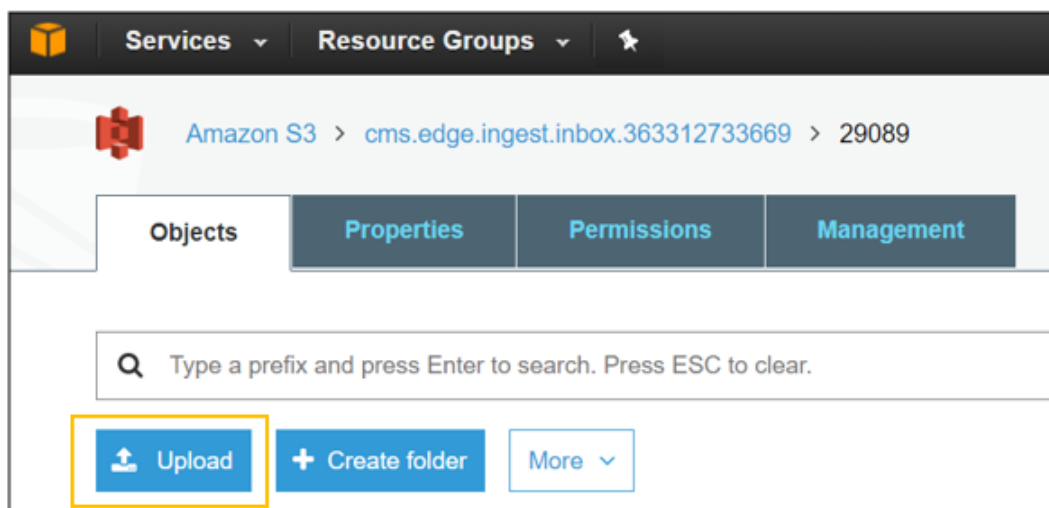


Figure 4-10: Select Upload

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.

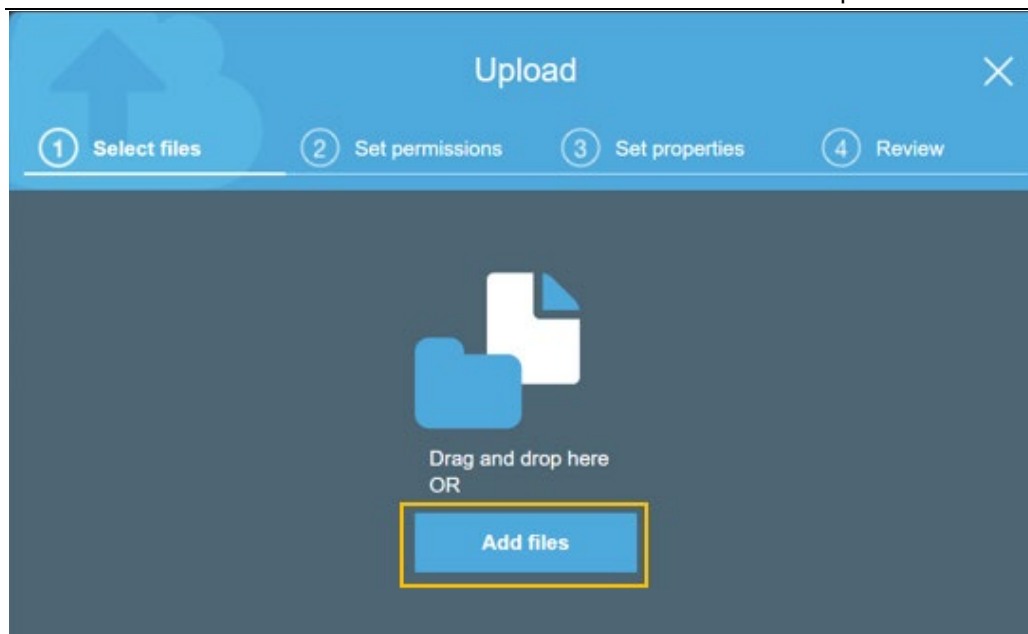


Figure 4-11: Upload - Select Files and Folder

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

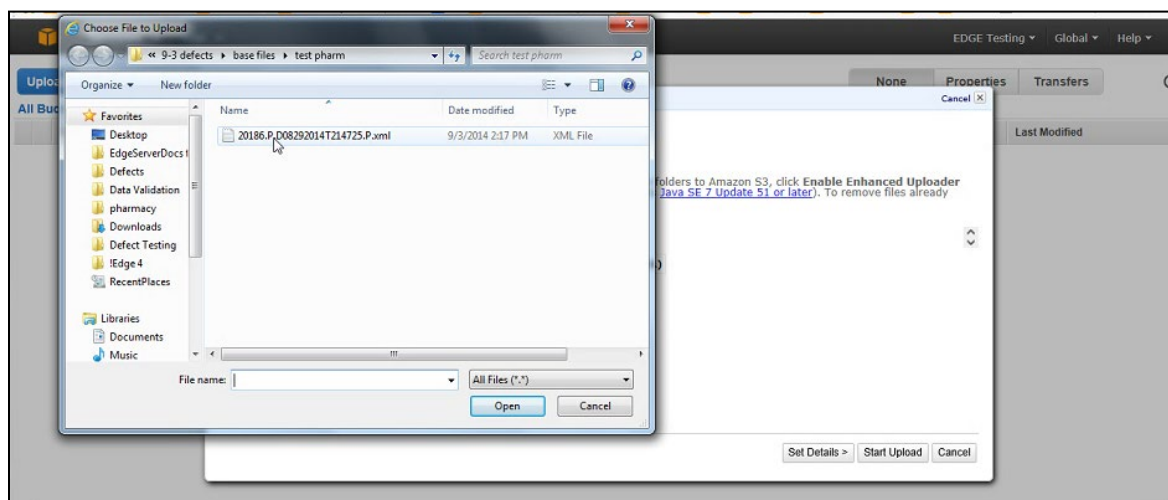


Figure 4-12: Choose File to Upload

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.

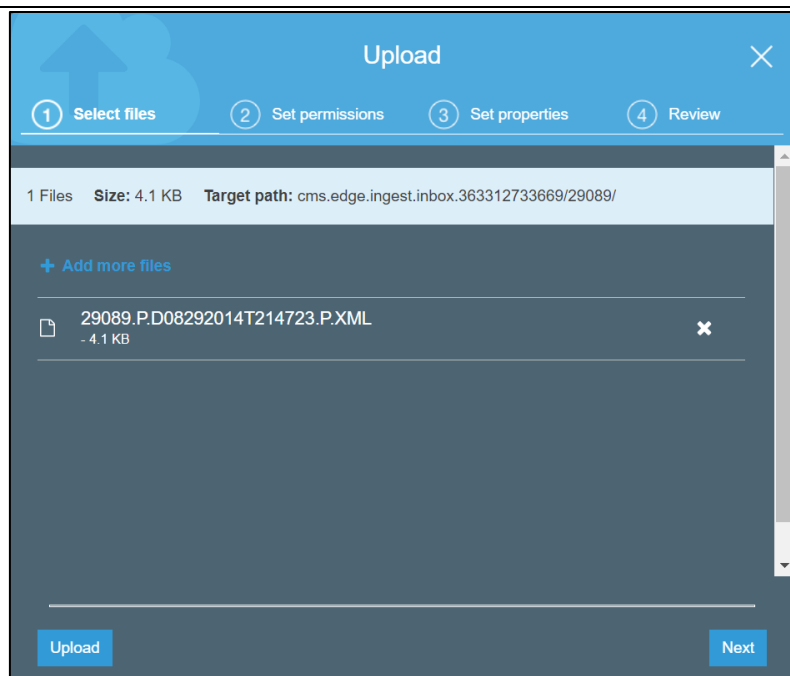


Figure 4-13: Attached File in Select Files

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.

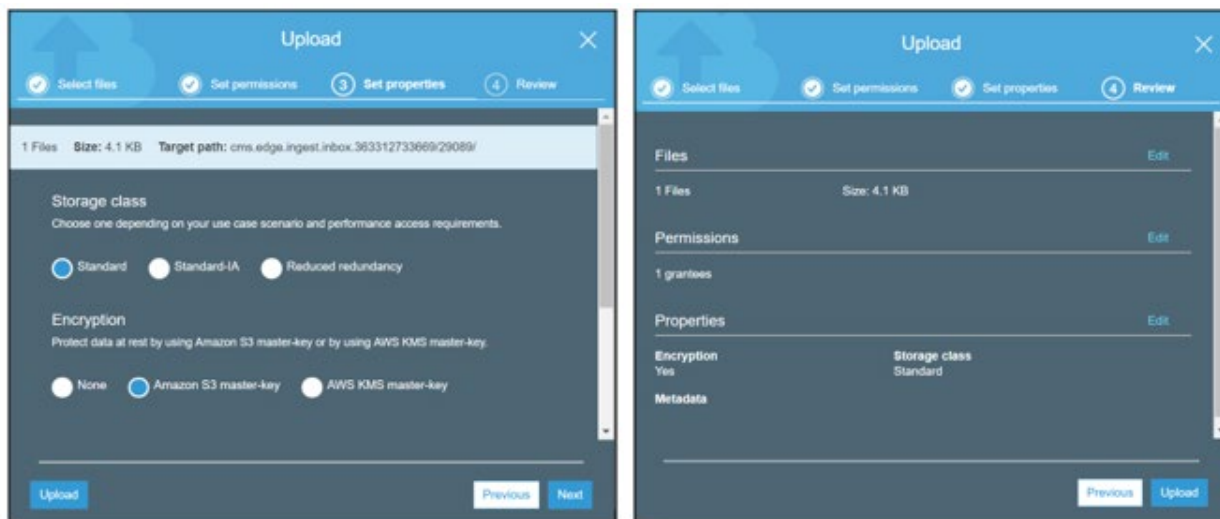


Figure 4-14: Set Details and Upload



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.

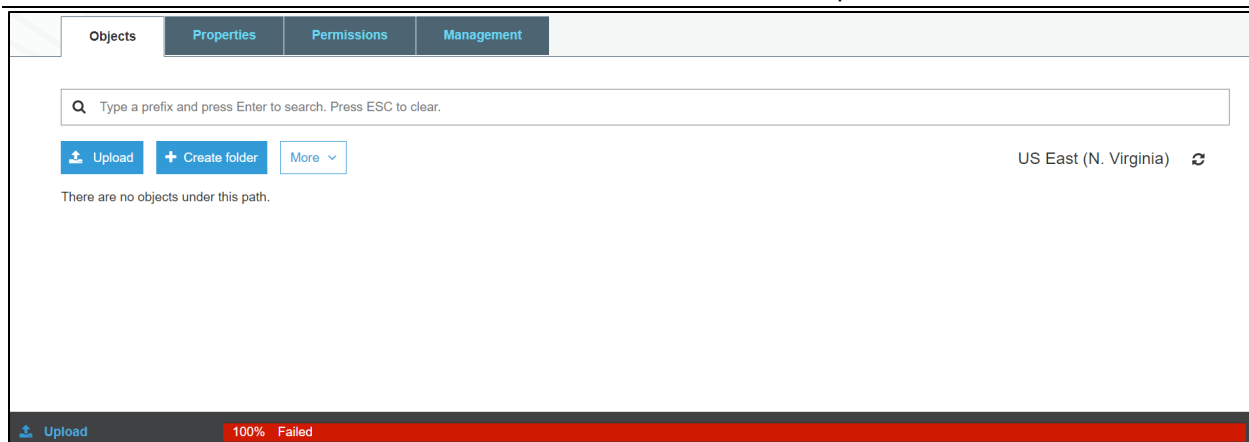


Figure 4-15: File Upload Error

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.

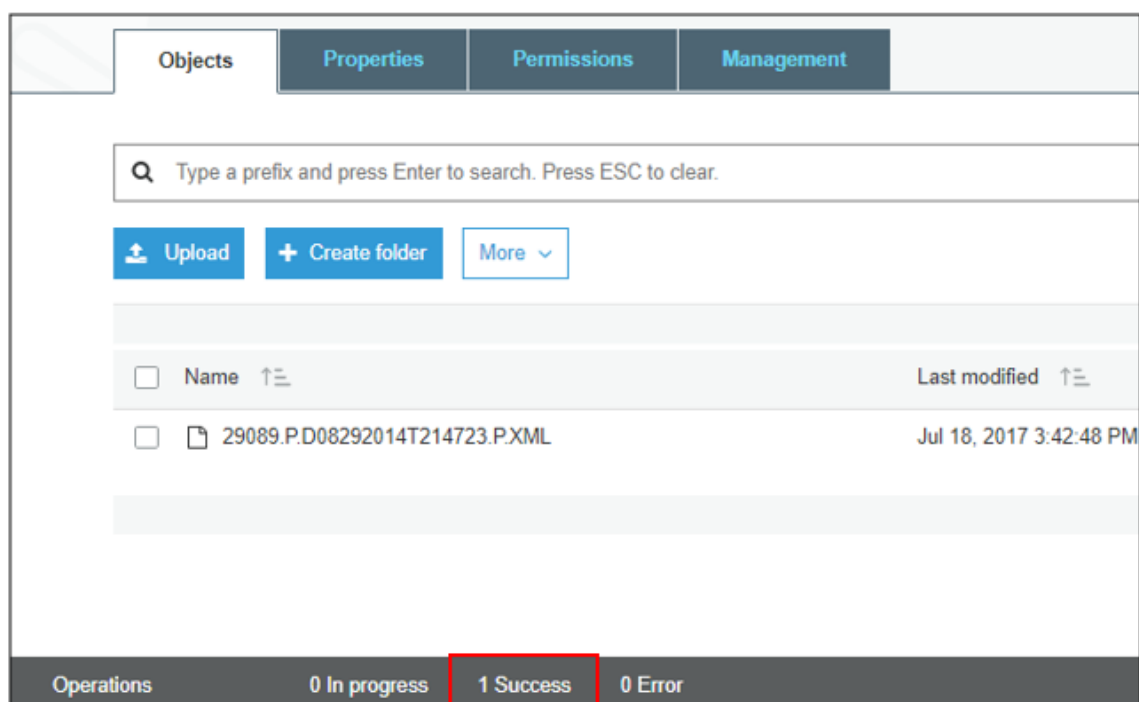


Figure 4-16: Upload Complete

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.

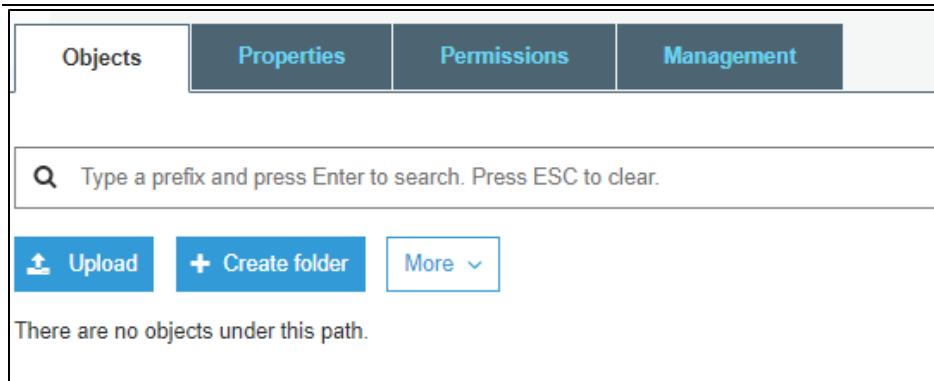


Figure 4-17: File Picked Up for Processing

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.

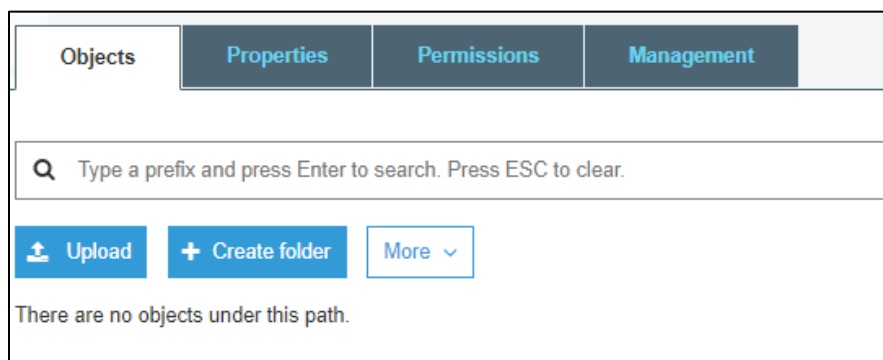


Figure 4-18: Refresh Inbox

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

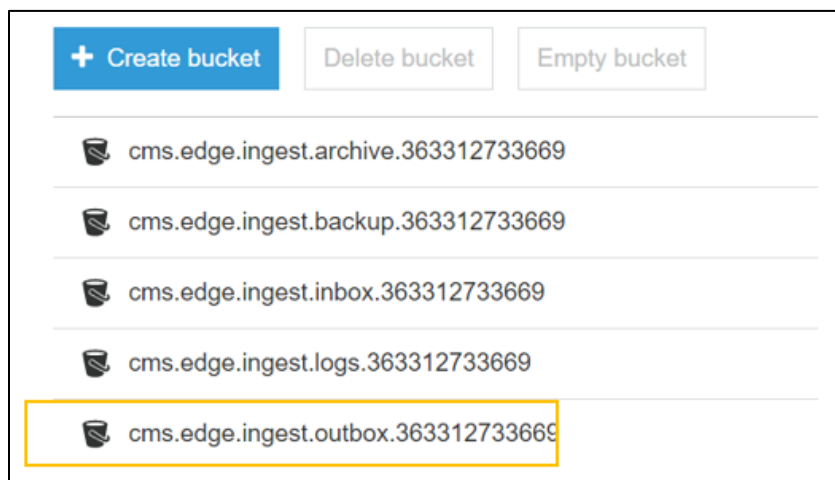


Figure 4-19: Select Outbox

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

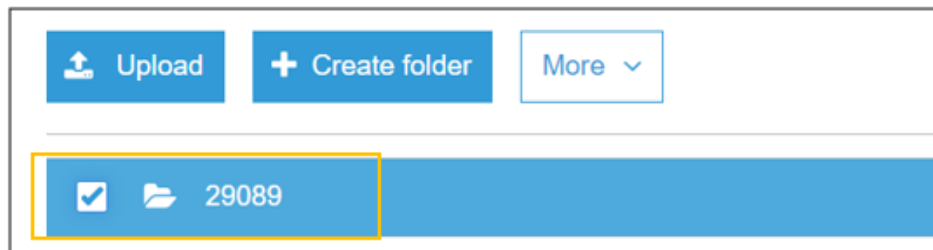


Figure 4-20: Select Issuer ID

- 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 4.1.3 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.

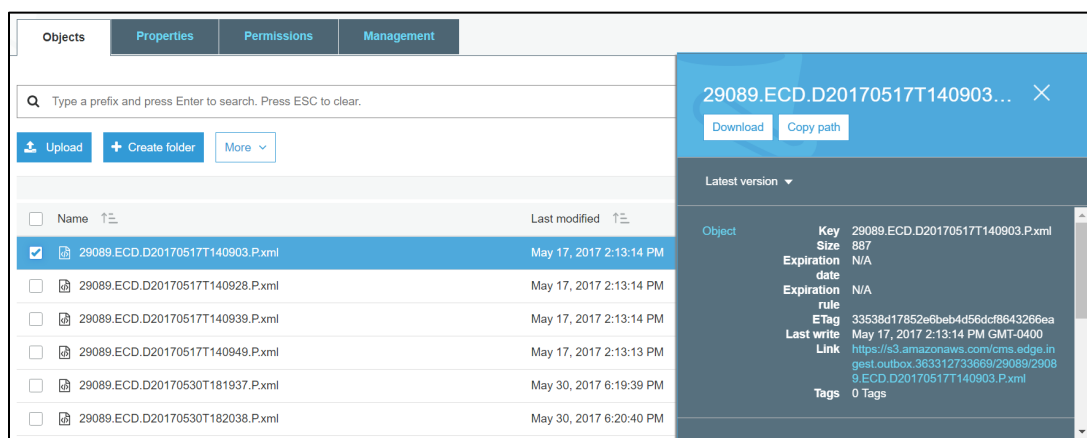


Figure 4-21: Locate and Download Report

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

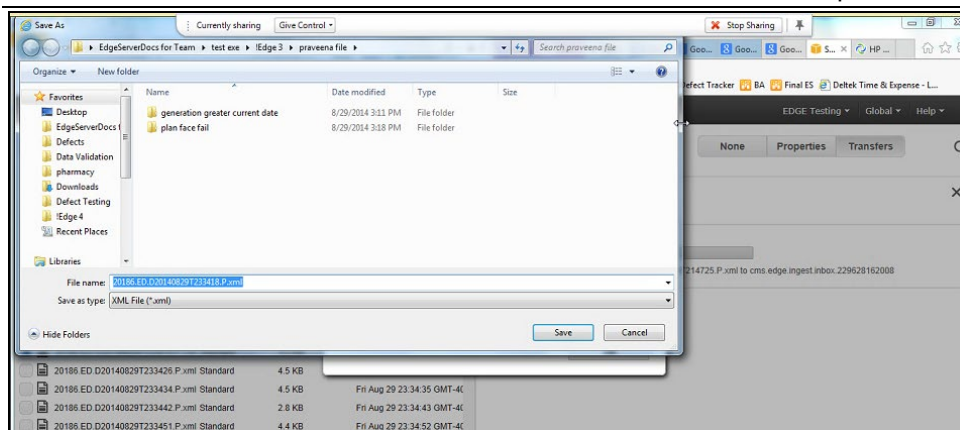


Figure 4-22: Save Downloaded Report

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 3.5.4: AWS EDGE Server 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.

4.1.5 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 3.4.1: Server Setup.

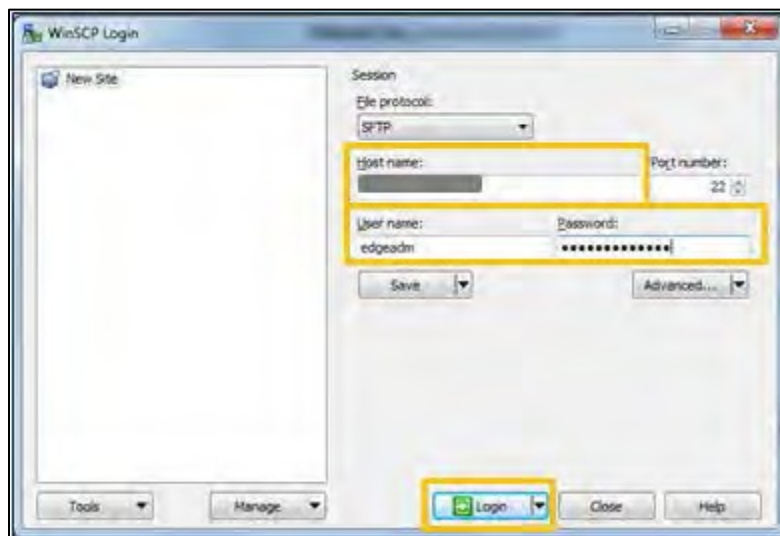


Figure 4-23: WinSCP Login Screen

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.

