

Table of Contents

1	Introduction.....	1
1.1	Intended Audience	1
1.2	Objective of This Guide.....	1
1.3	System Overview	1
1.4	Hardware and Software Requirements for CCQAS 2.10.0.0 Users	2
1.5	User Resources.....	2
1.5.1	The Help Menu	2
1.5.2	MHS Help Desk.....	5
1.5.3	User Aids inside a CCQAS Record	6
2	Overview of the CCQAS Credentialing and Privileging Process.....	10
2.1	The CCQAS Credentials Record	10
2.2	The CCQAS Privilege Application.....	11
2.3	The CCQAS Privilege Application Review Process	12
3	Creating and Maintaining CCQAS 2.10.0.0 User Accounts	14
3.1	Self Service Registration.....	15
3.2	Processing Requests for New User Accounts	19
3.2.1	Verifying Applicants' Need for Access to CCQAS	19
3.2.2	Processing the Application	19
3.2.3	CC/MSSP/CM-Generated Applications	22
3.2.4	User Accounts for New Provider Applicants.....	24
3.2.5	User Accounts for Module Users.....	26
3.2.6	Generating User Accounts from Existing Provider Credentials Records.....	35
3.3	Adding Roles to Existing User Accounts	36
3.3.1	Adding the Provider Role to an Existing "Module User" Account	36
3.3.2	Adding "Module User" Role to an Existing Provider Account.....	38
3.4	Deactivating and Reactivating User Accounts	40
3.5	Using CCQAS for the First Time	43
3.5.1	Receiving a New Username and Temporary Password.....	43
3.5.2	Accessing CCQAS for the First Time	43
3.6	Maintaining CCQAS User Accounts	47
3.6.1	Updating User Personal and Contact Information	47

3.6.2	Changing an Active Password	49
3.6.3	Locking and Unlocking User Accounts	50
4	Managing Facility Privilege Lists	51
4.1	The Privilege Management Function.....	52
4.2	Initial Privilege Catalog Configuration.....	56
4.3	Maintenance of Facility Privilege Catalogs	56
5	Processing the 1 st E-Application for Clinical Privileges.....	58
5.1	User Roles in the Privilege Approval Process	58
5.2	The Work List	59
5.3	Notifications.....	60
5.4	Types of Privilege Applications.....	61
5.5	Initial Review of a Privilege Application	64
5.5.1	The Provider Summary Tab.....	65
5.5.2	The Position Tab.....	67
5.5.3	The Privileges Tab	68
5.5.4	The Documents Tab.....	69
5.5.5	The Comments Tab.....	71
5.5.6	Taking Action on a Privilege Application	72
5.5.7	Reassigning Ownership of an Application to Another CC/MSSP/CM	72
5.5.8	Taking Ownership of an Application from another CC/MSSP/CM.....	73
5.5.9	Setting an Application as Urgent	74
5.6	Routing a Privilege Application for Primary Source Verification.....	76
5.7	Primary Source Verification of a Privilege Application by CC/MSSP/CM.....	76
5.8	Primary Source Verification of a Privilege Application by the CVO	82
5.9	Building Workflow for Application Review	83
5.10	Tracking an Application in Review	86
5.11	Pulling an Application Out of the Review Process.....	88
5.12	Level 1 Review of an Application	89
5.13	Levels 2, 3, and 4 Review of an Application.....	94
5.14	Levels 5 or 6 (Committee) Review of an Application.....	95
5.15	Review of an Application by the PA	96
5.16	Completing the Application Approval Process.....	98
5.17	The Updated Provider Credentials Record	103

5.18	Managing Privileging Workload: The PAC Supervisor Role.....	105
6	Managing Provider Credentials Records	108
6.1	Creation of a New Record by the Credentials Staff.....	108
6.2	Searching for a Provider's Credentials Record.....	110
6.2.1	Searching for Records within the Facility/Unit	110
6.2.2	Using the Advanced Search Function.....	114
6.2.3	Locating Provider Records at Other Facilities or Units.....	118
6.3	The Provider Credentials Record.....	121
6.3.1	The Profile Section	122
6.3.2	The Military Section	123
6.3.3	The Identification Section.....	124
6.3.4	The Contact Information Section.....	125
6.3.5	The License/Certification/Registration (Lic/Cert/Reg) Section	126
6.3.6	The Drug Enforcement Agency/Controlled Dangerous Substances Section.....	132
6.3.7	The Education/Training Section	134
6.3.8	The Specialty Section	139
6.3.9	The Affiliation Section	142
6.3.10	The Continuing Education Section	144
6.3.11	The Contingency Training Section	145
6.3.12	The Custody History Section	149
6.3.13	The Work History Section	149
6.3.14	The Privileges Section	152
6.3.15	The Provider Photo Section	154
6.3.16	The Documents Section	155
6.3.17	The Remarks Section	157
6.4	Updating Credentials Records Using Batch Processing	161
6.5	Deactivating a Credentials Record.....	162
6.6	Generating Provider Mailing Labels.....	163
7	Modification of Provider Credentials and Clinical Privileges	166
7.1	Generating an Application for Modification or Augmentation of Privileges	166
7.2	Processing an Application for Modification or Augmentation of Privileges	169
8	ICTB Process	172
8.1	Requesting an ICTB at the Gaining Location.....	172

8.2	Initiating the ICTB at the Sending Location.....	176
8.3	The ICTB Assignment Record.....	179
8.4	The Transaction Table	180
8.5	The Transfer (ICTB) Application for Clinical Privileges.....	182
8.6	Processing an ICTB Transfer Application for Clinical Privileges.....	184
8.7	Cancelling an ICTB	186
8.8	Ending an ICTB	186
8.9	PAR for ICTB Duty	187
8.10	The ICTB Process for Navy Facilities	187
9	Permanent Changes of Station Process.....	189
9.1	Requesting a PCS at the Gaining Location.....	190
9.2	Initiating the PCS at the Sending Location.....	194
9.3	The Transferred Provider Credentials Record	197
9.4	Transaction Table for Incoming PCS Transactions	197
9.5	The Transfer (PCS) Application for Clinical Privileges.....	198
9.6	Processing a PCS Transfer Application for Clinical Privileges.....	200
9.7	PAR for the PCS Application.....	203
9.8	Cancelling a PCS	203
9.9	Changes to the CCQAS User Account after a PCS Transaction	203
10	Renewal of Clinical Privileges.....	204
10.1	Auto-Generating an Application for Renewal of Clinical Privileges	204
10.2	Manually Generating a Renewal Application for Clinical Privileges	206
10.3	The Renewal Application	208
10.4	Processing an Application for Renewal of Clinical Privileges.....	209
10.5	PAR for the Renewal Application	211
11	The PAR.....	212
11.1	Automated Initiation of the PAR Process.....	213
11.2	Manual Initiation of the PAR Process	214
11.3	Routing of the PAR.....	214
11.4	Completing the PAR – The PAR Evaluator Role.....	216
11.5	Reviewing the PAR-The PAR Reviewer Role	229
11.6	Reviewing the PAR-The Provider Role.....	230
11.7	Bypassing the Automated PAR Process	231

11.8	Cancelling the Setup PAR Task.....	232
11.9	Terminating or Reassigning a PAR In-Process	233
12	Generating Credentialing and Privileging Letters	235
12.1	Command Information for Letter Generation.....	235
12.2	Generating Letters for Individual Providers	237
12.2.1	Generating a Letter from Letters Menu	237
12.2.2	Generating a Letter from Inside a Credentials Record or Privilege Application..	243
12.3	Printing a Letter from CCQAS	243
12.4	Exporting a Letter to Microsoft® Word	244
12.5	Generating Batch Letters	246
13	Generating Standard Credentials and Privileging Reports	248
13.1	Generating a Standard Credentials Report.....	248
13.2	Generating a Standard Privileging Report	258
13.3	Printing a Standard Report.....	260
13.4	Cancelling a Standard Report	260
13.5	Exporting a Report to Microsoft® Word or Excel	260
14	Generating Ad-Hoc Credentials Reports	261
14.1	Generating an Ad-Hoc Credentials Report.....	261
14.2	Saving an Ad-Hoc Report Query for Future Use.....	261
14.3	Running an Ad-Hoc Report from a Saved Query.....	261
14.4	Deleting a Saved Query	262
14.5	Printing an Ad-Hoc Report	262
14.6	Exporting an Ad-Hoc Report to Microsoft ® Word or Excel	262
14.7	Sample Ad-Hoc Reports	262
15	System Management.....	262
16	Branch Clinic Management	262
16.1	Adding a Branch Clinic	262
16.2	Privileging at a Branch Clinic.....	266
17	Custody Transfer.....	270
	Appendix A - Credentialing and Privileging Data Dictionary.....	A-1
	Appendix B - Directives, Regulations, Instructions, HA Policy Memoranda, and References .	B-1
	Appendix C - FAQs - Creating and Maintaining CCQAS 2.10.0.0 User Accounts.....	C-1
	Appendix D - FAQs - Managing Facility Privilege Lists	D-1

Appendix E - FAQs - Processing the 1st E-Application for Clinical Privileges	E-1
Appendix F - FAQs - Modification of Provider Credentials and Clinical Privileges.....	F-1
Appendix G - FAQs - ICTB Process	G-1
Appendix H - FAQs - Renewal of Clinical Privileges.....	H-1
Appendix I - FAQs - The PAR	I-1
Appendix J - FAQs - Generating Ad-Hoc Credentials Reports.....	J-1

Table of Figures

Figure 1: Help Menu	3
Figure 2: MHS Learn ELearning Application – Home Page.....	4
Figure 3: Calendar Icon	6
Figure 4: A–Z Sort Function for Field Code	7
Figure 5: A–Z Sort Function for Field Code Description.....	8
Figure 6: Record Advance Keys	9
Figure 7: ‘Hidden Menu’ Button	9
Figure 8: Hidden Menu.....	10
Figure 9: Provider Credentials Record	11
Figure 10: Provider Privilege Application.....	12
Figure 11: Privilege Application Review Process	14
Figure 12: ‘CCQAS User Registration’ Button	16
Figure 13: CCQAS Privacy Act Statement.....	16
Figure 14: CCQAS Registration Screen	17
Figure 15: CCQAS Registration Screen – Provider Applicant.....	17
Figure 16: CCQAS User Registration Screen – Module User.....	18
Figure 17: CCQAS Registration Confirmation Screen.....	19
Figure 18: New Applicant Message.....	19
Figure 19: Applicant Processing Menu Item	20
Figure 20: Applicant Processing Screen	20
Figure 21: User Application Screen.....	21
Figure 22: User Added Message.....	21
Figure 23: User Processing Menu Item	22
Figure 24: User Search Screen.....	23

Figure 25: User Application Screen.....	23
Figure 26: ‘Demographics’ Tab for a Provider Applicant.....	24
Figure 27: ‘MTF’ Tab for a Provider Applicant.....	25
Figure 28: ‘Permissions’ Tab for a Provider Applicant.....	25
Figure 29: ‘Demographics’ Tab for an Other (Module Users).....	26
Figure 30: ‘MTF’ Tab for a Module User.....	27
Figure 31: Privileging Roles/Permissions for a Module User.....	27
Figure 32: Credentials Roles.....	29
Figure 33: Credentials Insert Permissions.....	30
Figure 34: Privileging Roles.....	30
Figure 35: Risk Management Permissions.....	31
Figure 36: Adverse Actions Permissions.....	31
Figure 37: System Admin Permissions.....	32
Figure 38: “Superuser Admin” Role Permissions.....	33
Figure 39: Reporting Permissions.....	33
Figure 40: “Superuser” Role Permissions.....	34
Figure 41: Grant Provider Access Menu Item.....	35
Figure 42: Similar User Account(s) Screen.....	37
Figure 43: ‘MTF’ Tab for a Dual User’s Account.....	37
Figure 44: User Search Screen.....	38
Figure 45: User Listing Screen after a Search.....	39
Figure 46: ‘MTF’ Tab for a Provider User Account.....	39
Figure 47: ‘MTF’ Tab for a Dual User’s Account.....	40
Figure 48: Deactivate Menu Item.....	41
Figure 49: Deactivate User Confirmation Message.....	41
Figure 50: Activate Menu Item.....	41
Figure 51: Activate User Confirmation Message.....	42
Figure 52: New Password Issued Message.....	42
Figure 53: CCQAS Privacy Act Statement.....	44
Figure 54: Login Screen.....	45
Figure 55: Temporary Password Alert.....	45
Figure 56: Random Password Generator Screen.....	46
Figure 57: Security Briefing.....	46

Figure 58: User Profile Menu Item for a Module User	47
Figure 59: Update User Screen for Other (Module Users)	47
Figure 60: User Processing Menu Item	48
Figure 61: User Search Screen.....	48
Figure 62: Change Password Menu Item.....	49
Figure 63: Password Expiration Warning.....	49
Figure 64: Reset Password Menu Item	50
Figure 65: Account Locked Indicator	51
Figure 66: CCQAS Privileging Management Menu Item	52
Figure 67: Privilege Management Screen and Category Pick List	52
Figure 68: Privilege List for Family Medicine	53
Figure 69: Examples of Family Medicine Core Privileges.....	53
Figure 70: View Privilege Menu Item	54
Figure 71: View Privilege Option.....	55
Figure 72: Limitations/Restrictions Option	55
Figure 73: Limitations/Restrictions View.....	56
Figure 74: Comment Option for Change to Privilege Designation	57
Figure 75: Privilege Audit Trail.....	57
Figure 76: Work List Screen for the CC/MSSP/CM	60
Figure 77: Status, Role, and Date Options for Work List.....	60
Figure 78: Messaging Menu Item	61
Figure 79: Disabling the Email Notification for the CC/MSSP/CM	61
Figure 80: My Applications Screen	62
Figure 81: My Application Hidden Menu	63
Figure 82: ‘Pending Applications’ Tab.....	63
Figure 83: Reactivate Menu Item	64
Figure 84: Work List Task – Application Ready for Review	64
Figure 85: Assign PAC Screen	65
Figure 86: ‘Provider Summary’ Tab.....	66
Figure 87: ‘Expanded Provider Summary’ Tab.....	66
Figure 88: ‘Position’ Tab.....	67
Figure 89: ‘Privileges’ Tab for Army General Surgery.....	68
Figure 90: ‘Documents’ Tab.....	69

Figure 91: Add Documents Screen	70
Figure 92: ‘Comments’ Tab.....	71
Figure 93: Add Comments Screen.....	71
Figure 94: Action Options for E-Applications.....	72
Figure 95: Re-assign Screen	72
Figure 96: ‘Application Reassignment’ Button	73
Figure 97: Application Reassignment Screen.....	73
Figure 98: Urgent Application Menu Item	74
Figure 99: Urgent Application Window	75
Figure 100: Urgent Application Confirmation Message	75
Figure 101: Urgent Application Task	75
Figure 102: Select PSV Screen	76
Figure 103: Complete PSV Task	77
Figure 104: Assign PSV Screen.....	77
Figure 105: Provider PSV Summary Screen	77
Figure 106: PSV Information Section.....	79
Figure 107: NPDB/HIPDB Section	81
Figure 108: NPDB/HIPDB Update Warning Message.....	81
Figure 109: PSV Complete Message	82
Figure 110: PSV Complete/Action Required Task.....	83
Figure 111: ‘Application Routing’ Button.....	83
Figure 112: ‘Application Routing Summary’ Tab.....	84
Figure 113: ‘Application Routing UIC’ Tab	84
Figure 114: In Review Status Indicator	86
Figure 115: ‘Task Log’ Tab.....	87
Figure 116: ‘Comments’ Tab.....	87
Figure 117: Retrieving an Application in Review	88
Figure 118: Work List for a Level 1 Reviewer.....	89
Figure 119: ‘Privileges’ Tab for a Level 1 Reviewer	89
Figure 120: Reviewer Comment Screen	90
Figure 121: Reviewer Recommendation Screen.....	91
Figure 122: Application Returned/Action Required Task	92
Figure 123: ‘Comments’ Tab of a Returned Application	92

Figure 124: Recommendation Detail Screen	93
Figure 125: Return to Provider Screen	93
Figure 126: Red Flag Icon for Review Levels 2-6	94
Figure 127: Recommendation Count Menu Item	95
Figure 128: Recommendation Count Screen	95
Figure 129: ‘Privileges’ Tab for Privileging Authority Review	97
Figure 130: PA Decision Screen.....	98
Figure 131: ‘Notifications’ Button.....	99
Figure 132: Notification Routing Screen.....	99
Figure 133: Provider ‘Acknowledge’ Button on Summary Page	101
Figure 134: Privileged Provider Information Report.....	101
Figure 135: Provider “Acknowledgment” Page	102
Figure 136: Provider Acknowledgement Notification.....	102
Figure 137: ‘Complete’ Button.....	102
Figure 138: ‘My Applications’ Tab with a Closed Application	103
Figure 139: Privileges Section in the Credentials Record	103
Figure 140: Privileged Provider Information Report.....	104
Figure 141: Provider Position Screen	105
Figure 142: PAC Supervisor Role on the ‘Permissions’ Tab	106
Figure 143: Submitted Applications Screen	106
Figure 144: Application Reassignment Screen.....	107
Figure 145: Re-Assign CC/CM/MSSP Screen	107
Figure 146: Reassign Confirmation Screen	108
Figure 147: Provider Search Menu Item.....	108
Figure 148: Add Provider Screen	109
Figure 149: Credentials Provider Search Screen	110
Figure 150: Search Result screen.....	113
Figure 151: Advanced Search Screen	114
Figure 152: Example Query using Advanced Search Functionality.....	117
Figure 153: Provider Locator Function.....	119
Figure 154: MTF Contacts Menu Item	120
Figure 155: Update MTF Contact Screen.....	120
Figure 156: Opening a Credentials Record.....	121

Figure 157: Navigation Bar	121
Figure 158: Profile Section	122
Figure 159: Figure 6.3-4. Military Section of Profile	123
Figure 160: Identification Section	124
Figure 161: Add Identification Screen.....	124
Figure 162: Contact Information Section	125
Figure 163: Updating a Primary Phone Number	126
Figure 164: Lic/Cert/Reg Section	126
Figure 165: State License/Certification/Registration Screen.....	127
Figure 166: Admin Waiver Field.....	129
Figure 167: National Certification/Registration Screen	130
Figure 168: Unlicensed Information Screen	132
Figure 169: DEA/CDS Section.....	133
Figure 170: DEA/CDS Screen.....	133
Figure 171: Education/Training Section.....	134
Figure 172: Qualifying Degree Record.....	135
Figure 173: Institution Search Screen.....	136
Figure 174: ‘Post Graduate Training’ Tab.....	137
Figure 175: Post Graduate Training Record	137
Figure 176: ECFMG Tab	139
Figure 177: Specialty Section	140
Figure 178: Adding a Specialty	140
Figure 179: Board Certification Section	141
Figure 180: Board Search Screen	142
Figure 181: Affiliation Section	143
Figure 182: ‘Academic Affiliations’ Tab	143
Figure 183: ‘Organizational Memberships’ Tab.....	144
Figure 184: Continuing Education Section.....	144
Figure 185: Continuing Education Record	145
Figure 186: Contingency Training Section.....	145
Figure 187: Contingency Training Record	146
Figure 188: References Section	146
Figure 189: Reference Record	147

Figure 190: Databank Queries Section	148
Figure 191: Custody History Section.....	149
Figure 192: Work History Section.....	150
Figure 193: ‘Assignment’ Tab.....	150
Figure 194: MTF Assignment Record	151
Figure 195: ‘Work History Privileges’ Tab	152
Figure 196: ‘Tracker Status’ Tab.....	152
Figure 197: Privileges Section.....	153
Figure 198: Provider Privileges Screen	153
Figure 199: Privileged Provider Information Report.....	154
Figure 200: Photo Section.....	155
Figure 201: Documents Section.....	156
Figure 202: PARs/Snapshots listing	157
Figure 203: Remarks Section.....	157
Figure 204: Provider Remarks Section	158
Figure 205: Provider Remarks Window	158
Figure 206: Provider Remarks Type Screen.....	159
Figure 207: Provider Remarks Type Screen.....	159
Figure 208: Provider Remarks Type Screen.....	160
Figure 209: Provider Remarks Menu Options	160
Figure 210: Credentialing Batch Process Menu	161
Figure 211: Action Section of the Credentials Provider Search Screen	161
Figure 212: Continuing Education Batch Training Screen.....	162
Figure 213: Deactivate Provider Menu Item	163
Figure 214: Deactivate Provider Screen	163
Figure 215: Mailing Labels Menu Item.....	164
Figure 216: ‘Provider Mailing Label’ Radio Button	164
Figure 217: ‘Batch Labels’ Tab	165
Figure 218: Batch Labels Options	165
Figure 219: Request Modification Menu Item.....	167
Figure 220: Application Modification Instructions Screen	167
Figure 221: Provider Application (Modification).....	168
Figure 222: Provider Task – Complete Application, Modification	169

Figure 223: CC/MSSP/CM Task – Application Ready to Review, Modification.....	170
Figure 224: NPDB/HIPDB/FSMB Provider Summary	170
Figure 225: Flagged Credentials on the Modification Application	171
Figure 226: Flagged Privileges on the Modification Application	171
Figure 227: Assignment Menu Item on the Search Results Tab	173
Figure 228: Request ICTB action on Assignment Screen	174
Figure 229: Request ICTB Screen at Gaining Location	174
Figure 230: New Incoming Broadcast Message Alert for Sending Location.....	175
Figure 231: Broadcast Messages Menu Item at the Sending Location.....	175
Figure 232: Broadcast Message Menu Item	176
Figure 233: Work History Section on Navigation Menu.....	177
Figure 234: Initiate ICTB Menu Option	177
Figure 235: ICTB Form	178
Figure 236: Email Address and Phone Number Fields for User Account.....	179
Figure 237: Search Results Screen for the Sending Location.....	179
Figure 238: Search Results Screen for the Gaining Location.....	180
Figure 239: New Incoming Credentials Transaction Window	181
Figure 240: Accessing the Transaction Table.....	181
Figure 241: The Provider Transactions Screen for an Incoming ICTB.....	182
Figure 242: Provider Task – Complete Application, Transfer (ICTB).....	182
Figure 243: Transfer(ICTB) Application for Privileges	183
Figure 244: Gaining CC/MSSP/CM’s Pending Applications Tab	184
Figure 245: Gaining CC/MSSP/CM Task – Transfer (ICTB) Application	184
Figure 246: Provider PSV Summary Screen for the ICTB Application.....	185
Figure 247: Cancel ICTB Menu Item	186
Figure 248: End ICTB Menu Item.....	186
Figure 249: Gaining CC/MSSP/CM Task – Setup PAR	187
Figure 250: ICTB Privilege Request Screen.....	188
Figure 251: Appendix Q Letter.....	188
Figure 252: E-Signed Appendix Q	189
Figure 253: Assignment Menu Item on the ‘Provider Locator’ Tab	191
Figure 254: Request PCS Screen	192
Figure 255: Request PCS Message Screen	192

Figure 256: New Incoming Broadcast Message Alert.....	193
Figure 257: Broadcast Message Menu Item	193
Figure 258: Broadcast Message Menu Item	194
Figure 259: Open Menu Item.....	195
Figure 260: Initiate PCS Screen.....	195
Figure 261: Initiate PCS Prompts Screen	196
Figure 262: Initiate PCS Screen for 1st E-Application.....	196
Figure 263: Accessing the Transaction Table.....	197
Figure 264: Provider Transactions Screen for Incoming PCS.....	198
Figure 265: Provider Task – Complete Application, Transfer (PCS).....	199
Figure 266: Transfer (PCS) Application for Privileges	199
Figure 267: Gaining CC/MSSP/CM’s ‘Pending Applications’ Tab.....	201
Figure 268: Gaining CC/MSSP/CM Task – Application Ready for Review, Transfer (PCS) ...	201
Figure 269: Flagged Section for State License/Certification Registration Screen	202
Figure 270: Sending CC/MSSP/CM Task – Setup PAR	203
Figure 271: Outstanding Tasks Warning Message	204
Figure 272: Command Parameters Menu Item.....	205
Figure 273: Renewal Days Parameters on the Command Parameters Screen.....	205
Figure 274: Provider Work List Item – Complete Renewal Application	206
Figure 275: Open Credentials Record.....	207
Figure 276: Initiate Renewal Application.....	207
Figure 277: Initiate Renewal Screen.....	208
Figure 278: Provider Application (Renewal).....	208
Figure 279: CC/MSSP/CM Task – Renewal Application Ready for Review	210
Figure 280: Modified Section for State License/Certification/Registration	211
Figure 281: CC/MSSP/CM Task – Setup PAR	212
Figure 282: CC/MSSP/CM Work List Item – Setup PAR	213
Figure 283: Initiate PAR Menu Item	214
Figure 284: PAR Routing Screen	215
Figure 285: PAR Evaluator Work List Task – Complete PAR	216
Figure 286: Profile Section of the PAR	217
Figure 287: Privileges Evaluated Section for the Army PAR	218
Figure 288: Privileges Evaluated Section for the Navy PAR with Unacceptable	219

Figure 289: Privileges Evaluated Section for the Air Force PAR	219
Figure 290: Quality Management Measures Section of the PAR.....	220
Figure 291: Types of Quality Management Measures.....	220
Figure 292: Facility-Wide Measures Section of the PAR	221
Figure 293: Types of Facility-Wide Measures	222
Figure 294: Practice Volume Section of the PAR	223
Figure 295: Professional Development Section of the PAR.....	224
Figure 296: Clinical/Technical Performance Questions Section of the PAR.....	225
Figure 297: Personal Evaluation Questions Section of the PAR.....	226
Figure 298: PAR Summary Form	227
Figure 299: E-Signature Section of the PAR.....	228
Figure 300: E-Signature Confirmation Screen	228
Figure 301: PAR Reviewer Work List Task – Review PAR.....	229
Figure 302: PAR Reviewer E-Signature Screen.....	229
Figure 303: Provider Work List Task – Review PAR.....	230
Figure 304: Provider E-Signature Screen	230
Figure 305: ‘Offline PAR’ Radio Button.....	231
Figure 306: Evaluator Work List Task – Complete Offline PAR	231
Figure 307: Offline PAR Notification	232
Figure 308: ‘Cancel PAR’ Button.....	232
Figure 309: Complete PAR Task Menu Options.....	233
Figure 310: Cancel PAR Warning Message	234
Figure 311: Re-assign Task Window.....	234
Figure 312: Command Parameters Menu Item.....	235
Figure 313: Command Parameters Screen.....	236
Figure 314: Letters Menu Item Provider Search.....	237
Figure 315: List of Provider Letters.....	238
Figure 316: Work History Letters Menu	238
Figure 317: DEA Multi–Purpose Letters	239
Figure 318: DEA Initial Application Form State Selection.....	239
Figure 319: Initial Application Letter Result.....	240
Figure 320: Notification of Change of Station	240
Figure 321: Return of Military DEA Registration Certificate	241

Figure 322: Expired Credentials Letters Selections.....	241
Figure 323: Pre-Populated Privileging Letter Transfer Message	242
Figure 324: Pre-Populated Privileging Letter with listed Categories	242
Figure 325: Verification Reference	243
Figure 326: Letter Print.....	244
Figure 327: Exploring the Letter.....	244
Figure 328: Save Electronic Copy	245
Figure 329: Save PDF Document	245
Figure 330: Action Section of the Credentials Provider Search Screen	246
Figure 331: Batch ICTB Letter Screen	247
Figure 332: Additional ICTB Information Screen.....	247
Figure 333: ICTB Batch Letter	248
Figure 334: Accessing the CCQAS Standard Credentialing Reports.....	248
Figure 335: List of Standard Credentials Reports.....	249
Figure 336: Parameter Screen for the Training Expiration Report.....	249
Figure 337: Example of Training Expiration Report Parameter Screen.....	257
Figure 338: Reporting Options	258
Figure 339: Blank Privilege Application Report	258
Figure 340: Accessing the CCQAS Standard Privileging Reports.....	258
Figure 341: List of Standard Credentials Reports.....	259
Figure 342: Privilege Finder Report	260
Figure 343: Exporting a Report to Word or Excel.....	260
Figure 344: Data Copied Message Window	261
Figure 345: Sample Excel Spreadsheet with CCQAS Report	261
Figure 346: MTF Contacts Page	263
Figure 347: UIC Selection for Branch Clinic	264
Figure 348: Add Branch Clinic.....	265
Figure 349: Branch Clinic Record	265
Figure 350: Delete Branch Clinic	266
Figure 351: Branch Clinics on 'Position' Tab for Provider E-App.....	267
Figure 352: Privileges Section for Branch Clinics	267
Figure 353: Reviewer Routing Page	268
Figure 354: Reviewer Routing Page for Branch Clinic	268

Figure 355: Summary Page for Reviewer Routing.....269
Figure 356: PA Review of Privileges for Parent/Branch Clinics269
Figure 357: PA Decision Screen.....270

List of Tables

Table 1: Types of Privilege Applications61
Table 2: Mapping of Data from the Credentials File to the Advanced Search Function.....115
Table 3: Operators for Advanced Search Function.....116
Table 4: Descriptions of CCQAS Standard Credentialing Reports251
Table 5: Descriptions of CCQAS Standard Privileging Reports259

DRAFT

1 Introduction

1.1 Intended Audience

The intended audience of this document includes all Centralized Credentials Quality Assurance System (CCQAS) users. Current users who are familiar with the 2.9.0.0 version may use this guide as a reference to understand the new features of 2.10.0.0, and new users may use this guide to familiarize themselves with the application in general.