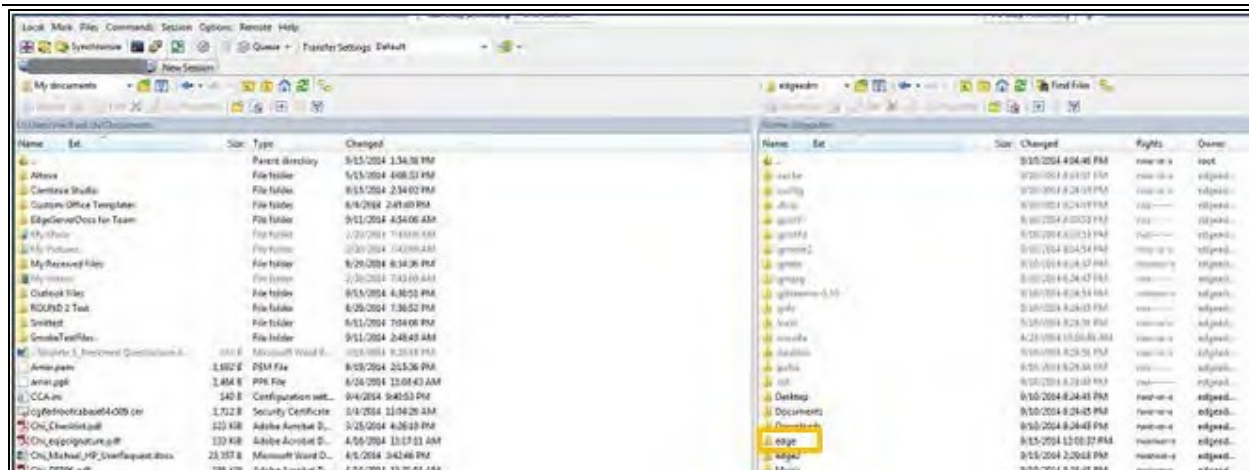


Figure 4-24: Edge Folder

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

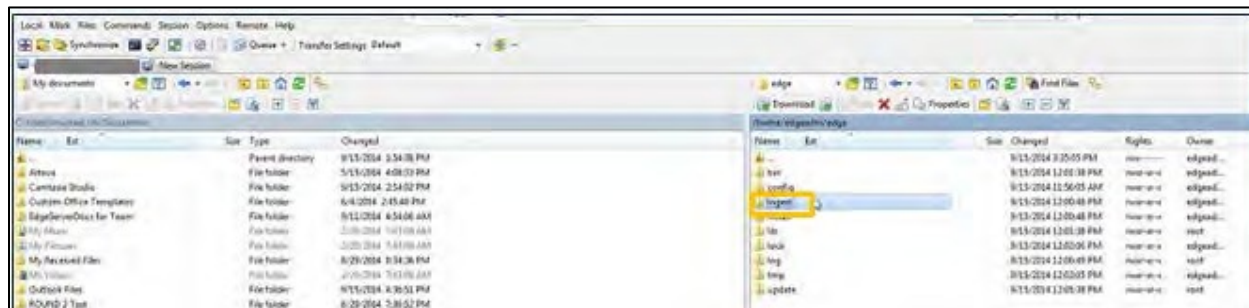


Figure 4-25: Ingest Folder

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



Figure 4-26: Inbox Folder

- 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.

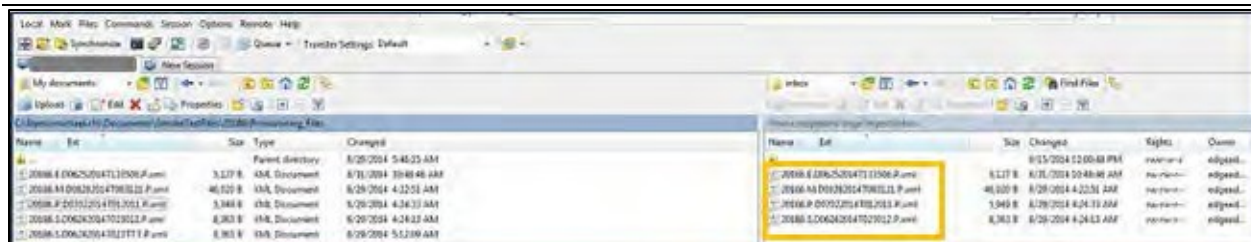


Figure 4-27: Drag and Drop Upload Files to Server

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.

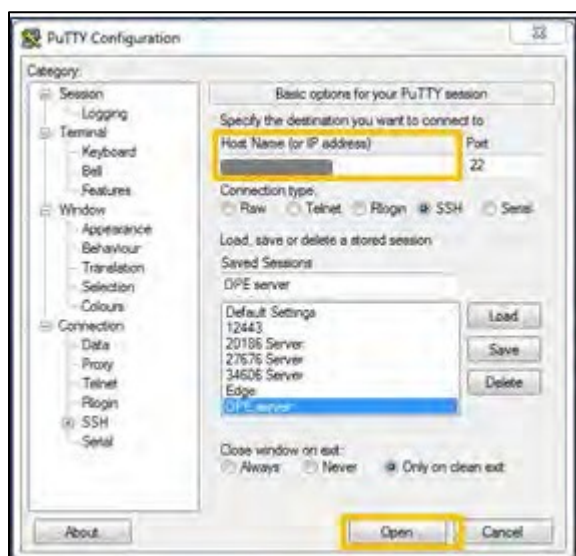


Figure 4-28: PuTTY Login Screen

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



Figure 4-29: Enter Username and Password

- 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.

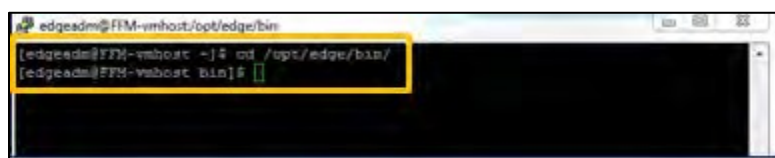


Figure 4-30: Open OPT Folder

8. 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`

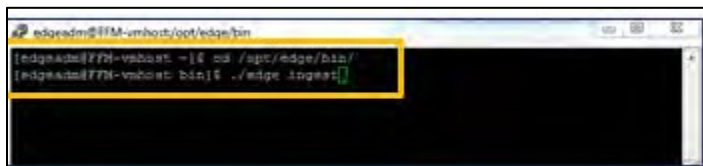


Figure 4-31: Run EDGE Ingest Command to Process Files

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

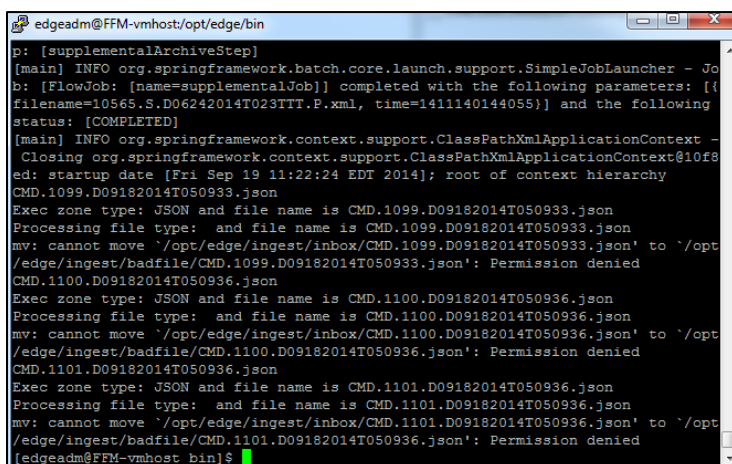


Figure 4-32: Files Processing Complete

10. 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.

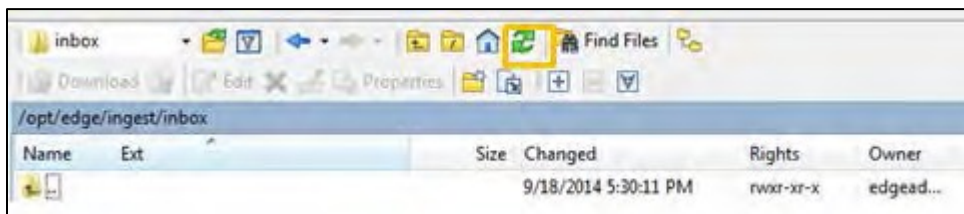


Figure 4-33: Refresh Inbox

Locate Outbound Reports

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



Figure 4-34: Navigate to Ingest Folder

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

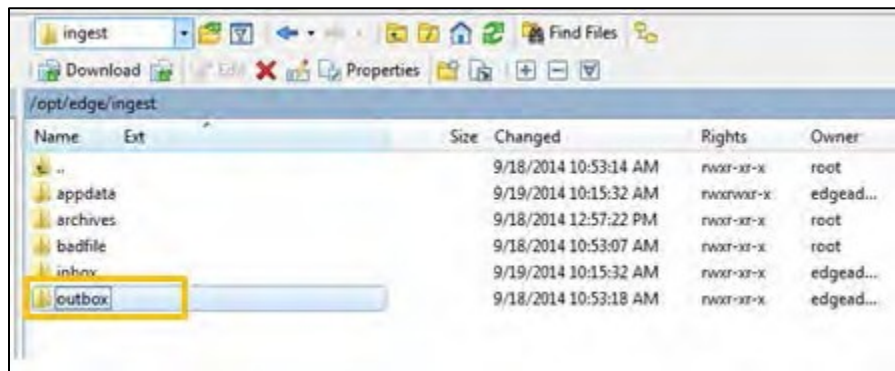


Figure 4-35: Open Outbox Folder

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

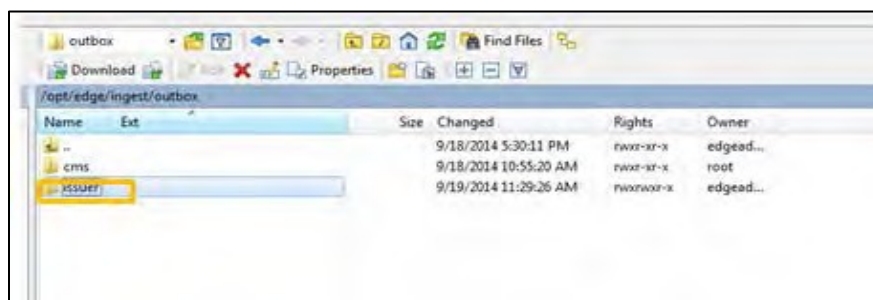


Figure 4-36: Open Issuer Folder

14. 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 4.1.3: 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

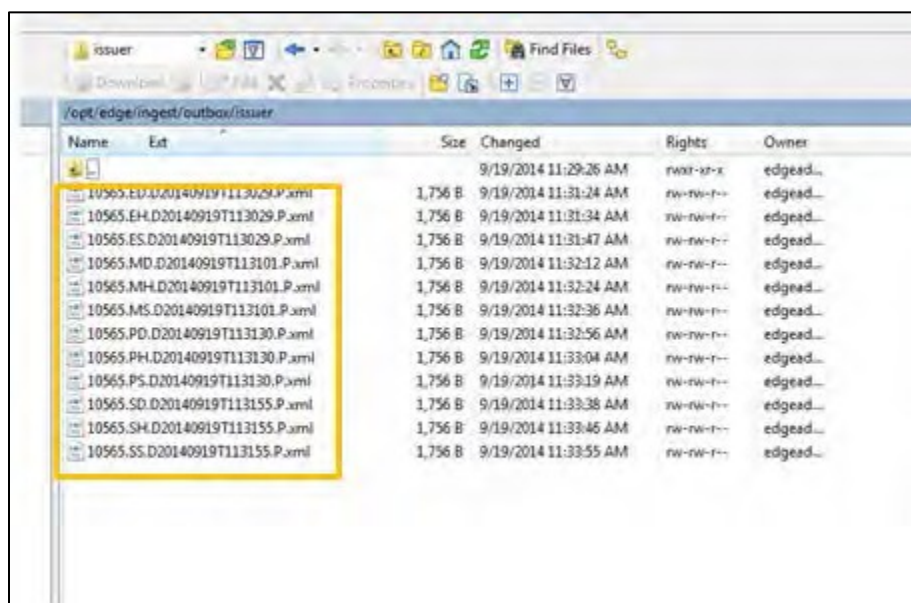


Figure 4-37: Outbound Reports Folder

15. 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

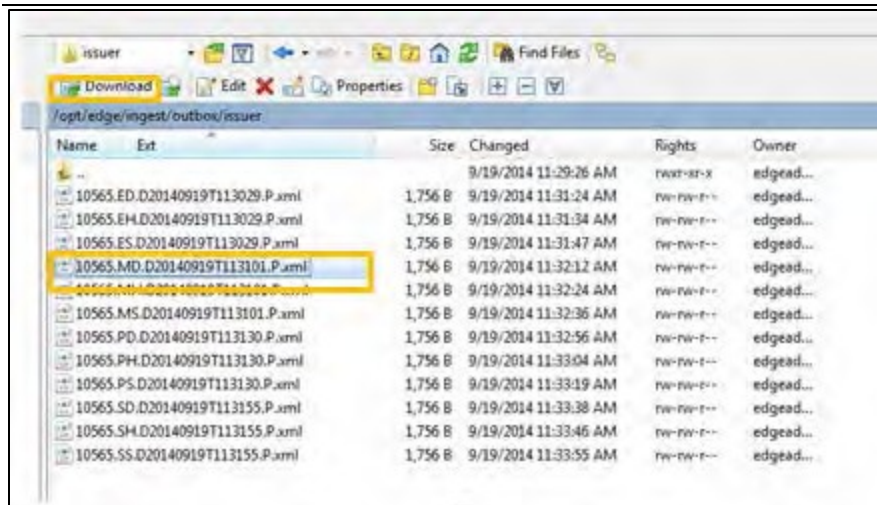


Figure 4-38: Locate Report to Download

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

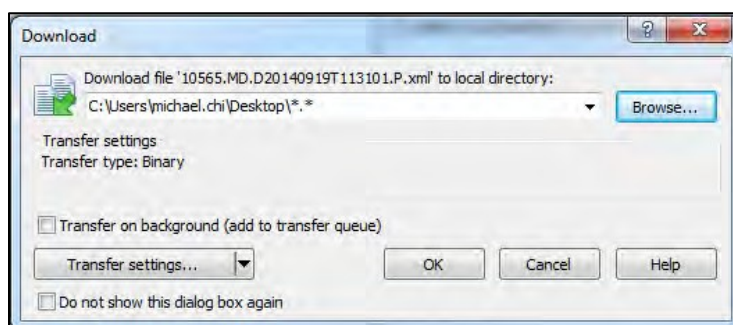


Figure 4-39: Download and Save Report

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.

4.1.6 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	ERRORTYPEID	STATUS_TYPE	CLAIM_IDENTIFIER	MEDICAL_SAVE_LINE_NUM
Enrollment coverage dates are not within the plan effective start and end dates	1	E	LogicalErrorType	6	4	I		NULL

Figure 4-40: 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 for further troubleshooting:

Appendix A: Enrollee File Ingest Job Error Messages

Appendix B: Pharmacy File Ingest Error Messages

Appendix C: Supplemental File Ingest Informational and Error Message; and

Appendix D: Medical File Ingest Informational and Error Messages - 244 contains more information about common ingest job error messages for each type of file. Refer to these appendices for further troubleshooting.

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.

4.1.7 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.



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/lib:/opt/edge/li
b/* org.springframework.batch.core.launch.support.CommandLineJobRunner edge-application.xml medicalJob time=1458166577423 file
name=57964.M.D10092014T120205.1.xml
```

Figure 4-41: 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 4-42: 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.



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 4-43: 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.



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 4-44: 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 4.1.6: 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 because
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 4-45: 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 4-46: Pharmacy Claims Accepted Records Query Results



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 4.1.6: 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.

4.1.8 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>
    <statusCode>R</statusCode>
  </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 4-47: 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.

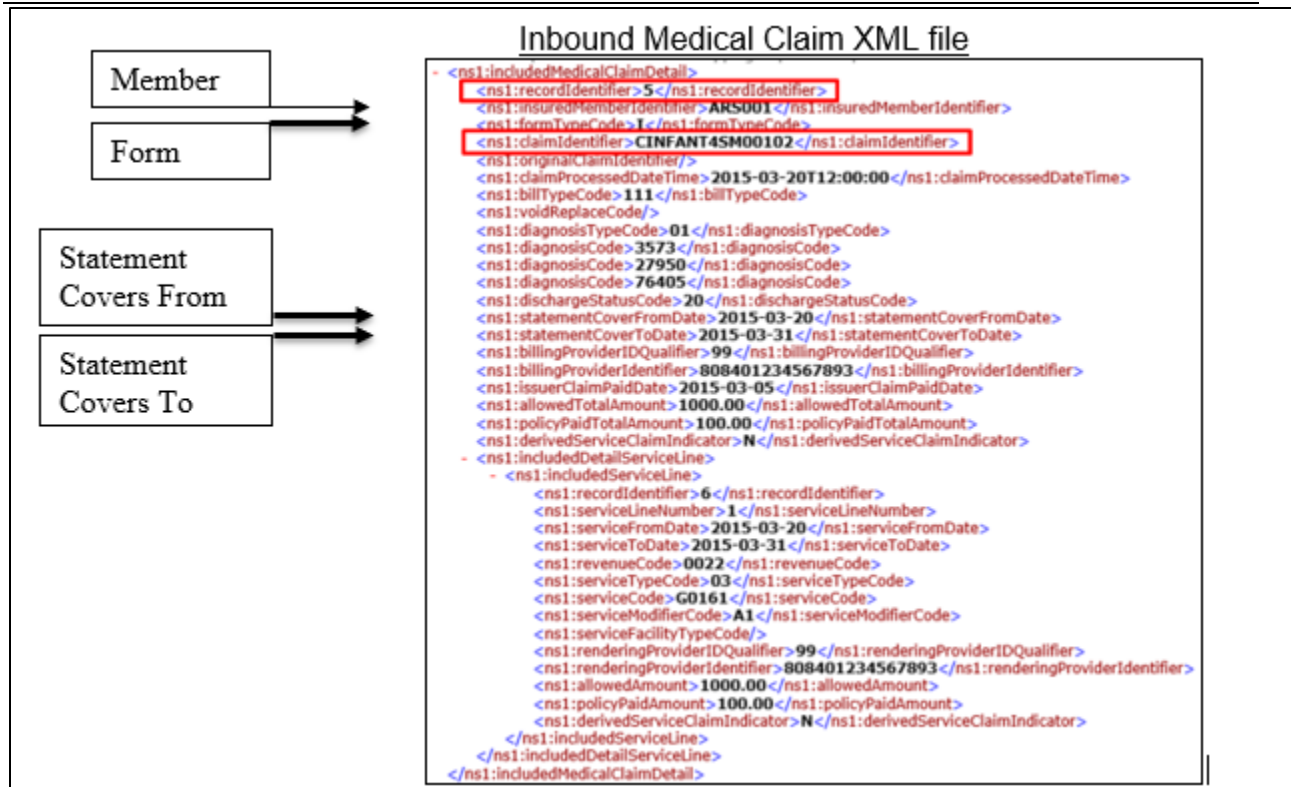


Figure 4-48: Example Inbound Claim

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 4-49: Example Query Output for Overlapping Query to Identify the Active Claim

The query result indicates the Claim ID that already exists as an active claim in the medical claim table and 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 4-50: 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 4-51: 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: CADULT4SMOO102
RECEIVED_INSURED_MEMBER_ID: ARSO02
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 4-52: Example Query Output for Potential Duplicate Claims: Institutional Outpatient Claims

The query result indicates the Claim ID that already exists as an active claim in the medical claim table and 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 4-53: 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.

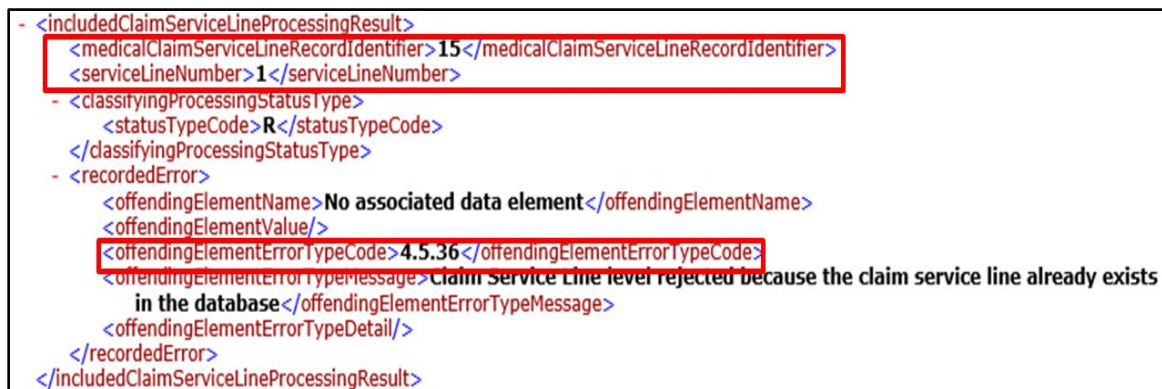
Follow the steps below to identify the existing claim that caused the inbound claim to be rejected due to the duplicate logic:

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>
    <statusCode>R</statusCode>
  </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 4-54: 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 4-55: 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 4-56: Example Query Output for Potential Duplicate Claims: Professional Claims

The query result indicates the Claim ID that already exists as an active claim in the medical claim table and 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 4.1.8: Troubleshooting Help for Claims Rejected as Duplicate.

```
• SELECT
mc.MEDICAL_CLAIM_ID,
mcsl.MEDICAL_SRVC_LINE_NUM,
mcsm.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 4-57: 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 4-58: 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 that already exists as an active claim in the pharmacy claim table and 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.

4.2 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.



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.

4.2.1 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.

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

Table 4-1: 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.
- edge truncate TEST - edge truncate validation	This command requires issuers to submit a one (1)-time permission request to the CMS. Issuers submit truncation requests through the EDGE Server Truncation Web form. The web form is available at https://acapaymentoperations.secure.force.com/EDGEServerTruncation 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. Once permission is granted, CMS will provide a script that can be executed at any time. This script does not expire and can be used as often as desired. The command will delete all data from the test schema data tables. There is no option to delete or truncate a single table or a subset of data. The production schema and common tables will be unaffected. Refer to Section 5.4: Truncation Requests for more information.

Command	Result
edge truncate PROD	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 available at https://acapaymentoperations.secure.force.com/EDGEServerTruncation 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. Once permission is granted, CMS will provide a script that can be executed only during the timeframe indicated. If the user is unable to execute the command in the given timeframe, the user must request an extension. This command will delete all data from the production schema data tables in EDGE server. There is no option to delete or truncate a single table or a subset of data. The test schema and common tables will be unaffected.
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.
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 5.2: Disaster Recovery for more information.

Command	Result
- 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 H: EDGE Server Reports and Local Commands and the Interface Control Document –RARI Addendum found in Section 4.1.2: Interface Control Document
- 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 H: EDGE Server Reports and Local Commands and in the Interface Control Document - RARI Addendum found in Section 4.1.2: Interface Control Document.
- edge report RA_RS_Transfer_Prelim YYYY test - edge report RA_RS_Transfer_Prelim YYYY prod - edge report RA_RS_Transfer_Prelim YYYY validation - edge report HCRP_NATIONAL_P RELIM YYYY test - edge report HCRP_NATIONAL_P RELIM YYYY prod - edge report HCRP_NATIONAL_P RELIM 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 Statistics (RADVPS) Report Descriptions of all reports can be found in Appendix H: EDGE Server Reports and Local Commands and in the Interface Control Document - RARI Addendum found in Section 4.1.2 Interface Control Document. 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 H: EDGE Server Reports and Local Commands and in the Interface Control Document – RARI Addendum found in Section 4.1.2: Interface Control Document

4.2.2 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 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 BY.

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 4-59: 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 4-60: 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 BY along with the order in which they will be staged. For further details, refer to Appendix H: EDGE Server Reports and Local Commands.

Table 4-2: 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 H: 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 H: EDGE Server Reports and Local Commands for the detailed description of each RI report.

CMS Staged Remote Commands	Description
- 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 H: EDGE Server Reports and Local Commands for the detailed description of each RA report.
- 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 H: 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 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 H: 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.

CMS Staged Remote Commands	Description
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 RI Analytic Calculation and Report (RIAR) and sends it to CMS.
- HCRP_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.

4.2.3 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 4.3.4 Storage Requirements 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 (DB) mount point for insufficient space, which is needed to successfully execute the copy remote command.



The system capacity must be at least double the size of the EDGE_SRVR_PROD schema 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:

5. Log into ESM portal in HIOS and click on the **Manage EDGE Server** button. Refer to Section 3.2.1: Accessing the ESM Website for additional steps.



Figure 4-61: EDGE Server Home

6. 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 4-62: EDGE Server Worklist and List of Servers

7. 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.



Figure 4-63: Copy Prod Data to Validation/Test Buttons

8. 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:

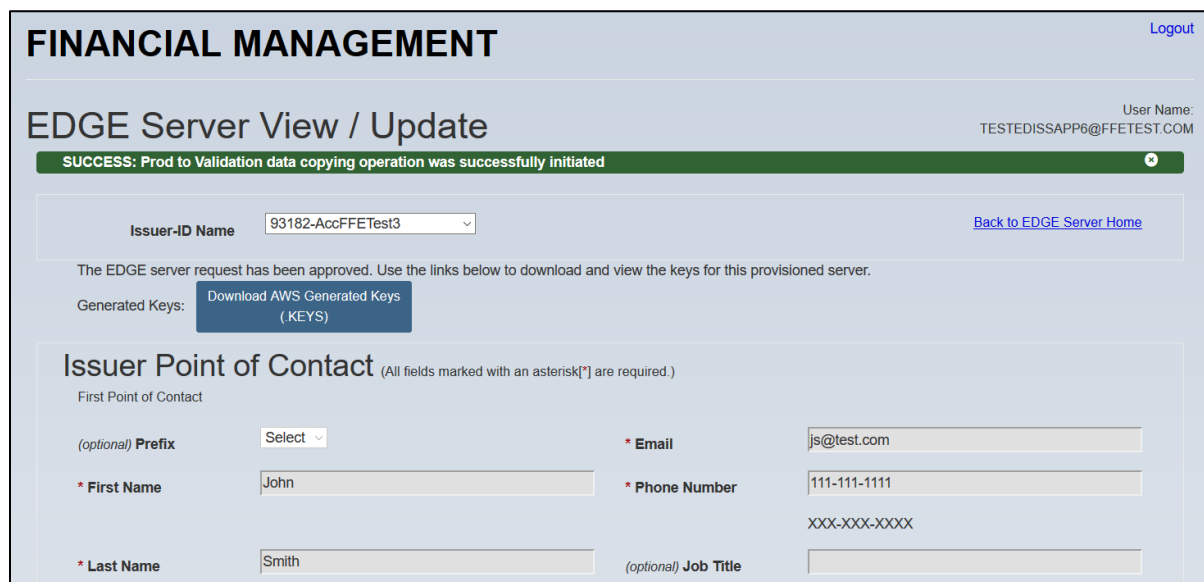


Figure 4-64: Prod to Test Success Message

9. 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: [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:

* First Name: * Last Name:

* Email: * Phone Number:

(optional) Job Title:

Figure 4-65: Prod to Test Failure Message

10. 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: [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:

* First Name: * Last Name:

* Email: * Phone Number:

(optional) Job Title:

Figure 4-66: Prod to Test Informational Message

11. 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 4-67: Execute Copy Command

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.

12. 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 4-68: EDGE Schemas

13. 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 **Error! Bookmark not defined.**Appendix G: 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.

4.2.4 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:

1. Clear all files under /tmp/ directory by running the following command:

- `rm -rf /tmp/*`



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.

2. If your server has not been rebooted for an extensive period of time, consider rebooting the server.
3. 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`

4. Restart MySQL service by running:

- `sudo service mysqld restart`



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.

4.2.5 Common Command Errors

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

4.3 Configuration

This section provides requirements for proper EDGE application configuration in order to maximize functionality.

4.3.1 edge.properties

Below is a sample edge.properties file and the contents that should be included. The edge.properties file is located on your EDGE server in the following location: /opt/edge/config.

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

```
#
#Sun MAY 18 14:49:13 EST 2017
db_port=3306
aws_s3_command=edge.commands.prod
db_password=*****
region=us-east-1
db_host=localhost
aws_s3_data=edge.data.prod
edgerequestid=
batch_csv_file_location_path=${local_file_ingest}/appdata
edgeserver=
local_file_ingest=${batch_location}/ingest
aws_s3_bin=edge.binaries.prod
batch_outbound_reports_cms_path=${local_file_ingest}/outbox/cms/
issuer=35671
batch_outbound_reports_es_id=EdgeServer_35671
batch_location=${EDGE_HOME}
batch_outbound_reports_issuer_path=${local_file_ingest}/outbox/issuer/
db_user=edgedbuser
batch_outbound_reports_es_version=100
batch_input_xml_file_path=${local_file_ingest}/inbox/
batch_archive_file_location_path=${local_file_ingest}/archives
edgeserver_size=L
edge_type=OP
aws_s3_bin_validation=edge.binaries.validation
aws_s3_data_validation=edge.data.validation
aws_s3_command_validation=edge.commands.validation
```

Figure 4-69: edge.properties file

4.3.2 my.cnf

Below is a sample my.cnf file and the contents that should be included. The my.cnf file is located on your EDGE server in the following location: /opt/edge/config. Please contact a FMCC representative at EDGE_Server_Data@cms.hhs.gov before making any changes to the file.

```
# For advice on how to change settings please see
# http://dev.mysql.com/doc/refman/5.7/en/server-configuration-defaults.html

[mysqld]
#
# Remove leading # and set to the amount of RAM for the most important data
# cache in MySQL. Start at 70% of total RAM for dedicated server, else 10%.
# innodb_buffer_pool_size = 128M
#
# Remove leading # to turn on a very important data integrity option: logging
# changes to the binary log between backups.
# log_bin
#
# Remove leading # to set options mainly useful for reporting servers.
# The server defaults are faster for transactions and fast SELECTs.
# Adjust sizes as needed, experiment to find the optimal values.
# join_buffer_size = 128M
# sort_buffer_size = 2M
# read_rnd_buffer_size = 2M
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock

# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid

secure_file_priv=''

sql_mode = "STRICT_TRANS_TABLES,NO_ZERO_DATE,ERROR FOR DIVISION BY ZERO,NO AUTO CREATE USER,NO ENGINE SUBSTITUTION"
```

Figure 4-70: Sample: my.cnf File

4.3.3 Directory Ownership

Below is a screenshot of the /opt/edge directory and schemas with associated ownership. This view can be found by navigating to the directory and viewing in list form. Please contact the FMCC at EDGE_Server_Data@cms.hhs.gov before making any changes to this file. /opt/edge

```
[ec2-user@edgeServer-29089 ~]$ ls -ltr
total 50432
-rw-r--r--. 1 root      root          165 Apr 11 18:14 install.out
-rw-r--r--. 1 root      root           0 Apr 11 18:14 install.err
-rw-r--r--. 1 root      root           81 Apr 11 18:14 1
-rw-rw-r--. 1 ec2-user ec2-user    266666 May 15 17:58 index.html
-rw-rw-r--. 1 ec2-user ec2-user 25585210 Jul 18 15:04  edge_common.sql
-rw-rw-r--. 1 ec2-user ec2-user     784 Jul 18 15:14 edge_common_v_sql.sql
-rw-rw-r--. 1 ec2-user ec2-user    118256 Jul 18 15:28 edge_prod.sql
-rw-rw-r--. 1 ec2-user ec2-user    118569 Jul 18 15:29 edge_test.sql
-rw-rw-r--. 1 ec2-user ec2-user    119365 Jul 18 15:31 edge_validation.sql
-rw-rw-r--. 1 ec2-user ec2-user 25396283 Jul 18 15:31 edge_common_v.sql
-rw-rw-r--. 1 ec2-user ec2-user     12287 Jul 18 15:32 edge_common.sql
[ec2-user@edgeServer-29089 ~]$
```

Figure 4-71: Sample: Ownership of Directories (Image1 of 2)

```
[ec2-user@edgeServer-29089 ~]$ cd /opt/edge
You have new mail in /var/spool/mail/ec2-user
[ec2-user@edgeServer-29089 edge]$ ls -ltr
total 60
drwxr-xr-x. 2 ec2-user ec2-user  4096 Apr 11 18:23 bin
drwxr-xr-x. 8 ec2-user ec2-user  4096 May 30 17:44 ingest
drwxr-xr-x. 2 ec2-user ec2-user 12288 May 30 18:10 lib
drwxr-xr-x. 6 ec2-user ec2-user  4096 May 30 18:10 update
drwxr-xr-x. 2 ec2-user ec2-user  4096 May 30 18:17 tmp-validation
drwxr-xr-x. 2 ec2-user ec2-user 12288 May 30 18:17 lib-validation
drwxr-xr-x. 6 ec2-user ec2-user  4096 May 30 18:17 update-validation
drwxr-xr-x. 3 ec2-user ec2-user  4096 May 30 18:20 tmp
-rw-rw-r--. 1 ec2-user ec2-user     0 Jul 12 15:14 edge.log
drwxr-xr-x. 2 ec2-user ec2-user  4096 Jul 12 15:17 log
drwxr-xr-x. 2 ec2-user ec2-user  4096 Jul 18 14:13 config
drwxr-xr-x. 2 ec2-user ec2-user  4096 Jul 18 16:07 lock
```

Figure 4-72: Sample: Ownership of Directories (Image 2 of 2)

4.3.4 Storage Requirements

Issuers are required to have sufficient storage requirements to participate in EDGE programs. Issuers can identify server storage by following the below three (3) steps. These steps are referenced in Sections 4.2.3 Prod to Test and Prod to Validation Copy Command and 5.3.1 Pre-Archive Steps.

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

- Log on to the server and access the properties file by entering:
- `cd /opt/edge/config`

- view edge.properties

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

Figure 4-73: Edge.properties - DB User (Image 1 of 2)

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

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

Figure 74: Edge.properties - DB User (Image 2 of 2)



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

Step 2: Identify Custom Schemas, if Applicable

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

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

Figure 4-75: Schemas Check

Step 3: Check Current Storage Space Usage by Database Schemas

Issuers should verify they have sufficient storage space to accommodate EDGE activities (example: the archive data and the new BY data that will be restored and submitted through the archive process). The following steps can be used to check the DB storage space currently used by DB schemas on the MySQL server.



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

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

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

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

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

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

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

mysql>
```

Figure 4-76: MySQL - DB User Login

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

1. Run the following **SQL** from MySQL shell to check storage space.
 - a. `SELECT table_schema "Data Base Name",`

```
sum( data_length + index_length ) / 1024 /
1024 "Data Base Size in MB"
FROM information_schema.TABLES
GROUP BY table_schema;
```