1.2 Objective of This Guide

The objective of this guide is to provide an on-the-job reference for CCQAS users at military treatment facilities (MTFs) and units. This guide is designed to assist users with the management of CCQAS user accounts, privilege lists, and the primary source verification, routing, review, and approval of online privilege applications, and maintenance of Provider credentials records in the facilities and units for which they are responsible. It is assumed that users already have a good working knowledge of the business processes pertaining to the credentialing and privileging of health care providers. Policy and procedural guidance have been incorporated into this guide to the extent dictated by Service leadership. Users should direct questions regarding policy and procedures not addressed in this guide to their respective Service-level credentialing and privileging authority (PA).

Information within this document, including screenshot images, is current as of the date of preparation. Any differences noted between this document and the current version of the CCQAS application is due to modifications and enhancements made after this document was prepared.

1.3 System Overview

The Centralized Credentials Quality Assurance System, version 2.10.0.0 (CCQAS 2.10.0.0) is a standard Department of Defense (DoD) migration system jointly undertaken, operated, and controlled by the Army, Navy, and Air Force medical departments within the overall corporate sponsorship and policies of the Office of the Assistant Secretary of Defense for Health Affairs (OASD [HA]). The Defense Health Services System (DHSS) is responsible for the development, deployment, and maintenance of CCQAS 2.10.0.0 and any subsequent versions. CCQAS is a Web-based worldwide credentialing, privileging, risk management, and adverse actions application that supports medical personnel readiness. CCQAS enables the military medical community to electronically manage Provider credentialing and privileging, malpractice and disability claims, and adverse action investigations of physicians, dentists, nurses, pharmacists, and other medical support personnel.

CCQAS supports personnel at all levels of DoD with credentialing and privileging activities. The system provides the following features:

- Maintains and tracks the credentials and privileging history of more than 170,000 military and civilian health care providers, including Active Duty, Reserves, and National Guard

- Contains comprehensive Provider demographic, specialty, licensing, training, education, privileges, medical readiness/mobilization, assignment history, and Provider photographs for identification purposes
- Enables Providers to complete and submit an application for clinical privileges online
- Automates the online review and approval of a Provider's application for privileges and renewal of privileges
- Expedites the transfer of Provider credentialing and privileging information for temporary change of assignment (i.e., Inter-facility Credentials Transfer Brief [ICTB]) or Permanent Change of Station (PCS)
- Enables the online completion of Provider Performance Assessment Reports (PARs)
- Enables the automated generation of routine letters and forms that are needed to manage a Provider's professional credentials
- Provides a robust standard and ad hoc reporting capability
- Optimizes accuracy and efficiency of credentials review activities
- Meets DoD and the Joint Commission on Accreditation of Healthcare Organizations' (JCAHCO's) accreditation requirements
- Improves the ability of the Services to respond to medical readiness requirements

1.4 Hardware and Software Requirements for CCQAS 2.10.0.0 Users

CCQAS is a Web-based, Common Access Card/Personal Identity Verification (CAC/PIV) enforced application that is housed on a secure server, maintained by the Defense Information Systems Agency (DISA). All CCQAS data is stored in this server, which is maintained in accordance with DoD security requirements in order to protect the confidentiality of the data it contains and to permit access only to approved users. Approved users can access CCQAS via the Internet from any workstation configured for connectivity to the Internet. In order for CCQAS to function properly, users must access the application using the Internet Explorer (IE) version 6.0 (or higher) Web browser. The use of other Internet browsers is not recommended. No additional client software is required to access or to use CCQAS 2.10.0.0.

Note: The version of IE that is currently on the user's workstation may be viewed by clicking the IE icon and then selecting *About Internet Explorer* from the Help menu. If a version upgrade is needed, users should coordinate with their local network administrators to have the new version installed. The upgrade is readily available on the Internet at no charge.

1.5 User Resources

A number of resources are available to support CCQAS users on-the-job. These include links within the CCQAS application to relevant documentation and websites, as well as tools embedded within the CCQAS interface that help users populate individual data fields.

1.5.1 The Help Menu

CCQAS users may access a list of resources within the CCQAS application by selecting **Help** from the main menu bar along the top of the screen, as depicted in Figure 1 below.

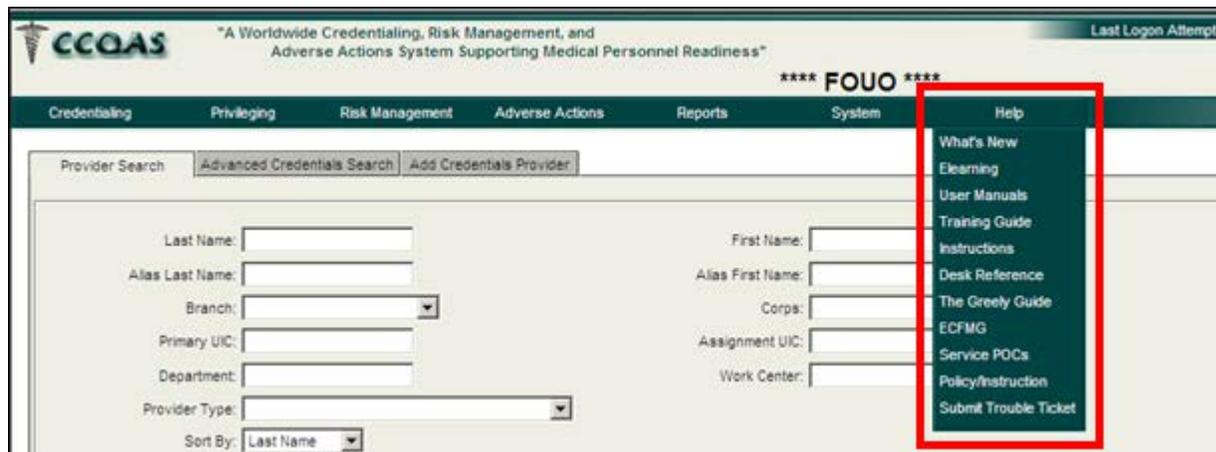


Figure 1: Help Menu

1.5.1.1 What's New Link

This link, which is located on the **Help** menu, takes users to a listing of change requests (CRs) that have been implemented in CCQAS. The CRs are grouped into numbered releases; each time a group of CRs is implemented, the version number for the CCQAS application is increased incrementally. The version number associated with the release and the release date are listed at the top of each grouping of CRs. Details pertaining to CRs in each release may be viewed by clicking the *Release Notes* link.

1.5.1.2 Elearning Link

This link takes users to the Military Health System (MHS) Learn ELearning application (i.e., MHS Learn), as depicted in Figure 2 below. The ELearning application is designed to provide basic navigational and functional training for new or returning CCQAS users. The ELearning application consists of a series of structured modules and courses that walk users through the processing of a sample privilege application from the perspective of a Provider, a credentialing and privileging staff member, a Reviewer, or a PA. ELearning courses are highly recommended for new CCQAS users and other users who would like a refresher course in system use.

Users may also access the ELearning application directly from the Internet at the following Uniform Resource Locator (URL):

<https://mhslearn.csd.disa.mil/ilearn/en/learner/mhs/portal/home.jsp>.

Users may self-register using the *MHS Staff Training* link to access the ELearning application. After users are logged in, they may choose from a number of available courses, including those for CCQAS.



Figure 2: MHS Learn ELearning Application – Home Page

1.5.1.3 User Manuals Link

This link takes users to read-only versions of this and other CCQAS user manuals. These user manuals are designed to provide on-the-job functional support for CCQAS users who are already proficient in system navigation. Users may open these manuals directly from the CCQAS application or save them to their workstation for later use.

1.5.1.4 Training Guide Link

This link takes users to read-only versions of available CCQAS training guides. Training guides are designed to help new CCQAS users navigate through the screens, tabs, and sections of the CCQAS application. Users may open these guides directly from the CCQAS application or save them to their workstation for later use. New users are also strongly encouraged to complete the appropriate courses offered by the MHS Learn ELearning application.

1.5.1.5 Instructions Link

This link contains instructions for creating mailing labels and updating Batch Readiness. Each section opens a Microsoft (MS) Word document with detailed instructions for each of the above functions.

1.5.1.6 Desk Reference Link

This link takes users to the home page for *The Credentialing and Privileging Desk Reference (CPDR) Online*, published by HCPro, Inc. This reference includes contact information for educational organizations, licensing agencies, specialty boards, practitioner databanks, and specialty associations, as well as information about the National Committee for Quality Assurance (NCQA) and Joint Commission on Accreditation of Healthcare Organizations' (JCAHO) standards.

1.5.1.7 Greely Guide Link

This link takes users to an online version of the *Greely Company Guide to Medical Staff Bylaws*, published by HCPro, Inc.

1.5.1.8 ECFMG Link

This link takes users to the home page of the Educational Commission for Foreign Medical Graduates (ECFMG) website and provides general information, requirements, publications, and schedules pertaining to ECFMG certifications.

1.5.1.9 Service POCs Link

This link takes users to a listing of Service points of contact (POCs) for Service credentialing and privileging, risk management policies, and the CCQAS application in general. Phone and email contact information is provided for each POC.

1.5.1.10 Policy/Instruction Link

This link takes users to the Service-specific website, where they may find instructions, guidance, publications, and other resources, including Service credentialing and privileging policy.

1.5.1.11 Submit Trouble Ticket Link

This link opens a window that enables CCQAS users to create a trouble ticket. Users are directed through a series of questions about the nature of the problem they are experiencing. Users are encouraged to submit a trouble ticket only after the problem has been investigated by the local network staff and CCQAS administrator to confirm the problem is not a result of network or user account management issues.

1.5.2 MHS Help Desk

Users may also contact the MHS Helpdesk for any questions pertaining to CCQAS, including system security, system operation, training, functional and technical issues, system errors, usernames and passwords, access issues, and system recommendations. Helpdesk personnel may be reached at 1-800-600-9332 (Continental United States [CONUS]) or 1-866-637-8725 (Outside the Continental United States [OCONUS]). In the event that the MHS Helpdesk is unresponsive by phone, users may contact the Helpdesk via email: mhssc@tma.csd.mil. Users

are advised to consult with their local and Service-level CCQAS manager prior to contacting the MHS Helpdesk when they attempt to resolve a CCQAS-related problem.

1.5.3 User Aids inside a CCQAS Record

Throughout the CCQAS application, mouse-enabled tools are embedded to make CCQAS more user-friendly. These tools are designed to ease the entry of data into a record or provide users with information that allows them to better understand the meaning or definition of a data field. These tools are described in more detail in the following sub-sections.

1.5.3.1 The Calendar Function

Users may enter dates into CCQAS date fields in one of two ways. They may enter the date manually into the field using one of three acceptable date formats. The acceptable date formats for any date field are MM/DD/YYYY, MM-DD-YYYY, or MMDDYYYY. In all cases, the 4-digit year is required for CCQAS to accept a manually-entered date correctly.

Users may also use the Calendar function to populate a date field by clicking the **Calendar** icon , as depicted in Figure 3 below.

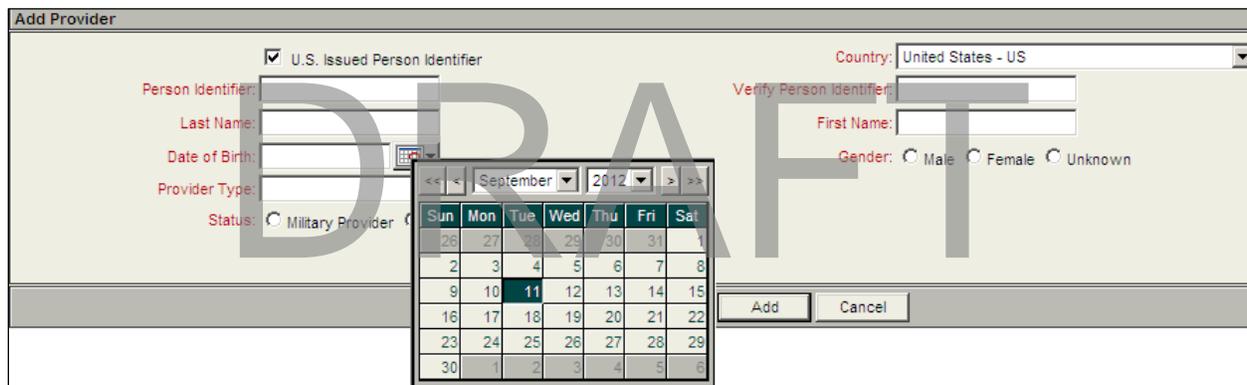


Figure 3: Calendar Icon

To enter the desired date, users first select the year and month from the pick lists at the top of the calendar. After users select the correct year and month, they click the desired day of the month. When users select the day, the calendar function automatically closes and the selected date populates the date field. If an error was made in the entry of the date, users may simply reopen the calendar and enter a new date.

1.5.3.2 The Search Function

For some data fields, the list of possible values are too numerous to fit in an on-screen pick list. When this occurs, CCQAS provides users with a search function to help them find a specific value to populate a data field. Search functions are identified by the **Binoculars** icon  next to the data field. By clicking this icon, a window opens that allows users to enter search criteria. When searching for a value using the search function, users should enter key words or phrases that will help to narrow the search quickly. Each of the available search functions in CCQAS

operates a little differently, and are discussed in more detail throughout relevant sections of this manual.

1.5.3.3 The A–Z Sort Function

Some pick lists contain data values that include both a code and a code description. CCQAS enables users to sort the list of values in the pick list numerically by code or alphabetically by code description. For example, Figure 4 below depicts the pick list for **Field** (in the **License/Certification/Registration** section of the credentials record). The values are listed in numerical order by field code.

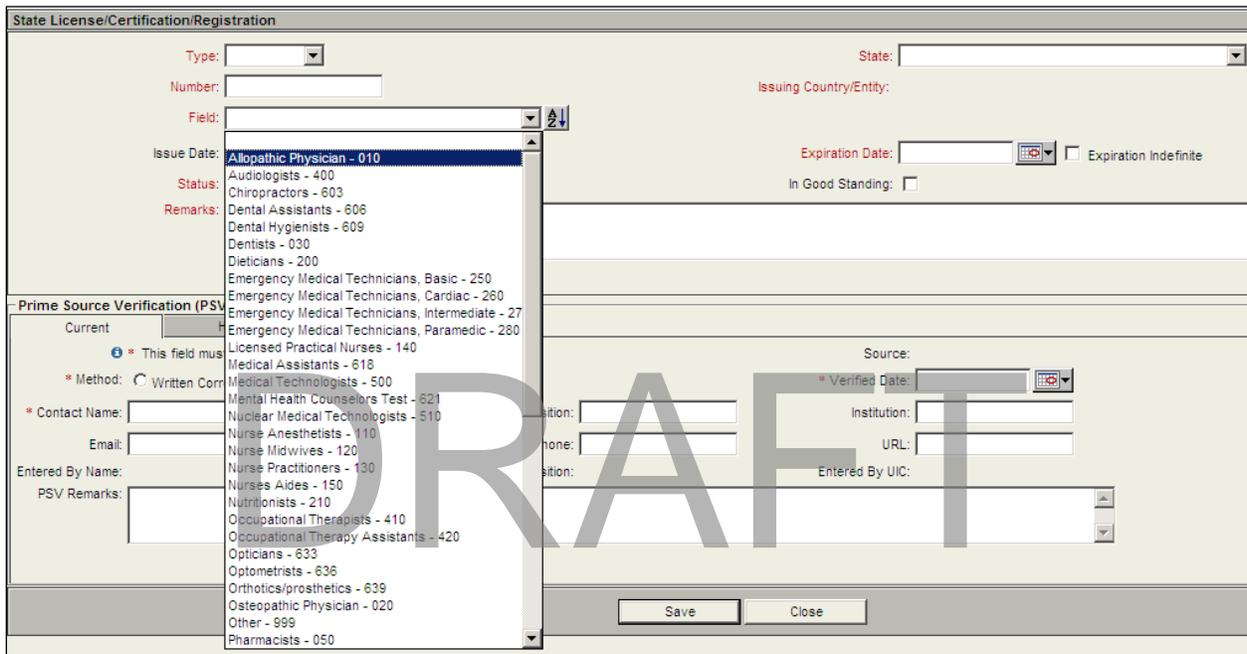


Figure 4: A–Z Sort Function for Field Code

When users close this pick list and click the **Sort** icon , the pick list is re-displayed in alphabetical order by field description, as depicted in Figure 5 below.

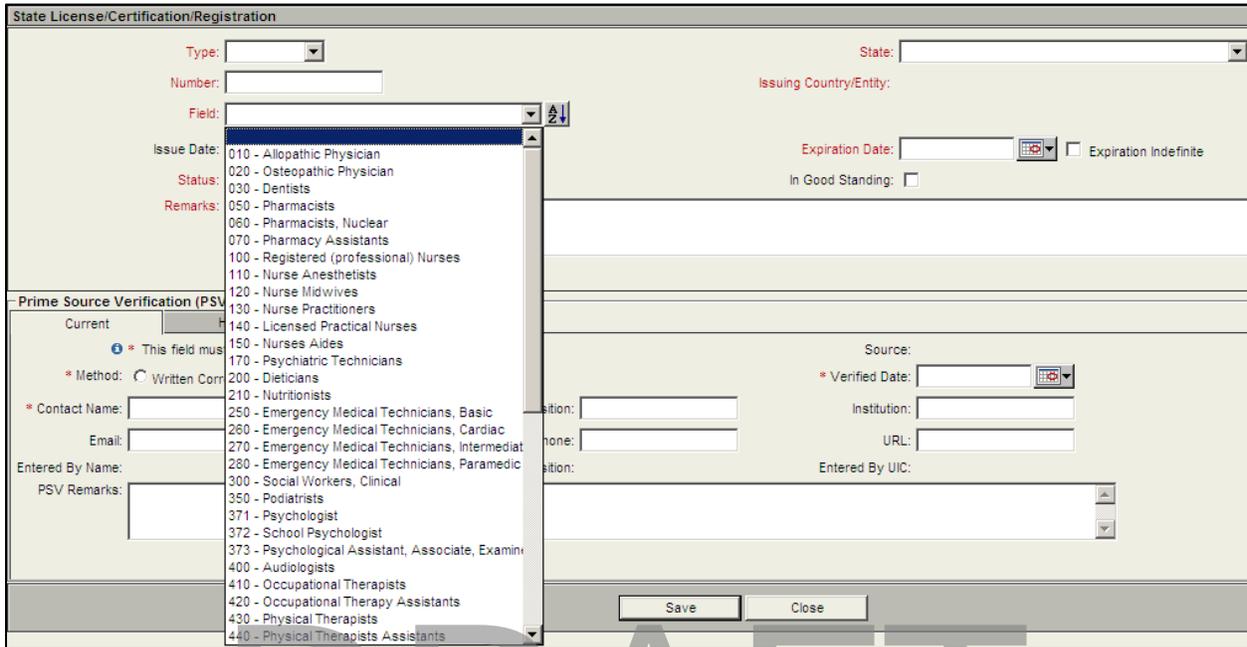


Figure 5: A–Z Sort Function for Field Code Description

In the CCQAS Credentialing and Privileging Data Dictionary, pick lists that have this sort function are denoted by [A-Z] in the **Field Type** column.

1.5.3.4 The Spell Check Function

For large, free text fields, CCQAS provides users with a spell check function. To use this function, users click the **Spell Check** icon  after they have entered text into the field. It is important to note that this tool is an automated function that may not catch errors in context and meaning. All entries into CCQAS should be manually reviewed to ensure that the text is error-free.

In the CCQAS Credentialing and Privileging Data Dictionary, text fields that have the spell-check function are denoted by [ABC] in the **Field Type** column.

1.5.3.5 The Record Advance Keys

Users may advance to the same section of an adjacent credentials record on the **Search Results** screen by clicking one of the two buttons in the upper right-hand corner of the credentials record. This function enables users to move directly to the previous or next record in the search results listing without having to execute the extra mouse clicks necessary to close one credentials record and open another. The **Record Advance** keys are depicted in Figure 6 below.



Figure 6: Record Advance Keys

1.5.3.6 Hidden Menu Button

The **Hidden Menu** button, which is to the left of a record in a listing, reveals a hidden menu that allows users to execute additional functionality on a selected record. Figure 7 below depicts the **Hidden Menu** button next to a sample record.

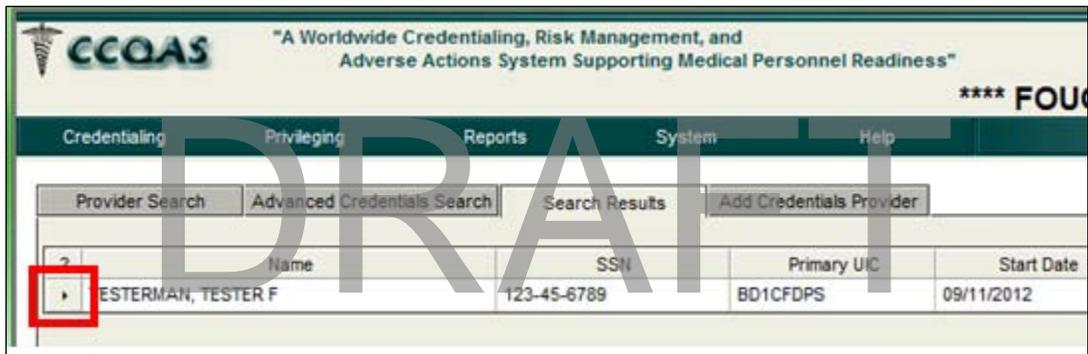


Figure 7: 'Hidden Menu' Button

The menu options vary depending on where the hidden menu is located in the application. Users may also view the hidden menu by right-clicking on the specific record, as depicted in Figure 8 below.

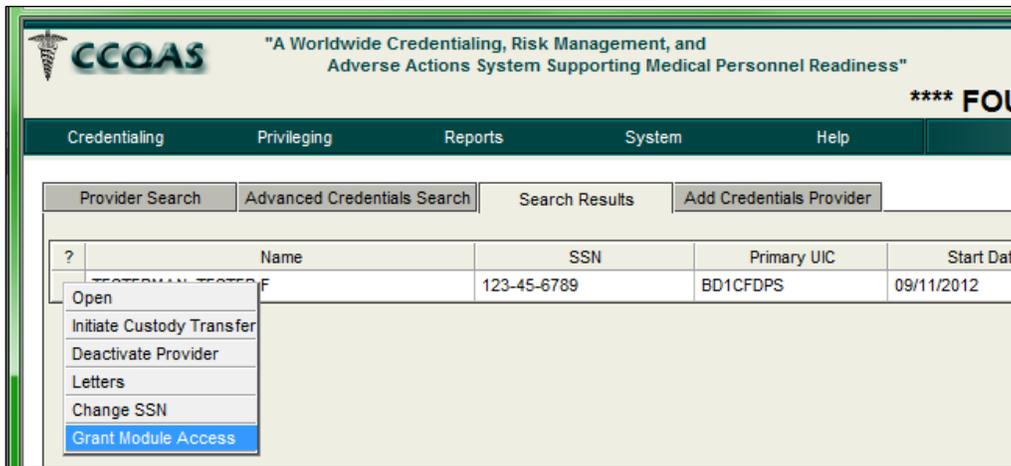


Figure 8: Hidden Menu

2 Overview of the CCQAS Credentialing and Privileging Process

Credentialing and privileging are processes by which a health care provider's training, experience, and other qualifications are assessed in order to approve the Provider to render health care services in military hospitals and clinics. CCQAS supports these processes by providing online facilitation of the entry, update, validation, and review of a Provider's credentials in an efficient and timely manner. The CCQAS Provider credentials record and the CCQAS privilege application are the two electronic documents that provide the basis for the CCQAS credentialing and privilege processes.

It is important to note that the benefits of CCQAS as a documentation, tracking, and reporting tool may only be fully realized if users understand and comply with their facility's and Service's credentialing and privileging policies and guidelines. Users should maintain a good working knowledge of these references and consult with their Service leadership if questions arise.

2.1 The CCQAS Credentials Record

Credentialing is the process of compiling, validating, and verifying qualifications of Providers to provide health care services. The core component of the CCQAS Credentials module is the electronic credentials file, which enables the capture and update of all of a Provider's qualifications that are relevant to his or her ability to render health care services to patients. CCQAS also enables the documentation of the date, method, and details when primary source verification (PSV) is performed on credentials that require PSV. The credentials record is organized into sections that are accessible by clicking the section name in a navigation bar on the left side of the screen, as depicted in Figure 9 below. Each section of the credentials record is discussed in detail in [Section 6](#).

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/11/2012 09:19:36 -04:00 Submit Ticket Security Briefing Logoff B01CFDPS

**** FOUO ****

Credentialing Privileging Reports System Help

Provider Close Provider Record

Name: TESTER TESTERMAN JR Branch: F11 Rank: SMSgt Corps: EN AOC/Desig/AFSC: 4C051
 SSN: 123-45-6789 Primary UIC: BD1CFDPS Cred Status: Active Input Clerk: CM21

Profile
 Identification
 Contact Information
 Lic/Cert/Reg
 DEA/CDS
 Education/Training
 Specialty
 Affiliation
 Continuing Education
 Contingency Training
 References
 Databank Queries
 Custody History
 Work History
 Privileges
 Documents
 Remarks

please complete the alias section.

First Name: TESTER MI: F Suffix: JR Title:
 Person ID: 123-45-6789
 Date of Birth: 04/23/1968 Citizenship: United States - US
 NPI: * Source DMHRSI

No Photo Available
 Upload, Edit Photo

Force (USAF)
 Senior Master Sergeant
 AOC/Desig/AFSC: 4C051 - Mental Health Service Journeyman
 Accession: DA - Direct Accession

Alias First Name Alias MI Suffix NPDB

**** FOUO ****

Done Internet | Protected Mode: On 100% 1:03 PM

Figure 9: Provider Credentials Record

The CCQAS credentials record is a dynamic record that grows as Providers gain additional qualifications and experience, and follows them as they move to new duty stations within the MHS. A CCQAS credentials record is created or updated in one of two ways. Data may be directly entered into a credentials record by the facility credentials staff using the CCQAS Credentialing module. This process is discussed in detail in [Section 6](#). A credentials record may also be created or updated by importing verified credentials data from a Provider's privilege application into the Credentialing module. This process is discussed further throughout [Section 5](#).

2.2 The CCQAS Privilege Application

Privileging is the process of determining specific procedures and treatments that Providers may perform in the facility. This process requires facility personnel to identify the clinical procedures and treatments or "privileges" that are supported at their facility, as well as the training and experience requirements necessary to authorize a Provider to perform each privilege. A Provider's qualifications are then reviewed to determine if he or she meets the requirements to perform requested privileges. CCQAS supports this privileging process by compiling all relevant credentials and other data needed to make a privileging decision into an online privilege application package. The structure and content of a privilege application is similar to that of a

credentials record, with some additional sections that are required for the privilege application review process. Figure 10 below depicts the structure and content of a sample Provider privilege application.

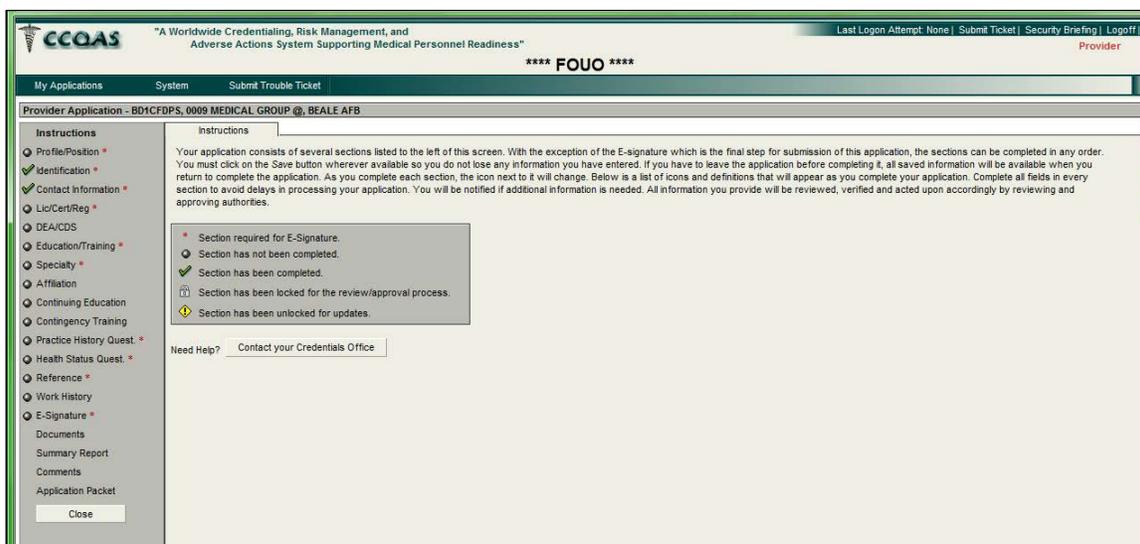


Figure 10: Provider Privilege Application

The privileging process is repeated a minimum of every two years at each location where a Provider renders care to patients. A privilege application is created each time a Provider needs to request or renew privileges at a given location. The privilege application is pre-populated with data residing in the Provider's credentials record at the time the application is created, so that the Provider only needs to add any new credentials that he or she has obtained since the last privileging cycle. After the Provider completes and E-signs his or her application online, the application package is routed through a formal review process. This review process is discussed in more detail in the next section and throughout [Section 5](#).

A privilege application is only 'active' while privileging is in process. After a privilege application is approved by the PA, the application itself becomes a view-only historical document. Any new credentials information entered into the privilege application is automatically imported into the Provider's credentials record after the application has passed through the PSV process. This ensures that the CCQAS credentials record remains current with the most recent, validated credentials data available for the Provider.

2.3 The CCQAS Privilege Application Review Process

CCQAS facilitates the application review process by providing access to the online application package according to the individual user's role in the privileging process. The CCQAS roles that pertain directly to the privileging process include the roles of "Provider," "Reviewer" (includes individual and committee Reviewers), "PA," and the credentials coordinator ('CC' for Army)/medical staff services professional ('MSSP' for Navy)/credentials manager ('CM' for Air Force), hereafter referred to as the "CC/MSSP/CM." Other roles are also defined for individuals involved in the Performance Assessment Report (PAR) process.

The CCQAS privilege application review process may be summarized as follows:

- A Provider completes and submits his or her application for clinical privileges online
- The assigned CC/MSSP/CM receives, reviews, and performs the required PSV on the application. In Air Force facilities, the PSV may also be performed by a Centralized Verification Office (CVO). Following completion of the PSV, the Provider's credentials record is updated with any new or updated credentials data present in the Provider's privilege application
- The CC/MSSP/CM routes the verified application to selected Reviewers, according to the review procedures established by the facility and the specialty(s) in which the Provider is requesting privileges
- The Level 1 Reviewer issues their recommendation for granting the requested privileges to the Provider after reviewing the application. This Reviewer is typically the department head or clinical supervisor under which the Provider is working. CCQAS requires all privilege applications to undergo review Level 1 review
- Other individual and committee levels of review are performed. CCQAS has made these levels of review optional so that each facility may tailor the review process to meet their own requirements
- The PA reviews the application and issues the final approval decision. CCQAS requires all privilege applications to undergo review by the PA
- The CC/MSSP/CM routes the notification of awarded privileges to the Provider and other individuals that should be informed of the award
- The Provider acknowledges the award of privileges
- The CC/MSSP/CM accepts the acknowledgement which completes the application process

The CCQAS application review process is summarized in Figure 11 below.

Email notifications are generated by CCQAS to alert each individual in the review process when it is time to take action on the application. Throughout the review process, the CC/MSSP/CM is responsible for ensuring the process continues to move forward until the application process is closed. The CC/MSSP/CM may retrieve an application currently in review, add or change assigned Reviewers, or return the application to the Provider at any time during the review process if the privilege application needs changes or additions.

During the application review process, Reviewers have access to Provider's privilege application and additional information they need to render a decision to recommend the award of privileges to the Provider. A recommendation in favor of the requested privileges must be rendered at all levels of review before a privilege application can be reviewed and approved by the PA. If a situation arises where a Reviewer does not concur with the privileges requested by the Provider, the application is returned to the CC/MSSP/CM. The CC/MSSP/CM coordinates resolution of the issue outside of CCQAS and re-routes the application through the review process to obtain consensus on a recommendation in favor of the awarded privileges. It is important to note that CCQAS is designed to facilitate the forward processing and award of clinical privileges. If a decision is made to deny a Provider's request for clinical privileges, the denial process should be

handled outside of the CCQAS system to ensure the Provider's rights to due process are preserved.

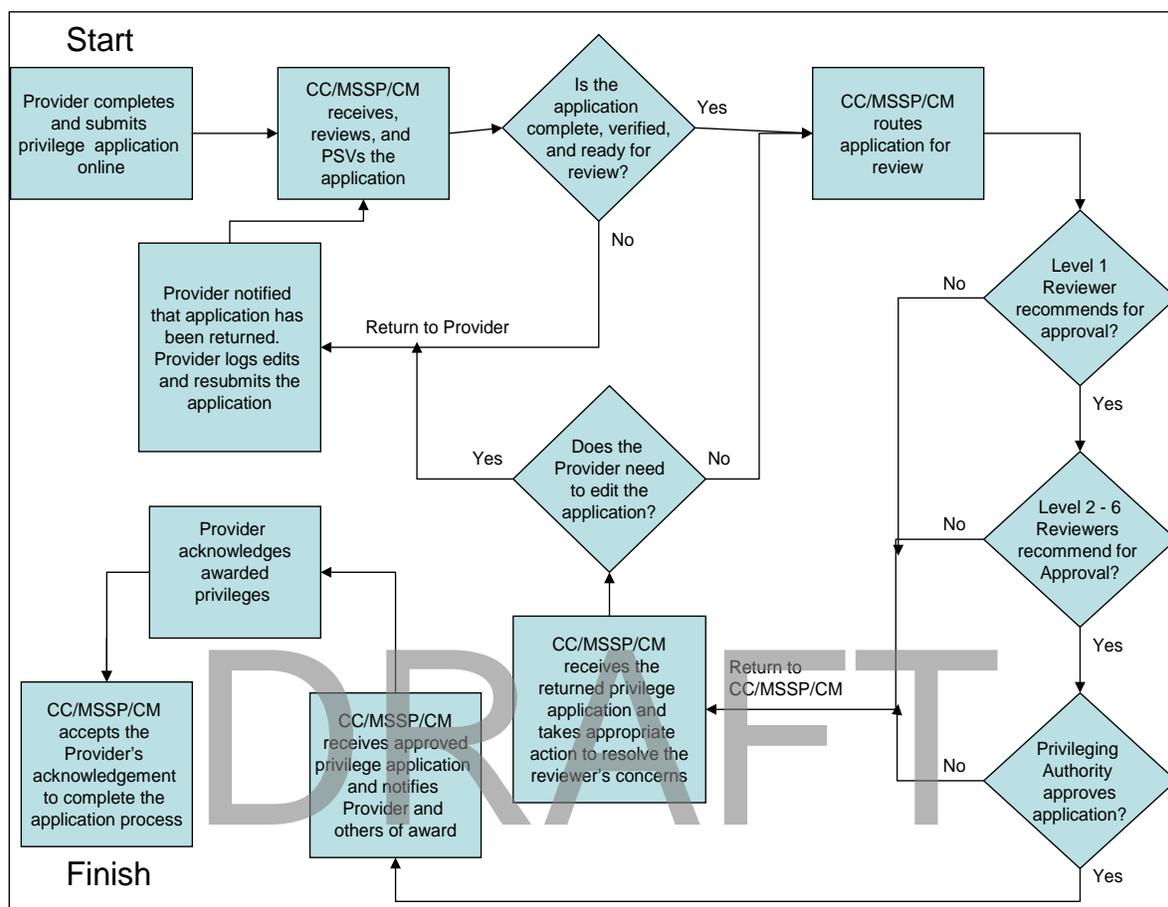


Figure 11: Privilege Application Review Process

3 Creating and Maintaining CCQAS 2.10.0.0 User Accounts

All facility personnel who participate in the online privilege application, review, and approval process require a CCQAS user account. In addition to the administrative personnel who use the credentials and risk management functionality, Providers who are applying for clinical privileges online and those personnel who are responsible for evaluating clinical performance of staff members also require access to CCQAS. In most cases, the responsibility for creating user accounts is assigned to one or more CC/MSSP/CMs at each facility or unit. The processes associated with the creation of new CCQAS user accounts are addressed in Sections [3.1](#) and [3.2](#).

After a user account is created, the maintenance of user accounts becomes the joint responsibility of an account holder and a CC/MSSP/CM, who are responsible for managing user accounts. Over time, it is likely that a user's account might require updating to reflect changes in personal information, job responsibilities, or location. Guidance regarding updating user information, permissions, and maintaining user accounts is provided in Sections [3.3](#) through [3.6](#).

All individuals who require access to CCQAS and do not yet have a user account are considered “new CCQAS users.” As CCQAS 2.10.0.0 is being implemented at a facility or unit, new user accounts must be created for every individual involved in the privileging process, including Providers, Reviewers, the PA, and those who are responsible for assessing performance of their clinical staff. After CCQAS 2.10.0.0 is fully implemented, the number of “new CCQAS users” will decrease, and the need to create new user accounts will be limited to new military accessions or civilian employees who are working in the MHS for the first time. The creation of new user accounts may be initiated in one of three ways:

- Prospective users may self-register for a new user account. The request form is then processed by a CC/MSSP/CM via the “Applicant Processing” function
- CC/MSSP/CMs may create a new user account through the “User Processing” function
- CC/MSSP/CMs may initiate the creation of a user account for a Provider with an existing credentials record in CCQAS via the Credentialing module. This is the preferred method for integrating Providers into the CCQAS electronic privileging process who already hold privileges in the facility or unit

The sections below discuss the creation of a new user account by each of these methods.

3.1 Self Service Registration

Prospective CCQAS users may apply online for an account using the self-service registration function. Users can access the online registration form from the CCQAS login screen.

Note: Prospective CCQAS users need a valid CAC or PIV card to access the site.

After the Single Sign-On (SSO) authentication process is completed, users enter a CAC or PIV Personal Identification Number (PIN). After reading and verifying the DoD warning message, users click **OK**. The self-registration process begins when users click the **Registration** button on the left-hand side of the screen, as depicted in Figure 12 below.

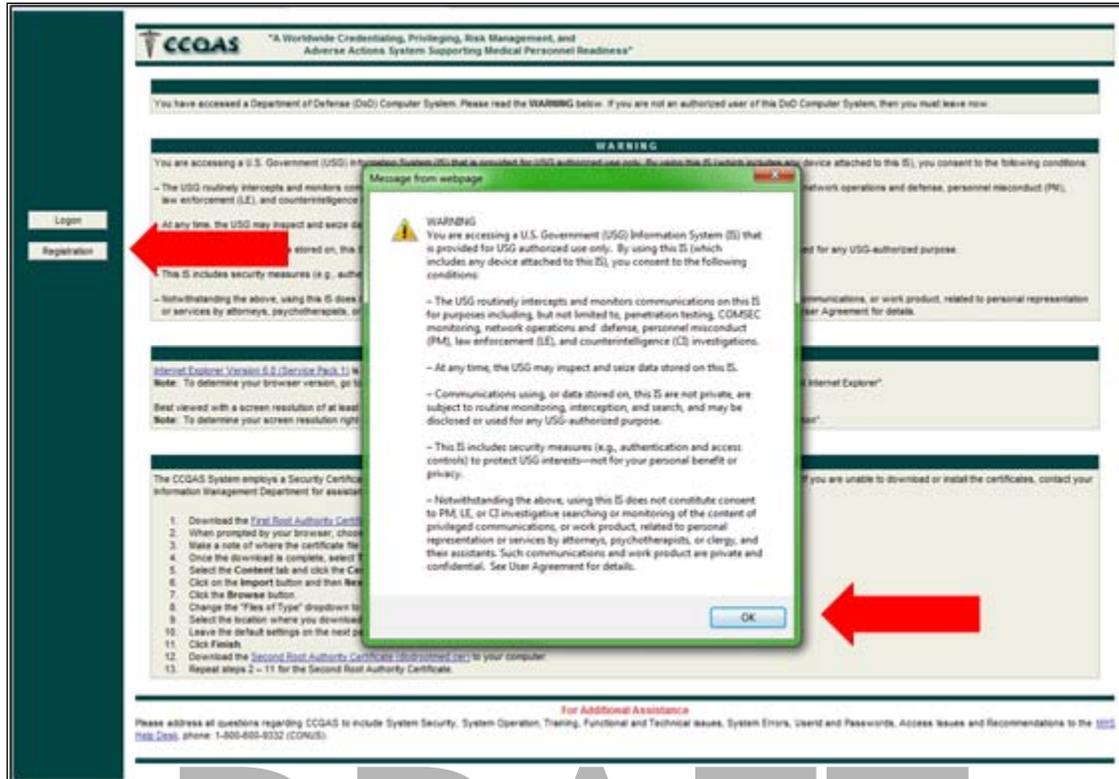


Figure 12: 'CCQAS User Registration' Button

Before completing a registration, users must read and verify the CCQAS Privacy Act Statement by selecting the **Affirmative** radio button, as depicted in Figure 13 below. The system does not allow prospective registrants to continue unless they select this radio button.

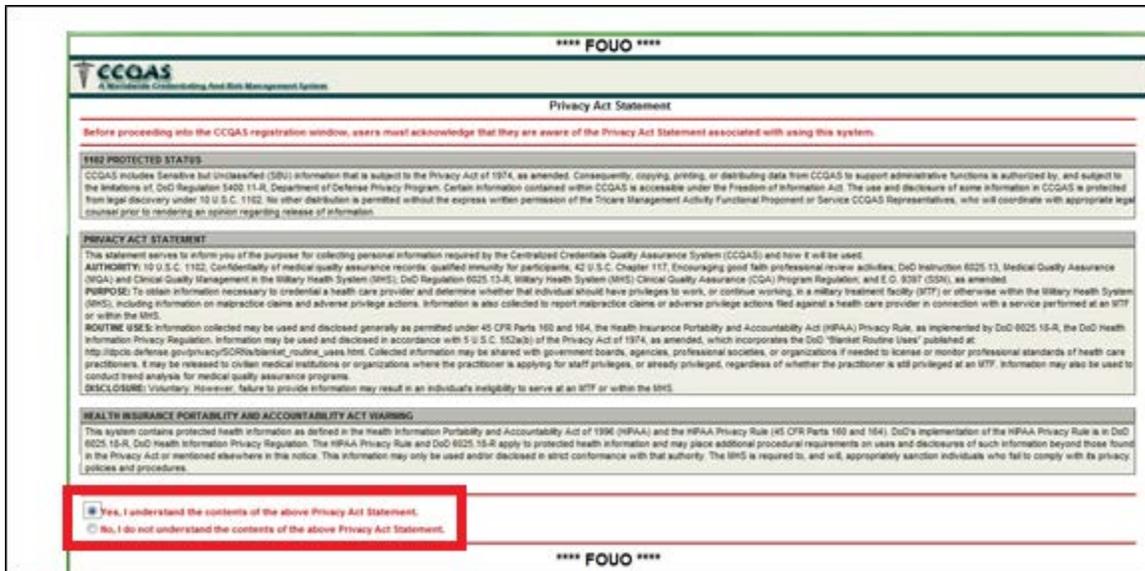


Figure 13: CCQAS Privacy Act Statement

Instructions for completing the online form are provided at the top of the screen. Those data fields labeled with red text are required for CCQAS to accept the application, as depicted in Figure 14 below.

The requirements for completing the registration form vary depending on the value selected for “**User Type**”. For the purposes of user account creation, applicants are classified either as “*Provider Applicant*” or as “*Module User*.”

**** FOUO ****

INSTRUCTIONS

To request a CCQAS user ID and password, complete the sections below. After completing the required sections, click the **SUBMIT** button to transmit your request. Once a user ID and password have been assigned, you will be notified via email. The CCQAS Security Manager at your activity will then grant permissions to your user ID, enabling you to access specific data and functions within CCQAS based upon your work assignment.

REGISTRATION

System Request
 User Type:

UIC:

User Information
 Person ID Type:
 Person ID: Confirm Person ID:
 Last Name: First Name: Middle Initial:
 Gender: Male Female Birth Date: Email:
 Phone Type: Phone:

Submit Reset Print Form Cancel

**** FOUO ****

Figure 14: CCQAS Registration Screen

Applicants should select “**User Type = Provider Applicant**” if they are a Provider who requires access to CCQAS for the purpose of requesting clinical privileges or submitting credentials as a member of the Clinical Support Staff. When applicants select “**User Type = Provider Applicant**,” they are also required to designate themselves as a military or civilian Provider. Provider Applicants do not need to complete the **Registration Validation** section. Figure 15 below depicts the **CCQAS Registration** screen.

**** FOUO ****

INSTRUCTIONS

To request a CCQAS user ID and password, complete the sections below. After completing the required sections, click the **SUBMIT** button to transmit your request. Once a user ID and password have been assigned, you will be notified via email. The CCQAS Security Manager at your activity will then grant permissions to your user ID, enabling you to access specific data and functions within CCQAS based upon your work assignment.

REGISTRATION

System Request
 User Type: Provider Applicant

UIC: BD1CFDPS

User Information
 Person ID Type: Social Security Number
 Person ID: ***** Confirm Person ID: *****
 Last Name: Testerman First Name: Tester Middle Initial: F
 Gender: Male Female Birth Date: 04/23/1968 Email: email@emailDomain.com
 Phone Type: Home Phone: (703) 555-1234
 Status: Military Provider Civilian Provider

Submit Reset Print Form Cancel

**** FOUO ****

Figure 15: CCQAS Registration Screen – Provider Applicant

Note: Applicants should designate their “**Status = Military Provider**” if they are applying for privileges or Clinical Support Staff positions at the designated facility or unit as uniformed service members (i.e., active duty service members, reserve or guard Providers on annual training, service members on temporary assignment, or deployed service members). Applicants who apply to render patient care as civilian employees or contractors at that facility or unit should designate their “**Status = Civilian Provider.**”

Applicants should select “**User Type = Module User**” (depicted in Figure 16 below) if they intend to review or approve applications for clinical privileges, or if they are administrative staff members who require access to CCQAS for the purpose of managing credentials records or other functions supported by the Risk Management or Adverse Actions functionality in CCQAS. If applicants select “**User Type = Module User**”, they are required to select the modules to which they are requesting access. CC/MSSP/CMs, Reviewers of privileging applications, the PA, personnel responsible for generating and reviewing clinical performance appraisals, and staff members who manage facility privilege lists should request access to the Privileging module. Module User applicants are also required to complete the **Registration Validation** section of the application.

The screenshot shows a web-based registration form for CCQAS. At the top, it says '**** FOUO ****' and 'INSTRUCTIONS'. Below that, it says 'REGISTRATION'. The form is divided into three main sections: 'System Request', 'User Information', and 'Registration Validation'. The 'System Request' section has a dropdown for 'User Type' set to 'Module User' and a 'UIC' field with 'BD1CFPS'. The 'User Information' section includes fields for 'Person ID Type' (Social Security Number), 'Person ID', 'Last Name' (Tul), 'Gender' (Male selected), 'Phone Type' (Home), 'First Name' (Jettro), 'Birth Date' (09/15/1966), 'Middle Initial', 'Email' (email@email.com), and 'Phone' (202) 555-7090. The 'Registration Validation' section has fields for 'Last Name' (Aquilung), 'Comm Phone' (202) 555-4567, 'Comm Fax', 'First Name' (Michael), 'DSN Phone', 'DSN Fax', 'Middle Name', 'Email', and 'Rank/Position'. At the bottom, there are buttons for 'Submit', 'Reset', 'Print Form', and 'Cancel'. The 'Submit' button is highlighted with a red box. A large 'DRAFT' watermark is overlaid on the form.

Figure 16: CCQAS User Registration Screen – Module User

All applicants must specify the Unit Identification Code (UIC) for their application. They must select the UIC associated with the location where the Provider, Reviewer, or staff member will be working.

Though not all remaining fields on the form are labeled as “required”, applicants should be encouraged to populate the form as much as possible, since CC/MSSP/CMs use the information on this form to verify an applicant’s identity and need for system access. **An accurate email address is critical**, since the applicant will be issued an individual username and temporary password via email.

After applicants have entered all information on the form, they click **Submit**, as depicted in Figure 16 above. The process by which CC/MSSP/CMs create a new user account for an applicant is discussed in the next section.

CCQAS returns a confirmation of application submission, as depicted in Figure 17 below. Applicants may either print or close this application. Click **Close**, and applicants are returned to the login screen.

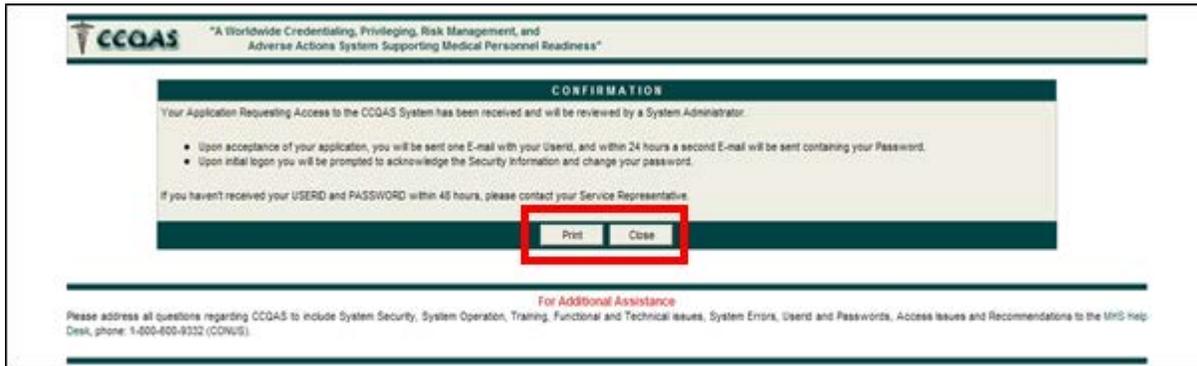


Figure 17: CCQAS Registration Confirmation Screen

3.2 Processing Requests for New User Accounts

This section describes the process for requesting new user accounts.

3.2.1 Verifying Applicants' Need for Access to CCQAS

CC/MSSP/CMs who are assigned the responsibility for managing user accounts at a facility or unit must verify each applicant's need for access to CCQAS prior to processing the request for a user account. It is important for CC/MSSP/CMs to understand the applicant's job responsibilities and role clearly in the privileging process in order to assign the correct roles and permissions to the account. CC/MSSP/CMs should confirm the 'need to access' with the appropriate departmental supervisor where the applicant will be using CCQAS.

3.2.2 Processing the Application

CCQAS alerts CC/MSSP/CMs to new requests for user accounts with a message, as depicted in Figure 18 below. This message displays when CC/MSSP/CMs log in to CCQAS.

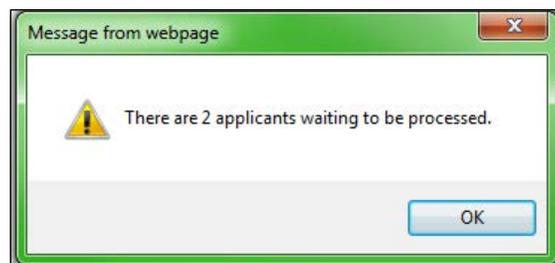


Figure 18: New Applicant Message

After CC/MSSP/CMs are logged in, they may process a new user's application by selecting **Applicant Processing** from the **System** menu, as depicted in Figure 19 below.

Note: **Applicant Processing** is only used to process applications submitted via the self-service registration screen. CC/MSSP/CMs may also initiate the creation of a new user account through the **User Processing** function, as discussed in the following sections.

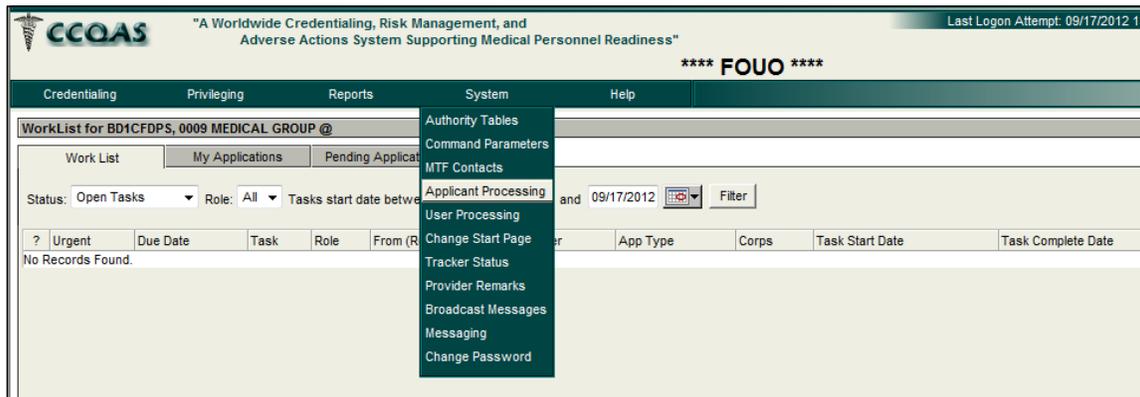


Figure 19: Applicant Processing Menu Item

CC/MSSP/CMs may open the new application record by selecting **Process** from the hidden menu of actions for the applicant's record, as depicted in Figure 20 below.



Figure 20: Applicant Processing Screen

The **User Application** displays, as depicted in Figure 21 below. The application contains the information submitted by the applicant. Any updates to the applicant's personal information may be made on the **User Application** screen. When all information is correct, click **Save**, and then click **Process** to set up the permissions for the applicant's new user account.

Figure 21: User Application Screen

When applicants select **Process**, they receive a message, as depicted in Figure 22 below. The message indicates that a new user's account has been added to CCQAS. Also, the user being added receives two (2) emails. One announces that his or her account has been created in CCQAS and contains the user's username. The username is typically the user's last name and first initial of his or her first name. The second email contains the user's password. The user needs both of these credentials and a valid CAC or PIV card to initially log in to the system.