```
mysql> SELECT table_schema "Data Base Name",
-> sum( data_length + index_length ) / 1024 /
-> 1024 "Data Base Size in MB"
-> FROM information_schema.TABLES
-> GROUP BY table_schema;
+-----+-----+
| Data Base Name | Data Base Size in MB |
+-----+-----+
| EDGE_SRVR_COMMON | 67.01562500 |
| EDGE_SRVR_COMMON_V | 66.84375000 |
| EDGE_SRVR_PROD | 3.73437500 |
| EDGE_SRVR_TEST | 2.95312500 |
| EDGE_SRVR_VALIDATION | 2.95312500 |
| information_schema | 0.15625000 |
+-----+-----+
6 rows in set (0.03 sec)
```

Figure 4-77: Schema Storage Space

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



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

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

- exit
- cd /opt/edge/config

- Based on DB size, issuers can increase the space available on the DB Mount points for the back-up schemas and also for upcoming file ingests. To check the available space, enter the following command:

- df -k /var/lib/mysql

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

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

Figure 4-78: DB Mount Points

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

- df -k /opt/edge

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

Figure 4-79: DB Backup - Space Check

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

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

In such cases, additional storage space is required to be added



There is no difference between space and storage space. The command will fail when there is insufficient space. To resolve this error, issuers need to contact their internal infrastructure team to increase space.

EDGE Server Storage

For errors related to EDGE Server Storage and/or insufficient capacity issues for AWS, open up a ticket with AWS and open a case with the FMCC in order to assist in supporting solution. Please update your FMCC representative on the progress.

The following steps provides guidance for submitting a ticket with AWS. The example ticket is requesting additional storage.

1. Click on the **Help** dropdown in the upper right corner of the screen.

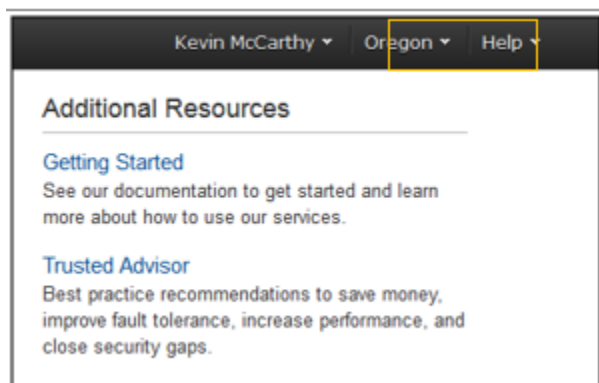


Figure 4-80: Help Dropdown Location

2. Select **Support** from the choices available in the Help dropdown.

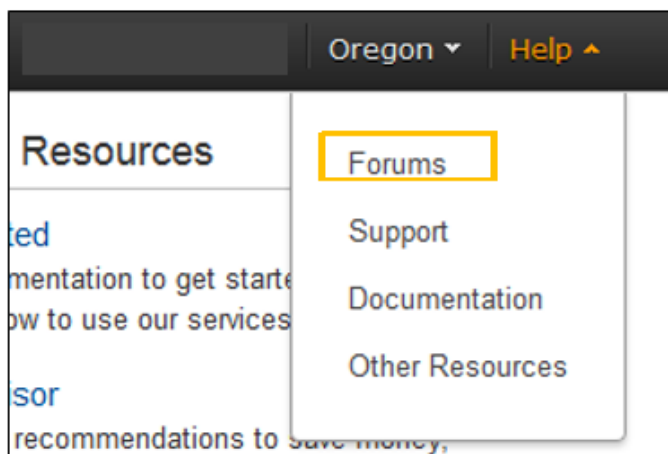


Figure 4-81: Expanded Help Dropdown

3. The AWS Support Center section will appear. Click the ***Open a new case*** button.

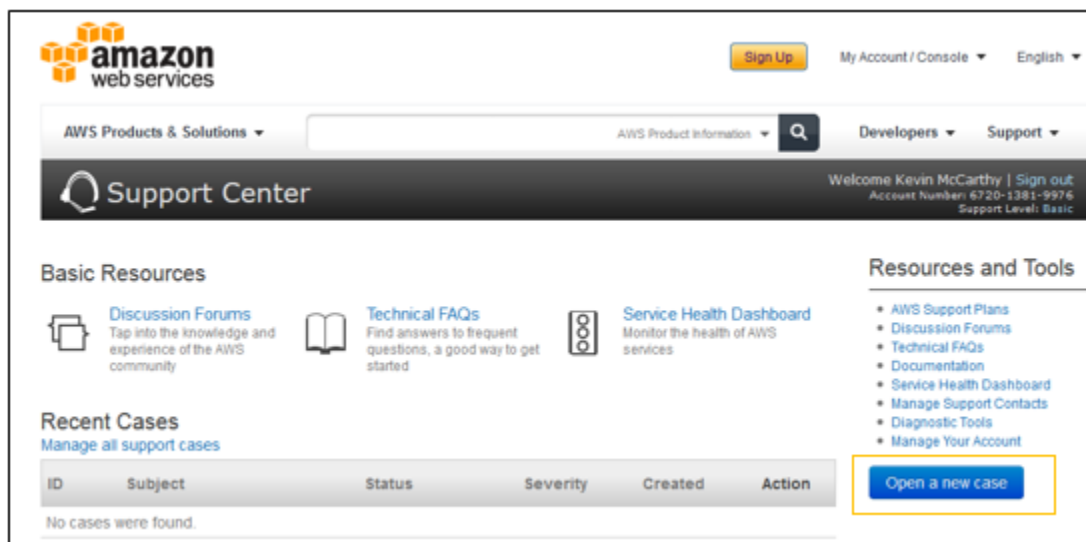


Figure 4-82: AWS Support Center

4. Select the ***Service Limit Increase*** option.

Figure 4-83: “Open a new case” Screen

5. Complete the **Open a new case** form:
 - a. Click on the Limit Type dropdown and select *EC2 Instances*
 - b. Enter *10* for New Instance Limit

- c. Click on the **EC2 Region** dropdown and select the AWS geographic location:
 - us-east-1 / US Standard (Virginia)
 - us-west-1 (Northern California)
 - us-west-2 (Oregon)
- d. Select *Linux/OpenSolaris* from the Operating System dropdown
- e. Click on the **Primary Instance Type** dropdown and select one (1) of the following three (3) choices:
 - c3.xlarge (Equivalent to small on the Server Size Estimation Table and Provisioning Template)
 - c3.2xlarge (Equivalent to medium on the Server Size Estimation Table and Provisioning Template)
 - c3.4xlarge (Equivalent to large on the Server Size Estimation Table and Provisioning Template)

Table 4-3: Server Size Estimation

Primary Instance Type	Size	Number of Enrollees	Claims Processing Throughput per Hour
c3.xlarge	Small	1,000,000	500,000
c3.2xlarge	Medium	5,000,000	1,000,000
c3.4xlarge	Large	20,000,000	2,000,000

- f. Click on the **Frequency of Usage** dropdown and select ***Always On***
- g. Enter “*Requesting EC2 service limit increase*” into the Use Case Description textbox
- h. Fill out Contact Information
- i. Click on **Web**.
- j. Click on either **Web** or **Phone** for Contact Method.

The limit can potentially be increased in less than 30 minutes if you select the call option whereas the web option may take longer.

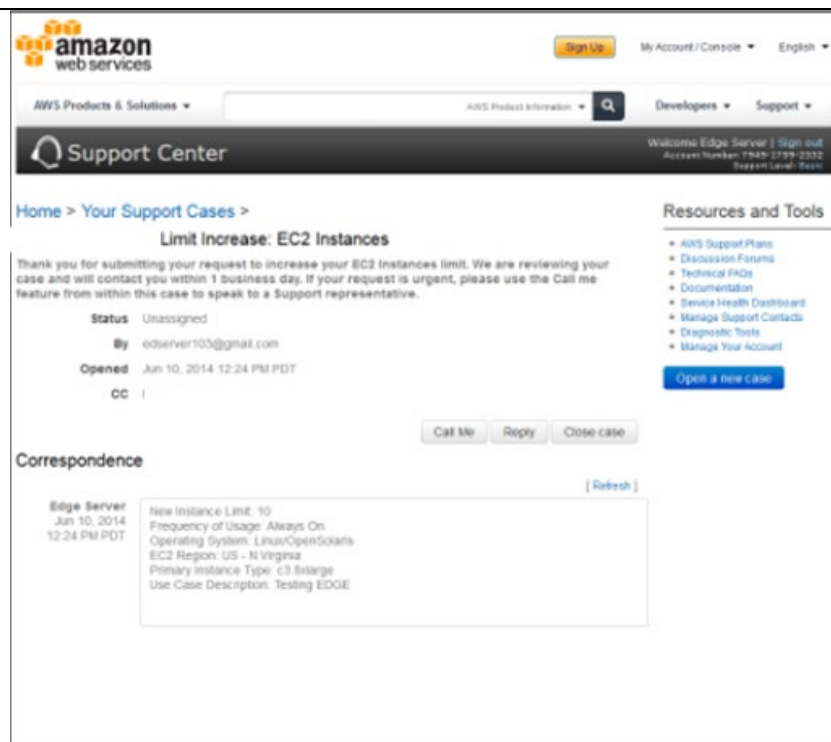


Figure 4-84: AWS Service Limit Request - Call Me or Web Choice



Issuers should wait until AWS increases the service increase before proceeding to the next section. AWS will send an email notification once the service increase is complete. The typical turnaround time for this process is 48 hours.

4.3.5 Automated Job Scheduling

Currently there is one (1) application that is executed by the CRON scheduler. Future functionality needing CRON jobs will be documented in this table.

Table 4-4: CRON Jobs

Application Name	Schedule	Description
Inbox Poll	Every five (5) minutes (Default setting)	Polls the EDGE Server Inbox for issuer XML files to process. This application also executes the appropriate batch job depending on the data file retrieved from the EDGE Server Inbox

The scheduled execution of this CRON job can be modified. The CRON job can be turned off at the discretion of the issuer's operations team. If this CRON job is turned off, then the issuer data will need to be processed manually by executing the EDGE command job detailed in Section 4.2.1: Local Commands.

4.4 Application Error Logging

In addition to the operating system OS logs located on the EDGE server, the EDGE server application tracks informational and error messages to the EDGE.log file located in the **/opt/edge/logs** directory. The default configuration of the EDGE server is to have the EDGE server application only log errors to the EDGE.log file; however, more detailed logging can be enabled as outlined in the following section.

4.4.1 Application Debug Level

To better troubleshoot errors, it is helpful to adjust the EDGE server settings to either DEBUG or WARN log settings. Please see the below table for guidance to change these settings:

Table 4-5: Application Debug Level

Category	Log Setting	Steps	Additional Steps
EDGE Server Settings	DEBUG Log Setting	1. Log in into the server 2. Go to configuration directory (<i>This could vary based on Issuer configuration</i>) • <code>cd /opt/edge/config</code> 3. Edit the logback.xml • <code>vi logback.xml</code> 4. Edit this line • <code><logger level="WARN" name="gov.hhs.cms"/></code> 5. Change it to • <code><logger level="DEBUG" name="gov.hhs.cms"/></code> 6. Save the file and exit	Must revert back to WARN as part of the full process
EDGE Server Settings	WARN Log Setting	1. Login into the server 2. Go to configuration directory (This could vary based on issuer configuration) • <code>cd /opt/edge/config</code> 3. Edit the logback.xml • <code>vi logback.xml</code> 4. Edit this line • <code><logger level="DEBUG" name="gov.hhs.cms"/></code> 5. Change it to • <code><logger level="WARN" name="gov.hhs.cms"/></code> 6. Save the file and exit	None

4.4.2 Common Application Errors

Application errors occur when the server is not properly set up or has become non-compliant. Common application errors can be documented in the edge.log. Refer to Appendix E: Common Errors for a list of common errors in the edge.log and their resolutions. Appendix E contains common errors related to remote commands, 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.

Section 5 - Backup and Maintenance Procedures

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

A local command has been provided to back up the EDGE Server MySQL database server, as will be described in Section 5.1.1: Backup Command. However, the issuer's operations team is responsible for executing this command and placing the resulting backup file onto a safe repository. Issuers can either use the CMS provided backup command or follow their own backup processes.

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

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

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

5.1 Backup and Data Retention Policy

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

For example, for BY2014, data must be retained on an active EDGE server until June 30, 2017. The 10-year data retention requirement is met 10 years after the final calculation of a BY and therefore, BY2014 data must be retained until June 30, 2025.

Required:

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

- Storage of the EDGE data SQL tables is the minimum requirement to meet the data retention policy.

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

TPA Considerations:



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

Recommendations:

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

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

If the host of the EDGE server is changed during the three (3) year data retention period, the data must be migrated to the new active server for that HIOS ID for the duration of the data retention period. After this period, the determination in maintaining the EDGE server is at the discretion of the owner. If an issuer switches from one (1) TPA to another TPA, the issuer must move their entire data backup using the same

issuer ID to the new server that they plan on using to submit EDGE server data for RA/RI. The second TPA is then responsible for maintaining their MySQL data in an active, query-able status.

Issuers will need to ensure three (3) years of data is accessible on a single active EDGE server regardless of the party responsible for maintaining or storing the EDGE server data except as outlined below. After three (3) years, the data may be stored as .sql files in a location of the issuer's choice. For example,

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

5.1.1 Backup Command

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

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

- `./edge dbbackup`

The backup command **will** include:

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

The backup command **will not** include:

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

Issuer's Responsibilities:

1. The backup command will not back up any XML ingest files submitted to the server or output XML files generated by the server. CMS

recommends that the issuer backs up the XML ingest files submitted to the server for processing and the generated XML output files for the current processing year and any year for which they have submitted an appeal, in the event that the XML files are needed for research.

2. Once the backup files are generated, it is the issuer's responsibility to store the database tables and files in a secure location, off the EDGE server, in a manner that meets their internal IT backup policies.

5.1.2 Pre-Step Checklist

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

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

5.1.3 Executing the Backup Command - AWS Server

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



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

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

Logging into PuTTY

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

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

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

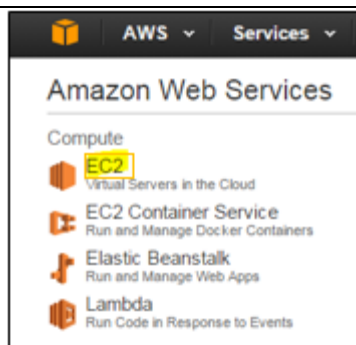


Figure 5-1: AWS Account - EC2

3. Click on “Running Instances”.

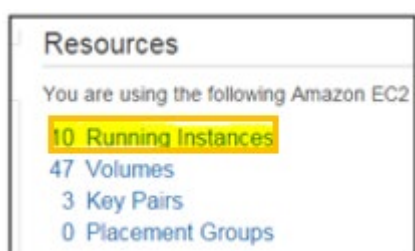


Figure 5-2: AWS Account - Running Instances

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

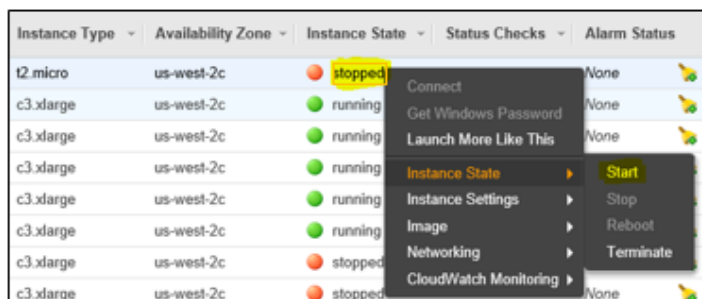


Figure 5-3: AWS Account - Instance State

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

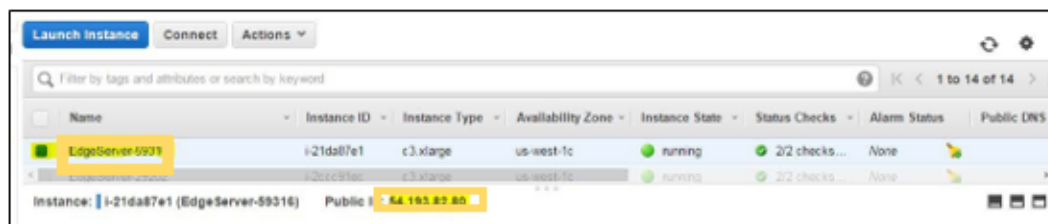


Figure 5-4: AWS Account - Public IP Address

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

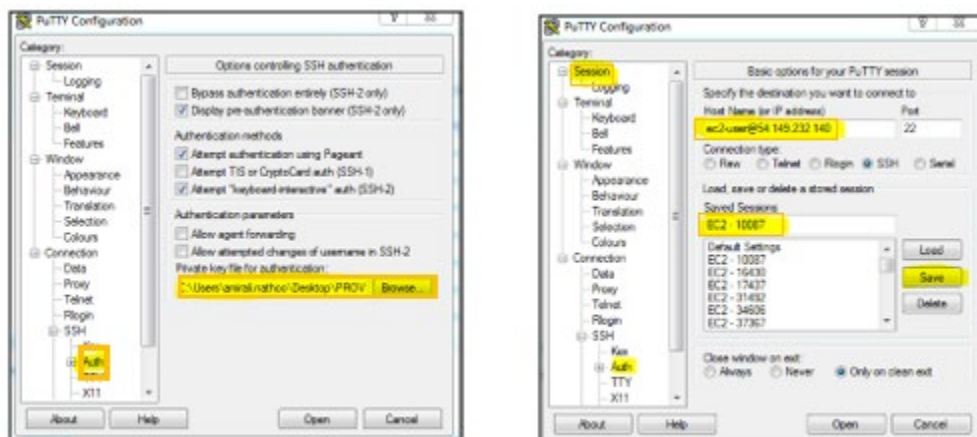


Figure 5-5: Logging into PuTTY

Verifying the Schema Information

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

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

- show schemas

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

Figure 5-6: DB Schemas

9. Verify all your schemas are present.
10. At the MySQL command prompt, exit back to the UNIX command prompt by executing:

- quit

11. At the command prompt, type the command:

- `./edge dbbackup`

and press “**enter**”.

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

Figure 5-7: Backup Command Prompt for AWS Server

12. Wait for the backup process to complete successfully.

Verifying the Backup for an AWS Server

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

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

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



Figure 5-8: AWS S3 Folder

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

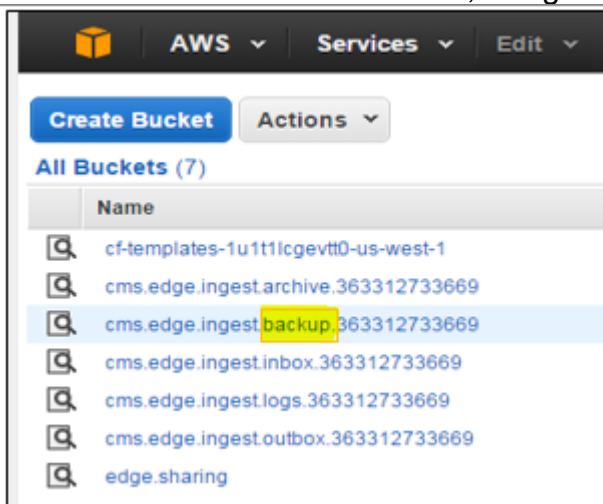
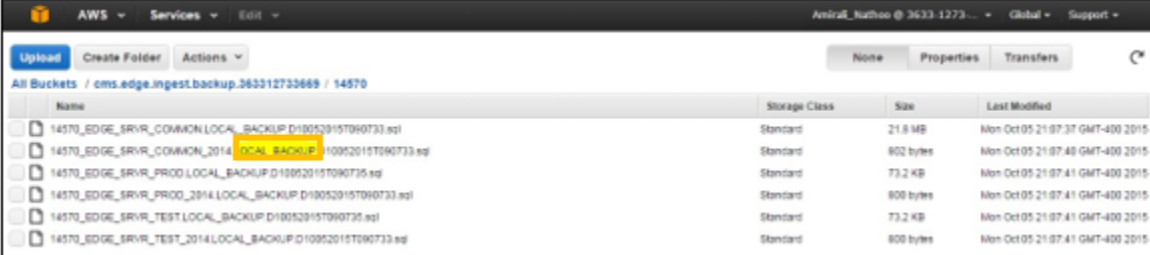


Figure 5-9: S3 Backup Folder

16. Select your server ID and click on it to enter the folder.
17. Verify that your backup is visible inside the folder.
 - a) Verify the backup for all your schemas are created with *IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql*
 - b) Verify the date the backup files were created (Should be current date and time).



Name	Storage Class	Size	Last Modified
14570_EDGE_SRVR_COMMON_LOCAL_BACKUP.D10052015T090733.sql	Standard	21.8 MB	Mon Oct 05 21:07:37 GMT-400 2015
14570_EDGE_SRVR_COMMON_2014_LOCAL_BACKUP.D10052015T090733.sql	Standard	802 bytes	Mon Oct 05 21:07:48 GMT-400 2015
14570_EDGE_SRVR_PROD_LOCAL_BACKUP.D10052015T090735.sql	Standard	73.2 KB	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRVR_PROD_2014_LOCAL_BACKUP.D10052015T090733.sql	Standard	800 bytes	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRVR_TEST_LOCAL_BACKUP.D10052015T090735.sql	Standard	73.2 KB	Mon Oct 05 21:07:41 GMT-400 2015
14570_EDGE_SRVR_TEST_2014_LOCAL_BACKUP.D10052015T090733.sql	Standard	800 bytes	Mon Oct 05 21:07:41 GMT-400 2015

Figure 5-10: Verify Creation of Backup Files

Accessing your Backup files from an AWS Server



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

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

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



Figure 5-11: S3 Folder Page

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

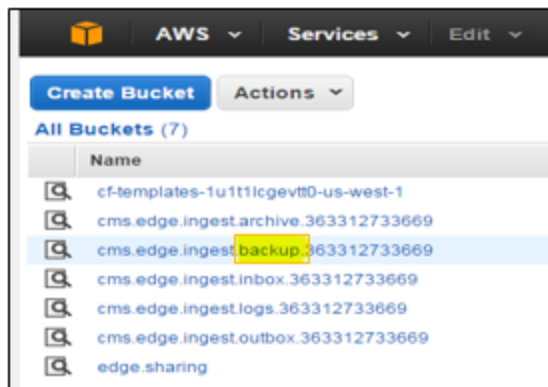


Figure 5-12: Backup Folder Link

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

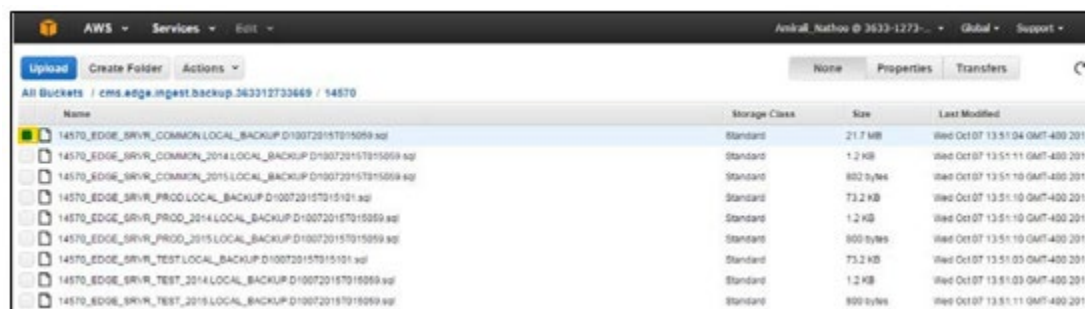


Figure 5-13: Selecting Backup File (Image 1 of 3)

23. Right click on the selected file and click on the “Download” link.

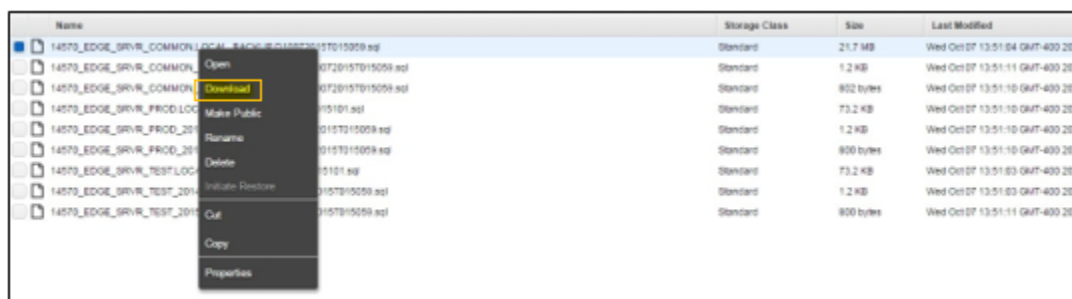


Figure 5-14: Selecting Backup File (Image 2 of 3)

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



Figure 5-15: Selecting Back up File (Image 3 of 3)

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

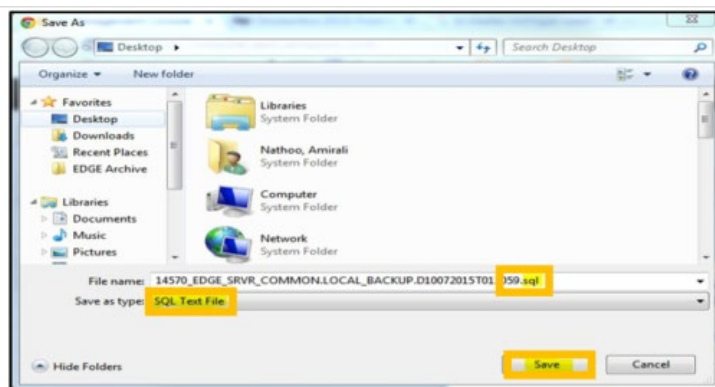


Figure 5-16: Saving the Backup File

5.1.4 Executing the Backup Command - On-Premise Server

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



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

26. Connect to the OP EDGE server using PuTTY or your preferred SSH client.

27. Navigate to the **cd /opt/edge/bin** folder.

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

Figure 5-17: Navigate to opt/edge/bin folder

28. At the command prompt, execute the command:

- **./edge dbbackup**

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

Figure 5-18: OP Backup Command Prompt

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

Verifying the Backup for an OP Server

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

30. Log in to the OP server.

31. Execute the following commands to navigate to the backup folder and view contents:

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

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

Figure 5-19: Ingest Backup Command

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

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

```
[ec2-user@HPT1_OP_80991 backup]$ ll
total 64396
-rw-rw-r--. 1 ec2-user ec2-user      791 Oct  6 13:17 80991_EDGE_SRVR_COMMON_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user 22914528 Oct  6 13:17 80991_EDGE_SRVR_COMMON.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user      789 Oct  6 13:17 80991_EDGE_SRVR_PROD_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user    78009 Oct  6 13:17 80991_EDGE_SRVR_PROD.LOCAL_BACKUP.D10062015T011742.sql
-rw-rw-r--. 1 ec2-user ec2-user      789 Oct  6 13:17 80991_EDGE_SRVR_TEST_2014.LOCAL_BACKUP.D10062015T011738.sql
-rw-rw-r--. 1 ec2-user ec2-user    78009 Oct  6 13:17 80991_EDGE_SRVR_TEST.LOCAL_BACKUP.D10062015T011741.sql
```

Figure 5-20: Confirming Creation of Backup File for OP Extraction

Saving your Backup Files from an OP Server



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

33. Retrieve your IP Address.

34. Log in to WinSCP

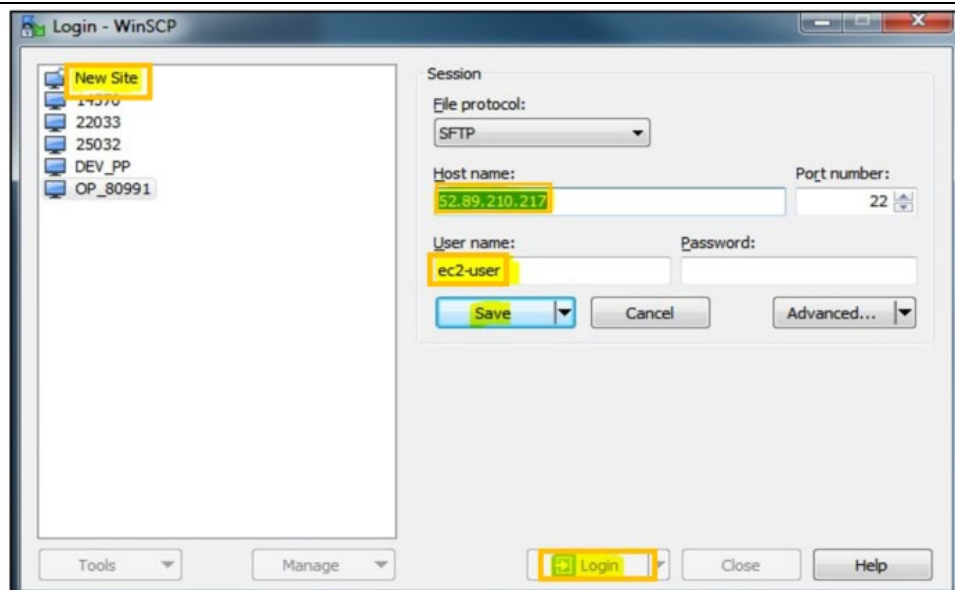


Figure 5-21: Log in to WinSCP

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

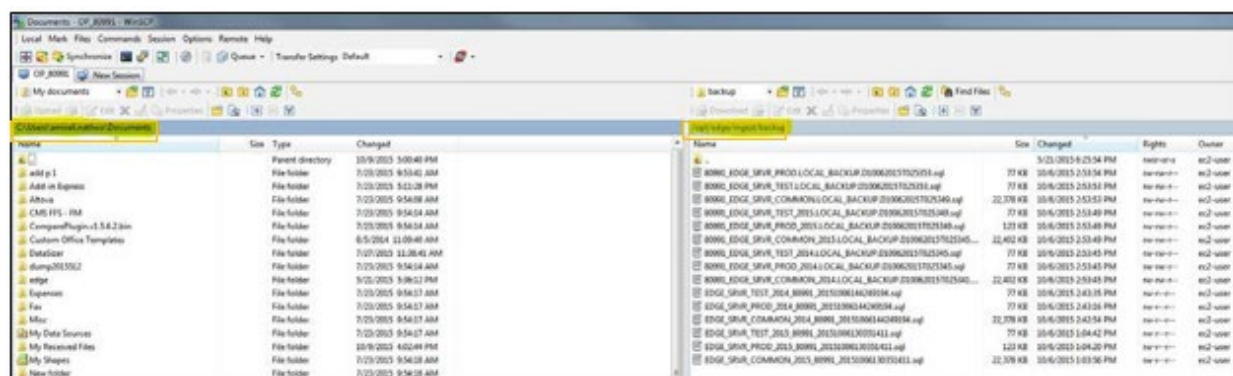


Figure 5-22: Ingest Folder

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

5.1.5 Restoring from Backup Files

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

Issuers must contact an FMCC Service Representative Team for technical assistance for both OP or AWS servers. CMS encourages issuers to report issuer-based problems

as soon as possible so that, to the extent feasible, CMS can provide assistance to issuers to resolve those problems before the final data submission deadline. The FMCC Service Representative will work with the issuers to provide the best approach to resolve the specific scenario identified.



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

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

5.2 Disaster Recovery

CMS has established an EDGE Server Disaster Recovery Process in the event of a disaster or emergency that impacts an issuer's EDGE server. The purpose of this section is to outline the steps that are required to be performed on the EDGE server to assist issuers in resuming data submission and ensuring that the data is included in the RA and RI program calculations. The recovery process requires routine server backup as outlined in Section 5: Backup and Maintenance Procedures.

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

Table 5-1: Disaster Recovery Responsibilities

Task	Team	Description
Disaster recovery plan	Issuer Operation's Team	Create and maintain a disaster recovery process and procedures for restoring the EDGE server in case of a catastrophic data loss
Storing backup files	Issuer Operation's Team	Place backup files (e.g., application files, DB backup files, etc.) in accordance with the disaster recovery plan

Task	Team	Description
Restore EDGE server environment	Issuer Operation's Team EDGE Server Help Desk	Ensure the EDGE server application has all necessary supported software and is on the latest EDGE version. Please see Section 5.5: EDGE Server Application and Software Stack Version Updates for more information. The EDGE Server help desk will only assist the issuer in provisioning or installing a new EDGE server in case of a catastrophic failure
Disaster Recovery Site, if applicable	Issuer Operation's Team	If applicable, the issuer's operational team will be responsible for maintaining an EDGE Server disaster recovery site as outlined by the Issuer's disaster recovery policies and procedures.

5.2.1 Inform CMS of the Disaster Recovery Event

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

5.2.2 Recreate Server

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

AWS: A new AWS server will be re-provisioned using the steps in Section 3.5.4: AWS EDGE Server Provisioning.

OP: Issuers should install the new server using the steps in Section 3.4.3: On-Premise EDGE Server Provisioning. They will need to download the following from the ESM console: 'edge.keys', 'edge.properties' and the installation kit and proceed with the re-provisioning as instructed in the documentations.

During the disaster recovery process, servers (either AWS or OP) should meet the set of software requirements outlined in the following sections before restoring backup files and installing the EDGE application software. Please see Section 5.5: EDGE Server Application and Software Stack Version Updates for the latest Red Hat Enterprise Linux (RHEL), MySQL and Java versions. Issuers who want to install a different version

should first contact the FMCC Service Representative Team to ensure it complies with current CMS guidelines and EDGE software.

5.2.3 Backup Restoration

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

5.2.4 Backup Verification

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

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

5.3 Annual Archive Process

The EDGE server data submission deadline for the previous BY is typically the last day in April. The [EDGE Server Timeline](#), available in the REGTAP library (www.regtap.info) provides the year specific deadlines for data submission. CMS implemented a blackout period after the submission deadline in order for the annual RA payments and charges processes to be performed. Once CMS has finished the BY payments and/or charges, a command will be sent to issuers' EDGE servers to archive the data on the server for future audit purposes. During the archive process, the production tables will be cleared and claim and supplemental data, already submitted and accepted for the current BY, will be restored. This eliminates the need for data resubmission and will make the system ready for additional data for the current BY.

Note: For example, after the data submission deadline on April 30, 2017, the current BY will be 2018 and the previous BY will be 2017.

On May 1st, or the subsequent business day, all data submissions for the previous BY will be blacked out. However, during the blackout period, issuers will be able to submit medical claims, pharmacy claims, and supplemental diagnosis records for the current BY. Enrollment data for the current BY may not be submitted during the blackout period. All current BY claims and supplemental data submitted through April 30th will be restored to the production tables during the archive process.

Records that will be restored include:

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

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

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

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

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

Issuers who want to sync their PROD and TEST zone after the archive occurs will need to truncate the TEST zone to clear the tables. Section 4.2.3: Prod to Test and Prod to Validation Copy Command provides steps if issuers would like to sync their two (2) zones. Issuers who have received a TEST zone truncation script before, may use the same script. Refer to Section 5.4: Truncation Requests to request a truncation.

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



Beginning with the archive of BY2017 data, issuers will be required to attest, through the **Annual Archive Confirmation Web Form**, that the archive and the restoration of 2018 BY data was successful.

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

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

5.3.1 Pre-Archive Steps

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

- Log on to the server and access the properties file by entering:

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

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

Figure 5-23: Edge.properties - DB User (Image 1 of 2)

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

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

Figure 5-24: Edge.properties - DB User (Image 2 of 2)

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

Step 2: Identify Custom Schemas, if Applicable

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

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

Figure 5-25: Schemas Check

Step 3: Validate Current Table Counts within Schemas

The following steps outline how to confirm the count of the tables in the current schemas. This information is used to confirm that the new archive schemas are created successfully after the Archive command is executed.

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

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

Step 4: Validate Current Record Counts within the Tables

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

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



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

- a. Please execute the commands in Appendix I: Data Validation Queries Before Archive Command
 - Save the results of the record counts for reporting purposes.
 - Complete the remaining Pre-Archive steps (Steps 5 & 6).

Step 5: Check Current Storage Space Usage by Database Schemas

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



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

- Log in to the MySQL shell using the **db-user**, as shown below.
 - `mysql --host localhost -u edgedbuser -p`

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

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

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

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

mysql>
```