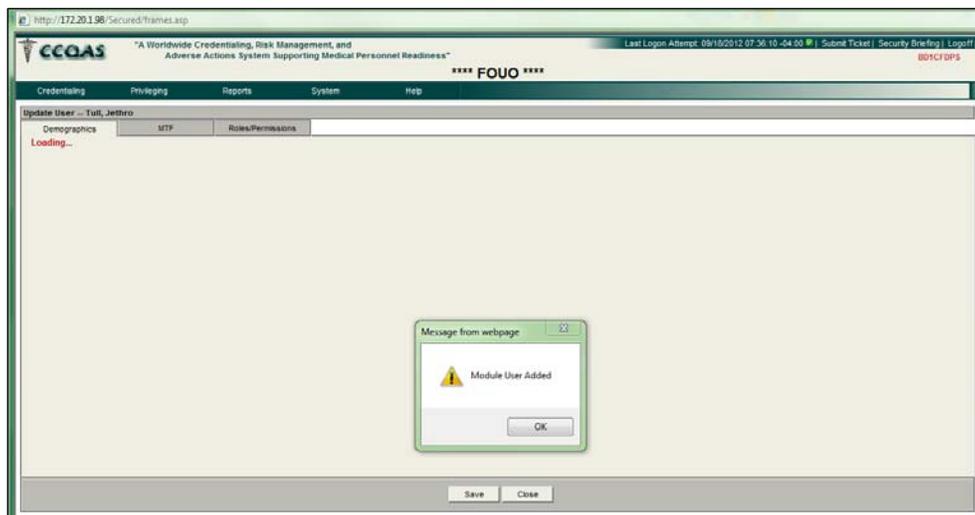


Figure 22: User Added Message

CC/MSSP/CMs should exercise care to ensure that multiple user accounts are not created for the same CCQAS user. When CC/MSSP/CMs select **Process**, CCQAS searches its database for an existing user account. CCQAS displays a **Similar User Account(s) Found** screen when it finds existing user accounts with a matching social security number (SSN) (for Provider accounts), or a combination of matching first and last name and date of birth (refer to Figure 42).

CC/MSSP/CMs should follow the instructions on the screen to either access the existing user account or continue to process the request for a new user account. CC/MSSP/CMs should avoid creating multiple user accounts for the same individual.

3.2.3 CC/MSSP/CM-Generated Applications

CC/MSSP/CMs may wish to create the CCQAS user account directly, without requiring the applicant to complete the online registration form. Using this method, CC/MSSP/CMs may create a new user account directly via the **User Processing** function, which is accessed through the **System** main menu. Figure 23 below depicts the selection of the **User Processing** menu item.

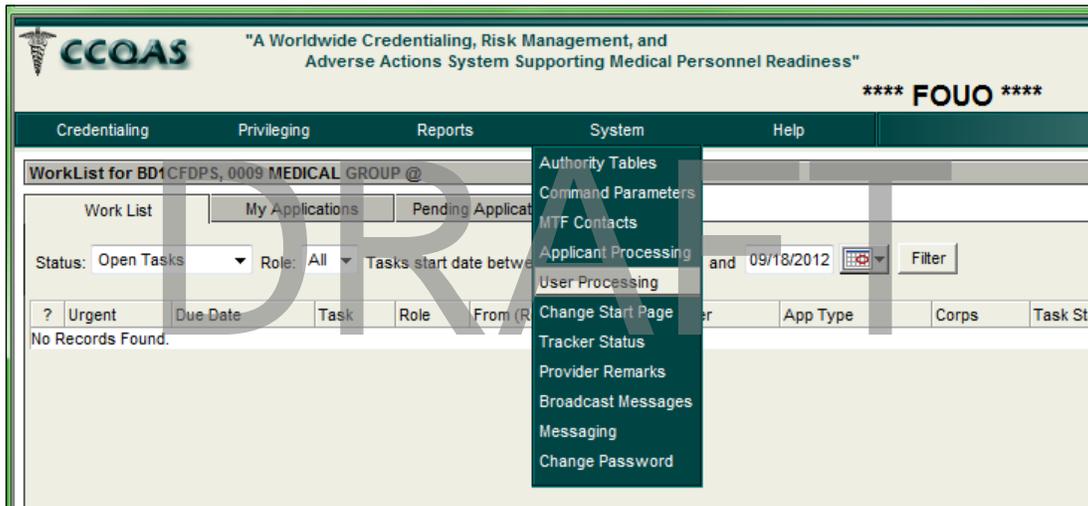


Figure 23: User Processing Menu Item

The **User Search** screen appears, as depicted in Figure 24 below. CC/MSSP/CMs may add a new user by clicking the **Add User** tab or the **Add User** button at the bottom of the screen.

Figure 24: User Search Screen

The **User Application** screen appears, as depicted in Figure 25 below. A CCQAS Administrator then completes the application on behalf of the applicant. As long as the CC/MSSP/CM has already validated the applicant's need to access CCQAS and the level of permissions required, the CCQAS Administrator may then initiate the creation of the new user account by clicking **Process**.

Figure 25: User Application Screen

Note: From this point forward, the application process is the same regardless of whether the applicant applied for the user account via the **Self-Service Registration** screen, or the user account was created by a CC/MSSP/CM through the **User Processing** screen.

Once again, CC/MSSP/CMs should exercise care to ensure that multiple user accounts are not created for the same CCQAS user. If CCQAS finds existing user accounts with a matching SSN (for Provider accounts), or a combination of matching first and last name and date of birth, it displays a **Similar User Account(s) Found** screen, as depicted in Figure 42.. CC/MSSP/CMs should follow the instructions on the screen to either access the existing user account or continue to process the request for a new user account. CC/MSSP/CMs should avoid creating multiple user accounts for the same individual.

3.2.4 User Accounts for New Provider Applicants

After a user has been added to CCQAS, his or her account is displayed on the **Update User** screen as a series of tabs, as depicted in Figure 26 below.

The first of the three tabs, the **Demographics** tab, may be used in the future to update the user’s personal information, lock and unlock the user’s account, and issue new passwords to the user as necessary. The user account displayed on the **Demographics** tab is an account for a Provider, as indicated by the “Provider User Only” text in red at the top of the tab.

The screenshot shows the 'Update User' screen for a provider applicant. The 'Demographics' tab is active, and the user's information is displayed. A red arrow points to the text 'Provider User Only' in red at the top of the tab. The user information includes: Last Name: Smith, First Name: William, Middle Name: (blank), Birth Date: 09/17/1980, Gender: Male, Phone: (215) 886-1234, Email: smith@email.com. The user account information includes: User ID: 0079623193, Password: (masked), and Account Locked: (checkbox). The user information section includes fields for Last Name, First Name, Middle Name, Birth Date, Gender, Phone, and Email. The supervisor information section includes fields for Last Name, First Name, Middle Name, Current Phone, Old Phone, Current Fax, and Old Fax. The user's position is listed as 'Credentialing Coordinator'.

Figure 26: 'Demographics' Tab for a Provider Applicant

Note: If the applicant is a “Provider Applicant,” no further action is needed. The creation of the user account has been completed. Providers will receive their username and password via two separate emails sent to the email address listed on the **Demographics** tab. Providers will also receive a third email notification, indicating the presence of an item in his or her work list with “**Task = Complete Application**”. The work list is discussed in detail in [Section 5](#). If the applicant is for a “Module User,” processing must be continued to designate the role and permissions that are assigned to the user’s account. This action is described in more detail in the next section.

The second of the three tabs, the **MTF** tab, provides two important pieces of information. The upper portion of the screen lists the UICs for the facilities and units where the user requires access to CCQAS as a “Module User.” The user depicted in Figure 27 below is a Provider applicant only, and therefore has no UICs listed in this section of the screen.

The UICs listed on the lower portion of the screen are the facilities and units where the user, in the role of a Provider, holds clinical privileges or where an application for clinical privileges is currently under review. The sample Provider in Figure 27 has one privilege application in progress at one UIC. This privilege application was created when the user was granted access to CCQAS as a “Provider Applicant.”

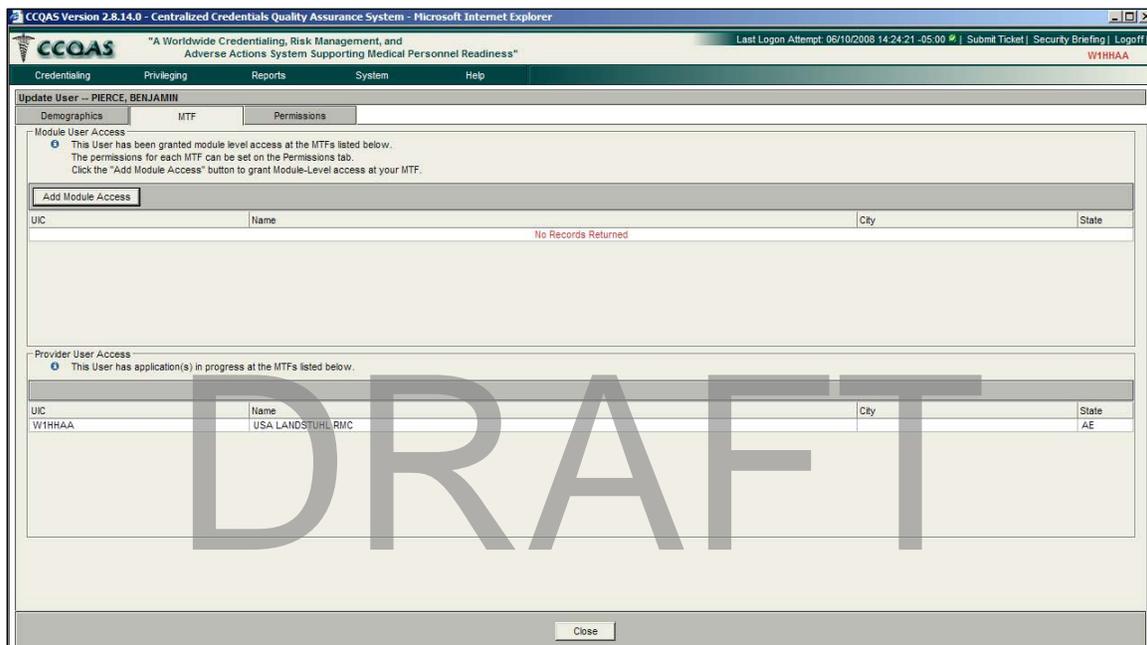


Figure 27: ‘MTF’ Tab for a Provider Applicant

The third tab, the **Permissions** tab, is where roles and permissions are assigned to a user’s account. The **Permissions** tab is depicted in Figure 28 below.



Figure 28: ‘Permissions’ Tab for a Provider Applicant

For “Provider Applicants,” no roles or permissions need to be configured for their user account. By processing the application as described above, a Provider is automatically granted the appropriate level of access needed to complete and submit applications for clinical privileges and

the Provider's 1st E-Application for clinical privileges is automatically generated (refer to [Section 5](#)). After privileges are created, additional roles as a "Module User" may be added to the Provider's user account. The process of adding roles to an existing account is discussed in [Section 3.3](#).

3.2.5 User Accounts for Module Users

The **Demographics** tab for "Module Users" is similar to that for "Provider Applicants," but also includes an indication of the CCQAS modules to which the user has access. The user account displayed on the **Demographics** tab in Figure 29 below is an account for a user who requested access to the "Credentialing" and "Privileging" modules in CCQAS.

Figure 29: 'Demographics' Tab for an Other (Module Users)

The upper portion of the **MTF** tab lists the UIC where the "Module User" was granted access to CCQAS, as depicted in Figure 30 below. This record was automatically created by CCQAS when the sample user was granted access to CCQAS. If the user has access to CCQAS at more than one facility or unit, multiple UICs are displayed here.

The lower portion of the screen reflects the facilities or units where the user, in the role of a Provider, holds current clinical privileges or where an application for clinical privileges is currently under review. The sample Provider depicted in Figure 30 has access as a "Module User" at UIC BD1CFDPS and no active privilege applications anywhere in CCQAS.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/18/2012 15:25:28 -04:00 Submit Ticket | Security Briefing | Logout
**** FOUO **** BD1CFDPS

Credentialing Privileging Reports System Help

Update User -- Tull, Jethro

Demographics MTF Roles/Permissions

Module User Access
 This User has been granted module level access at the MTFs listed below.
 The permissions for each MTF can be set on the Permissions tab.
 Click the "Add Module Access" button to grant Module-Level access at your MTF.

Add Module Access

UIC	Name	City	State
BD1CFDPS	0009 MEDICAL GROUP @	BEALE AFB	CA

Provider User Access
 This User has application(s) in progress at the MTFs listed below.

UIC	Name	City	State
No Records Returned			

Close

Figure 30: 'MTF' Tab for a Module User

The individual permissions for "Module User" for each UIC are assigned on the **Roles/Permissions** tab, as depicted in Figure 31 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/19/2012 10:22:38 -04:00 Submit Ticket | Security Briefing | Logout
**** FOUO **** BD1CFDPS

Credentialing Privileging Reports System Help

Update User -- Tull, Jethro

Demographics MTF Roles/Permissions

*** This is the MTF for these specified Permissions *** BD1CFDPS

	Privileging	Risk Management	Adverse Actions	System Admin	Reporting
Privileging Module	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
PAC	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
PAC Supervisor	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
CVO	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
CVO Supervisor	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
Reviewer	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
Privileging Authority	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
PAR Evaluator	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
PAR Reviewer	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
CLP Administrator	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes
State License Waiver Endorser	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Yes

Note: Permissions are cumulative.
 INSERT includes UPDATE and READ
 DELETE includes INSERT, UPDATE, and READ

Save Close

Figure 31: Privileging Roles/Permissions for a Module User

Each user is granted a specific set of roles/permissions based on his or her role in the privileging process. The CCQAS privileging module defines nine (9) unique roles to which are attached a pre-defined set of permissions for the Privileging module:

- **Professional Affairs Coordinators (PACs)** (also known as CC/MSSP/CMs):
Professional Affairs office staff who are responsible for ensuring Providers' credentials

are in order, for tracking and managing the review and approval of an application for clinical privileges, and for managing CCQAS user accounts for their facility or unit

- **PAC Supervisors:** CC/MSSP/CM staff members who are responsible for overseeing and managing the privileging workload assigned to credentials staff members within a UIC
- **CVOs:** CVO staff members or other credentialing personnel who perform the PSV of Provider credentialing data. The PSV function may also be performed by individuals who are assigned the CC/MSSP/CM role
- **CVO Supervisors:** CVO staff members who are responsible for overseeing and managing the workload assigned to CVO staff members
- **Reviewers:** Clinical staff privileging committee members who have been assigned the responsibility for reviewing and recommending actions on applications for privileges. Reviewers may include the Provider’s supervisor, the specialty, service or section chief, the department chair, and/or the members and chair of the executive committee of the medical or dental staff (i.e., Executive Committee of the Medical Staff, Executive Committee of the Dental Staff [ECOMS/ECODS])
- **PAs:** Usually MTF commanders or other designated personnel who are responsible for final approval of applications for clinical privileges
- **Common Language Privileging (CLP) Administrators:** The individual(s) who has or have been assigned responsibility for managing the privilege catalog at their unit or facility. Depending on the size of the MTF or other determining factors, this role may also be played by CC/MSSP/CMs. The privilege catalog is based on Common Language Privileging, hence the abbreviation “CLP”
- **PAR Evaluators:** Supervisors, service chiefs, department chairs or other clinical personnel who are responsible for completing and submitting a PAR on a Provider
- **PAR Reviewers:** Clinical staff members who are responsible for reviewing a PAR submitted by a PAR Evaluator

The Credentials, Privileging, System Administrator, and Reporting sections of User Processing are defined by the aforementioned roles. To view the permissions for each role, select the role by clicking it, as depicted in Figure 32 below. A screen appears and displays the Read-Only permissions for that particular role selected (refer to Figure 33 below). When users select the **Close** button at the bottom of the screen, the role permissions screen closes and returns them to the **Role** screen. When users select the binary value of “Yes” or “No” for the role, the permissions within that role are set.

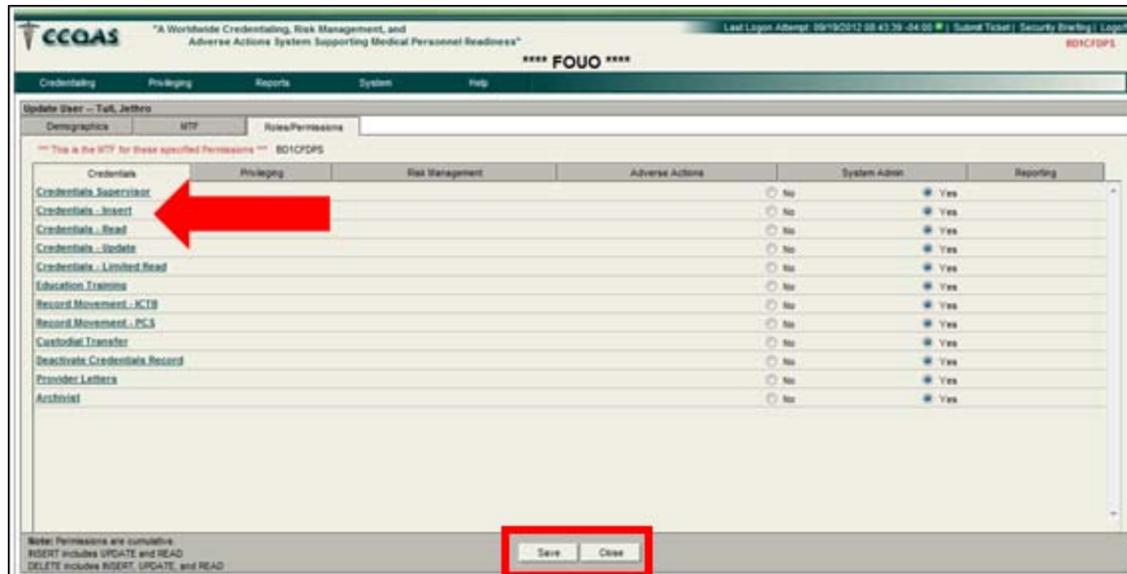


Figure 32: Credentials Roles

All roles and permissions default to “No” or “None”, so that action must be taken only on those that should be granted to the user. With the exception of the “CC/MSSP/CM” and “CVO” roles, most users only require access to the Privileging module, and the roles may be set when users select the appropriate radio buttons for each role they intend to perform. Users may save the roles to the user account by clicking **Save**, and then clicking **Close** to complete the processing of the application.

Individuals who perform the “CC/MSSP/CM” and “CVO” roles typically require access to multiple modules to include Privileging, Credentialing, System Administration, and Reporting modules. Access to these other modules may be granted by designating tab- and screen-level permissions for the other modules listed on the **Permissions** tab.

The **Credentials** tab contains the most extensive list of roles/permissions (refer to Figure 32 and Figure 33), which determines the extent to which the account holder can view, edit, delete, or transact Provider credentials records or the information contained therein. The levels for the permissions within each role are cumulative going from left to right across the screen. For example, if a user is given “Insert” permissions for “Specialty,” he or she can view the **Specialty** section of the Provider credentials record, “Update” information contained therein, and “Insert” new specialty records, if appropriate. The account holder, however, cannot “Delete” any specialty records contained in the **Specialty** section of any credentials record. Figure 33 below depicts the **Specialty** section of a Provider credentials record.

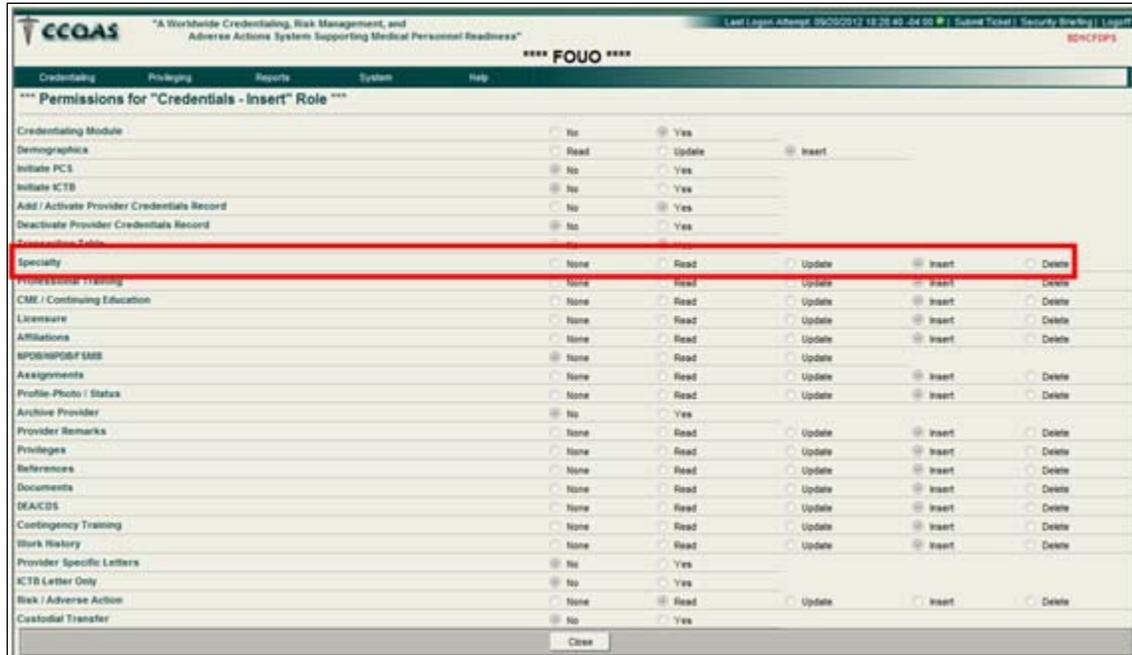


Figure 33: Credentials Insert Permissions

The **Privileging** tab contains permissions that determine whether account holders may view and process electronic applications (i.e., e-Apps) for Providers. This tab determines the role users have in the e-App process, as defined earlier in this section. Users may have multiple roles in the e-App process (e.g., PAC, Reviewer) depending on what permissions are set for them. Figure 34 depicts the privileging roles for a sample user.

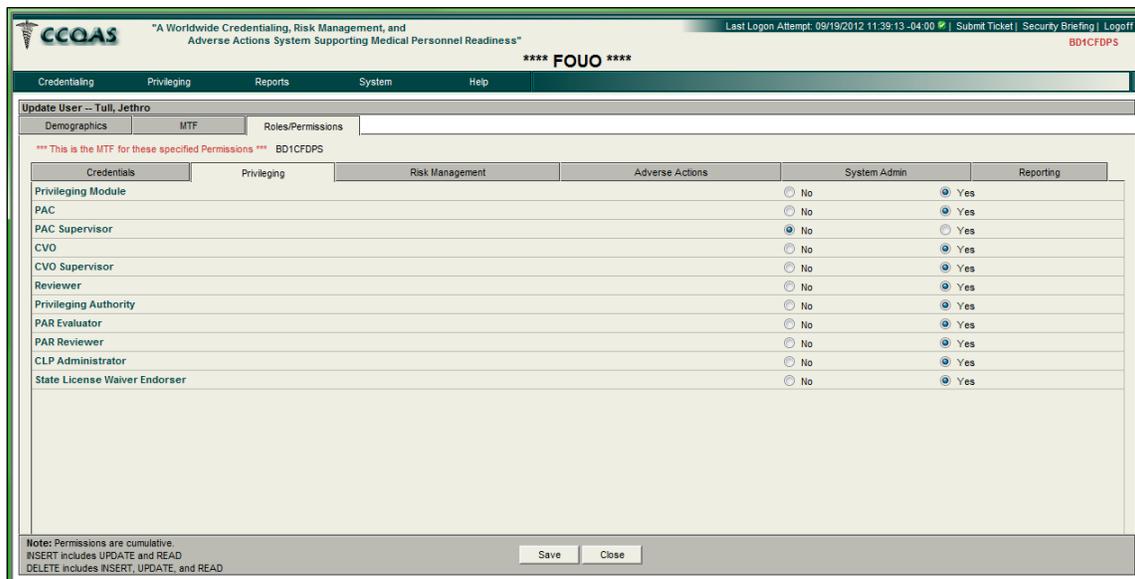


Figure 34: Privileging Roles

The **Risk Management** tab contains permissions that determine whether account holders may process Risk Management incidents, Navy Jagman claims, Air Force Potential Compensable Events (PCEs), Risk Management claims, and Disability claims. In many of these sub-categories within Risk Management, not only is it possible to set the user's general access to the sub-categories, but the level of access for each area in the sub-category can also be defined. In Figure 35 below, the sample user has permissions to the PCE module and can read, update, and insert data in all sections of a PCE, but cannot delete data.

Module	Read	Update	Insert	Delete
Transaction Log	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Classification	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Contact	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Checklist	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Financial	<input type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	<input checked="" type="radio"/> Delete
OTSG	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Delete	
Admin Tracker	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Claim Remarks	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Add RM Record	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Potential Compensable Event (PCE) Module				
PCE Management	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Overview	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	
Location	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Delete
Patient	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Delete
Provider	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Delete
PCE Assessment	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Delete
Attribution	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Delete
Outcome	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	

Figure 35: Risk Management Permissions

The **Adverse Actions** tab, depicted in Figure 36 below, contains permissions that determine whether account holders may access, add, update, or remove adverse actions cases. Like the Risk Management module, administrative personnel are able to define the level of access given to a user for each area.

Module	Read	Update	Insert	Delete
Adverse Action Module	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Transaction Log	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Refueling	<input type="radio"/> No	<input checked="" type="radio"/> Yes		
Adverse Action Case	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input type="radio"/> Delete
Initial Action	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	<input type="radio"/> Delete
Investigation	<input type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	<input checked="" type="radio"/> Insert
UC&J	<input type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	<input checked="" type="radio"/> Insert
Professional Review	<input type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	<input checked="" type="radio"/> Insert
PA Decision	<input type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	<input checked="" type="radio"/> Delete
Appeal	<input type="radio"/> None	<input type="radio"/> Read	<input checked="" type="radio"/> Update	
Regional Review	<input checked="" type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	
OTSG Review	<input type="radio"/> None	<input type="radio"/> Read	<input type="radio"/> Update	<input checked="" type="radio"/> Delete
Decision Summary	<input type="radio"/> None	<input checked="" type="radio"/> Read		

Figure 36: Adverse Actions Permissions

The **System Admin** tab, depicted in Figure 37 below, contains permissions that determine whether account holders may process new user accounts, access the Command Parameters and MTF Contacts, , and set other permissions associated with the management of the credentialing process at the facility or unit. Most permissions listed on this tab are binary, meaning a “Yes” assignment provides account holders with full permission to view, edit, or delete information associated with these screens or functions. If “No” is assigned, the account holder does not have access to the screen or its functionality.

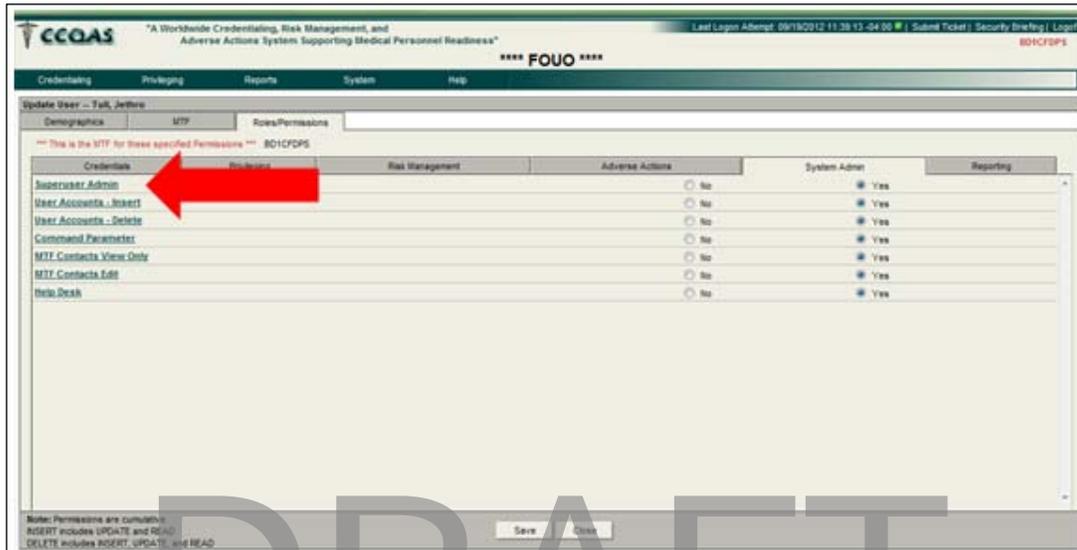


Figure 37: System Admin Permissions

Note: The binary role “Superuser Admin” is located on the **System Admin** tab, which controls additional role-based permissions. When users select “Yes” for this role, these permissions are set but are not seen on this tab. To view these permissions, click **Superuser Admin**. A “read-only” screen appears with a list of permissions specific to the “Superuser” role. Click **Close** to return to the **System Admin** tab. The “Batch NPDB Request Flag” permission should be enabled so that the sample account holder, depicted in Figure 38 below, can perform batch National Practitioner Data Bank (NPDB) queries.

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/19/2012 16:11:45 -04:00 Submit Ticket Security Briefing Logout **** FOUO **** B01CFDPS

Credentialing Privileging Reports System Help

*** Permissions for "Superuser Admin" Role ***

Function	None	Read	Update	Insert	Delete
User Accounts	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
User Roles/Permissions	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Command Parameters Maintenance	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MTF Contacts	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tracker Status Lookup	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provider Remarks Lookup	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Batch NPDB Request Flag	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Password Unlock	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Password Reset	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Close

Figure 38: "Superuser Admin" Role Permissions

The **Reporting** tab, depicted in Figure 39 below, contains permissions that allow account holders to access the standard and ad hoc reporting functions and the letter-generation capabilities for each CCQAS module, as well as the NPDB query function. Like the **System Admin** tab, the permissions listed on this tab are binary, which provides account holders with either no access, or full access to the indicated function.

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/19/2012 11:39:17 -04:00 Submit Ticket Security Briefing Logout **** FOUO **** B01CFDPS

Credentialing Privileging Reports System Help

Update User - Tuill, Jethro

Demographics MTF Roles/Permissions

*** This is the MTF for these specified Permissions *** B01CFDPS

Role	No	Yes	System Admin	Reporting
Superuser	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Standard Privileging User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Standard Credentials Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Ad Hoc Credentials Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Standard Risk Management Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
RM Letters User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Ad Hoc Risk Management Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Standard Adverse Actions Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Ad Hoc Adverse Actions Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
DoD Report User	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
NPDB Query	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Note: Permissions are cumulative.
INSERT includes UPDATE and READ
DELETE includes INSERT, UPDATE, and READ

Save Close

Figure 39: Reporting Permissions

Note: The binary role "Superuser" is located on the **Reporting** tab, which controls additional role-based permissions. When users select "Yes" for this role, these permissions are set but are not seen on this tab. To view these permissions, click **Superuser**. A "read-only" screen appears

with a list of permissions specific to the Superuser role. Click **Close** to return to the **Reporting** tab, as depicted in Figure 40 below.



Figure 40: “Superuser” Role Permissions

The **User Management** function within CCQAS allows anyone who has permissions to grant other users permission(s) up to what the “grantor” already holds. Permission to access the Reporting module (refer to Figure 39 above), for example, cannot be granted by CC/MSSP/CMs or CVOs who do not themselves have permission to access this module. CC/MSSP/CMs who have been assigned the responsibility of processing CCQAS user accounts are able to assign roles on the **Privileging** tab that they themselves are not assigned. For example, CC/MSSP/CMs may assign the role of “Reviewer” to one of their department heads, without having the role of “Reviewer” assigned to their own user account. CC/MSSP/CMs’ ability to grant permissions to the **Credentialing** and other CCQAS modules, however, is limited to only those permissions that they hold. CCQAS does not allow CC/MSSP/CMs to grant to others permissions in these modules that are more expansive than their own.

Finally, all permissions are UIC-specific, so that an account holder may have different roles or permissions at different facilities, depending on his or her job responsibilities at each location. The permissions for each UIC must be assigned by UIC personnel. For example, if COL Smith functions as a Reviewer at Brooke Army Medical Center (BAMC), and a Reviewer and PAR Evaluator at William Beaumont Army Medical Center (WBAMC), the CC at BAMC can only assign the “Reviewer” role to COL Smith for the BAMC UIC. The CC at WBAMC has to assign the roles of “Reviewer” and “PAR Evaluator” to COL Smith for the WBAMC UIC. Service-level personnel and some selected facility personnel, however, do have the ability to assign roles and permissions across all UICs. Users should consult with their supervisor if questions arise concerning the granting of roles and permissions at multiple locations.

3.2.6 Generating User Accounts from Existing Provider Credentials Records

CCQAS allows CC/MSSP/CMs to generate a user account for Providers who already have an active credentials record in the CCQAS database. This is the preferred method for creating new user accounts for Providers as CCQAS 2.10.0.0 is being implemented at the facility or unit. The new user account for the Provider, however, should only be created close to the time when the Provider is due for re-privileging, to ensure that his or her privilege application contains the most current credentials information.

To initiate this process, CC/MSSP/CMs perform a search for the Provider's record in the Credentialing module, as depicted in Figure 41 below. On the **Search Results** tab, click the hidden menu of actions for the Provider's credentials record, and then select **Grant Provider Access**.



Figure 41: Grant Provider Access Menu Item

Note: The **Grant Provider Access** option can also be used for Providers who have access to CCQAS as a “Module User” but whose user account has not yet been linked to an existing credentials record. If the user account for the “Module User” was linked to the individual’s credentials record at the time the “Module User” account was created, the user already has access to CCQAS as a Provider, but no privilege application has yet been generated for the Provider to complete. CC/MSSP/CMs may use the **Initiate Application** menu item to generate the 1st E-application for a Provider. This is located in the **Work History** section on the **Assignments** tab, which is discussed in [Section 5](#) of this guide.

If a Provider’s credentials record has not yet been linked to a user account, CCQAS uses the information inside the Provider’s credentials record to create the new user account, and redirects CC/MSSP/CMs to the **Roles/Permissions** tab of **User Processing**. CC/MSSP/CMs may then proceed with processing the user account.

The **Grant Provider Access** function has several important features:

- This function only associates the “Provider” role with the user account; it cannot be used to grant other roles such as “Reviewer” or “Privileging Authority” to the individual
- This function may only be performed once. The menu item disappears after an active credentials record has been associated with a user account
- The Provider’s 1st E-Application for clinical privileges automatically generates. This application pre-populates with the credentials data from his or her current credentials record at the time the menu option was selected

After privileges are created, additional roles as a Privileging module user may be added to the Provider’s user account. The process of adding roles to existing user accounts is addressed in [Section 3.3](#).

3.3 Adding Roles to Existing User Accounts

This section describes the process of adding roles to existing user accounts.

3.3.1 Adding the Provider Role to an Existing “Module User” Account

In most cases, individuals who use the Privileging module, such as Reviewers, the PA, and PAR Evaluators, are also Providers. If an individual initially applies for a user account as a “Privileging” module user, he or she likely requires the role of “Provider” added to the individual’s user account at some later time when his or her privileges need to be renewed.

Note: The role of “Provider” should not be added to the user’s account until the Provider is due to fill out a 1st E-Application for privileges in CCQAS either to renew current privileges or apply for privileges at another facility or unit for a PCS.

The addition of the “Provider” role may be initiated in one of several ways:

- If a Provider already has an active credentials record in CCQAS, CC/MSSP/CMs may use the **Grant Provider Access** function in the Credentialing module (refer to [Section 3.2.6](#)). If **Grant Provider Access** is not available from the menu of actions, it means the Provider’s credentials record has already been linked with a user account
- The Provider may re-register for a user account and specify “**Type = Provider Applicant**” on the registration form. CC/MSSP/CMs may then begin processing the request via the **Applicant Processing** function (refer to [Section 3.2.2](#))
- CC/MSSP/CMs may initiate the process of adding a new user via the **User Processing** function, and specify “**Type = Provider Applicant**” on the “User Application” screen (refer to [Section 3.2.3](#))

Regardless of whether users or CC/MSSP/CMs initiate the creation of a user account, after the processing begins, CCQAS checks against the existing user accounts to determine if an individual with the same name and birth date is already a CCQAS user. If a match is found, CCQAS enables CC/MSSP/CMs to link the registration form with the existing user’s account via the **Similar User Account(s) Found** screen, as depicted in Figure 42 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Similar User Account(s) Found

The following is a list of User Account(s) already on file that are potential matches to the person you are adding. A potential match means that the existing record and the one being added have the same last name, first name, first initial, and date of birth. If the person you are trying to add matches a record below, double click the record or click the **DETAILS** button. If the person you are adding does not match a record below, click on the "User Not Found" button to proceed with adding a new user account. To terminate the add process, click on the "Close" button. If you are adding a Provider Requesting Privileges, or you select a User Account that has an existing Credential record, the system will next check to see if you will be allowed to add a new Credential record at B01CFDPS. If a record has a User Status of "Inactive", you can reactivate the record by double clicking on the record or by clicking the arrow.

User ID	User Type	Name	Date of Birth	UIC(x)	Position	Email Address	Contact Phone	Provider?	Last Login Date
0009	Module	TuL, Jeffre	09/18/1966	B01CFDPS		EMAL@EMAL.COM	Home: (202) 555-7999	No	09/29/2012

User Not Found Close

Figure 42: Similar User Account(s) Screen

The registration form may be linked to the existing user account by clicking the small arrow to the left of the matching user's record. CCQAS opens the existing user account for the individual. The MTF tab in the user's account reflects the addition of the "Provider" role by displaying a record line on the bottom half of the screen, as depicted in Figure 43 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Update User -- TESTERMAN, TESTER

Demographics MTF Roles/Permissions

Module User Access

This User has been granted module level access at the MTFs listed below. The permissions for each MTF can be set on the Permissions tab. Click the "Add Module Access" button to grant Module-Level access at your MTF.

Add Module Access

UIC	Name	City	State
B01CFDPS	0009 MEDICAL GROUP @	BEALE AFB	CA

Provider User Access

This User has application(s) in progress at the MTFs listed below.

UIC	Name	City	State
B01CFDPS	0009 MEDICAL GROUP @	BEALE AFB	CA

Note: Permissions are cumulative. INSERT includes UPDATE and READ. DELETE includes INSERT, UPDATE, and READ.

Close

Figure 43: 'MTF' Tab for a Dual User's Account

The **Permissions** tab should continue to reflect the roles and permissions that were originally assigned to the user account. The addition of the “Provider” role does not alter any of the previously-assigned roles or permissions at the UIC. When the role of “Provider” is added to the user’s account, the 1st E-application is also generated for the Provider to request clinical privileges online using the CCQAS application.

Note: If the **Similar People Found** screen appears but none of the users listed on the screen matches the Provider who is being added to CCQAS, CC/MSSP/CMs may click **Close** to cancel the process, or click **Add New User** to proceed with the process of creating a new user account in CCQAS for the Provider.

3.3.2 Adding “Module User” Role to an Existing Provider Account

Depending on where they are in their privileging cycle when they become CCQAS users, some users may require access to CCQAS in the role of “Provider” first, and later need access as “Module User”. Users may initiate the process for adding one or more “Module User” roles to an existing Provider account by selecting **User Processing** from the **System** main menu. The **User Search** screen appears, as depicted in Figure 44 below. To locate an existing Provider’s user account, enter the Provider’s Last Name or other search criteria, and then select the radio button for **User Type = Provider Users**. Click **Search**.

The screenshot shows the CCQAS User Search interface. The header includes the CCQAS logo and navigation tabs for Credentiaing, Privileging, Reports, System, and Help. A large "DRAFT" watermark is overlaid on the screen. The main content area is titled "User Search" and contains several sections: "User Details" with a "Last Name" field containing "JONES" and a "UIC" field containing "804C00PS"; "User Type" with radio buttons for "Module Users", "Provider Users" (which is selected), and "Other"; and "Account Details" with checkboxes for "Expired Accounts", "Locked Accounts", "Intentionally Locked Accounts", and "Temporary Accounts". At the bottom, there is a "Record Count: 1" and a "Search" button highlighted with a red box.

Figure 44: User Search Screen

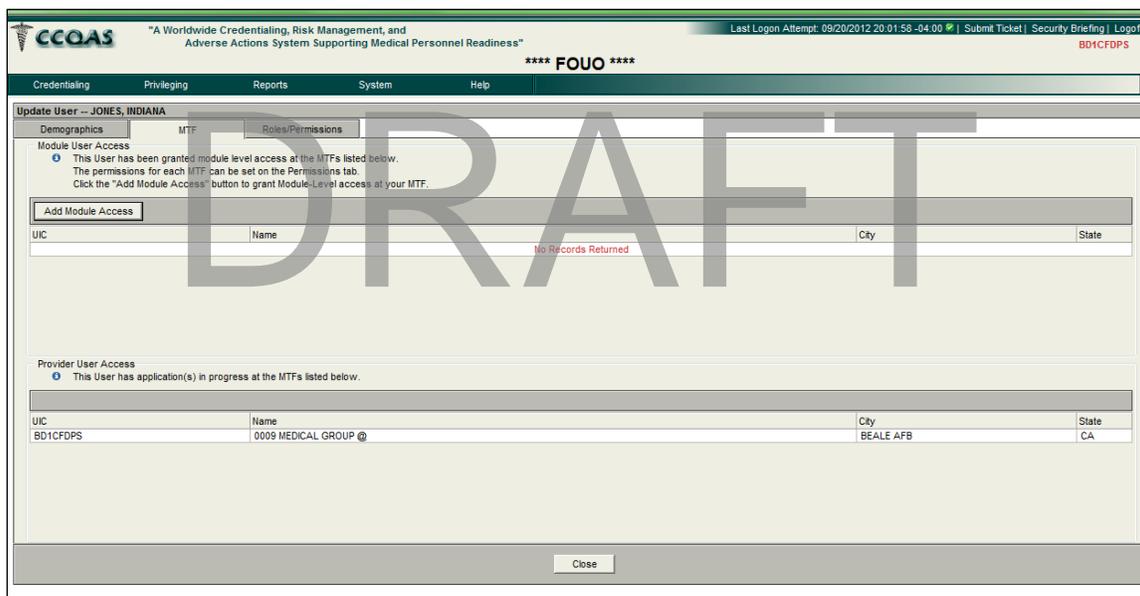
The **User Listing** screen appears, as depicted in Figure 45 below. This screen displays all existing user accounts at the facility or unit that meet the search criteria.



Name	User ID	Type	Primary UIC	Position	Primary Phone	Primary Email	Last Logon	Expiration	Temporary	Acct. Locked	Intent. Locked	Deactivated Date
JONES, INDIANA	JONES120120	Provider			(703) 555-7878	email@email.com		11/19/2012	Yes	No	No	

Figure 45: User Listing Screen after a Search

After the user account is opened, the process of adding the “Module User” role(s) is initiated on the **MTF** tab. Initially, the Provider’s user account has no UICs listed on the upper half of the screen, as depicted in Figure 46.



Update User -- JONES, INDIANA

Demographics | **MTF** | Roles/Permissions

Module User Access
 This User has been granted module level access at the MTFs listed below.
 The permissions for each MTF can be set on the Permissions tab.
 Click the "Add Module Access" button to grant Module-Level access at your MTF.

UIC	Name	City	State
No Records Returned			

Provider User Access
 This User has application(s) in progress at the MTFs listed below.

UIC	Name	City	State
BD1CFDPS	0009 MEDICAL GROUP @	BEALE AFB	CA

Figure 46: 'MTF' Tab for a Provider User Account

To grant the Provider access to the Privileging module, click **Add Module Access** at the top of the screen. This action automatically creates a UIC record in the upper portion of the screen, as depicted in Figure 47 below. This record indicates that *Module User* access has been added to the Provider's account.

The appropriate roles and permissions may then be assigned to the user on the **Roles/Permissions** tab. After the changes on the **Roles/Permissions** tab are saved, and the user's account is closed, the Provider will have access to CCQAS, with assigned roles and permissions associated with his or her user account.

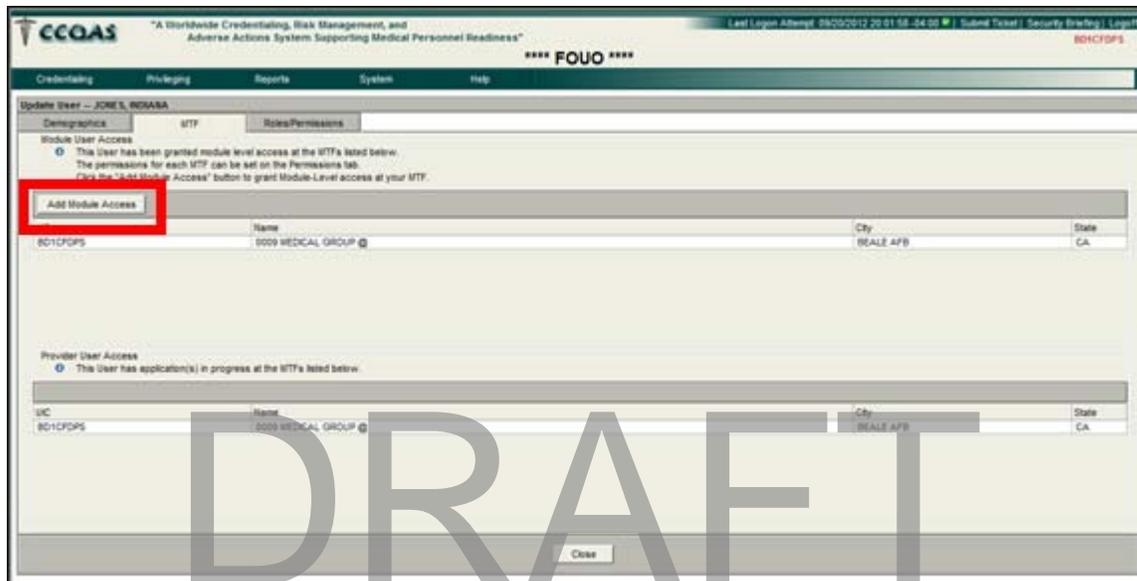


Figure 47: 'MTF' Tab for a Dual User's Account

3.4 Deactivating and Reactivating User Accounts

Under normal circumstances, CC/MSSP/CMs should not have to deactivate a user account while a user is still actively working within the MHS. After a user account has been associated with a Provider's credentials record, CCQAS should automatically transfer the user account to the gaining UIC, when a PCS or ICTB transaction is performed on the credentials record. Likewise, if the Provider's credentials record has been archived or PCS'ed to a non-privileging UIC, CCQAS should automatically deactivate the associated user account. DoD rules also require CCQAS to deactivate a user's account if 365 days lapse without the user logging in to the system. While this situation is unlikely to impact CCQAS module users, it is very likely to impact Providers who only access the system to renew clinical privileges at their current location or apply for clinical privileges at a new duty station.

Note: If CC/MSSP/CMs wish to restrict a user's access to CCQAS at the unit, the user account should NOT be deactivated, since this impairs the user's access to CCQAS at all locations. Instead, CC/MSSP/CMs should simply adjust or remove the user's permissions at his or her unit, to control the user's level of access to CCQAS.

Occasionally, however, it is appropriate for CCQAS administrators to deactivate a user account when the user has entered an inactive status, separated from military service, or terminated employment with the DoD. CCQAS administrators may deactivate a user account through the **User Processing** function, which is available from the **System** main menu. On the **User Listing** screen, select **Deactivate** from the menu of actions available for each record, as depicted in Figure 48 below.



Figure 48: Deactivate Menu Item

After a user account is deactivated in CCQAS, only users with permissions to reactivate user accounts may enable it again. Thus, prudent CC/MSSP/CMs must ensure it is appropriate to deactivate a user account before actually doing so. When CC/MSSP/CMs select **Deactivate**, they are asked to confirm the intent to deactivate the user account, as depicted in Figure 49 below.

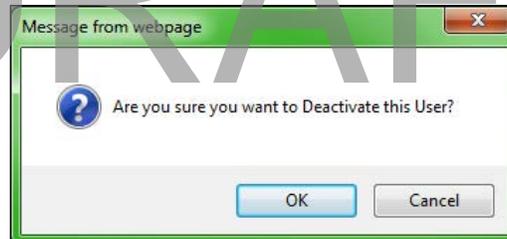


Figure 49: Deactivate User Confirmation Message

Authorized users may reactivate a deactivated user account at any time by selecting **Activate** from the menu of options for the account, as depicted in Figure 50 below.



Figure 50: Activate Menu Item

When authorized users select **Activate**, they are asked to confirm their intent to reactivate the user account, as depicted in Figure 51 below.

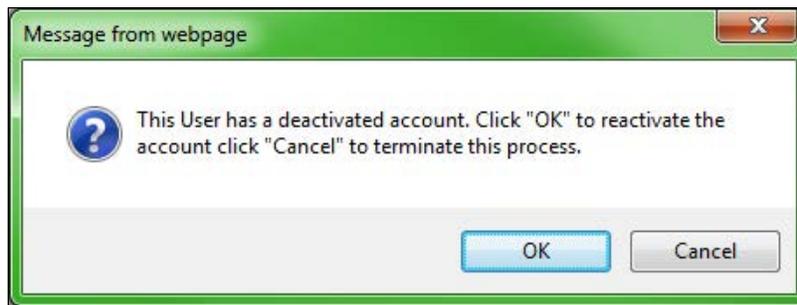


Figure 51: Activate User Confirmation Message

After the intent to reactivate the user account is confirmed, the **Update User** screen displays with a message, as depicted in Figure 52 below. The message indicates that an email was sent to the user which contains a new temporary password.

Since the new password will be sent to the primary email address in the user's account, it is prudent to confirm that the primary email account is still valid. If it is not, then CC/MSSP/CMs should update and save the new email address in the user account, and then click **Issue New Password**.

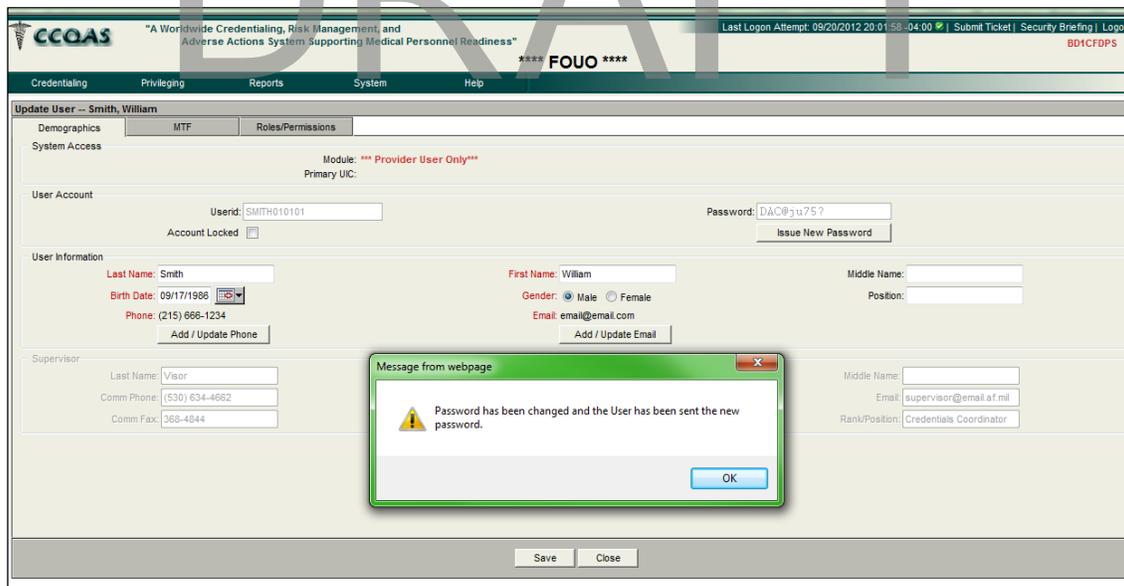


Figure 52: New Password Issued Message

After a user account has been reactivated, the user will begin to receive the automated email notifications and work list items consistent with roles and permissions assigned to the user account at each UIC where he or she has access to CCQAS. If the user is a Provider, then CCQAS does not automatically generate a new privileging application when the user account is

reactivated. CC/MSSP/CMs use the **Initiate Application** option, available from the hidden menu of actions on the Provider's credentials record, to generate a new application for the Provider to request clinical privileges.

3.5 Using CCQAS for the First Time

This section describes the process of using CCQAS for the first time.

3.5.1 Receiving a New Username and Temporary Password

After a new user account has been set up, CCQAS notifies the new user of his or her username and a temporary password via an automated email message. Passwords for CCQAS are automatically generated and consist of a random string of characters, numbers, and symbols that conform with DoD Information Systems security requirements as follows:

- Nine characters in length
- Contain at least one uppercase letter
- Contain at least one lower case letter
- Contain at least one number
- Contain at least one special character

The username and the password are both case-sensitive.

Note: Do not use the **Caps Lock** feature when entering the username and password.

The username and temporary password issued to a new user is valid for 60 days from the date the account was created. If the new user does not log in to the application at least once within this 60 day time period, the CCQAS-issued password will be deactivated and the user will have to request a new password from the CC/MSSP/CM.

3.5.2 Accessing CCQAS for the First Time

Before users access CCQAS for the first time, they need to ensure they have a valid CAC or PIV card. This card is required to authenticate users both on the DoD secured network and in the application. CCQAS does not allow access without a valid CAC or PIV card.

A number of actions are required the first time users access CCQAS, which include the following:

- Loading security certificates
- Reviewing and acknowledging the security briefing
- Changing the temporary password
- Verifying user roles and permissions

Optional actions that help users streamline their access to the CCQAS include the following:

- Creating a desktop icon for CCQAS
- Changing the start page

Each of these actions is described in the sections below.

3.5.2.1 Loading Security Certificates

Certain rules pertaining to security have to be adhered to when accessing an automated information system within the DoD network. When accessing CCQAS for the first time, network protocols may present first-time users with a message requiring security certificates to be loaded into their computer to protect data that is sent across the Internet. Users will receive another link for instructions and a wizard function for these certificates, which must be downloaded and retained in their computer's hard drive prior to using CCQAS.

3.5.2.2 Logging in to CCQAS

To log in to CCQAS, users must insert a valid CAC or PIV card in the card reader of their computer. The card reader can be built-in or an external Universal Serial Bus (USB) reader. When users enter the CCQAS URL, <https://ccqas.csd.disa.mil>, the **CCQAS Privacy Act Statement** screen appears, as depicted in Figure 53 below. Users select the **Affirmative** radio button after they have read the statement. CCQAS does not allow access to the system without users selecting the **Affirmative** radio button. Users are then directed to the **DoD Network Authentication** screen, where the electronic credentials from their CAC or PIV card is authenticated.