Figure 5-26: MySQL - DB User Login

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

- Run the following **SQL** from MySQL shell to check storage space.

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

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

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

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

Figure 5-27: Schema Storage Space

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



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

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

- exit
- cd /opt/edge/config

To check the available space, enter the following command:

- df -k /var/lib/mysql

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

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

Figure 5-28: DB Mount Points

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

- df -k /opt/edge

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

Figure 5-29: DB Backup - Space Check

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

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



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

Step 6: Verify Grant Permissions for 'DB User'

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



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

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

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

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

Figure 5-30 Obtain root password

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

- `mysql -u root -p`

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

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

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

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

mysql>
```

Figure 5-31: MySQL Login for Remote Command Execution

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

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

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

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

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

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

Figure 5-32: Grant Privileges

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

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

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

Figure 5-33: Show Grants

For issuers with CUSTOM SCHEMAS only

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

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

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



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

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

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

5.3.2 Archive Steps

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

YEAR_END_BACKUP_DB

Step 7: Start Database Archive Process

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

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

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

- edge queue execute
- edge version

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

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

OR

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

Figure 5-34: Local Edge Commands to Execute the Remote Command

Step 8: Validate Remote Command Status is Executed

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

- mysql --host localhost -u edgedbuser -p

- USE EDGE_SRVR_COMMON
- SELECT * FROM REMOTE_CMD_QUEUE WHERE REMOTE_CMD_TYPE= 'YEAR_END_BACKUP_DB' and REMOTE_CMD_CREATED_DT > 'YYYY-06-30\G;

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