**** FOUO ****	
	
Privacy Act Statement	
Before proceeding into the CCQAS registration window, users must acknowledge that they are aware of the Privacy Act Statement associated with using this system.	
1102 PROTECTED STATUS	
CCQAS includes Sensitive but Unclassified (SBU) information that is subject to the Privacy Act of 1974, as amended. Consequently, copying, printing, or distributing data from CCQAS to support administrative functions is authorized by, and subject to the limitations of, DoD Regulation 5400.11-R, Department of Defense Privacy Program. Certain information contained within CCQAS is accessible under the Freedom of Information Act. The use and disclosure of some information in CCQAS is protected from legal discovery under 10 U.S.C. 1102. No other distribution is permitted without the express written permission of the TriCare Management Activity Functional Proponent or Service CCQAS Representatives, who will coordinate with appropriate legal counsel prior to rendering an opinion regarding release of information.	
PRIVACY ACT STATEMENT	
This statement serves to inform you of the purpose for collecting personal information required by the Centralized Credentials Quality Assurance System (CCQAS) and how it will be used.	
AUTHORITY: 10 U.S.C. 1102, Confidentiality of medical quality assurance records; qualified immunity for participants; 42 U.S.C. Chapter 117, Encouraging good faith professional review activities; DoD Instruction 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); DoD Regulation 6025.13-R, Military Health System (MHS) Clinical Quality Assurance (CQA) Program Regulation; and E.O. 9397 (SSI), as amended.	
PURPOSE: To obtain information necessary to credential a health care provider and determine whether that individual should have privileges to work, or continue working, in a military treatment facility (MTF) or otherwise within the Military Health System (MHS), including information on malpractice claims and adverse privilege actions. Information is also collected to report malpractice claims or adverse privilege actions filed against a health care provider in connection with a service performed at an MTF or within the MHS.	
ROUTINE USES: Information collected may be used and disclosed generally as permitted under 45 CFR Parts 160 and 164, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, as implemented by DoD 6025.18-R, the DoD Health Information Privacy Regulation. Information may be used and disclosed in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD "Blanket Routine Uses" published at: http://dpcbc.defense.gov/privacy/SORNs/blanket_routine_uses.html . Collected information may be shared with government boards, agencies, professional societies, or organizations if needed to license or monitor professional standards of health care practitioners. It may be released to civilian medical institutions or organizations where the practitioner is applying for staff privileges, or already privileged, regardless of whether the practitioner is still privileged at an MTF. Information may also be used to conduct trend analysis for medical quality assurance programs.	
DISCLOSURE: Voluntary. However, failure to provide information may result in an individual's ineligibility to serve at an MTF or within the MHS.	
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT WARNING	
This system contains protected health information as defined in the Health Information Portability and Accountability Act of 1996 (HIPAA) and the HIPAA Privacy Rule (45 CFR Parts 160 and 164). DoD's implementation of the HIPAA Privacy Rule is in DoD 6025.18-R, DoD Health Information Privacy Regulation. The HIPAA Privacy Rule and DoD 6025.18-R apply to protected health information and may place additional procedural requirements on uses and disclosures of such information beyond those found in the Privacy Act or mentioned elsewhere in this notice. This information may only be used and/or disclosed in strict conformance with that authority. The MHS is required to, and will, appropriately sanction individuals who fail to comply with its privacy policies and procedures.	
<input checked="" type="radio"/> Yes, I understand the contents of the above Privacy Act Statement. <input type="radio"/> No, I do not understand the contents of the above Privacy Act Statement.	
**** FOUO ****	

Figure 53: CCQAS Privacy Act Statement

After users are authenticated on to the network, they enter their username and password in the appropriate fields on the **Login** screen, as depicted in Figure 54 below, and then click **Login**. Both the username and password for CCQAS are *case sensitive*. Press the **[Shift]** key, rather than the **[Caps Lock]** key. The username is always upper case.

**** FOUO ****

CCQAS "A Worldwide Credentialing, Privileging, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness"

Log-On

Enter your user name and password to login. Please note that user name and password **ARE** case-sensitive.

User Name:

Password:

For Additional Assistance

Please address all questions regarding CCQAS to include System Security, System Operation, Training, Functional and Technical issues, System Errors, Userid and Passwords, Access Issues and Recommendations to the MHS Help Desk, phone: 1-800-600-9332 (CONUS).

**** FOUO ****

Figure 54: Login Screen

If users unsuccessfully attempt to log in more than twice, they receive a message that their account has been locked, as depicted in Figure 55 below. Users must contact their CC/MSSP/CM or the CCQAS Helpdesk to have their account unlocked before proceeding.

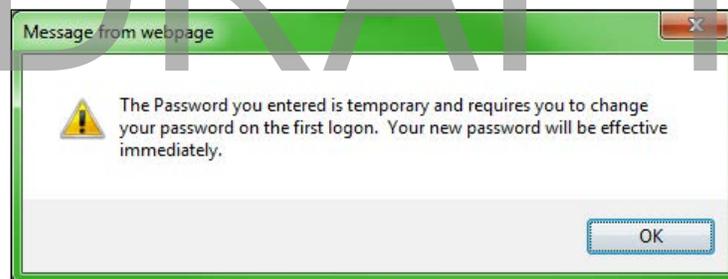


Figure 55: Temporary Password Alert

3.5.2.3 Changing a Temporary Password

After users log in for the first time, they are prompted to change their temporary password, as depicted in Figure 56 below. The username remains unchanged, and CCQAS randomly generates a new password. Users click the **I like this password** button if the password is acceptable; otherwise, the system generates a new one every time users click the **I do not like this password** button.

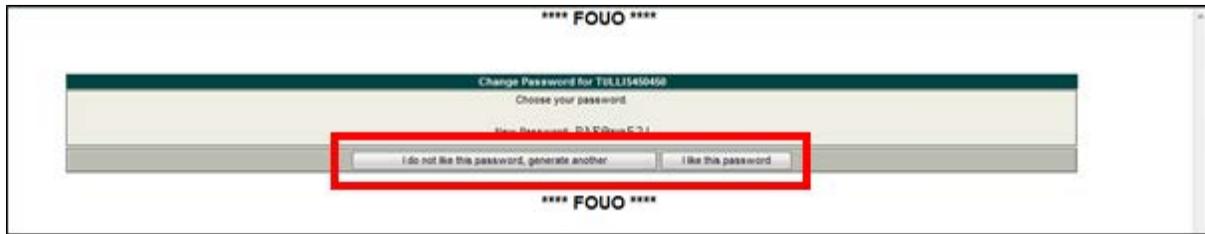


Figure 56: Random Password Generator Screen

After users successfully log in to the system for the first time, their Electronic Data Identifying Person Number (EDIPN) from their CAC or PIV card is linked to their account in the database. From this point, they only need to have their CAC or PIV card for access, eliminating the need for a username and password.

3.5.2.4 Security Briefing

After users log in, they are presented with a security briefing, as depicted in Figure 57 below. Users must read the briefing and acknowledge their understanding of the information it contains by selecting the appropriate radio button at the bottom of the briefing, and then clicking **Submit**. This action completes the login process.

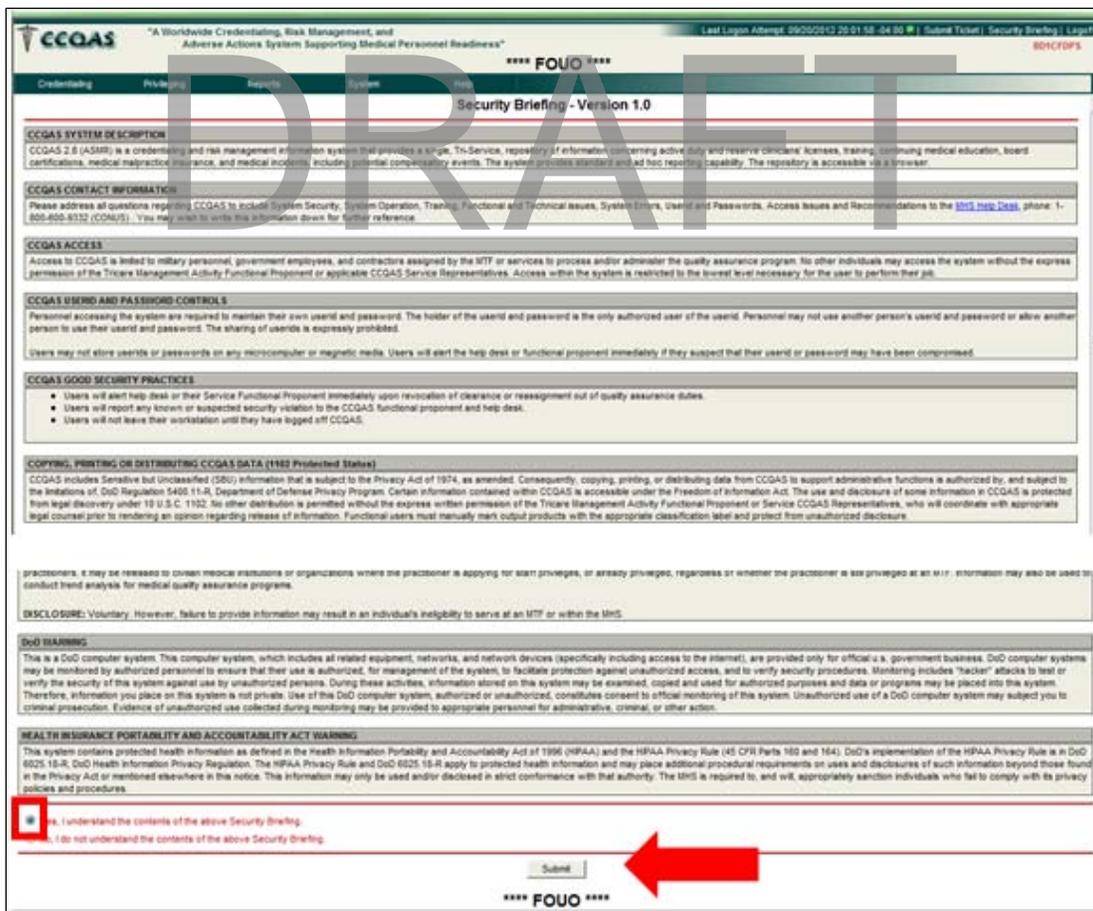


Figure 57: Security Briefing

3.6 Maintaining CCQAS User Accounts

This section describes the process for maintaining CCQAS user accounts.

3.6.1 Updating User Personal and Contact Information

CCQAS users should make updates to demographic and contact information as soon as possible after changes occur. Reviewers and other Privileging module users should be encouraged to update their own information through the **User Profile** feature in CCQAS, which account holders may access directly through their **System** main menu, as depicted in Figure 58 below.

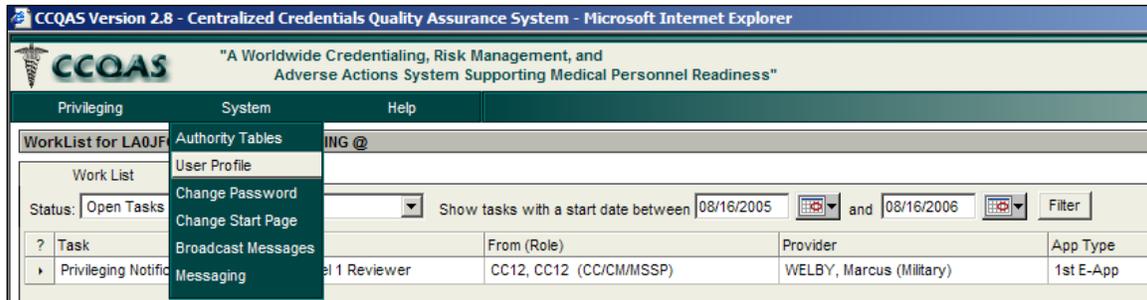


Figure 58: User Profile Menu Item for a Module User

The first tab from the user account, the **Demographics** tab, displays, as depicted in Figure 59 below.

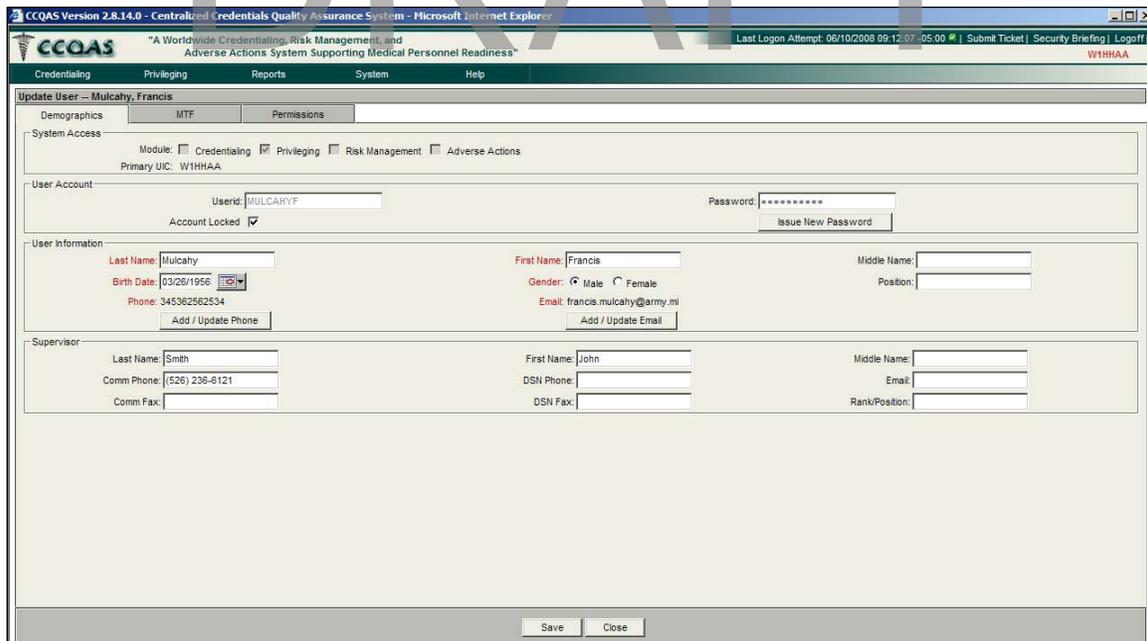


Figure 59: Update User Screen for Other (Module Users)

Users may add or update their own contact information or that of their supervisor. After the changes are saved, the account holder's information is updated in CCQAS.

Note: Users with “Provider” access only in CCQAS do not have access to the **System** main menu; therefore, they cannot access the **User Profile** functionality. Providers should update their contact information when they submit their next privilege application. If their contact information changes between privileging cycles, they should contact the credentials office directly to have updates made to their user account.

CC/MSSP/CMs may also update demographic and contact information for any user in their facility or unit through the **User Processing** function, as depicted in Figure 60 below.

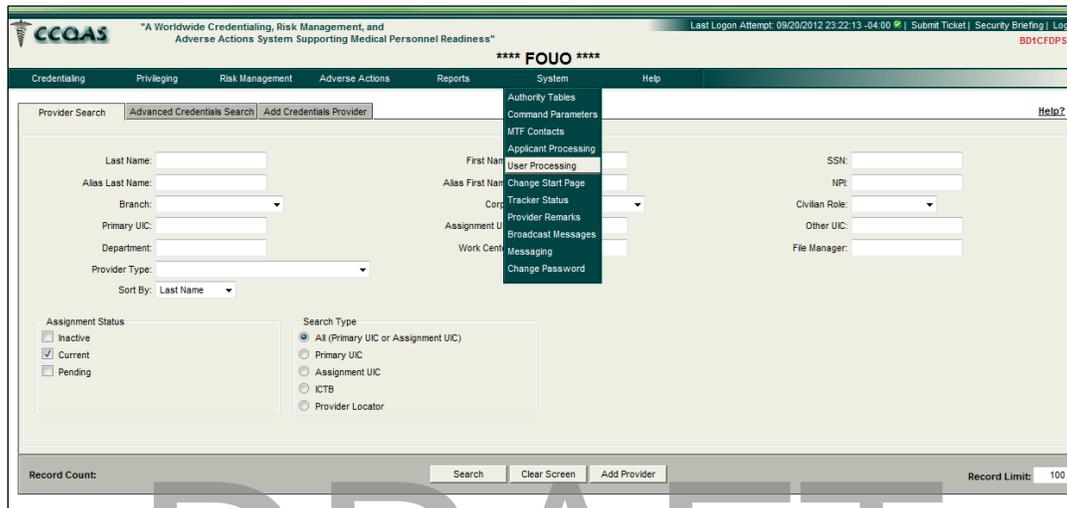


Figure 60: User Processing Menu Item

When CC/MSSP/CMs select **User Processing**, the **User Search** screen appears, as depicted in Figure 61 below.

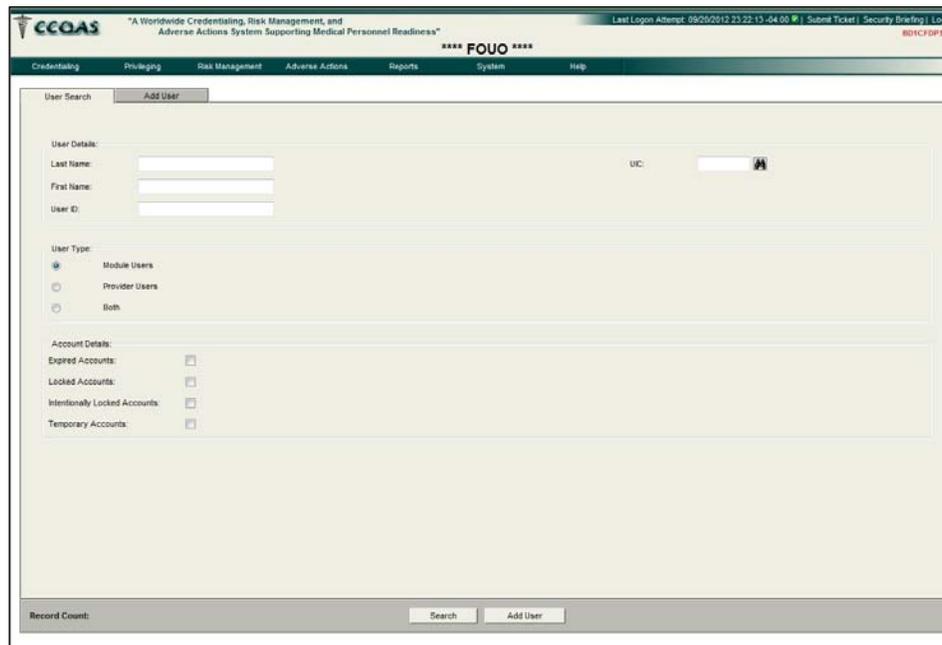


Figure 61: User Search Screen

CC/MSSP/CMs have the ability to search for their own record and update personal information on the **Demographics** tab. CC/MSSP/CMs may also use this screen to search for a desired account holder's record. When CC/MSSP/CMs locate and open the desired user account, the **Update User** screen appears, displaying the **Demographics** tab. The user's contact and supervisor information may then be updated, as appropriate. When CC/MSSP/CMs click **Save**, the changes are updated immediately in the CCQAS database. Changes to the user's access to CCQAS are performed on the **MTF** and **Permissions** tab, as discussed in [Section 3.3](#) above. CC/MSSP/CMs have limited ability to change the permissions assigned to their own account. CC/MSSP/CMs should contact their CCQAS facility or Service administrator to have permissions adjusted in their account.

3.6.2 Changing an Active Password

Module users may change their own password at any time, and should do so immediately if they feel its integrity has been compromised. To change a password, users click the **System** main menu, and then select **Change Password**, as depicted in Figure 62 below.

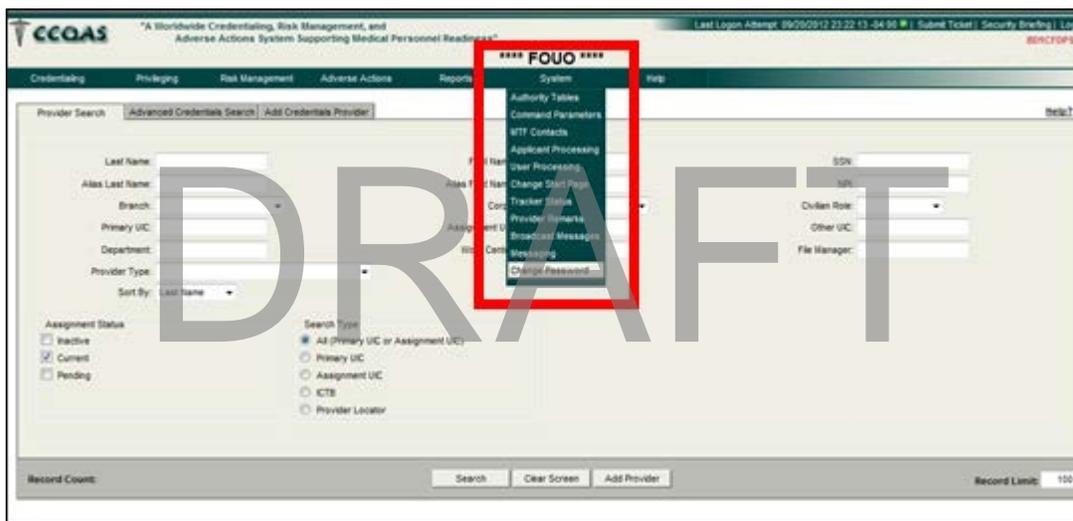


Figure 62: Change Password Menu Item

If a user's password is within 30 days of the expiration date, he or she will also receive a password expiration warning each time the user logs in to CCQAS, as depicted in Figure 63 below.

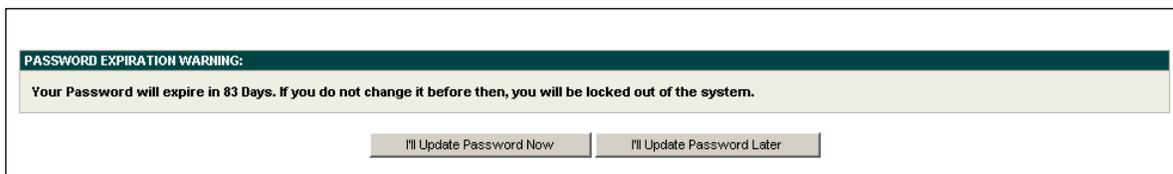


Figure 63: Password Expiration Warning

Users may update a password using the **Change Password** function at any time prior to the password expiration date.

Note: Users with “Provider” access only in CCQAS do not have access to the **System** menu; therefore, they cannot initiate a password change. When Providers need to have their password changed, they should contact the credentials office for assistance.

CC/MSSP/CMs may also initiate a password change on any user account by selecting **Reset Password** from the hidden menu of actions on the **User Listing** screen, as depicted in Figure 64 below. A **Reset Password** button is also available on the **Demographics** tab of the user’s account.

After CC/MSSP/CMs initiate the password change, the user will receive an automated email notification that contains his or her new temporary password, which is valid for the next 60 days.

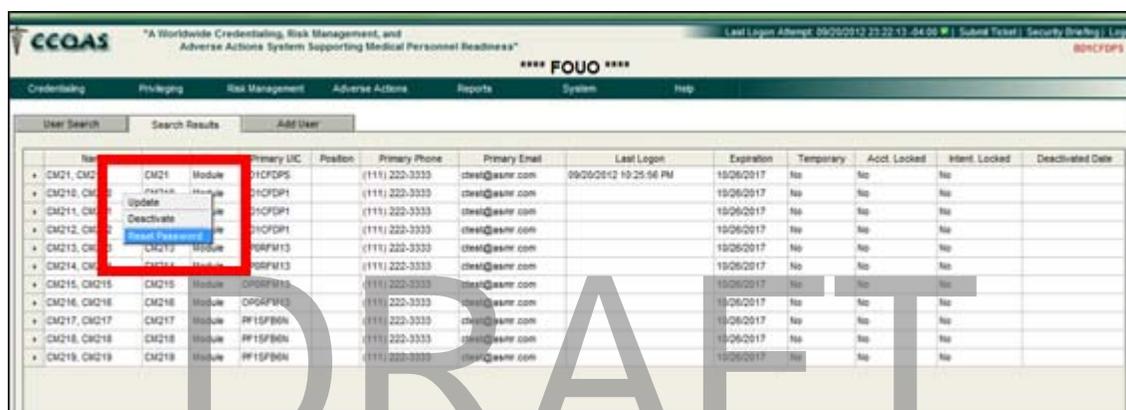


Figure 64: Reset Password Menu Item

3.6.3 Locking and Unlocking User Accounts

CC/MSSP/CMs may lock or unlock user accounts on the **Update User** screen. A CCQAS user account may be automatically locked by the application under the following circumstances:

- The account holder has failed to enter the correct password during each of three consecutive attempts to log in to the CCQAS application
- The password on the user account has expired

The account holder must then contact the CC/MSSP/CM or the MHS Helpdesk to unlock the account. When a user’s account has been locked in this manner, the Administrator may unlock the account by clicking the **Account Locked** box to remove the check mark. This action generates an automated email message to the account holder with a new temporary password. The account holder then logs in to CCQAS and obtains a new permanent password that is valid for the next 60 days.

Under certain circumstances, it may be appropriate to lock a user’s account intentionally to prevent him or her from accessing CCQAS. If a CC/MSSP/CM initiates the locking of a user account, the screen displays a message indicating the account was intentionally locked, as depicted in Figure 65 below.

After the issue with the account has been resolved, the account may be unlocked by clicking the **Account Locked** box again to remove the check mark. This action generates an automated email message to the account holder with a new, temporary password. The account holder then logs in to CCQAS and obtains a new, permanent password that is valid for the next 60 days.

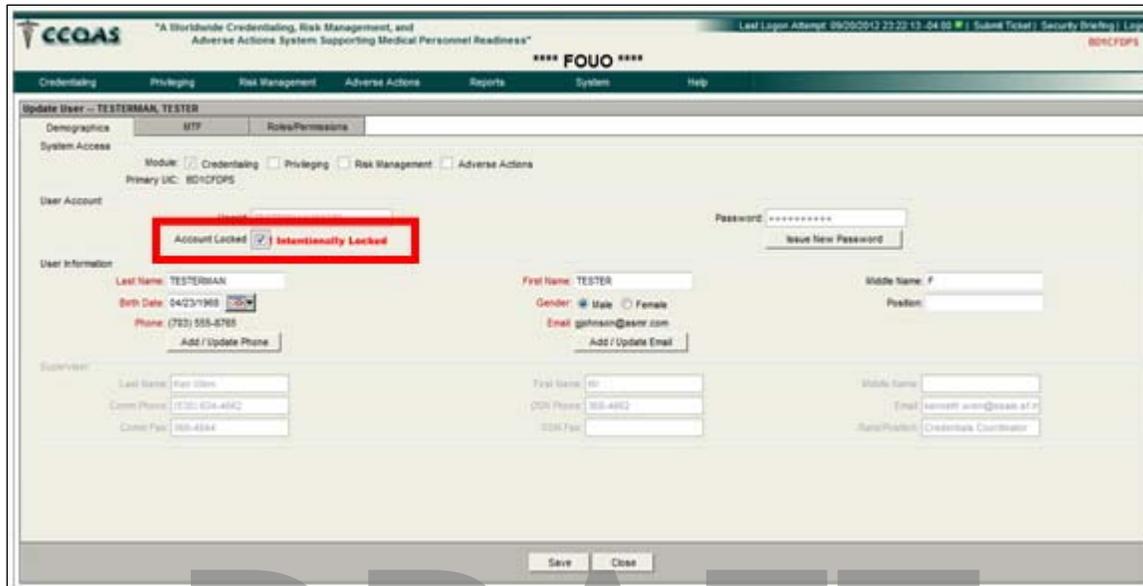


Figure 65: Account Locked Indicator

4 Managing Facility Privilege Lists

Prior to the implementation of CCQAS 2.10.0.0, each Service will have its own list of privileges and categories. After the deployment of 2.10.0.0, there will be one master privilege list for the Army, Air Force, and Navy. This section provides instructions on how to use the newly implemented Tri-Service Master Privilege List.

At least one CC/MSSP/CM at each privileging facility should be designated as the CLP Administrator, who is responsible for managing the privilege catalog for his or her facility. This privilege catalog consists of privilege lists for all specialties, and serves as an indicator of which privileges in each specialty are supported by the facility.

Each facility or unit configures its own privilege lists using the tri-service master privilege catalog. Service-level personnel or MTF-level CLP Administrators may create a new privilege list when a new specialty or privilege items are added, which are added in the 'Other' folder. Facility personnel may, however, modify a privilege to limit or restrict its scope. If a facility CLP Administrator wishes to add a new privilege that is not available from the tri-service master privilege catalog, he or she can add this new privilege to the 'Other' privilege list under the privilege category for that MTF.

4.1 The Privilege Management Function

The process of building a privilege catalog is initiated by selecting **Privilege Management** from the Privileging main menu, as depicted in Figure 66 below. Only users who possess CLP Administrator permissions have access to the **Privilege Management** function in CCQAS.

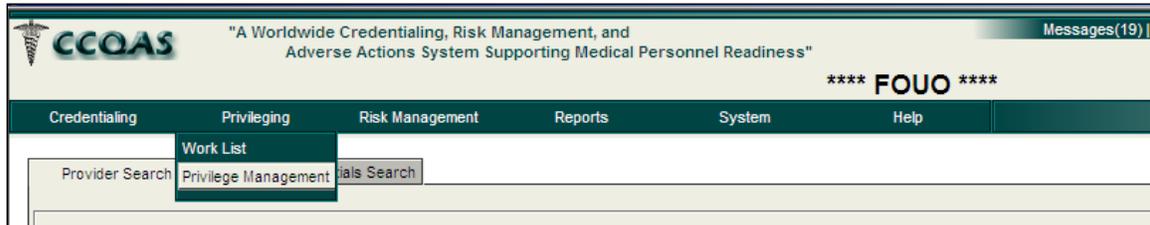


Figure 66: CCQAS Privileging Management Menu Item

When users select **Privilege Management**, the **Privilege Management** screen appears, as depicted in Figure 67 below. From this screen, users may select a privilege category (i.e., specialty) from the **Privilege Category** pick list.

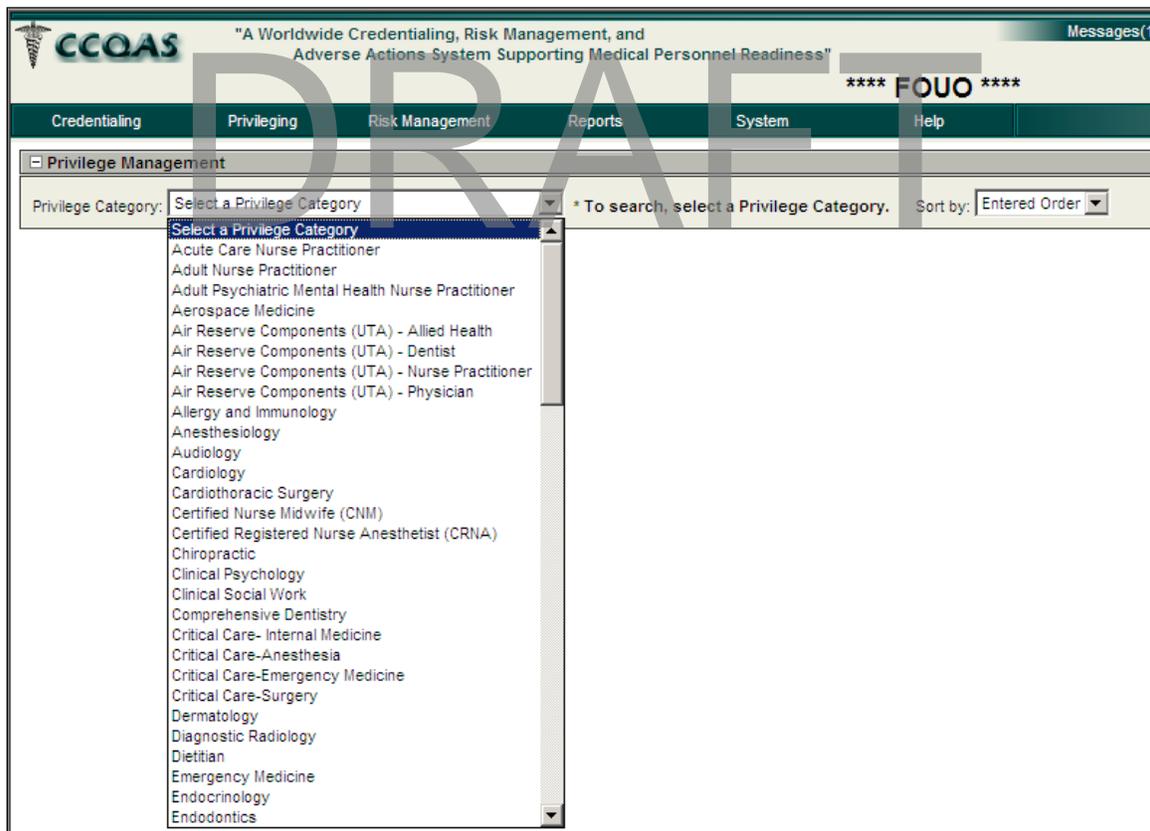


Figure 67: Privilege Management Screen and Category Pick List

Figure 68 below displays the privilege list for the **Family Medicine** category. The Army and Air Force use itemized privileges that enable Providers to request each privilege independently.

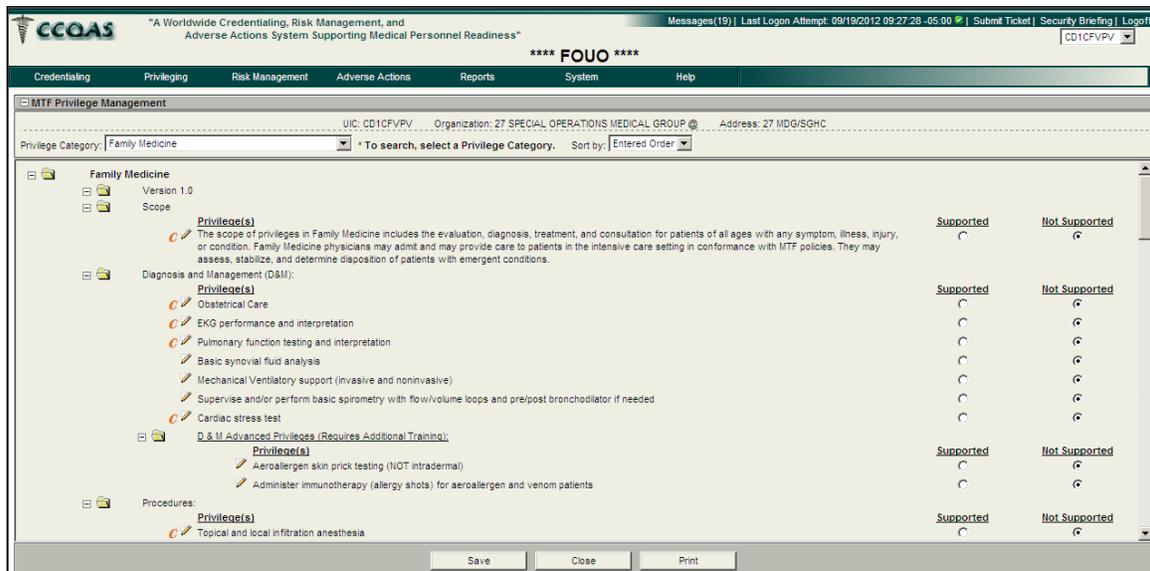


Figure 68: Privilege List for Family Medicine

The Navy uses core privileging, which requires most Providers to request a complete core set of privileges for their specialty; only supplemental privileges may be requested independently.

Thus, privileges included in the Core list of a category are marked with a , as depicted in Figure 69 below.

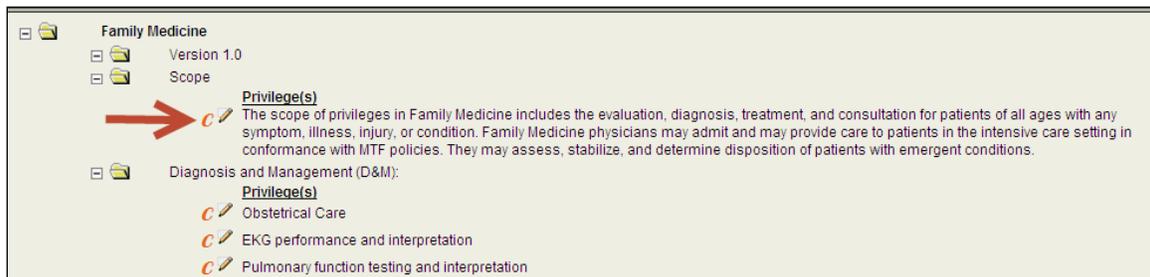


Figure 69: Examples of Family Medicine Core Privileges

The process of building the facility privilege catalog is the same for all Services. Facility CLP Administrators must designate the privileges that are supported within each specialty at their facility. While CLP Administrators are the individuals who enter the information in CCQAS, department heads and other appropriate clinical staff members should review and approve each list to ensure the accuracy of the information.

Facility support for each privilege item within a specialty is performed on the **MTF Privilege Management** screen (refer to Figure 67 and Figure 68 above). The following are important features of the **MTF Privilege Management** screen:

- The privilege lists may be expanded (+) or collapsed (-) by clicking the folder icon next to each list name.
- Users must designate whether or not the facility supports each individual privilege item by selecting the radio button in either the **Supported** or **Not Supported** column.
- If most or all privilege items within a given privilege list are supported by the facility, users may click the header **Supported** to default all radio buttons to that value. Individual privilege items may then be changed, as appropriate.
- If few or no privilege items within a given privilege list are supported by the facility, users may click the header **Not Supported** to default all radio buttons to that value. Individual privilege items may then be changed, as appropriate.
- All privilege items must be set to a default value of **Not Supported** until such time as the CLP Administrator changes the setting.
- All changes made to the privilege items are maintained in an audit log.

A hidden menu is available for each privilege item by clicking the  icon next to the privilege name. **View Privilege** and **Limitation/Restriction** are the menu options, as depicted in Figure 70 below.

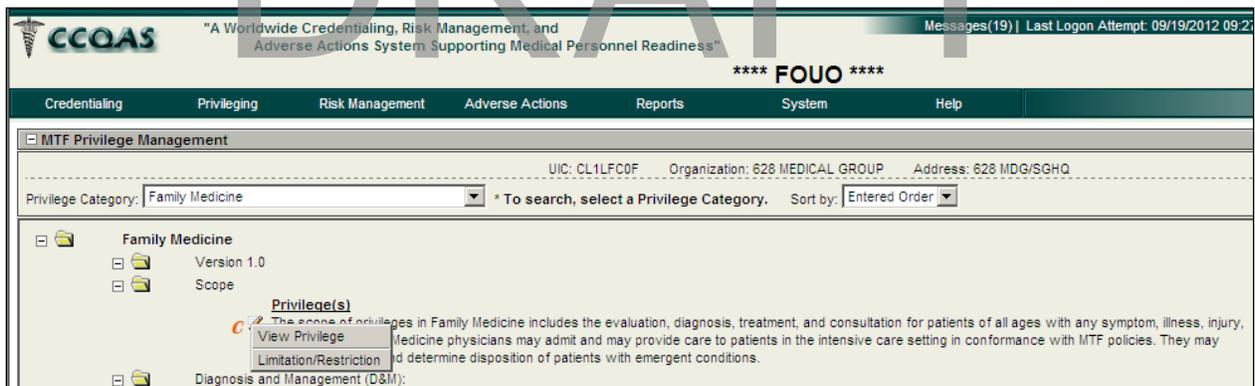


Figure 70: View Privilege Menu Item

The **View Privilege** option opens the **View/Edit Privilege** window, as depicted in Figure 71 below. This option provides a view-only description of the privilege item, and a check box indicator as to whether or not it is a Core privilege. When users click **Close**, they are returned to the **MTF Privilege Management** screen.



Figure 71: View Privilege Option

The **Limitation/Restriction** option also opens the **View Edit Privilege** window, as depicted in Figure 72 below. This option allows CLP Administrators to edit the privilege description to apply facility-specific limitations on the privilege item. Figure 72 below depicts the **Description** text field, where a sample CLP Administrator has updated *Cardiac MRI Interpretation* to *Cardiac MRI Interpretation-Adult Only*.

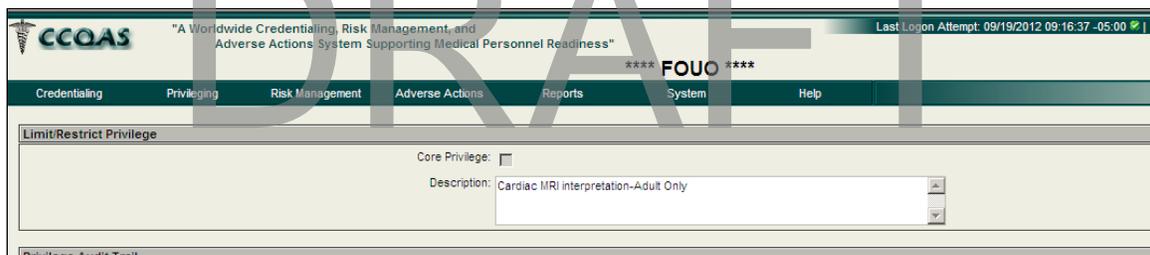


Figure 72: Limitations/Restrictions Option

When CLP Administrators click **Save**, the screen refreshes to display the **MTF Privilege Management** screen, as depicted in Figure 73 below. The new privilege item, **Cardiac MRI Interpretation-Adult Only**, has been added to the bottom of the folder. Note that the original privilege item, **Cardiac MRI Interpretation**, is retained in the list of privilege items. CLP Administrators would then retain the “**Not Supported**” designation for this original privilege item, and, instead, select the restricted privilege item (**Cardiac MRI Interpretation-Adult Only**) as “**Supported.**” This feature allows CLP Administrators to make appropriate modifications to privilege items to narrow the scope of the privilege that may be performed at their facility.

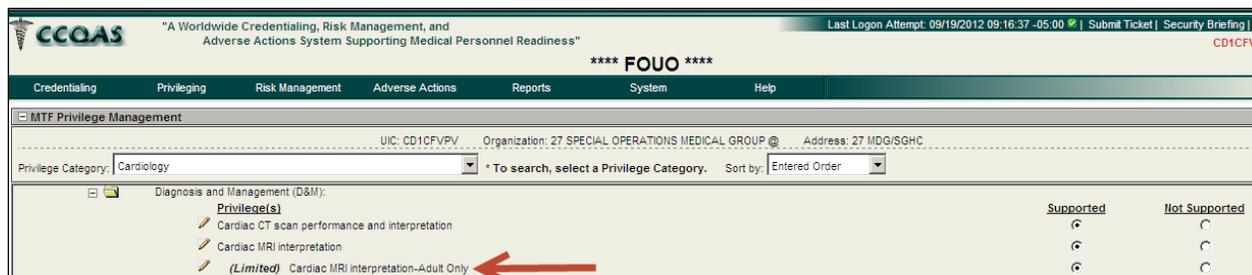


Figure 73: Limitations/Restrictions View

4.2 Initial Privilege Catalog Configuration

When CCQAS 2.10.0.0 is first implemented at a facility or unit, all privilege items are defaulted to “**Not Supported**”. The designated CLP Administrator must open the privilege list for every specialty supported by the facility and designate each individual privilege item that is performed at his or her location as “**Supported**”. Since the default setting for all privileges is “**Not Supported**”, no action is required for specialties or privilege items that are not supported at the CLP Administrator’s location. The creation of user accounts for Reviewers and Providers should only commence after this initial configuration effort has been performed for all specialties and privileges supported at the location.

4.3 Maintenance of Facility Privilege Catalogs

After CCQAS 2.10.0.0 has been implemented, CLP Administrators will be responsible for updating the facility privilege catalog to reflect changes in the facility or unit’s support for an individual privilege item as a result of changes in staffing, equipment, or mission. CLP Administrators may change the designation of support for individual privilege items at any time, according to the guidance provided in Sections [4.1](#) and [4.2](#).

After the initial configuration of a privilege item is performed, CCQAS prompts CLP Administrators to enter explanatory comments for any subsequent changes made to the privilege item, as depicted in Figure 74 below. CCQAS does not permit the entry of comments for status changes entered by clicking the group header. Thus, it is suggested that all changes made to privilege lists after the initial configuration effort be performed by updating each individual privilege in a group, so that privilege-specific comments may be entered.

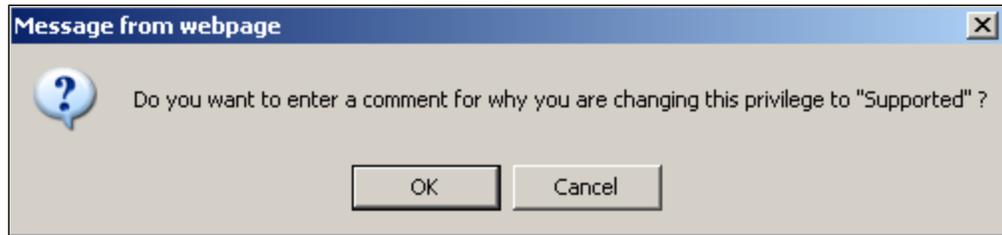


Figure 74: Comment Option for Change to Privilege Designation

When CLP Administrators enter and save the explanatory comments, the screen refreshes to display the updated list of supported privileges, as depicted in Figure 75 below. The date and time stamp and the comment associated with the change to the privilege item may be viewed by clicking **View Privilege** from the hidden menu of actions for the privilege item.

The **Privilege Audit Trail** section, on the lower half the screen, presents the audit information for each change made to that privilege item from the time of initial configuration going forward.

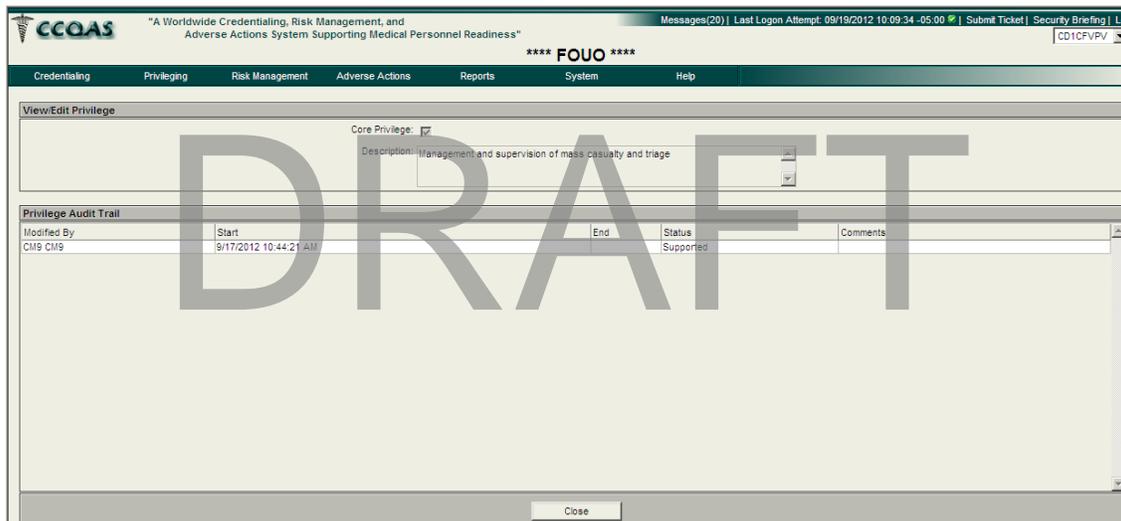


Figure 75: Privilege Audit Trail

When CLP Administrators change a privilege item from **“Not Supported”** to **“Supported”**, Providers who wish to be granted the newly supported privilege must request the privilege via a modification application. The modification application is discussed in [Section 7](#).

When CLP Administrators change a privilege item from **“Supported”** to **“Not Supported”**, some Providers may actively hold one or more of the privileges that are no longer supported at that location.

The addition of new privileges to the Tri-Service Master Privilege List may also require CLP Administrators to update their privilege catalog. When a new privilege is added to the master list, CCQAS sends an automated email message to the CCs/MSSPs/CMs at all locations, alerting them to the availability of the new privilege(s). Action to update the facility privilege catalog is only required if the facility supports the new privilege(s).

5 Processing the 1st E-Application for Clinical Privileges

CCQAS 2.10.0.0 provides a full online privilege request, review, and approval capability designed to support the privileging process at the facility- or unit-level. In order to realize the benefits of this capability, all individuals involved in the privileging process must have a user account in CCQAS with permissions that support their individual role(s) in the process. The creation of user accounts is addressed in [Section 3](#) of this user guide. The following sections describe the online privilege application process in the context of these user roles.

5.1 User Roles in the Privilege Approval Process

The following roles are needed to process an application for clinical privileges in CCQAS 2.10.0.0:

- **Providers:** Individual Providers seeking the approval of requested clinical privileges at their unit or facility
- **Primary PACs** (also known as CC/MSSP/CMs): Professional Affairs office staff who are responsible for ensuring Providers' credentials are in order, for tracking and managing the review and approval of an application for clinical privileges at their primary UIC, and for managing CCQAS user accounts for their facility or unit
 - **Non-Primary PACs** are the CC/MSSP/CMs responsible for a user's credentialing record at a user's non-primary UIC
- **PAC Supervisors:** CC/MSSP/CM staff members who are responsible for overseeing and managing the privileging workload assigned to credentials staff members within a UIC
- **CVOs:** CVO staff members or other credentialing personnel who perform the PSV of Provider credentialing data. The PSV function may also be performed by individuals who are assigned the CC/MSSP/CM role
- **CVO Supervisors:** CVO staff members who are responsible for overseeing and managing the workload assigned to CVO staff members
- **Reviewers:** Clinical staff privileging committee members who have been assigned the responsibility for reviewing and recommending actions on applications for privileges. Reviewers may include the Provider's supervisor, the specialty, service or section chief, the department chair, and/or the members and chair of the executive committee of the medical (dental) staff (ECOMS/ECODS)
 - **Non-Primary Reviewers** are the Level 1-level 4 Reviewers responsible for reviewing privileges requested at a user's non-primary UIC
- **PAs:** Usually MTF commanders or other designated personnel who are responsible for final approval of applications for clinical privileges at both Primary and Non-Primary UICS
- **CLP Administrators:** The individuals who have been assigned responsibility for managing the privilege catalog for their unit or facility. They are also responsible for indicating on the catalog whether their facility or unit can or cannot support each privilege item. Depending on the size of the MTF or other determining factors, this role

may also be played by CC/MSSP/CMs. The privilege catalog was based on common language privileging, hence the abbreviation, “CLP”

Additional roles are assigned to individuals who are responsible for generating and reviewing performance assessments for Providers:

- **PAR Evaluators:** Supervisors, service chiefs, department chairs or other clinical personnel who are responsible for completing and submitting a PAR on a Provider
- **PAR Reviewers:** Clinical staff members who are responsible for reviewing a PAR submitted by a PAR evaluator

In CCQAS 2.10.0.0, one individual may have multiple roles in the privileging process. For example:

- Providers may also be Reviewers (although CCQAS does not allow Providers to act as Reviewers for their own privilege application)
- PACs or CC/MSSP/CMs may also be CLP Administrators
- PAC Supervisors may also be PACs or CC/MSSP/CMs
- Reviewers may also be PAR Evaluators

It is also important to note that some roles are not involved in the processing of every privilege application. For example:

- If a CC/MSSP/CM at a facility performs the primary source verification of all the Provider’s credentials, then the CVO role will not be involved in the application review process
- A PAR is not required if an application for modification of privileges is being processed

Each role in CCQAS is differentiated from the others according to the permissions assigned to the user’s account. If an individual is responsible for multiple roles, his or her user account is assigned the permissions associated with all roles for which he or she is responsible. Refer to [Section 3](#) for details pertaining to the creation and maintenance of CCQAS user accounts.

5.2 The Work List

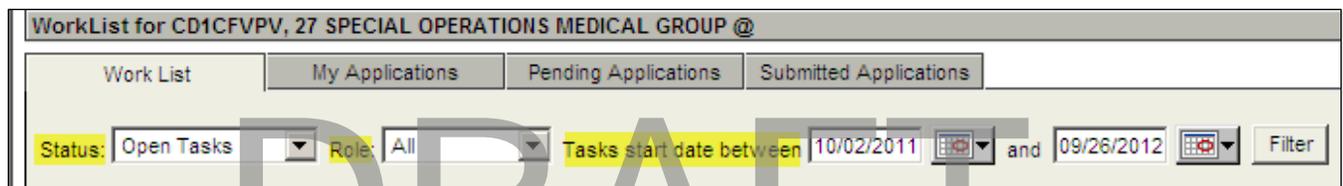
CCQAS 2.10.0.0 provides a work list to organize each user’s work list tasks. The work list, depicted in Figure 76 below, may be designated as the first screen users see after they log in to CCQAS.

?	Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv Expiration
▶	No		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	KENT, TRACY (Military)	1st E-App	Medical Corps	09/19/2012		
▶	No		Setup PAR	CC/CM/MSSP	N/A	JOBS, STEVE (Military)	1st E-App	Medical Corps	09/17/2012		09/17/2012
▶	No		Setup PAR	CC/CM/MSSP	N/A	JOBS, STEVE (Military)	1st E-App	Medical Corps	09/17/2012		09/17/2012
▶	No		Application Ready for Review	CC/CM/MSSP	PETERS, ROBERT (Provider)	PETERS, ROBERT (Military)	1st E-App	Medical Corps	08/27/2012		

Figure 76: Work List Screen for the CC/MSSP/CM

The following are important features of the **Work List** screen, which is depicted in Figure 77 below:

- The work list defaults to display tasks with “**Status = Open**”, which means users need to take some type of action with respect to the listed application
- When users select **Closed** from the **Status** pick list, the work list displays tasks that have already been completed
- For those users who have multiple roles in the privileging process, they may display all tasks in the same list by selecting “**Role = All**”; conversely, they may display only those tasks associated with a particular role by selecting the desired role from the pick list
- The work list defaults to display tasks for the past 30 days; the date range for displaying work list items may be changed by entering the desired **Start** and **End** dates, and then clicking the **Filter** button.

**Figure 77: Status, Role, and Date Options for Work List**

CCQAS sends an email notification to a user each time a new task is added to his or her work list. The notifications function is explained in more detail in the following section.

5.3 Notifications

Efficient and timely processing of the online application package requires coordination between all individuals involved with the privileging process without relying on face-to-face communication. CCQAS supports notifications that consist of automated email messages sent to individuals when action on a privilege application or other CCQAS-managed object is required. This notification is sent to the primary email address associated with a user’s CCQAS account. It is important that any changes to this email address be updated in a timely manner by either the user or the CC/MSSP/CM to ensure these notifications continue to reach the targeted individual.

CCQAS generates an email notification automatically when users receive a new task. While this functionality should prove helpful for Providers, Reviewers, and other roles that may not use CCQAS on a daily basis, daily users of CCQAS, such as a CC/MSSP/CMs may wish to disable these notifications. CC/MSSP/CMs may disable or turn off their own email notification function by clicking the **System** main menu, then selecting **Messaging** from the drop-down list. Figure 78 below depicts the **Messaging** menu item.

The screenshot shows the CCQAS web application interface. At the top, there is a header with the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". Below this is a navigation bar with tabs for Credentiaing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. The System menu is open, showing a list of items including Authority Tables, Command Parameters, MTF Contacts, Applicant Processing, User Processing, Change Start Page, Tracker Status, Provider Remarks, Broadcast Messages, and Messaging. The Messaging item is highlighted. Below the navigation bar, there is a section for "WorkList for CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @". This section includes filters for Status (Open Tasks), Role (All), and Tasks start date between 10/10/2011 and 10/04/2. Below the filters is a table with columns: Urgent, Due Date, Task, Role, From (Role), Pro, App Type, and Corps. The table contains four rows of data.

Urgent	Due Date	Task	Role	From (Role)	Pro	App Type	Corps
No		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	RE	1st E-App	Dental Corps
No		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	KE	1st E-App	Medical Corps
No		Setup PAR	CC/CM/MSSP	N/A	JO	1st E-App	Medical Corps
No		Setup PAR	CC/CM/MSSP	N/A	JO	1st E-App	Medical Corps

Figure 78: Messaging Menu Item

CC/MSSP/CMs then select **Email Notification**, as depicted in Figure 79 below. The email notifications may be turned off by following the instructions on the screen.