```
mysql> SELECT * FROM REMOTE_CMD_QUEUE WHERE REMOTE_CMD_TYPE= 'YEAR_END_BACKUP_DB' and REMOTE_CMD_CREATED_DT > '2017-06-01'\G;
***** 1 row *****
REMOTE_CMD_QUEUE_ID: 25
REMOTE_CMD_STATUS: EXECUTED
REMOTE_CMD_CREATED_DT: 2017-06-14 14:14:16
REMOTE_CMD_CREATED_DT: 2017-06-14 14:14:16
REMOTE_CMD_SCHEDULED_AT: 2017-06-14 00:00:00
REMOTE_CMD_EXPIRES_ON: NULL
PARAMETERS: ("JOB_ID": "86044", "YEAR": "2016", "BATCH_ID": "S02-2016-00020", "BATCH_TYPE": "YEAR_END_BACKUP_DB", "ZONE_TYPE": "P")
RESULTS: NULL
CREATED_DT: 2017-06-14 14:15:13
UPDATED_DT: 2017-06-14 00:00:00
1 row in set (0.00 sec)
```

Figure 5-35: Command Execution Confirmation

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

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

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

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

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

Figure 5-36: Command Execution Confirmation

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

- After validating the new schemas created, issuers should validate that new tables within those schemas were also created. Please enter the following commands and confirm the table count with the table counts from Step 3 USE EDGE_SRVR_COMMON_YYYY

- show tables;
- USE EDGE_SRVR_PROD_YYYY
- show tables;



Beginning in July 2018 (the BY2017 archive) issuers will be required to perform the following steps and attest to the successful archive and restoration of BY2018 data through the Annual Archive Confirmation Web Form.

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

Step 10: Validate Remote Command is Successful

- The below step outlines how to confirm the archive remote command completed successfully in the EDGE log files. Open the edge.log files by executing the following commands:

- cd /opt/edge/log
- ls -l
- view edge.log

- If the archive process is completed successfully, please verify the following:
 - Archive backup status will show as COMPLETED and code as 200 in log file.



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

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

Figure 5-37: Backup Completion Confirmation

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

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

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

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

Please enter the commands in Appendix I: Data Validation Queries Before Archive Command and confirm the record count of restored current BY data with the record counts from *Step 4: Validate Current Record Counts within the Tables*.

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

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

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

5.4 Truncation Requests

Database truncation is a process by which issuers can delete claim, supplemental diagnosis and enrollment data that has been submitted to the EDGE server in the production, test or validation zones.

The truncation command will delete **all data** from all schema data tables based on the zone indicated in the truncation script. There is no option to delete or truncate a single table or a subset of data in any zone. CMS reviews new truncation requests and truncation extension requests, then provides notification and instructions to issuers.

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



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

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

5.4.1 Truncation Request Approval

CMS has developed an EDGE Server Truncation Request web form for issuers requesting an EDGE server truncation or an extension for a previously approved truncation request.

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

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

A truncation request must be completed and submitted in a single session. It is recommended that you collect all necessary information before initiating the process.

Issuers are required to submit the web form with the following information to request permission to truncate production data.

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

The below steps will guide you through the truncation request process.

1. If your company's CEO Designate has changed, you must ensure the contact information has been updated in the EDGE Server Contact Database. Please access this [form](#) on the EDGE Server Contact Database to change your company's CEO Designate. Please access the EDGE Server Truncation Request web form through this [link](#).
2. After selecting the web form link, you will be directed to the **Welcome** page of the web form as shown below. Review the instructions and select the **Continue** button to advance to the Contact Information page.


[Guidance](#)

Welcome

The EDGE Server Truncation Request web form allows issuers participating in small group and individual market plans offered both on and off the Exchange and who have established an EDGE Server for the purposes of submitting data for Risk Adjustment to submit an EDGE Server truncation request or request an extension for a previously approved truncation request for CMS review and approval. Database truncation is a process by which issuers can delete claim, supplemental diagnosis, and enrollment data that has been submitted to the EDGE server in the Production, Test, or Validation Zone. The truncation command will delete all data from all schema data tables based on the zone indicated. There is no option to delete or truncate a single table or a subset of data in any zone.

Important Information about Test and Validation Truncation Scripts:

If you have previously received a truncation script for a specific HIOS ID for the Test or Validation Zone, you **do not** need to request a new truncation script for that HIOS ID. The Test and Validation Zone truncations do not expire and can be reused as often as needed.

Please note that this web form must be completed and submitted in a single session. We recommend that you collect all necessary information before initiating the process. Select the **Continue** button to begin.

If you exit the web form without submitting, all previously entered data will be lost.

Note: If your company's CEO Designate has changed, you **must** ensure the contact information has been updated in the EDGE Server Contact Database: <https://acapaymentoperations.secure.force.com/EdgeContactDatabase>. You cannot complete this process until the CEO Designate is correct.

By using this web form, you accept the terms and conditions. If you decline, you should not use the web form.

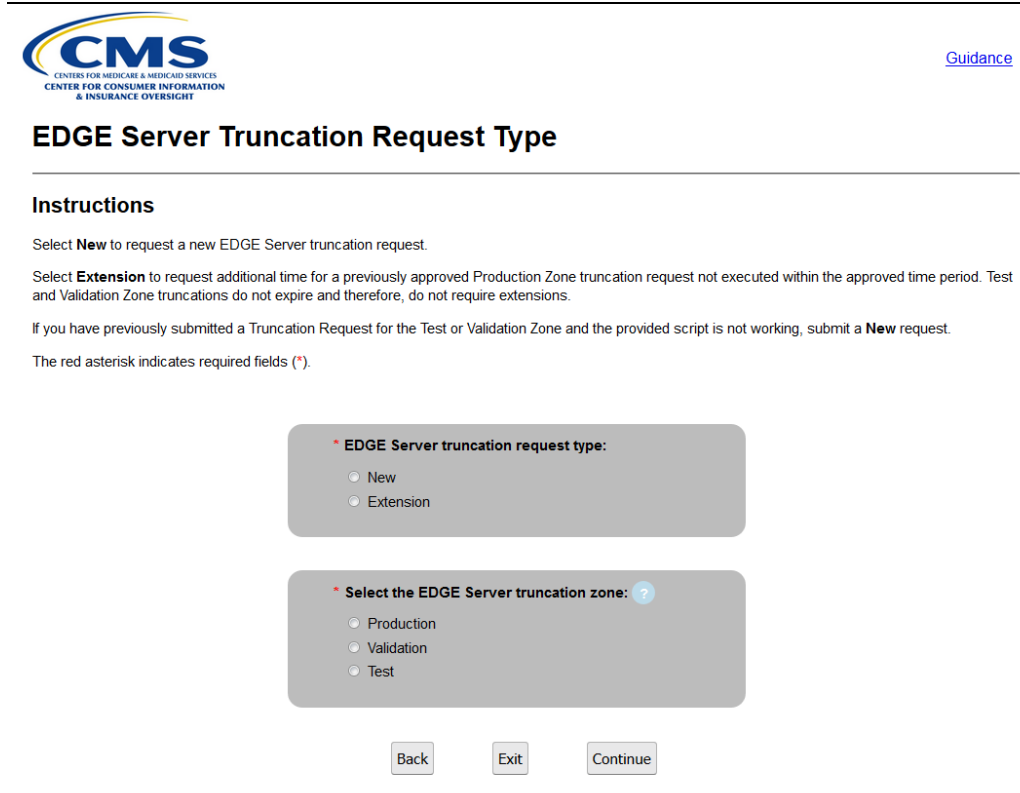
- This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network.
- This system is provided for Government-authorized use only.
- Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.
- Personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring.
- By using this system, you understand and consent to the following:
 - The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.
 - Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.

Figure 5-38: Welcome Page of Truncation Request Web Form

3. The Contact Information page collects Submitter and Alternate Contact information. You may enter the CEO Designate contact information as either the Submitter Contact or as the Alternate Contact.
4. After you enter the contact information, you will be directed to the **EDGE Server Truncation Request Type** page. The EDGE Server Truncation Request Type page provides the option to make a new request for EDGE server truncation or request an extension for a previously-approved truncation request.
5. After selecting New or Extension, select environment for truncation.



The test and validation zone options will not be displayed if you choose an extension request as extensions are not applicable for the test or validation zone. The scripts for test and validation zone truncations do not expire and can be reused at any time.



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

[Guidance](#)

EDGE Server Truncation Request Type

Instructions

Select **New** to request a new EDGE Server truncation request.

Select **Extension** to request additional time for a previously approved Production Zone truncation request not executed within the approved time period. Test and Validation Zone truncations do not expire and therefore, do not require extensions.

If you have previously submitted a Truncation Request for the Test or Validation Zone and the provided script is not working, submit a **New** request.

The red asterisk indicates required fields (*).

* EDGE Server truncation request type:

☐ New
☐ Extension

* Select the EDGE Server truncation zone: ?

☐ Production
☐ Validation
☐ Test

Figure 5-39: EDGE Server Truncation Request Type

6. If the new request option is selected, the form will proceed to the New EDGE Server Production Zone Truncation Request page or the New EDGE Server Test/Validation Zone Truncation Request page, based on your environment choice.



An EDGE Server truncation extension request may be made for a previously-approved truncation request that has not been executed and has not expired. If your previously-approved truncation request has expired, you must submit a new EDGE Server truncation request.

5.4.2 New EDGE Server Production Zone Truncation Request

This section provides instructions on how to make a new request for EDGE server production zone truncation.

1. Select the New radio button to request a new EDGE server truncation request.
2. Select the radio button for the production zone.
3. Select the Continue button. You will be directed to the New EDGE Server Production Zone Truncation Request page.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

[Guidance](#)

EDGE Server Truncation Request Type

Instructions

Select **New** to request a new EDGE Server truncation request.

Select **Extension** to request additional time for a previously approved Production Zone truncation request not executed within the approved time period. Test and Validation Zone truncations do not expire and therefore, do not require extensions.

If you have previously submitted a Truncation Request for the Test or Validation Zone and the provided script is not working, submit a **New** request.

The red asterisk indicates required fields (*).

* EDGE Server truncation request type:

☒ New
☐ Extension

* Select the EDGE Server truncation zone: ?

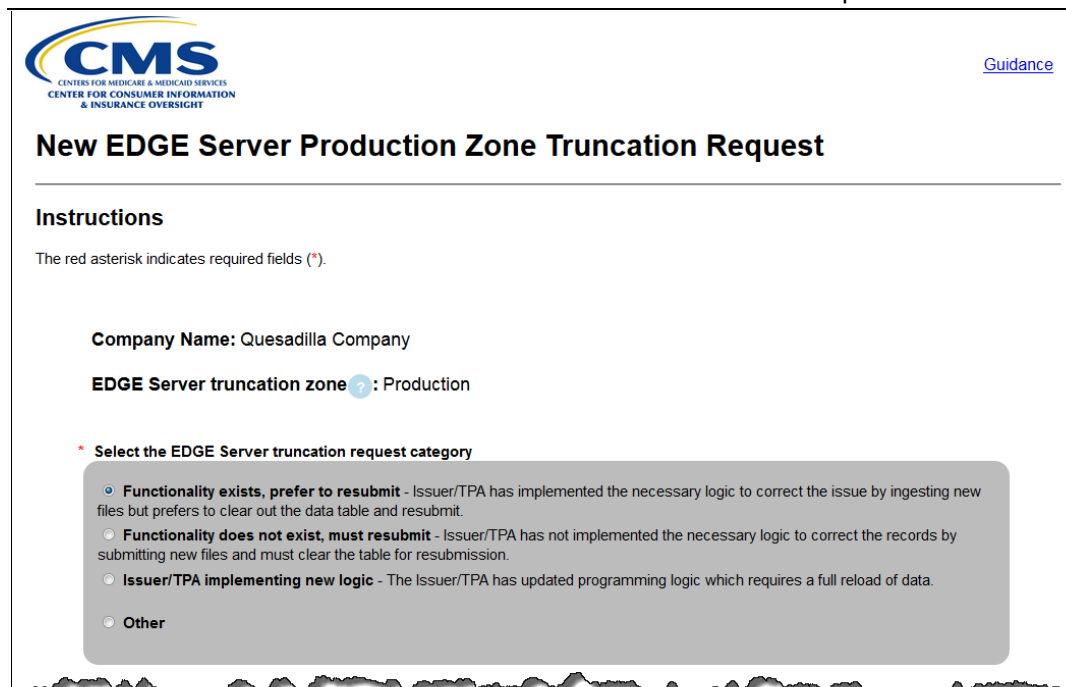
☒ Production
☐ Validation
☐ Test

Back Exit Continue

Figure 5-40: New EDGE Server Truncation Production Zone Request Radio Buttons

The new EDGE Server Production Zone Truncation Request page requires entry of information related to the type of and reasoning behind your production zone truncation request. Follow these steps to complete the New EDGE Server Production Zone Truncation Request page:

1. Select the appropriate radio button from the Select the EDGE server truncation request category:
 - Functionality exists, prefer to resubmit – issuer/TPA has implemented the necessary logic to correct the issue by ingesting new files but prefers to clear out the data table and resubmit.
 - Functionality does not exist, must resubmit - issuer/TPA has not implemented the necessary logic to correct the records by submitting new files and must clear the table for resubmission.
 - Issuer/TPA implementing new logic - The issuer/TPA has updated programming logic, which requires a full reload of data.
 - Other



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

[Guidance](#)

New EDGE Server Production Zone Truncation Request

Instructions

The red asterisk indicates required fields (*).

Company Name: Quesadilla Company

EDGE Server truncation zone ? : Production

* Select the EDGE Server truncation request category

- ☒ **Functionality exists, prefer to resubmit** - Issuer/TPA has implemented the necessary logic to correct the issue by ingesting new files but prefers to clear out the data table and resubmit.
- ☐ **Functionality does not exist, must resubmit** - Issuer/TPA has not implemented the necessary logic to correct the records by submitting new files and must clear the table for resubmission.
- ☐ **Issuer/TPA implementing new logic** - The Issuer/TPA has updated programming logic which requires a full reload of data.
- ☐ **Other**

Figure 5-41: Truncation Request Category Selection

2. Enter the reason for your truncation request, including specific details regarding the type of data affected (enrollment, medical claims, pharmacy claims, supplemental records) and an approximate count or percentage of your total records that need to be corrected in the Reason for EDGE server truncation request field. This field has a limit of 1,500 characters.



Provide a brief explanation as to when you plan to implement a solution that brings you into compliance if you selected the Functionality does not exist, must resubmit radio button (see Step 1).

Please provide specific details including the type of data affected (enrollment, medical claims, pharmacy, supplemental records) and an approximate count or percentage of your total records that need to be corrected. If you selected **Functionality does not exist, must resubmit**, please provide a brief explanation as to when you plan to implement a solution that brings you into compliance.

* Reason for EDGE Server truncation request: 65 of 1500 characters.

This is example text. This is example text. This is example text.

Limit 1,500 characters

Figure 5-42: Truncation Request Reason

3. Enter the planned truncation date in the *When do you plan to do the truncation?* Field.



This date must be at least one (1) business day from today's date.

Limit 1,500 characters

* When do you plan to do the truncation? ?

* When do you plan to re-load your data? ?

* Are your new files ready for submission?

* Have you run your data through the test zone?

* What were the test results?

08/24/2018

August 2018

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Figure 5-43: Planned Truncation Date

4. Enter your planned re-load date in the *When do you plan to re-load your data?* field. This date must be greater than or equal to the planned truncation date and must also be no more than seven (7) days after the planned truncation date.

Figure 5-44: Planned Re-load Date Selection

5. Select Yes or No from the *Are your new files ready for submission?* drop-down list.

Figure 5-45: Files Ready for Submission Selection

6. Select Yes or No from the *Have you run your data through the test zone?* drop-down list.

If	Then
Yes	The <i>What were the test results?</i> field is required. Enter your test results here. This field has a limit of 1,500 characters.
No	Continue to Step 7.

A screenshot of a web form titled "Data Test Selection". The form has a light gray background and a white border. It contains three main sections, each with a red asterisk indicating a required field. The first section is "Are your new files ready for submission?" with a "Yes" dropdown menu. The second section is "Have you run your data through the test zone?" with a "--None--" dropdown menu. The third section is "What were the test results?" with a large text area and a "Limit 1,500 characters" label. Below this is a fourth section, "Have you performed a back-up of your data on an external location/site?", with a "--None--" dropdown menu. The form is styled with a torn paper effect at the top and bottom edges.

Figure 5-46: Data Test Selection

7. Select Yes or No from the Have you performed a back-up of your data on an external location/site? drop-down list.

A screenshot of a web form titled "Data Back-up Selection". The form has a light gray background and a white border. It contains two main sections. The first section is "Have you performed a back-up of your data on an external location/site?" with a "--None--" dropdown menu. The second section is "Select the HIOS ID(s) for which you are requesting the EDGE Server truncation:" with a large text area and a "Limit 1,500 characters" label. The form is styled with a torn paper effect at the top and bottom edges.

Figure 5-47: Data Back-up Selection

8. Select the HIOS ID(s) you wish to request the EDGE server truncation from the Available HIOS ID(s) list. Use the arrows above the Available HIOS ID(s) list to move the applicable HIOS ID(s) to the Selected HIOS ID(s) list. Remove selected HIOS ID(s) by using the arrows above the Selected HIOS ID(s) list. You may filter the list of HIOS IDs by entering the HIOS ID or issuer legal business name in the Filter field.

Internal Use Only/ site?

*** Select the HIOS ID(s) for which you are requesting the EDGE Server truncation:**

Select HIOS ID(s) by using the arrows above the **Available HIOS ID(s)** list to move the applicable HIOS ID(s) to the **Selected HIOS ID(s)** list. Remove selected HIOS ID(s) by using the arrows above the **Selected HIOS ID(s)** list.

You may filter the list of HIOS IDs by entering the HIOS ID or issuer legal business name in the **Filter** field.

Available HIOS ID(s) Showing all 3	Selected HIOS ID Empty list
Filter → → → 33121 - Steak 33122 - Chicken 33123 - Cheese	Filter ← ← ←

If you have an FMCC case number related to the EDGE Server truncation request, enter it here: Limit 100 characters; separate case numbers with a comma.

Back Exit Continue

Figure 5-48: HIOS ID Selection

- Enter any FMCC case numbers, separated by commas, in the If you have an FMCC case number related to the EDGE Server truncation request, enter it here field.

 This field is optional and has a limit of 100 characters.

If you have an FMCC case number related to the EDGE Server truncation request, enter it here: Limit 100 characters; separate case numbers with a comma.

Back Exit Continue

Figure 5-49: FMCC Number Input

- Select the Continue button. You will be directed to the Summary page of the form.

Back Exit Continue 

Figure 5-50: Continue Button

5.4.3 New EDGE Server Test/Validation Truncation Request Page

This section provides instructions on how to make a new request for EDGE server test or validation zone truncation.

1. Select the New radio button to request a new EDGE server truncation request.
2. Select the radio button for the Test or Validation Zone.
3. Select the Continue button. You will be directed to the New EDGE Server Test/Validation Zone Truncation Request page.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

[Guidance](#)

EDGE Server Truncation Request Type

Instructions

Select **New** to request a new EDGE Server truncation request.

Select **Extension** to request additional time for a previously approved Production Zone truncation request not executed within the approved time period. Test and Validation Zone truncations do not expire and therefore, do not require extensions.

If you have previously submitted a Truncation Request for the Test or Validation Zones and the provided script is not working, submit a **New** request.

The red asterisk indicates required fields (*).

* EDGE Server truncation request type:

☒ New
☐ Extension

* Select the EDGE Server truncation zone: ?

☐ Production
☒ Validation
☐ Test

Back Exit Continue

Figure 5-51: New EDGE Server Truncation Test/Validation Zone Request Radio Buttons

The New EDGE Server Test/Validation Zone Truncation Request page requires entry of information related to the type of and reasoning behind your production zone truncation request. A new test or validation zone truncation request does not require a truncation date to be entered. The truncation start day will default to the next full business day after the request is submitted. Truncation scripts do not expire and can be reused as often as needed. If you have a current script that is not working, initiate a new test/validation zone truncation request.



The Company Name, EDGE Server truncation zone and Truncation Start Date are pre-populated.


[Guidance](#)

New EDGE Server Validation Zone Truncation Request

Instructions

A new Test or Validation Zone Truncation request does not require a truncation date to be entered. The truncation start day will default to the next full business day after the request is submitted.

Truncation scripts do not expire and can be reused as often as needed. If you have a current script that is not working, please complete the fields below.

The red asterisk indicates required fields (*).

Company Name: Quesadilla Company

EDGE Server truncation zone : Validation

Truncation Start Date: 8/22/2018

*** Select the HIOS ID(s) for which you are requesting the EDGE Server truncation:**

Select HIOS ID(s) by using the arrows above the **Available HIOS ID(s)** list to move the applicable HIOS ID(s) to the **Selected HIOS ID(s)** list. Remove selected HIOS ID(s) by using the arrows above the **Selected HIOS ID(s)** list.

You may filter the list of HIOS IDs by entering the HIOS ID or issuer legal business name in the **Filter** field.

Available HIOS ID(s) Showing all 3	Selected HIOS ID Empty list
Filter ↔ → 33121 - Steak 33122 - Chicken 33123 - Cheese	Filter ← ↔

If you have an FMCC case number related to the EDGE Server truncation request, enter it here:

Limit 100 characters; separate case numbers with a comma.

Figure 5-52: New EDGE Server Validation Zone Truncation Request Page

Follow these steps to complete the New EDGE Server Test/Validation Zone Truncation Request page:

1. Select the HIOS ID(s) you wish to request the EDGE server truncation from the Available HIOS ID(s) list. Use the arrows above the Available HIOS ID(s) list to move the applicable HIOS ID(s) to the Selected HIOS ID(s) list. Remove selected HIOS ID(s) by using the arrows above the Selected HIOS ID(s) list. You may filter the list of HIOS IDs by entering the HIOS ID or issuer legal business name in the Filter field.

Company Name: Quesadilla Company

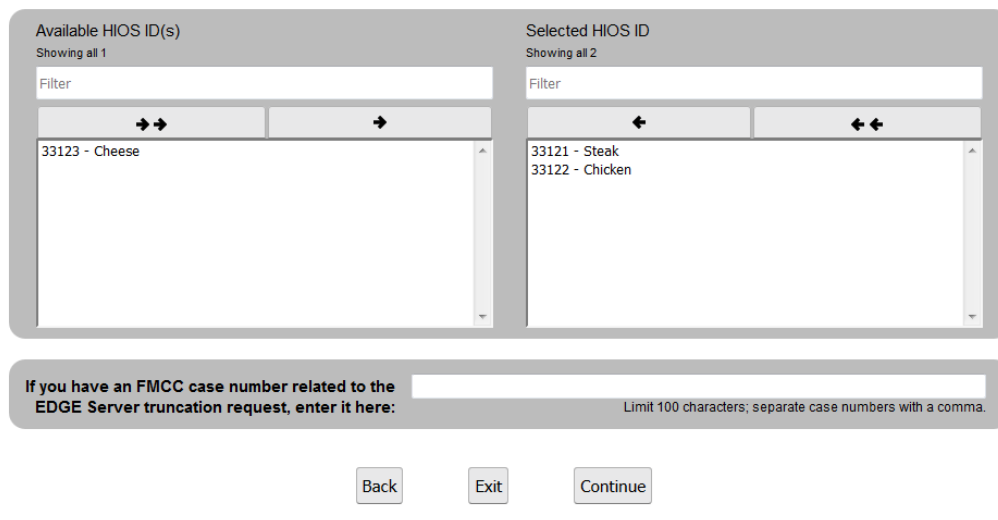
EDGE Server truncation zone : Validation

Truncation Start Date: 8/22/2018

*** Select the HIOS ID(s) for which you are requesting the EDGE Server truncation:**

Select HIOS ID(s) by using the arrows above the **Available HIOS ID(s)** list to move the applicable HIOS ID(s) to the **Selected HIOS ID(s)** list. Remove selected HIOS ID(s) by using the arrows above the **Selected HIOS ID(s)** list.

You may filter the list of HIOS IDs by entering the HIOS ID or issuer legal business name in the **Filter** field.



Available HIOS ID(s)
Showing all 1

Filter

33123 - Cheese

Selected HIOS ID
Showing all 2

Filter

33121 - Steak
33122 - Chicken

If you have an FMCC case number related to the EDGE Server truncation request, enter it here: Limit 100 characters; separate case numbers with a comma.

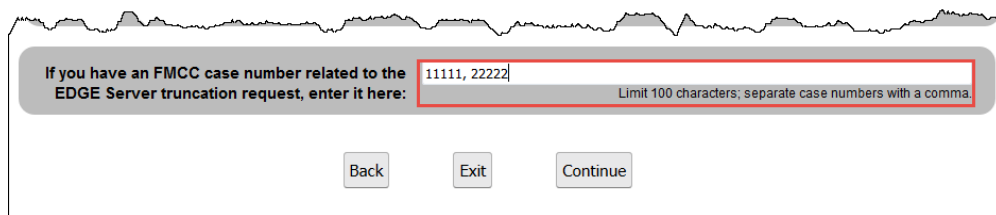
Back Exit Continue

Figure 5-53: HIOS ID Selection

Enter any FMCC case numbers, separated by commas, in the If you have an FMCC case number related to the EDGE server truncation request, enter it here field.



This field is optional and has a limit of 100 characters.



If you have an FMCC case number related to the EDGE Server truncation request, enter it here: 11111, 22222 Limit 100 characters; separate case numbers with a comma.

Back Exit Continue

Figure 5-54: FMCC Number Input

2. Select the **Continue** button. You will be directed to the summary page of the form.



Figure 5-55: Continue Button

5.4.4 EDGE Server Truncation Summary and Confirmation Pages

The Summary page allows you to view and edit EDGE server truncation request details and contact information. Follow these steps to complete the Summary page:

1. Review the EDGE Server Truncation Request(s) Summary table, which contains the details of each truncation request entered during this web form session. In the Action column, select the appropriate link as needed.
 - Select the View link to view the EDGE server truncation request details
 - Select the Edit link to update the EDGE server truncation request details
 - Select the Delete link to delete the EDGE server truncation request

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

[Guidance](#)

Summary

Company Name: Quesadilla Company

EDGE Server Truncation Request(s) Summary

Table Instructions

- Select the **View** link to view the EDGE server truncation request details
- Select the **Edit** link to update the EDGE server truncation request details.
- Select the **Delete** link to delete the EDGE server truncation request.

Action	Request Type	Truncation Zone	HIOS ID(s)	EDGE Server ID(s)	Planned Truncation Date
View Edit Delete	New	Production zone	33121	12345	8/24/2018
View Edit Delete	New	Production zone	33122	98765	8/24/2018

Figure 5-56: EDGE Server Truncation Request(s) Summary Table

- Review the contact information summary. If needed, select the **Edit Contact Information** button to update the information.

Contact Information

Select the **Edit Contact Information** button to update/edit contact information.

Submitter Contact Information

* First Name:	Jane	* Last Name:	Hebert
* Email Address:	chicken@quesadilla.food	* Job Title:	DBA Analyst
* Phone Number:	(555) 555-5555	Phone Extension:	

Alternate Contact Information

* First Name:	Katherine	* Last Name:	Brown
* Email Address:	veggie@quesadilla.food	* Job Title:	CFO
* Phone Number:	(111) 111-1111	Phone Extension:	

[Edit Contact Information](#)

Select the **Continue** button to enter another EDGE Server truncation request.

Select the **Submit** button to complete the EDGE server truncation request process.

Figure 5-57: Contact Information Summary

- Select the appropriate button to navigate to the appropriate page.

Table 5-2: Summary Page Navigation

If	Then
You need to enter another truncation request,	Select the Continue button to enter another EDGE server truncation request. The form will navigate to the EDGE Server Truncation Request Type page.
You have finished entering your truncation request(s),	Select the Submit button to complete the EDGE server truncation request process. The form will navigate to the Confirmation page.

After selecting the Submit button on the Summary page, an acknowledgement email will be sent to the email addresses provided. The PDF is the formal confirmation of your EDGE server truncation request submission. It is recommended that you save and print a PDF of the confirmation for your records. The PDF generated on the confirmation page will not be attached to the acknowledgment email.

Follow these steps to complete the Confirmation page:

1. Select the PDF button to print/save the confirmation for your records.



Confirmation

Warning: Please print the PDF for your records before selecting the Exit button.

Thank you for your submission.

An acknowledgement email has been sent to the email addresses provided. Print and save the PDF document for your records; it is the formal confirmation of your EDGE Server truncation request submission. The confirmation PDF includes your Truncation Request ID(s).

Submission End Time: 08/21/2018 12:04 PM

Acknowledgement email and submission information sent to the following email addresses:

chicken@quesadilla.food
veggie@quesadilla.food

Print/Save

Select the PDF button to generate a confirmation that contains the submitted EDGE Server truncation request(s) and the Truncation Request ID(s). Print and save this document for your records.



Figure 5-58: Confirmation Page

- Once your confirmation has been printed and/or saved, select the Exit button to exit the web form.



Figure 5-59: Exit Button

5.4.5 EDGE Server Truncation Extension Request

An EDGE server truncation extension request may be made for a previously approved production zone truncation request that has not been executed and has not expired.

Select the **Extension** radio button to request an extension on an existing EDGE server truncation request and select the **Continue** button. You will be directed to the EDGE Server Truncation Extension Request page.



The test and validation zone options will be disabled when you choose an extension request as extensions are not applicable to the test or validation zone. The scripts for test and validation zone truncations do not expire and can be reused at any time.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

[Guidance](#)

EDGE Server Truncation Request Type

Instructions

Select **New** to request a new EDGE Server truncation request.

Select **Extension** to request additional time for a previously approved Production Zone truncation request not executed within the approved time period. Test and Validation Zone truncations do not expire and therefore, do not require extensions.

If you have previously submitted a Truncation Request for the Test or Validation Zone and the provided script is not working, submit a **New** request.

The red asterisk indicates required fields (*).

*** EDGE Server truncation request type:**

☐ New

☒ Extension

*** Select the EDGE Server truncation zone: ?**

☒ Production

☐ Validation

☐ Test

Figure 5-60: EDGE Server Truncation Extension Request Radio Button

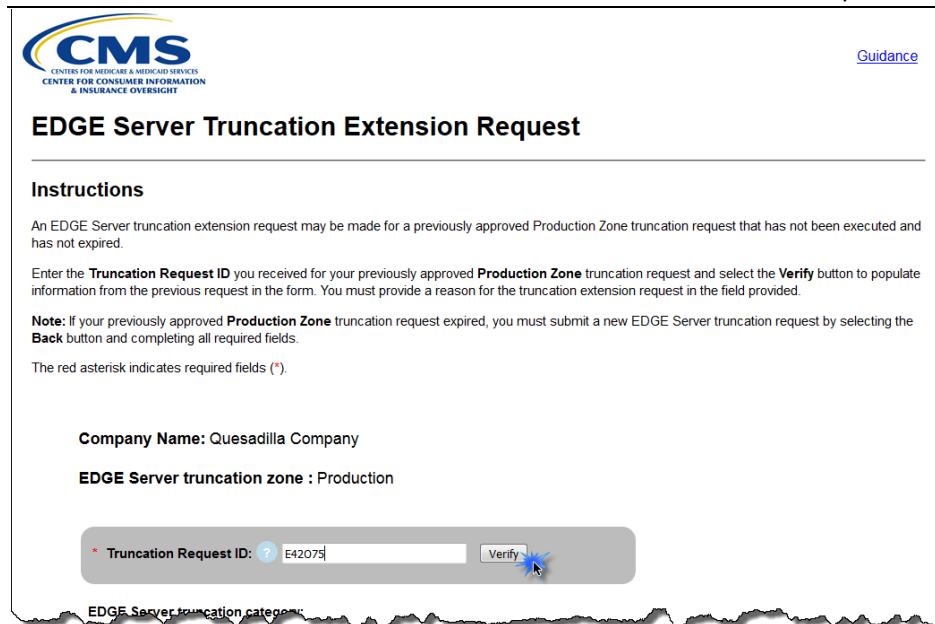
The EDGE Server Truncation Extension Request page requires you to enter the previous Truncation Request ID to populate information from that request.



If your previously approved production zone truncation request expired, you cannot submit a truncation extension request. You must submit a new EDGE server truncation request by selecting the **Back** button and completing all required fields for a new truncation request.

Follow these steps to complete the EDGE Server Truncation Extension Request page:

1. Enter the ID from your previously submitted request in the Truncation Request ID field. This was included in the approval email from CMS. If you cannot locate your Truncation Request ID, send an email to raripaymentoperations@cms.hhs.gov. Include at least one (1) HIOS ID and the words EDGE truncation in the subject line.
2. Select the **Verify** button to continue.



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

[Guidance](#)

EDGE Server Truncation Extension Request

Instructions

An EDGE Server truncation extension request may be made for a previously approved Production Zone truncation request that has not been executed and has not expired.

Enter the **Truncation Request ID** you received for your previously approved **Production Zone** truncation request and select the **Verify** button to populate information from the previous request in the form. You must provide a reason for the truncation extension request in the field provided.

Note: If your previously approved **Production Zone** truncation request expired, you must submit a new EDGE Server truncation request by selecting the **Back** button and completing all required fields.

The red asterisk indicates required fields (*).

Company Name: Quesadilla Company

EDGE Server truncation zone : Production

* **Truncation Request ID:**

EDGE Server truncation category:

Figure 5-61: Truncation Request ID

- Enter the reason for your truncation extension request, including the type of data affected (enrollment, medical claims, pharmacy claims, supplemental records) and an approximate count or percentage of your total records that need to be corrected, in the Reason for EDGE Server truncation extension field. This field has a limit of 1,500 characters.



Company Name: Quesadilla Company

EDGE Server truncation zone : Production

* **Truncation Request ID:**

EDGE Server truncation category: Functionality exists, prefer to resubmit

HIOS ID(s) for which you are requesting an extension for EDGE Server truncation: 33121

* **Reason for EDGE Server truncation extension:** 65 of 1500 characters.

Limit 1,500 characters

Figure 5-62: Truncation Extension Request Reason

- Enter the planned truncation date in the *When do you plan to do the truncation?* field.

 This date must be at least one (1) business day from today's date.

Limit 1,500 characters

* When do you plan to do the truncation? ? 08/24/2018

* When do you plan to re-load your data? ?

* Are your new files ready for submission?

* Have you run your data through the test zone?

* What were the test results?

August 2018

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Figure 5-63: Planned Truncation Date

- Enter your planned re-load date in the *When do you plan to re-load your data?* field. This date must be greater than or equal to the planned truncation date and must also be no more than seven (7) days after the planned truncation date.

* When do you plan to do the truncation? ? 08/24/2018

* When do you plan to re-load your data? ? 08/29/2018

* Are your new files ready for submission?

* Have you run your data through the test zone?

* What were the test results?

August 2018

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Figure 5-64: Planned Re-load Date Selection

- Select **Yes** or **No** from the *Are your new files ready for submission?* drop-down list.

* Are your new files ready for submission?

* Have you run your data through the test zone?

* What were the test results?

Figure 5-65: Files Ready for Submission Selection

7. Select **Yes** or **No** from the *Have you run your data through the test zone?* drop-down list.

Table 5-3: Test Results Selection

If	Then
Yes	The What were the test results? field is required. Enter your test results here. This field has a limit of 1,500 characters.
No	Continue to Step 8.

* Are your new files ready for submission?

* Have you run your data through the test zone?

* What were the test results?

Limit 1,500 characters

* Have you performed a back-up of your data on an external location/site?

Figure 5-66: Data Test Selection

8. Select **Yes** or **No** from the *Have you performed a back-up of your data on an external location/site?* drop-down list.

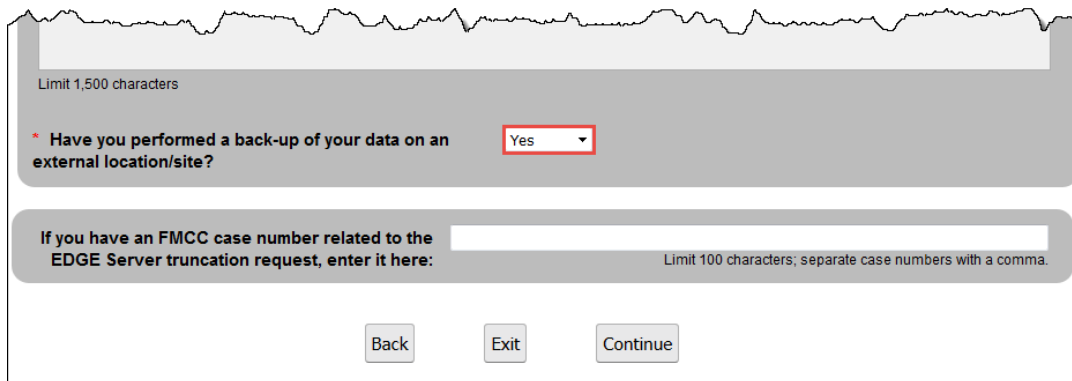


Figure 5-67: Data Back-up Selection

9. Enter any FMCC case numbers, separated by commas, in the *If you have an FMCC case number related to the EDGE server truncation request, enter it here* field.



This FMCC case number field is optional and has a limit of 100 characters.

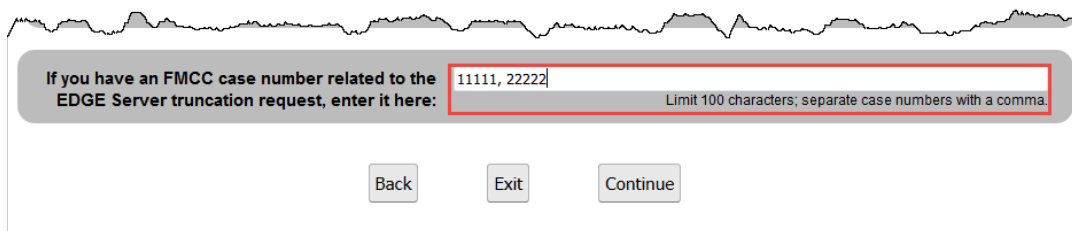


Figure 5-68: FMCC Number Input

10. Select the **Continue** button. You will be directed to the Summary page of the form.

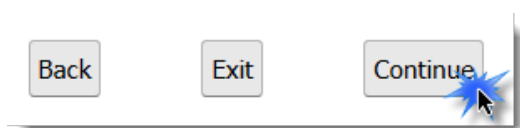
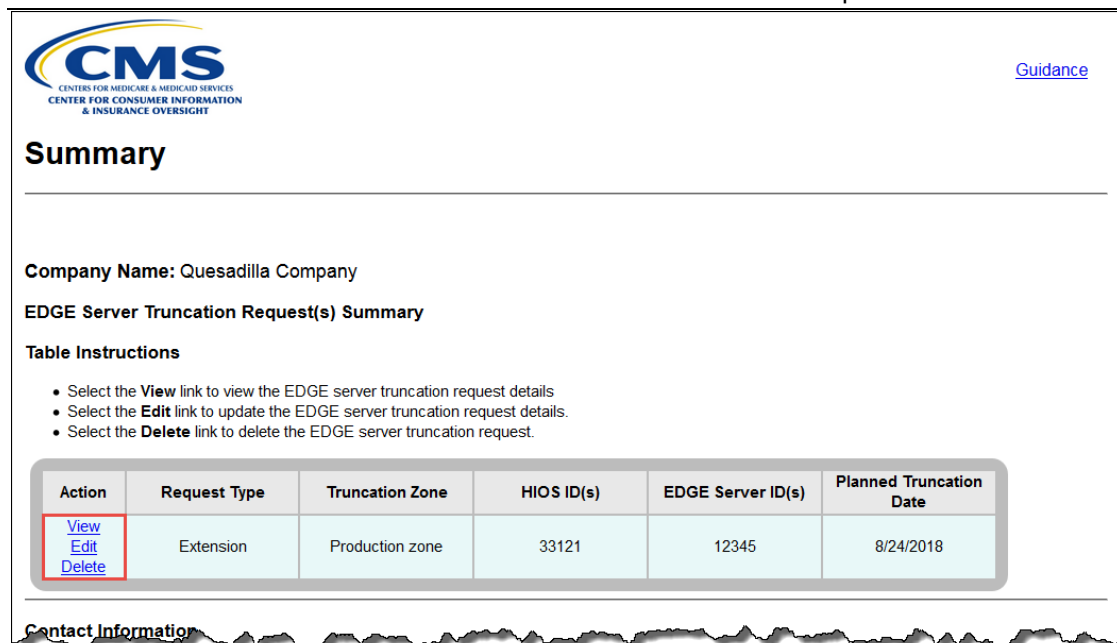


Figure 5-69: Continue Button

The Summary page allows you to view and edit EDGE server truncation request details and contact information. Follow these steps to complete the Summary page:

1. Review the EDGE Server Truncation Request(s) Summary table, which contains the details of each truncation request entered during this web form session. In the Action column, select the appropriate link as needed.
 - Select the **View** link to view the EDGE server truncation request details
 - Select the **Edit** link to update the EDGE server truncation request details
 - Select the **Delete** link to delete the EDGE server truncation request



Summary

Company Name: Quesadilla Company

EDGE Server Truncation Request(s) Summary

Table Instructions

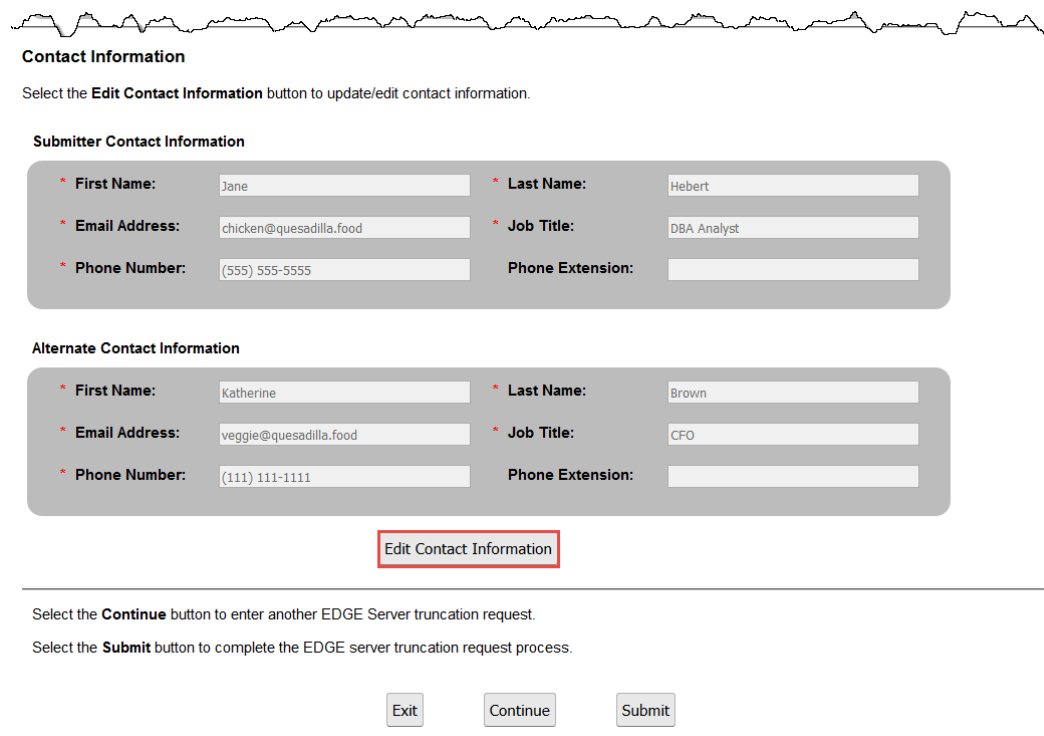
- Select the **View** link to view the EDGE server truncation request details.
- Select the **Edit** link to update the EDGE server truncation request details.
- Select the **Delete** link to delete the EDGE server truncation request.

Action	Request Type	Truncation Zone	HIOS ID(s)	EDGE Server ID(s)	Planned Truncation Date
View Edit Delete	Extension	Production zone	33121	12345	8/24/2018

Contact Information

Figure 8-70: EDGE Server Truncation Request(s) Summary Table

2. Review the Contact information summary. If needed, select the **Edit Contact Information** button to update the information.



Contact Information

Select the **Edit Contact Information** button to update/edit contact information.

Submitter Contact Information

* First Name: Jane * Last Name: Hebert

* Email Address: chicken@quesadilla.food * Job Title: DBA Analyst

* Phone Number: (555) 555-5555 Phone Extension:

Alternate Contact Information

* First Name: Katherine * Last Name: Brown

* Email Address: veggie@quesadilla.food * Job Title: CFO

* Phone Number: (111) 111-1111 Phone Extension:

Edit Contact Information

Select the **Continue** button to enter another EDGE Server truncation request.

Select the **Submit** button to complete the EDGE server truncation request process.

Exit Continue Submit

Figure 9-71: Contact Information Summary

3. Select the appropriate button to navigate to the appropriate page.

Table 5-4: Summary Page Navigation

If	Then
You need to enter another truncation request,	Select the Continue button to enter another EDGE server truncation request. The form will navigate to the EDGE Server Truncation Request Type page.
You have finished entering your truncation request(s),	Select the Submit button to complete the EDGE server truncation request process. The form will navigate to the Confirmation page.

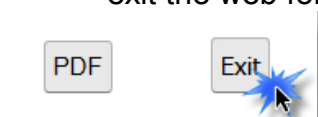
After selecting the **Submit** button on the summary page, an acknowledgement email will be sent to the email addresses provided. The PDF is the formal confirmation of your EDGE server truncation request submission. It is recommended that you save and print a PDF of the confirmation for your records. The PDF generated on the confirmation page will not be attached to the acknowledgment email.

Follow these steps to complete the Confirmation page:

1. Select the **PDF** button to print/save the confirmation for your records.

Figure 10-72: Confirmation Page

2. Once your confirmation has been printed and/or saved, select the **Exit** button to exit the web form.

**Figure 5-73: Exit Button**



CMS reviews and responds to truncation requests within two (2) business days. Truncation requests may be denied if the request is missing required items or a sufficient explanation is not provided.

5.4.6 Executing a Truncation Script

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

- edge truncate test
- edge truncate prod
- edge truncate val

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

5.5 EDGE Server Application and Software Stack Version Updates

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

Updates to the EDGE Server Application

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



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

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

- EDGE server web Registration site version number
- EDGE server application version number

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

When the new version is released, issuers can either manually execute the edge update command or enable CRON to pick up the release (see Section 4.2.1: Local Commands and Appendix H: EDGE Server Reports and Local Commands).

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

Updates to the Software Stack Version and Supporting Software

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

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

The EDGE server is initially deployed with OS updates consistent with National Institute of Standards and Technology (NIST) moderate security standards. Issuers are responsible for following CMS minimum guidance for patching their EDGE server instances. Issuers should follow leading practices for patching, including keeping track of patch levels and dependencies, aiming to patch critical vulnerabilities in hours or days, and subscribing to security mailing lists and news sources.

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

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

Section 6 - Reference Data

Reference data are categorized as Global Reference data and Plan Reference data. Neither global Reference data nor plan reference data require a scheduled maintenance release.

- Global Reference Data updates are deployed to all issuer servers.
 - Updates will typically be scheduled on a monthly basis.
- Plan Reference Data updates are deployed to issuer specific servers only.
 - Updates vary throughout the year based on a variety of factors including data submission deadlines, verification of changes (where applicable) and timing of requests.

The timing of the scheduled reference data updates is published in the EDGE Server Timeline available in the REGTAP library.

6.1 Global Reference Data

Global reference data are not issuer specific and are the same across all issuer EDGE servers. These data include many industry standard codes such as Diagnosis Codes, Service Codes (CPT and HCPCs only), Bill Types, etc. A complete list of reference data tables and a description of each column be found in Section 2.2: Data Model & Dictionary.

CMS provides tentative monthly updates to these tables to ensure that issuer has the latest reference data. Reference data updates occur independently of maintenance releases. This allows reference data updates to occur more frequently, which allows for more up - to - date codes, dates, and RA inclusion flags. Within five (5) business days of each monthly update, CMS will publish monthly Global Reference Data Files that provide summary and detailed information for each update. The files will be posted to REGTAP on the DDC Program Page.

Deployment will be similar to plan data updates. EDGE servers will automatically do a version check of global reference data. If an update is available, the EDGE server will be updated with the most recent version upon the initial of any local or remote EDGE command, including running the following command:

- `edge update`

Issuers may verify the modified codes by running a query on the last modified date.

6.2 Plan Data Source & Integration

The plan reference tables store issuer specific plan data elements to verify the Plan IDs and rating areas submitted on the inbound files and perform program calculations. Plan data are collected by CMS from various plan data sources as, indicated below, and are then integrated for deployment to issuers' EDGE servers.

When reusing a Plan ID from one (1) BY to the next, the metal level, market type, and product type must be the same to ensure the integrity of the Risk Adjustment program.

and adherence to uniform modification requirements established in 45 CFR 147.106 and in 45 CFR 144.103 (definition of “plan”). If the plan’s actuarial value changes, resulting in a metal level change, you must establish a new Plan ID for the following year.

Plan data are collected for use on issuer EDGE servers from the following four (4) sources:

- The Federally-facilitated Exchange (FFE) including State Partnership Exchange and State Based Exchange-Federal Platform
- State Based Exchange (SBE)
- Rates and Benefits Information System (RBIS) for Off-Exchange
- CMS and Issuer submitted EDGE templates

Please refer to Section 9 of the ESBR for information on Plan Reference Data sources and Plan Data Integration.

6.3 Plan Data Public Sources

Detailed information about the sources of the Plan Data and how the data are combined from multiple sources is explained in the EDGE Server Business Rules, Chapter 9.

Information on how to query the Plan Data tables is found in Section 6.3. CMS expects issuers to accurately maintain data in each of the main source systems outlined above (FFE, SBE and RBIS). Alteration of plan reference tables is not expected if the plan data is submitted to the main source systems in an accurate and timely manner. Issuers can also check submitted plans in public sources published by CMS.



Issuers must validate or attest to RBIS plan filings for their respective organization. Please contact the appropriate department within your organization frequently to ensure they meet the plan data submission deadlines. Failure to submit plan data timely will result in enrollment and claim records being rejected.

Submitted plan data information may be found in the public documents below:

Table 6-1: Public Documents Containing Plan Data

Public Document	Data Source	Plan Data Type	Description of Document
Uniform Rate Review Template (URRT)	URRT	All plan data types	Document summarizes the data used to determine rate increases for the entire single risk pool.

Public Document	Data Source	Plan Data Type	Description of Document
SBM Public Use Files (SBM PUF)	SERFF	State exchange	Document that lists plans that are available for the certified QHP plan year 2016 and 2017. The SBE PUF include plan and issuer level information for certified QHPs and stand-alone dental plans (SADPs) offered to individuals and small businesses through the SBES.
QHP Landscape Files	QHP	Federal exchange	Document presents basic information about certified Qualified Health Plans and Stand-alone Dental Plans. The files contain plan information by county, including plan type, category, rating area, and premiums for various rating scenarios.

6.4 Plan Data Records on Server

CMS routinely deploys reference data to the MySQL reference tables on issuers' EDGE servers. Each reference table contains data used to verify data values submitted on the enrollment, pharmacy, medical and supplemental diagnosis files. The INSRNC_PLAN reference table stores the issuer's on and off Marketplace plan offerings to verify the Plan IDs submitted on the inbound files. As per the EDGE Server Business Rules, this section provides additional details for identifying missing plan data.

For a plan to be active and usable, the plan must contain the following:

- Issuers must have the required "Market Year(s)" for the plans associated with their claims and enrollments for the records to be accepted regardless of the plan start and/or end date. The Market Year field indicates the year in which the plan is effective. A plan ID used in a claim or an enrollment period should be active in the market year corresponding to the start date of the claim or the enrollment period.
- A unique occurrence of a given INSRNC_PLAN_ID must be present for each required Market Year in an active state (ACTIVE_FL should be 'Y') for a plan to be considered active, regardless of the EFCTV_STRT_DT and EFCTV_END_DT of the plan.



During file processing, the EFCTV_STRT_DT and EFCTV_END_DT is not used to determine if a plan is effective during a BY. The EFCTV_END_DT is only used during file processing validation to identify when an Enrollment End Date is beyond the plan EFCTV_END_DT, in which case a warning will be displayed. The plan EFCTV_STRT_DT or EFCTV_END_DT cannot cause a rejection and CMS has started to default them to 1/1/2014-12/31/9999 to eliminate these warnings.

The following queries can be used at any time to identify the HIOS ID for the server and what is actively loaded on a server's plan reference table:

1. To identify the HIOS ID configured on the EDGE server. This query must return only one row.
 - ```
select * FROM ISSR_ORG
```
2. A row must exist in the "INSRNC\_PLAN" table of the "EDGE\_SRVR\_COMMON" schema for each 16-digit plan ID for each market year that you have enrollment. Execute the following query to determine whether the plan and variant exists:
  - ```
select * from EDGE_SRVR_COMMON.INSRNC_PLAN where  
INSRNC_PLAN_ID = <Insert 16-Digit Plan ID> and MARKETYEAR =  
<Insert Market Year> and ACTIVE_FL='Y';
```
3. A row must exist in your "ISSR_PLCY_RATG_AREA" table of the "EDGE_SRVR_COMMON" schema for each 16-digit plan ID, market year and rating area combination that you have enrollments for. Execute the following query to determine whether the rating area exists:
 - ```
select * from EDGE_SRVR_COMMON.ISSR_PLCY_RATG_AREA where
PLAN_ID = <Insert 16-Digit Plan ID> and MARKETYEAR = <Insert Market
Year> and ACTIVE_FL='Y';
```

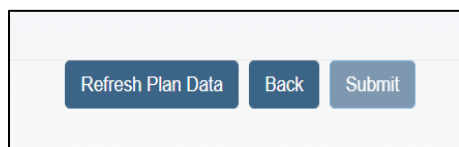
## 6.5 Plan Data Small Group Rollover

Beginning with the BY2018, CMS will rollover certified small group plans offered in the previous BY that are no longer offered for new enrollment in the current BY. Because small group plans do not follow the typical calendar year, CMS implemented this rollover process to streamline the plan data submission process for issuers. Please note, this process will **NOT** roll over plans that were rolled over in the previous year and will not rollover any inactive plans. If a plan has already been rolled over from the previous BY and it is offered for new enrollment, issuers must follow the normal off-exchange RBIS submission process and schedule.

## 6.6 Updating Plan Data

Issuers must submit their plan data to the applicable data sources that were previously mentioned so an issuer's plan data can be comprehensive and complete. In the event that plans are missing from the plan reference table, inaccurate plan data fields need to be updated, or plan data is causing rejections on claims, please follow the below steps:

1. Perform a plan data refresh on ESM (if CMS database is correct, but issuer tables are not synched).
  - a. To perform the refresh, log into ESM as mentioned in Section 3.2.1: Accessing the ESM Website, search your HIOS, and view your server. Scroll down to the bottom of the page and click the **Refresh Plan Data** button.



**Figure 6-1: Refresh Plan Data button on ESM**

- b. Wait a few seconds to allow the refresh to occur. If successful, the below message will appear.



**Figure 6-2: Refresh Plan Data Success Message**

- c. Log into your server and then run the below command

- edge update

If this step does not resolve your issue, then issuers should continue to step 2:

2. Consult with your plan data team to ensure that these plans were appropriately filed to the appropriate plan data sources during the correct market year.
3. Check the public documents containing plan data sources, as described in Table 6-1 . If plans do not match these public documents, please consult with your plan data team to ensure public filings need update.
  - a. For all missing plans, check URRT
  - b. For missing state on-exchange plans, check SBM PUF
  - c. For missing federal on-exchange plans, check QHP Landscape
4. Submit missing plans to the FMCC Service Representative Team at [Edge\\_Server\\_Data@cms.hhs.gov](mailto:Edge_Server_Data@cms.hhs.gov) so they may start the validation process.
  - For Off-Exchange plans - Starting with the BY2018 Off-Exchange plan data, Issuers should closely monitor RBIS quarterly data submissions and correct any errors and/or missing plans during the next RBIS submission window. Issuers should not rely on EDGE templates to correct their plan data as it is only to be used when other means of plan data updates are unavailable.



Please submit only missing/update-required plans to avoid any unintentional changes to your plan reference tables. If you are missing Off-Exchange and On-Exchange plans, then please submit two (2) separate inquiries to the FMCC team at [EDGE\\_Server\\_Data@cms.hhs.gov](mailto:EDGE_Server_Data@cms.hhs.gov).

## **Validation Process**

CMS expect all applicable plans, except Medicaid expansion private plans, to be submitted to the data source. When the FMCC team receives an issuer plan data template (IPDT), the plans and associated data elements will be validated with all of the data sources mentioned in Sections 6.2: Plan Data Source & Integration and 6.3: Plan Data Public Sources to ensure these plans are available for the submitted market year. CMS encourages issuers to send missing plans or plans that need corrections as soon as these plans are identified to allow sufficient validations to occur. The FMCC team will

individually work with each issuer's unique scenario and will inform the issuer if these plans successfully pass validations.

When plans have been loaded, run the below command and check your EDGE tables, as described in Section 6.4: Plan Data Records on Server.

- edge update

## Section 7 - Appendices

### Appendix A: Enrollee File Ingest Job Error Messages

Section 4.1.6 describes Ingest Validation Errors. This table list additional resources for troubleshooting.

**Table 7-1: 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                             |
| 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 B: Medical File Ingest Informational and Error Messages

Section 4.1.6 describes Ingest Validation Errors. This table list additional resources for troubleshooting.

**Table 7-2: 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 4.1.6 describes Ingest Validation Errors. This table list additional resources for troubleshooting.

**Table 7-3: 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-----<br>--->                                       | 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. |
| 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                                         |

| Error Message                           | Error Description                              | Cause                                          | Fix                      |
|-----------------------------------------|------------------------------------------------|------------------------------------------------|--------------------------|
| 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 4.1.6 describes Ingest Validation Errors. This table list additional resources for troubleshooting.

**Table 7-4: 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, 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 7-5: Common Error for Remote Commands**

| Category             | Error             | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Additional Steps                                     |
|----------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| EDGE Server Settings | DEBUG Log Setting | <ol style="list-style-type: none"><li>1. Login into the server</li><li>2. Go to configuration directory (This could vary based on Issuer configuration)<ul style="list-style-type: none"><li>• <code>cd /opt/edge/config</code></li></ul></li><li>3. Edit the logback.xml<ul style="list-style-type: none"><li>• <code>vi logback.xml</code></li></ul></li><li>4. Edit this line<ul style="list-style-type: none"><li>• <code>&lt;logger level="WARN" name="gov.hhs.cms"/&gt;</code></li></ul></li><li>5. Change it to<ul style="list-style-type: none"><li>• <code>&lt;logger level="DEBUG" name="gov.hhs.cms"/&gt;</code></li></ul></li><li>6. Save the file and exit</li></ol> | Must revert back to WARN as part of the full process |

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

| Category            | Error                                                                                                                                                                                                                                                                | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Additional Steps                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| EDGE Server Command | org.springframework.batch.item.ItemStreamException: Failed to initialize the reader                                                                                                                                                                                  | <p>Please go to the edge.properties under /opt/edge/config directory and add the streaming properties below.</p> <ul style="list-style-type: none"> <li>processor_reader_verifyCursorPosition=true</li> <li>processor_reader_fetchSize=0</li> </ul>                                                                                                                                                                                                                                                                                                                                                                  | Attempt file ingest again. If error persists, contact FMCC and provide your 1. edge.log.  |
| EDGE Server Access  | <p>ERROR g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception</p> <p>...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;</p> | <p>To obtain new AWS Access Key ID:</p> <ol style="list-style-type: none"> <li>1. Please log in to the ESM portal and click "Manage EDGE Server."</li> <li>2. Perform a search by your "Issuer HIOS ID" and then click "View" for this server.</li> <li>3. Next you will need to generate a new key by clicking "Download AWS/OP Generated Keys."</li> <li>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).</li> <li>5. Now copy the new key file you just generated from the ESM portal to /opt/edge/config.</li> </ol> | None                                                                                      |
| EDGE Server Access  | <p>ERROR g.h.c.f.f.e.a.s.EdgeLauncherImpl - Error during processing command</p> <p>com.amazonaws.AmazonClientException: Unable to calculate MD5 hash:</p> <p>/opt/edge/ingest/outbox/issuer/28162.RAPHCCER.D20160222T112034.T.xml (Permission denied)</p>            | <p>Confirm the output of the commands below. If edge application runs under user 'ec2-user':</p> <ul style="list-style-type: none"> <li>chown -R ec2-user:ec2-user /opt/edge (For AWS \$USER)</li> <li>chmod -R 755 /opt/edge</li> </ul>                                                                                                                                                                                                                                                                                                                                                                             | 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<br>g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception<br>...com.amazonaws.AmazonClientException: Unable to execute HTTP request: peer not authenticated                                                                                                  | <ol style="list-style-type: none"> <li>1. Add the following proxy related properties in /opt/edge/config/edge.properties <ul style="list-style-type: none"> <li>• proxy_host=xxx</li> <li>• proxy_port=xxxx</li> <li>• proxy_user=xxxx</li> <li>• proxy_password=xxxxx</li> </ul> </li> <li>2. Change log level to DEBUG for com.amazonaws and also in /opt/edge/config/logback.xml <ul style="list-style-type: none"> <li>• &lt;logger name="com.amazonaws" level="DEBUG" /&gt;</li> </ul> </li> <li>3. Run the following command <ul style="list-style-type: none"> <li>• ./edge version</li> </ul> </li> <li>4. Contact FMCC and provide the edge.log for review/next steps.</li> </ol> | None             |
| EDGE Server Access | ERROR<br>g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Unable to load 34808.APP_UPDATE.D10272016T051036.json to edge.data.prod<br>com.amazonaws.services.s3.model.AmazonS3Exception: Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied; | <p>To obtain new AWS Access Key ID:</p> <ol style="list-style-type: none"> <li>1. Please log in to the ESM portal and click "Manage EDGE Server."</li> <li>2. Perform a search by your "Issuer HIOS ID" and then click "View" for this server.</li> <li>3. Next you will need to generate a new key by clicking "Download AWS/OP Generated Keys."</li> <li>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).</li> <li>5. Now copy the new key file you just generated from the ESM portal to /opt/edge/config.</li> </ol>                                                                       | None             |

| Category             | Error                                                                                                                                                                                                                                                                                              | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Additional Steps                                               |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| EDGE Server Command  | ERROR<br>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br>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:<br><ul style="list-style-type: none"> <li>edge update</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                          | If error persists, contact FMCC and provide the<br>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.<br>Slides 12-14 in the <a href="#">EDGE Server 2015 Data Archive and Preparing for 2016 Data Submission</a> 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:<br><ul style="list-style-type: none"> <li>curl -x PROXY-SERVER:PORT -U USER:PASS URL</li> </ul>                                                                                                                                                                                                                                                                                                                                   | 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<br>g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception<br>...com.amazonaws.AmazonClientException: Unable to execute HTTP request:<br>edge.binaries.prod.s3.amazonaws.com | Contact the FMCC team and provide:<br>1. edge.log<br>2. edge.properties                                                                                                                                                                                                                          | None             |
| EDGE Server Error      | ERROR<br>gov.hhs.cms.ff.fm.edge.util.FileUtil - Cannot create directory                                                                                                      | Confirm the current EDGE version by executing the following command:<br><ul style="list-style-type: none"> <li>edge version</li> </ul> <p>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.</p> | 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<br>g.h.c.f.f.e.a.s.PhoneHomeClientImpl<br>- Unable to execute queue command. Incorrect result size: expected 1, actual 2<br>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: <ul style="list-style-type: none"> <li>SELECT<br/>               REMOTE_CMD_QUEUE_ID,<br/>               REMOTE_CMD_STATUS,<br/>               REMOTE_CMD_TYPE,<br/>               EXTERNAL_CMD_ID, RESULTS,<br/>               CREATED_DT, UPDATED_DT,<br/>               REMOTE_CMD_EXPIRES_ON<br/>               FROM<br/>               EDGE_SRVR_COMMON.REMOTE_CMD_QUEUE;</li> </ul> | None                                                                                       |
| EDGE Server Error      | Exception in thread "main"<br>java.lang.NoClassDefFoundError:<br>java/time/LocalDate                                                                                                                                                                                                                                                                                                                                    | Indicates incorrect Java Version. Download the latest version of Java as indicated in Section 5.5: EDGE Server Application and Software Stack Version Updates.                                                                                                                                                                                                                                                                                                                                                                                                                                  | Please download the latest Oracle Java version as detailed in Section 3.4.1: Server Setup. |
| File Ingest Issue      | ERROR<br>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br>org.springframework.dao.RecoverableDataAccessException: Attempt to process next row failed; ERROR<br>g.h.c.f.f.e.j.m.MedicalInlineProcessor - File failed header validation, rejecting file ERROR<br>g.h.c.f.f.e.r.FileAcceptRejectReportGenerator - REPPARAMS-----<br>>File Header Validation Failed---<br>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: <ol style="list-style-type: none"> <li>1. edge.log</li> <li>2. edge.properties</li> </ol>                                                                                                                                                                                                                                                                                                             | None                                                                                       |

| Category               | Error                                                                                                                                                                                                               | Solution                                                                                                                                                                                                                                        | Additional Steps                                                              |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| MySQL Error            | The MySQL server is running with the --secure-file-priv option, so it cannot execute this statement                                                                                                                 | <ol style="list-style-type: none"> <li>1. Open my.cnf</li> <li>2. Add the field: <ul style="list-style-type: none"> <li>• secure-file-priv=""</li> </ul> </li> <li>3. Restart MySQL</li> </ol>                                                  | None                                                                          |
| EDGE Server Command    | ERROR<br>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br>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. <ul style="list-style-type: none"> <li>• processor_reader_verifyCursorPosition=true</li> <li>• processor_reader_fetchSize=0</li> </ul> | Ask issuer to then attempt file ingest again. If error persists, contact FMCC |
| EDGE Server Update     | ERROR<br>g.h.c.f.f.e.d.i.SchemaBackupHelper - DataAccessException while re-creating target schema                                                                                                                   | Contact FMCC with your: <ol style="list-style-type: none"> <li>1. edge.log</li> <li>2. screenshots of /var/lib/mysql</li> </ol>                                                                                                                 | None                                                                          |
| EDGE Server Update     | ERROR<br>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: <ol style="list-style-type: none"> <li>1. edge.log</li> </ol>                                                                                                                                                           | None                                                                          |
| Remote Command Failure | ERROR<br>g.h.c.f.f.e.a.s.RemoteFileHandlerImpl - Exception<br>...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: <ol style="list-style-type: none"> <li>1. edge.log</li> </ol>                                                                                                                                                           | None                                                                          |

| Category               | Error                                                                                                                                                                              | Solution                                                                                                                                                    | Additional Steps |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Remote Command Failure | ERROR<br>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br>java.lang.OutOfMemoryError: GC overhead limit exceeded                                      | We would like to get the following information:<br>1. Edge.properties<br>2. Output of the following command including MySQL process<br>• Top<br>3. edge.log | None             |
| Remote Command Failure | ERROR<br>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br>org.springframework.dao.RecoverableDataAccessException: Attempt to process next row failed; | Contact FMCC with your:<br>1. edge.log                                                                                                                      | None             |
| Remote Command Failure | Caused by:<br>com.mysql.jdbc.exceptions.jdbc4.CommunicationsException: Communications link failure                                                                                 | Contact FMCC and provide:<br>1. Edge.properties<br>2. Output of the following command including MySQL process<br>• Top<br>3. Edge.log<br>4. my.cnf          | None             |

| Category               | Error                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Solution                                                                                                                                                                                                           | Additional Steps |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Remote Command Failure | <p>ERROR<br/>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br/>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</p> | <ol style="list-style-type: none"> <li>1. Restart MySQL</li> <li>2. Run a local command to the corresponding failure.</li> <li>3. Confirm if worked, if not provide FMCC with your edge.log for review.</li> </ol> | None             |
| Remote Command Failure | <p>ERROR<br/>o.s.batch.core.step.AbstractStep - Encountered an error executing the step<br/>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</p>                                                                                                             | <p>Contact FMCC with your:</p> <ol style="list-style-type: none"> <li>1. edge.log</li> </ol>                                                                                                                       | None             |

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

## Appendix F: Installer Policy Data

EDGE Installer Policy Data needed for Step 9 in Section 3.5.2: Request an AWS EDGE Server Instance. Copy and paste the below:

```
{
 "Statement": [
 {
 "Sid": "Stmt1",
 "Action": [
 "cloudformation:CreateStack",
 "cloudformation:DescribeStackEvents",
 "cloudformation:DescribeStackResource",
 "cloudformation:DescribeStackResources",
 "cloudformation:DescribeStacks",
 "cloudformation:ListStacks",
 "cloudformation:ListStackResources",
 "cloudformation>DeleteStacks"
],
 "Effect": "Allow",
 "Resource": "*"
 },
 {
 "Sid": "Stmt2",
 "Action": [
 "s3:CreateBucket",
 "s3:PutBucketAcl",
 "s3:GetBucketLocation",
 "s3:PutBucketPolicy",
 "s3:SetBucketPolicy",
 "s3:PutObject",
 "s3>DeleteObject"
],
 "Effect": "Allow",

```

```
"Resource": ""
},
{
 "Sid": "Stmt3",
 "Action": [
 "ec2:AllocateAddress",
 "ec2:AssignPrivateIpAddresses",
 "ec2:AssociateAddress",
 "ec2:AssociateDhcpOptions",
 "ec2:AssociateRouteTable",
 "ec2:AttachInternetGateway",
 "ec2:AttachNetworkInterface",
 "ec2:AttachVolume",
 "ec2:AuthorizeSecurityGroupEgress",
 "ec2:AuthorizeSecurityGroupIngress",
 "ec2:CreateCustomerGateway",
 "ec2:CreateDhcpOptions",
 "ec2:CreateInternetGateway",
 "ec2:CreateNetworkAcl",
 "ec2:CreateNetworkAclEntry",
 "ec2:CreateNetworkInterface",
 "ec2:CreateRoute",
 "ec2:CreateRouteTable",
 "ec2:CreateSecurityGroup",
 "ec2:CreateSubnet",
 "ec2:CreateTags",
 "ec2:CreateVolume",
 "ec2>DeleteCustomerGateway",
 "ec2>DeleteDhcpOptions",
 "ec2>DeleteInternetGateway",
 "ec2>DeleteNetworkAcl",
 "ec2>DeleteNetworkAclEntry",
 "ec2>DeleteNetworkInterface",
```

"ec2:DeleteRoute",  
"ec2:DeleteRouteTable",  
"ec2:DeleteSecurityGroup",  
"ec2:DeleteSubnet",  
"ec2:DeleteTags",  
"ec2:DeleteVolume",  
"ec2:DeleteVpc",  
    "ec2:CreateVpc",  
"ec2:DescribeAccountAttributes",  
"ec2:DescribeAddresses",  
"ec2:DescribeAvailabilityZones",  
"ec2:DescribeBundleTasks",  
"ec2:DescribeConversionTasks",  
"ec2:DescribeCustomerGateways",  
"ec2:DescribeDhcpOptions",  
"ec2:DescribeExportTasks",  
"ec2:DescribeImageAttribute",  
"ec2:DescribeImages",  
"ec2:DescribeInstanceAttribute",  
"ec2:DescribeInstanceState",  
"ec2:DescribeInstances",  
"ec2:DescribeInternetGateways",  
"ec2:DescribeKeyPairs",  
"ec2:DescribeLicenses",  
"ec2:DescribeNetworkAcls",  
"ec2:DescribeNetworkInterfaceAttribute",  
"ec2:DescribeNetworkInterfaces",  
"ec2:DescribePlacementGroups",  
"ec2:DescribeRegions",  
"ec2:DescribeReservedInstances",  
"ec2:DescribeReservedInstancesListings",  
"ec2:DescribeReservedInstancesModifications",  
"ec2:DescribeReservedInstancesOfferings",

"ec2:DescribeRouteTables",  
"ec2:DescribeSecurityGroups",  
"ec2:DescribeSnapshotAttribute",  
"ec2:DescribeSnapshots",  
"ec2:DescribeSpotDatafeedSubscription",  
"ec2:DescribeSpotInstanceRequests",  
"ec2:DescribeSpotPriceHistory",  
"ec2:DescribeSubnets",  
"ec2:DescribeTags",  
"ec2:DescribeVolumeAttribute",  
"ec2:DescribeVolumeStatus",  
"ec2:DescribeVolumes",  
"ec2:DescribeVpcAttribute",  
"ec2:DescribeVpcs",  
"ec2:DescribeVpcPeeringConnection",  
"ec2:DescribeVpnConnections",  
"ec2:DescribeVpnGateways",  
"ec2:DetachInternetGateway",  
"ec2:DetachNetworkInterface",  
"ec2:DetachVolume",  
"ec2:DisassociateAddress",  
"ec2:DisassociateRouteTable",  
"ec2:GetConsoleOutput",  
"ec2:ReleaseAddress",  
"ec2:ReportInstanceState",  
"ec2:RunInstances",  
"ec2:StartInstances",  
"ec2:StopInstances",  
    "ec2:Modify\*",  
    "ec2:ModifyVolumeAttribute",  
"ec2:ModifyVpcAttribute",  
"ec2:ModifyNetworkInterfaceAttribute",  
    "ec2:ReplaceNetworkAclAssociation",

```
 "ec2:UnassignPrivateIpAddresses"
],
 "Effect": "Allow",
 "Resource": "*"
},
{
 "Sid": "Stmt4",
 "Action": [
 "iam:CreateInstanceProfile",
 "iam:CreateRole",
 "iam>DeleteRole",
 "iam:PutRolePolicy",
 "iam:AddRoleToInstanceProfile",
 "iam:PassRole",
 "iam:RemoveRoleFromInstanceProfile",
 "iam>DeleteRolePolicy",
 "iam>DeleteInstanceProfile",
 "iam:GetRole",
 "iam:GetGroup",
 "iam:GetGroupPolicy",
 "iam:PutGroupPolicy",
 "iam:CreateGroup"
],
 "Effect": "Allow",
 "Resource": "*"
},
{
 "Sid": "Stmt5",
 "Action": [
 "sns:ListTopics",
 "sns:CreateTopic",
 "sns:SetTopicAttributes"
],
 "Effect": "Allow",
 "Resource": "*"
}
```

```
"Effect": "Allow",
"Resource": "*" }
]
}
```

## Appendix G: 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 Prod 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 H: 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 2 lists the local report command.

**Table 7-6: 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 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<br>CMS            |
| 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<br>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 | <p>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.</p> <p>Accepted (A) status: records passed all verifications.</p> <p>Rejected (R) status: records failed one (1) or more verifications.</p> <p>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.</p> | 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)<br><br>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<br><br>If the EDGE Server fails to produce a claim detail report, please review the "Missing Detail Report Troubleshooting Steps" in Section 4.1.7: 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<br>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<br><br>If the EDGE Server fails to produce a claim detail report, please review the "Missing Detail Report Troubleshooting Steps" in Section 4.1.7: 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<br>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                   |
| 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<br>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? |
|-------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------|
| 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report OrphanClaimEnrollee YYYY test<br><br>edge report OrphanClaimEnrollee YYYY prod<br><br>edge report OrphanClaimEnrollee YYYY validation | Executed Monthly<br><br>Command: ECS_REPORT      | Issuer<br><br>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<br><br>OR<br><br>CMS sends report specific remote command. | edge report OrphanClaimEnrollee YYYY test<br><br>edge report OrphanClaimEnrollee YYYY prod<br><br>edge report OrphanClaimEnrollee YYYY validation | Issuer: At any time<br><br>CMS: At least monthly | Issuer                   |
| 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<br><br>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 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<br>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<br>CMS            |
| 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<br>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<br>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? |
|-------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------------------|
| 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report RI_Prelim YYYY test<br><br>edge report RI_Prelim YYYY prod<br><br>edge report RI_Prelim YYYY validation | CMS: As of BY17, no longer run | Issuer                   |
| 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report RI_Prelim YYYY test<br><br>edge report RI_Prelim YYYY prod<br><br>edge report RI_Prelim YYYY validation | CMS: As of BY17, no longer run | Issuer<br><br>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 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report RA_RS_Transfer_Prelim YYYY test<br><br>edge report RA_RS_Transfer_Prelim YYYY prod<br><br>edge report RA_RS_Transfer_Prelim YYYY validation | CMS: At least monthly                                                                                                                 | Issuer                   |
| 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report RA_RS_Transfer_Prelim YYYY test<br><br>edge report RA_RS_Transfer_Prelim YYYY prod<br><br>edge report RA_RS_Transfer_Prelim YYYY validation | CMS: At least monthly<br><br>Note: A complete report for all accepted medical files is generated based on remote command sent by CMS. | Issuer<br><br>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 | 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report RA_RS_Transfer_Prelim YYYY test<br><br>edge report RA_RS_Transfer_Prelim YYYY prod<br><br>edge report RA_RS_Transfer_Prelim YYYY validation | CMS: At least monthly         | Issuer                   |
| 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<br><br>OR<br><br>CMS sends report specific remote command. | edge report RA_RS_Transfer_Prelim YYYY test<br><br>edge report RA_RS_Transfer_Prelim YYYY prod<br><br>edge report RA_RS_Transfer_Prelim YYYY validation | CMS: At least monthly         | Issuer<br><br>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 | RA Transfer Elements Extract (RATEE) Report | <p>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.</p> <p>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.</p> | <p>Issuer initiates report specific EDGE command</p> <p>OR</p> <p>CMS sends report specific remote command.</p> | <pre>edge report RA_RS_Transfer _Prelim YYYY test  edge report RA_RS_Transfer _Prelim YYYY prod  edge report RA_RS_Transfer _Prelim YYYY validation</pre> | CMS: At least monthly         | Issuer<br>CMS            |
| RISK ADJUSTMENT RISK SCORE & TRANSFER EXTRACT | RADV Population 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.                                                                       | <pre>edge report RA_RS_Transfer _Prelim YYYY test  edge report RA_RS_Transfer _Prelim YYYY prod  edge report RA_RS_Transfer _Prelim YYYY validation</pre> | CMS: At least monthly         | Issuer<br>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 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<br>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<br>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<br>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 active enrollment data that was submitted by the issuer in the enrollment XML for each enrollee included in the RADV IVA sample. 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<br>CMS            |
| Risk Adjustment Data Validation | RADV Medical Claim Extract (RADVMCE) Report | The RADVMCE Report contains all active RA-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<br>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<br>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<br>Enrollment Data Extract<br>Medical Claims Extract<br>Pharmacy Claims Extract<br>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 Risk Adjustment model and provide data for recalibration.<br><br>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.<br><br>The HCRPSR is generated after the HCRP batch job.                                                                                                                                                                                  | Issuer initiates report specific EDGE command<br><br>OR<br><br>CMS sends report specific remote command. | edge report HCRP_NATIONAL_PRELIM YYYY test<br><br>edge report HCRP_NATIONAL_PRELIM YYYY prod<br><br>edge report HCRP_NATIONAL_PRELIM YYYY validation | CMS: At least monthly         | Issuer<br><br>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 Report (HCRPDE) | <p>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.</p> <p>The HCRPSR is generated after the HCRP batch job.</p> | <p>Issuer initiates report specific EDGE command</p> <p>OR</p> <p>CMS sends report specific remote command.</p> | <p>edge report HCRP_NATIONAL_PRELIM <b>YYYY</b> test</p> <p>edge report HCRP_NATIONAL_PRELIM <b>YYYY</b> prod</p> <p>edge report HCRP_NATIONAL_PRELIM <b>YYYY</b> validation</p> | CMS: at least monthly         | Issuer<br>CMS            |

## Appendix I: Data Validation Queries Before Archive Command

The following zip file contains the Archive Validation Queries to ensure that the data counts are correct for the current BY.



ArchiveValidationQ  
ueries\_Before\_20180

## Appendix J: Referenced Documents

The following list of documents should be referenced as supporting documentation for the System Operations and Maintenance Manual:

**Table 7-7: Supporting Documents for O&MM**

| Name                                                   | Description                                                                                                                                                                                                                   | REGTAP link                                                                                                     |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 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. | <a href="https://www.regtap.info/reg_lib_arrye.php?i=2673">https://www.regtap.info/reg_lib_arrye.php?i=2673</a> |
| EDGE Server Contact Database User Guide                | Step-by-step guide to completing the web form reporting process that CMS will collect and maintain Issuer contact information.                                                                                                | <a href="https://www.regtap.info/reg_lib_arrye.php?i=1874">https://www.regtap.info/reg_lib_arrye.php?i=1874</a> |
| 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.                                                                                          | <a href="https://www.regtap.info/reg_lib_arrye.php?i=2576">https://www.regtap.info/reg_lib_arrye.php?i=2576</a> |
| EDGE Server Maintenance Release Notes                  | Provides version numbers, time of release and functions of new EDGE server versions.                                                                                                                                          | <a href="https://www.regtap.info/reg_lib_arrye.php?i=1732">https://www.regtap.info/reg_lib_arrye.php?i=1732</a> |
| EDGE Server Migration Job Aids                         | Provides steps to complete a server migration for AWS and OP servers.                                                                                                                                                         | <a href="https://www.regtap.info/reg_lib_arrye.php?i=2327">https://www.regtap.info/reg_lib_arrye.php?i=2327</a> |
| EDGE Server Production and Test Schema Data Dictionary | The Data Dictionary specifies what is collected in the table outlined in the data model for the Production schema.                                                                                                            | <a href="https://www.regtap.info/reg_lib_arrye.php?i=1727">https://www.regtap.info/reg_lib_arrye.php?i=1727</a> |
| EDGE Server Production Schema Data Model               | The Data Model in particular illustrates all the data tables in the Production schema in the EDGE server and how they relate to each other.                                                                                   | <a href="https://www.regtap.info/reg_lib_arrye.php?i=1728">https://www.regtap.info/reg_lib_arrye.php?i=1728</a> |
| EDGE Server Storage Calculator                         | Template to calculate how much storage is needed for the EDGE server                                                                                                                                                          | <a href="https://www.regtap.info/reg_lib_arrye.php?i=92">https://www.regtap.info/reg_lib_arrye.php?i=92</a>     |

| Name                                          | Description                                                                                                                                                                                                                                                                                                                                                           | REGTAP link                                                                                                 |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| EDGE Server Test Schema Data Model            | The Data Model in particular illustrates all the data tables in the Test schema in the EDGE server and how they relate to each other.                                                                                                                                                                                                                                 | <a href="https://www.regtap.info/reg_library.php?i=1729">https://www.regtap.info/reg_library.php?i=1729</a> |
| EDGE Server Timeline                          | Provides important deadlines for maintenance releases, command deployments, submission, etc.                                                                                                                                                                                                                                                                          | <a href="https://www.regtap.info/reg_library.php?i=1879">https://www.regtap.info/reg_library.php?i=1879</a> |
| EDGE Server Updates and Data Submission       | Provides new information for EDGE functionality, operations, and background for deadlines. Note that a new document is created annually.                                                                                                                                                                                                                              | <a href="https://www.regtap.info/reg_library.php?i=2411">https://www.regtap.info/reg_library.php?i=2411</a> |
| EDGE Server Validation Schema Data Dictionary | The Data Dictionary specifies what is collected in the table outlined in the data model for the Validation schema.                                                                                                                                                                                                                                                    | <a href="https://www.regtap.info/reg_library.php?i=2008">https://www.regtap.info/reg_library.php?i=2008</a> |
| EDGE Server Validation Schema Data Model      | The Data Model in particular illustrates all the data tables in the Validation schema in the EDGE server and how they relate to each other.                                                                                                                                                                                                                           | <a href="https://www.regtap.info/reg_library.php?i=2009">https://www.regtap.info/reg_library.php?i=2009</a> |
| EDGE Server XML XSD Zip File Contents Job Aid | Breakdown of the list of XML/XSD for inbound and outbound reports.                                                                                                                                                                                                                                                                                                    | <a href="https://www.regtap.info/reg_library.php?i=2624">https://www.regtap.info/reg_library.php?i=2624</a> |
| High Cost Pool Reference Guide                | This document provides issuers with an overview of the HCRP calculations and associated EDGE reporting for the BY2018.<br><br>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. | <a href="https://www.regtap.info/reg_library.php?i=2672">https://www.regtap.info/reg_library.php?i=2672</a> |
| Interface Control Document - RARI Addendum    | Describes the relationship between CMS and the issuer's EDGE server. This document serves to define additional reports that will be produced by the issuer's EDGE servers as a supplement to the ICD.                                                                                                                                                                 | <a href="https://www.regtap.info/reg_library.php?i=2626">https://www.regtap.info/reg_library.php?i=2626</a> |

| Name                             | Description                                                                                                                                                                                                                                                                                                                          | REGTAP link                                                                                                 |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 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, to give the development team guidance on the architecture of the system to be developed. Also helps ensure compatibility between system segments and components. | <a href="https://www.regtap.info/reg_library.php?i=2591">https://www.regtap.info/reg_library.php?i=2591</a> |
| XML/XSD Inbound Files            | Provides the structure and layout of the inbound files                                                                                                                                                                                                                                                                               | <a href="https://www.regtap.info/reg_library.php?i=2187">https://www.regtap.info/reg_library.php?i=2187</a> |
| XML/XSD Outbound Files           | Provides the structure and layout of the outbound files                                                                                                                                                                                                                                                                              | <a href="https://www.regtap.info/reg_library.php?i=2623">https://www.regtap.info/reg_library.php?i=2623</a> |