The screenshot shows the "Email Notification" settings page in the CCQAS system. The page has a navigation bar at the top with tabs for Credentiaing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. Below the navigation bar, there is a section for "Email Notification" with a sub-section for "Privileging". The main content area contains the question "Would you like to receive email notifications?" with radio buttons for "Yes" and "No". The "No" radio button is selected. Below the question is a "Save" button.

Figure 79: Disabling the Email Notification for the CC/MSSP/CM

Note: Only CC/MSSP/CMs can disable the notification function. CCQAS does not allow notifications to be disabled for Providers, Reviewers, or other roles in the privileging process.

5.4 Types of Privilege Applications

CCQAS classifies privilege applications according to a Provider's privileging status at a given facility or unit, for a given assignment. There are several different types of applications, as listed in Table 1 below.

After an application is submitted and processed through the CCQAS workflow for the first time, all subsequent applications are identified as one of the other application types.

Table 1: Types of Privilege Applications

Type	Description
1st E-App	The first online application that is submitted by a Provider in CCQAS. The first online application is generally submitted when a new Provider is entered into the system, but may also apply when requesting privileges for the first time at a new UIC
Modification	An application for a modification of clinical privileges that were previously

Type	Description
	granted or approved through the CCQAS workflow process at the assigned duty station
Transfer (ICTB)	An application for privileges at a temporary duty location (i.e., gaining facility) after privileges were previously granted at the assigned location (i.e., sending facility). Simply referred to as “ICTB” because this transfer requires an inter-facility credentials brief (i.e., ICTB)
Transfer (PCS)	Following a PCS, an application for privileges at the new duty location (i.e., gaining facility) after privileges were granted through the CCQAS workflow process at the previously assigned duty station (i.e., losing facility)
Renewal	An application for renewal of clinical privileges which are due to expire, and which were previously granted through the CCQAS workflow process at the same duty station

Newly-accessed clinical support staff (CSS) personnel and others who typically are not eligible for privileging must also complete and submit an E-application. This ensures their credentials information is completely and correctly entered into the CCQAS database. Modification and Renewal applications generally only apply to privileged Providers, but CSS who are military personnel may also have Transfer (ICTB or PCS) applications.

A record of all privilege applications processed through CCQAS by CC/MSSP/CMs is maintained on the **My Applications** screen, and may be accessed by clicking the **My Applications** tab, as depicted in Figure 80 below.

Urgent	Provider	Application Type	Application Status	Provider Phone	App Submitted	Priv Effective	Priv Expiration
No	ALLEN, PAUL	1st E-App	Closed	123456	10/01/2012	10/01/2012	09/30/2014
No	JOBS, STEVE	1st E-App	Closed	369852	09/17/2012	09/17/2012	09/17/2012
		1st E-App	In Review	(369) 852-1470	09/19/2012		
	ERT	1st E-App	Submitted	123-4567	08/27/2012		
	S	1st E-App	In Review	(320) 145-8987	09/28/2012		
		1st E-App	Closed	1234	09/18/2012	09/18/2012	09/17/2014

Figure 80: My Applications Screen

The following are important features of the **My Applications** screen:

- Users may search for a particular Provider application by entering the **Provider Last Name**, and then clicking the **Filter** button
- The **Application** screen defaults to display applications submitted in the past year. The date range for displaying submitted applications may be changed by entering the desired **Start** and **End** dates, and then clicking the **Filter** button
- The application may be opened and viewed by selecting **Open** from the hidden menu of actions, or by double-clicking the line item
- Applications that have previously been approved, terminated, or are otherwise not active are presented in read-only format
- A hidden menu of actions is available for each application, as depicted in Figure 81, below. This menu enables CC/MSSP/CMs to View/Log comments (refer to [Section 5.10](#)), initiate the PAR (refer to [Section 11](#)) for the associated privileging period, generate a Credentialing/Privileging Inquiry letter for a Provider, apply an urgent status to the application (refer to [Section 5.5.9](#)), unlock a section of the application, terminate an application, or complete the application process.

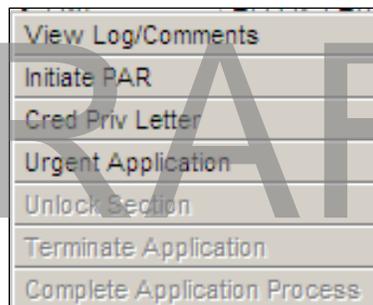


Figure 81: My Application Hidden Menu

The **Pending Applications** tab gives CC/MSSP/CMs visibility of all outstanding applications at their facility or unit and the time elapsed since a Provider first received an email notification directing him or her to complete an E-application in CCQAS. Figure 82 below depicts the **Pending Applications** tab.

WorkList for CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @							
Work List		My Applications	Pending Applications	Submitted Applications			
Show applications that were initiated between		07/07/2012	and	10/05/2012	Status:	Pending	Filter
?	Provider	Application Type	Status	Provider Phone	Application Task Initiated	Provider Started Completing	Number of Days Completing
▶	BISHOP, BRIAN	1st E-App	Pending	(369) 852-1470	09/25/2012	09/25/2012	10
▶	CAROLLA, ADAM	1st E-App	Pending	(523) 696-8541	09/25/2012	09/25/2012	10
▶	CAROLLA, ADAM	1st E-App	Pending	(523) 696-8541	09/25/2012		
▶	CAROLLA, ADAM	1st E-App	Pending	23859820	09/25/2012		
▶	CAROLLA, ADAM	1st E-App	Pending	1 (324) 545-8743	09/25/2012		
▶	ROSEN, ALLISON	1st E-App	Pending	(321) 456-9870	09/25/2012	09/25/2012	10
▶	SIMMS, DAVE	1st E-App	Pending	123456777	09/25/2012	09/25/2012	10
▶	TEST112233554, WILL	Transfer (ICTB)	Pending	234234234	09/17/2012		

Figure 82: 'Pending Applications' Tab

Applications are assigned a status of **Pending**, **Terminated**, or **Noncompliant**. Applications are considered **Pending** if they were generated during the date range specified at the top of the tab, but have not yet been completed and submitted by the Provider. Applications in **Terminated** or **Noncompliant** status are applications that were closed by a CC/MSSP/CM during the specified date range, prior to completion of the review and approval process.

In order to terminate an application or designate it as noncompliant, CC/MSSP/CMs select the desired action from the hidden menu for the application record. If CC/MSSP/CMs select **Terminate Application**, they are required to enter comments explaining the reason for the termination. Typically, an application is terminated if it was generated in error, or a Provider no longer needs to request privileges at that time. If the Provider has failed to complete his or her privilege application in the necessary period of time, CC/MSSP/CMs should select the option to **Set Noncompliant**.

Applications that are terminated or designated as noncompliant are removed from the Provider's work list and no further action may be taken on the application by any CCQAS user. CC/MSSP/CMs may reactivate a terminated or noncompliant application at any time by selecting **Reactivate** from the hidden menu of actions, as depicted in Figure 83 below.

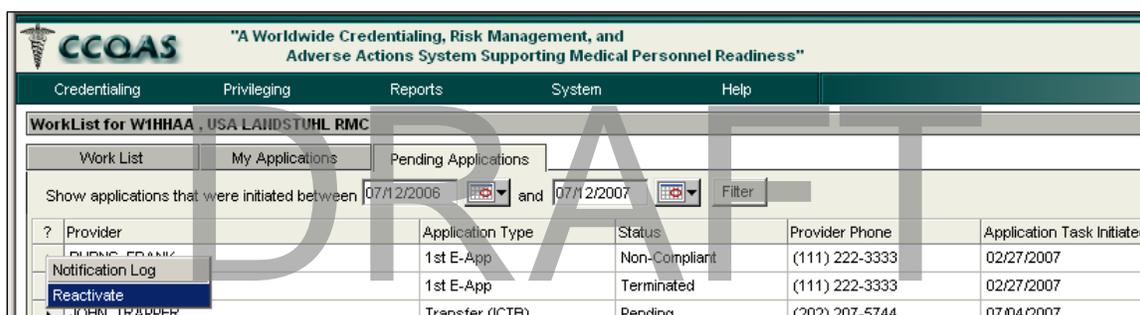


Figure 83: Reactivate Menu Item

5.5 Initial Review of a Privilege Application

After Providers E-signs and submit their application online, the CC/MSSP/CM receives a new work list item with "**Task = Application Ready for Review**". The application may be viewed from the work list by selecting **Open** from the hidden menu, as depicted in Figure 84 below, or double-clicking anywhere on the record line item.

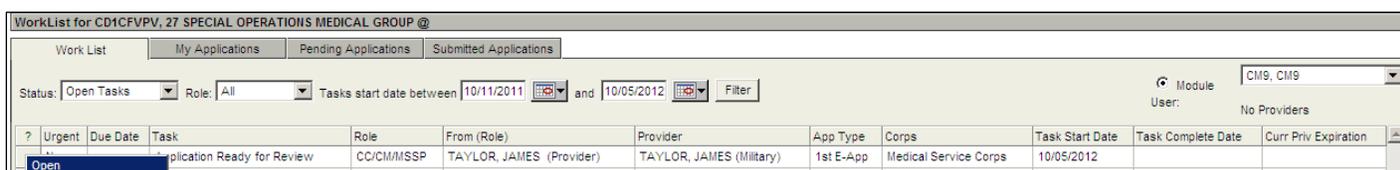


Figure 84: Work List Task – Application Ready for Review

CCQAS displays a message window asking CC/MSSP/CMs if they assume responsibility for processing the application. This message window is depicted in Figure 85 below. This feature was built into CCQAS to accommodate larger facilities and units in which multiple staff members share the credentialing and privileging workload. If CC/MSSP/CMs are the only staff members at their facility or unit who manage privilege applications, they select **Yes**. If the privileging workload is shared across staff members, CC/MSSP/CMs only select **Yes** for those applications for which they are personally responsible.

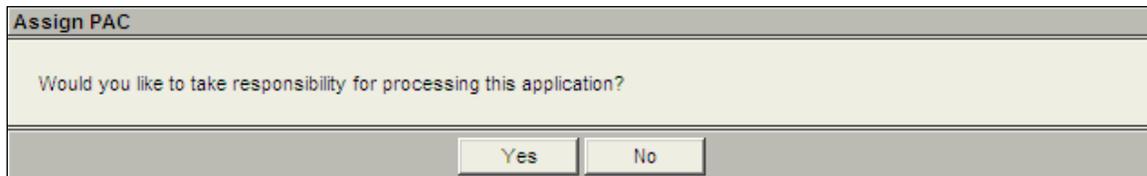


Figure 85: Assign PAC Screen

In order to move forward in the review process with this application, CC/MSSP/CMs must click **Yes**. If they select **No**, the work list item remains active in all CC/MSSP/CMs' work lists for the facility or unit until ownership of the application is accepted by one of them, at which time, the item disappears from the work list of the other CMs/MSSPs/CCs, and is viewable only in the work list of the responsible party.

Accepting responsibility for processing the application has several implications:

- The accepting CC/MSSP/CM becomes the sole custodian of the privileging application and the only credentialing staff member at his or her facility or unit who may route the application for PSV, review, or approval; return the application to the Provider; or terminate the processing of the application
- The accepting CC/MSSP/CM becomes the only credentialing staff member who receives email notifications or work list items pertaining to the privilege application
- The accepting CC/MSSP/CM may reassign the application to another CC/MSSP/CM in his or her unit or facility at any time during application processing, but, in doing so, will lose custody of the application after it is reassigned

After a CC/MSSP/CM accepts responsibility for the application by clicking **Yes**, the E-application is returned as a series of tabs, which are explained in more detail in the following section.

5.5.1 The Provider Summary Tab

The **Provider Summary** tab is the first tab in the privilege application, as depicted in Figure 86 below. This tab displays demographic information that Providers entered into the **Profile**, **Identification**, and **Contact** sections of the electronic application.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Login Attempt: 10/05/2012 08:35:56 -05:00 Submit Ticket | Security Briefing | Log Out

**** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Provider Application Review - JAMES TAYLOR, 100554444

Provider Summary Position Privileges Documents Comments [Expand All](#) [Collapse All](#) [Print Summary](#)

Profile

Name:	TAYLOR, JAMES	Gender:	Male	Date of Birth:	09/29/1983	No Photo Available
Branch:	F11 - Air Force (USAF)	Rank:	GEN - General	Corps:	MSC - Medical Service Corps	
AOC/Design/AFSC:	40CQA - Medical Commander - Medical Services	Accession:	DA - Direct Accession			
How the provider entered service						

Identification

Identification Type	Identification Number	State
Social Security Number	100-55-4444	

Contact - Phone

Phone Number	Phone Type	Primary
123456789	Home	Yes

Contact - Email

Email Address	Primary
JESSICA.NEWTON@ASMR.COM	Yes

Contact - Address

Address Type	Full Address	Primary
Home	123 STREET EUGENE OR	Yes

[View Credentials](#)

Return to Provider PSV Re-assign CC/IM/ISSP Terminate Close

Figure 86: 'Provider Summary' Tab

The remainder of the credentials information in the application may be viewed by clicking the **View Credentials** button, as depicted in Figure 87 below.

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Provider Application Review - JAMES TAYLOR, 100554444

Provider Summary Position Privileges Documents Comments [Expand All](#) [Collapse All](#) [Print Summary](#)

Profile

Name:	TAYLOR, JAMES	Gender:	Male	Date of Birth:	09/29/1983	No Photo Available
Branch:	F11 - Air Force (USAF)	Rank:	GEN - General	Corps:	MSC - Medical Service Corps	
AOC/Design/AFSC:	40CQA - Medical Commander - Medical Services	Accession:	DA - Direct Accession			
How the provider entered service						

Identification

Identification Type	Identification Number	State
Social Security Number	100-55-4444	

Contact - Phone

Phone Number	Phone Type	Primary
123456789	Home	Yes

Contact - Email

Email Address	Primary
JESSICA.NEWTON@ASMR.COM	Yes

Contact - Address

Address Type	Full Address	Primary
Home	123 STREET EUGENE OR	Yes

State License/Certification/Registration

Type	State	Number	Field	Status	Expires	ADM Waiver
License	Illinois	123	School Psychologist	Active	Indefinite	No

National Certification/Registration [No Data]

Unlicensed Information [No Data]

Drug Enforcement Agency (DEA) / Controlled Dangerous Substances (CDS) [No Data]

Return to Provider PSV Re-assign CC/IM/ISSP Terminate Close

Figure 87: 'Expanded Provider Summary' Tab

The screen refreshes to display all credentials entered into the privilege application for the Provider. The following are important features of the expanded **Provider Summary** screen:

- The credentials information is presented in read-only format; if changes or additions are required, CC/MSSP/CMs must return the application to the Provider, who makes the appropriate changes as instructed by his or her CC/MSSP/CM through either a comment within the application itself, or outside the system through a telephone call or email
- Specific sections in the application include data fields for documenting PSV information; these fields may not be populated until the application is submitted for PSV
- Each section of the application may be expanded or collapsed by clicking the [+] or [-] to the left of the section label
- A hardcopy listing of the whole electronic application package may be printed by clicking **Print Summary** in the upper right-hand corner of the **Provider Summary** tab
- CC/MSSP/CMs may add a note to the Reviewers by clicking the **Empty Note** (📄) icon for a section. Once a note is added, the **Empty Note** icon (📄) becomes a **Filled Note** (📄) icon. Only CC/MSSP/CMs have this capability. When routed to the Reviewers, the **Filled Note** icon is replaced by a **Red Flag** icon (🚩) to indicate to the Reviewers that a CC/MSSP/CM has added a note and that the Reviewers need to pay particular attention to the section. Notes entered by a CC/MSSP/CM are viewable by the Reviewers during the review process, but are not visible to a Provider.

Prior to processing the application, CC/MSSP/CMs should review all credentials information entered by the Provider for accuracy and completeness.

5.5.2 The Position Tab

The **Position** tab is the second tab in the privilege application. This tab displays the information that Providers entered in the **Position** section of the electronic application, as depicted in Figure 88 below.

UIC	Name	Location	Request Admitting Privileges?
<input checked="" type="checkbox"/>	CD1CFVPV	27 MDG/SGHC, NIM	<input type="checkbox"/> Parent

Figure 88: 'Position' Tab

The **Position** tab allows CC/MSSP/CMs to determine what type of Provider submitted the application and whether or not clinical privileges are being requested with the application. If the Provider is a member of the CSS, his or her application does not include a request for clinical privileges.

Note: It is imperative for CC/MSSP/CMs to verify whether the Provider is requesting privileges with this application. If the Provider selected the **No** radio button, but it is believed that this Provider should be privileged, CC/MSSP/CMs should consult the Provider and/or the clinical supervisor to confirm. The application should be returned to the Provider with the instructions to edit the application with his or her request for privileges.

CC/MSSP/CMs can edit the remainder of the fields on the **Position** tab. This is the only information in the application packet that CC/MSSP/CMs may edit at this point in the application process. If CC/MSSP/CMs change any information previously entered by the Provider, the Provider should be notified regarding the nature and justification for the change; otherwise, CC/MSSP/CMs may return the application to the Provider for him or her to make the change as instructed.

5.5.3 The Privileges Tab

The **Privileges** tab, depicted in Figure 89 below, lists all of the privileges associated with the specialty or specialties in which a Provider is requesting privileges, at parent and branch clinics, and his or her requested delineation for each privilege item. For Army and Air Force facilities, delineations are either **Fully Competent, With Supervision, or Not Requested**. For Navy facilities, delineations are either **Yes** or **No**.

Note: CC/MSSP/CMs or CLP Administrators should already have configured the privilege catalog to indicate which privileges their facility can or cannot support. The system automatically displays non-supported privileges as **Not Supported** when the application is routed to the Reviewers. Providers, however, should be instructed to request all privileges they are qualified to perform, regardless of what is or is not supported.

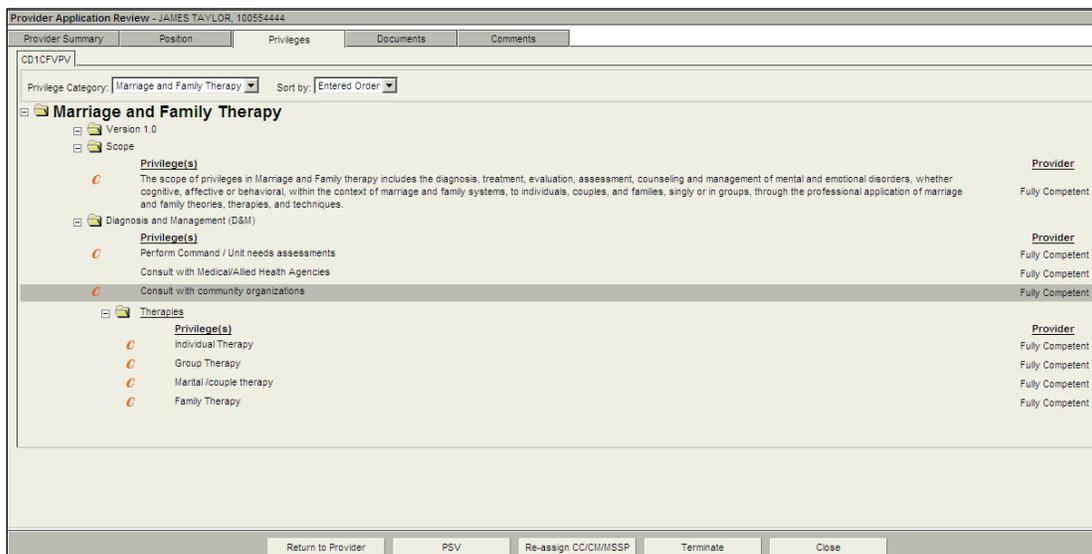


Figure 89: 'Privileges' Tab for Army General Surgery

The following are important features of the **Privileges** tab:

- All privilege delineations are read-only to CC/MSSP/CMs; if changes in privilege delineations are needed, CC/MSSP/CMs must return the application to the Provider with a request to make the appropriate changes
- Privilege lists contained within folders (📁) may be expanded or collapsed by clicking the [+] or [-] to the left of the icon
- The **Privileges** tab is inactive for applications submitted by CSS personnel or Providers who are not requesting clinical privileges with their application

CC/MSSP/CMs should review the **Privilege Category** drop-down list (depicted in Figure 89 above) on the **Privileges** tab to identify all specialties for which the Provider is requesting clinical privileges. This information is required when assigning individuals to review the application, since multiple Level 1 Reviewers are generally needed if the Provider is requesting privileges in more than one specialty.

5.5.4 The Documents Tab

CCQAS 2.10.0.0 enables users to upload documents into the **Documents** tab that are needed to support the privileging process and maintain current credentials records.

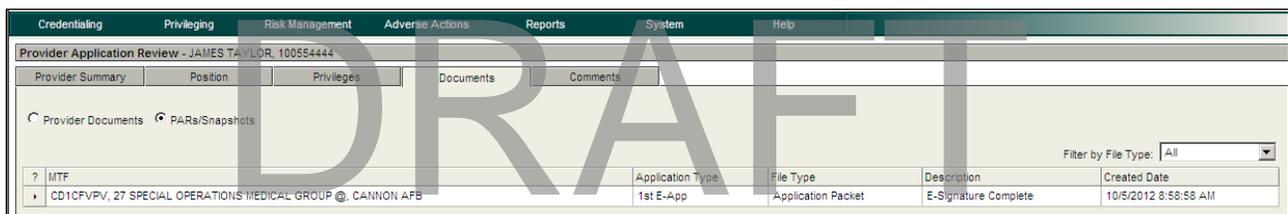


Figure 90: 'Documents' Tab

The following are important features of the **Documents** tab:

- In order to be uploaded into CCQAS, each individual document must be 5 megabytes (MB) or less in size and have a .pdf, .jpeg, or .gif file extension
- **Provider Documents** or **PARs/Snapshots** documents may be displayed by selecting the appropriate radio button at the top of the tab, as depicted in Figure 90 above. Snapshots are CCQAS-generated Portable Document Format (PDF) files of the privilege application created each time the application is E-signed by a Provider or PA
- The list of documents associated with the application may be searched by selecting the desired document type from the **Filter by File Type** pick list
- The summary line for each uploaded document includes the type of document, when it was uploaded and by whom, and the name of the file that was uploaded
- The document may be viewed by double-clicking on the line item, after which a **File Download** dialog box appears. Click **Open** to view the document, or click **Save** to save the document in your hard drive or some other storage device

- The **User Name** reflects the individual who uploaded the document to the application and the **Upload Date** reflects the date and time the document was originally uploaded

CCQAS allows Providers to upload specific types of documents into their application prior to submitting it, including the following:

- License, certification and/or registration
- Diploma
- Specialty Board Certifications
- ECFMG Certification
- Training Certificates
- Continuing Medical Education/Continuing Education Units (CMEs/CEUs) (continuing education training documents)
- Proof of contingency training (e.g., Basic Life Support [BLS]; Advanced Cardiac Life Support [ACLS]; Pediatric Advanced Life Support [PALS]; Combat Casualty Care Course [C4]; Chemical, Biological, Radiological, and Nuclear [CBRNE], etc.)

When Providers upload any documents into the application, they are listed on the **Documents** tab when a CC/MSSP/CM receives the application. CC/MSSP/CMs may also upload a Provider's documents into CCQAS, as well as other document types that the Provider does not have permission to upload, by clicking the **Add** button. Figure 91 below depicts the **Add Documents** screen, where Providers and CC/MSSP/CMs can upload documents.

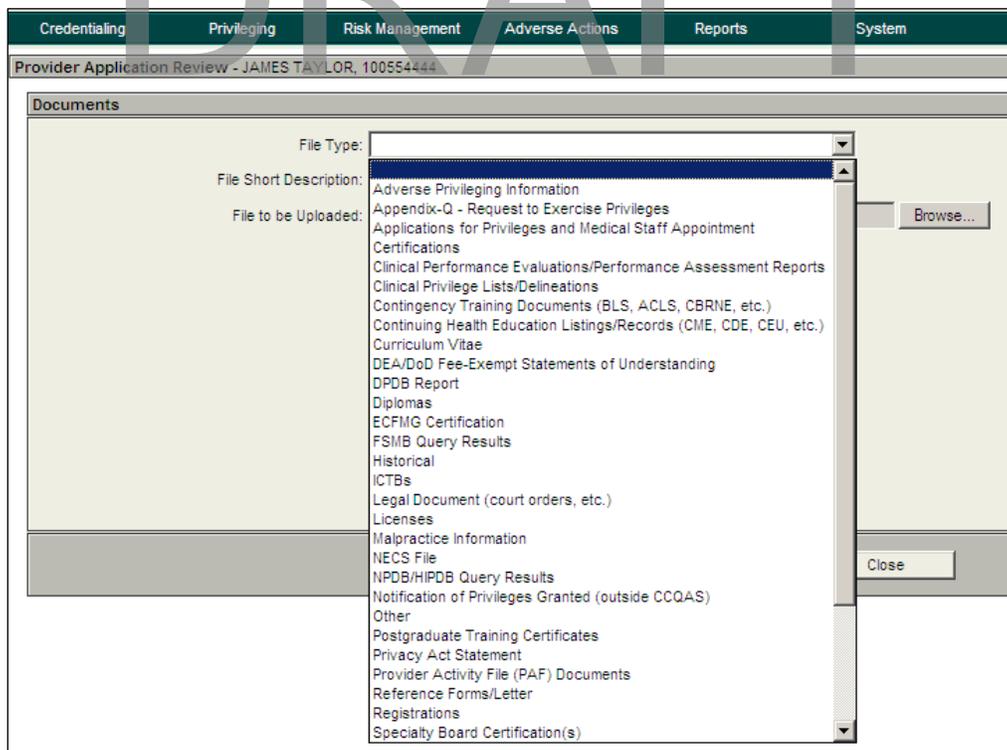


Figure 91: Add Documents Screen

Providers can view all documents uploaded in CCQAS regardless of who uploaded the document into their application. Prior to the submission of an application, Providers may delete documents they uploaded and associated with their application. Once an application is submitted, PSV'ed and routed for review, the attached documents may no longer be deleted. After the application is routed for review, documents uploaded by CC/MSSP/CMs can no longer be deleted.

5.5.5 The Comments Tab

The **Comments** tab displays a summary record for all comments entered into the application as it proceeds through the review process. Figure 92 below depicts the **Comments** tab.

Role	User	Action	Comment	Date
Provider	TAYLOR, JAMES	Provider Submit		10/05/2012

Figure 92: 'Comments' Tab

The complete record of the comments may be viewed by selecting **View** from the hidden menu of actions for the summary record. A new comment may be added by clicking the **Add** button, as depicted in Figure 93.^[RJ1]

Figure 93: Add Comments Screen

Providers may or may not be able to view comments entered into the submitted application, depending on when they were entered. Comments that Providers can view include the following:

- Comments entered by Providers when they submit their application
- Comments entered by CC/MSSP/CMs if/when an application is returned to Providers with a request for edits or additional information on the application

Providers cannot view comments generated during the application review process, such as those entered by CC/MSSP/CMs on the **Provider Summary** screen or comments entered by Reviewers when they issue their recommendation for or against approval of the application. All

review comments are maintained as part of the historical record for the application, but viewable only to those directly involved in the application review process.

5.5.6 Taking Action on a Privilege Application

After reviewing the privilege application for completeness, CC/MSSP/CMs are ready to take action on the application. To do so, they select one of the buttons provided at the bottom of any tab within the application package, as depicted in Figure 94 below:

- The **Return to Provider** button routes the application back to a Provider who originally submitted it. CC/MSSP/CMs are required to enter comments or instructions to Providers when they select this option. Providers then receive an email notification and a task, instructing them to access CCQAS, review the CC/MSSP/CM comments and modify the application accordingly
- The **PSV** button submits the application for PSV, which may be done by CC/MSSP/CMs or CVOs. Further processing of the application may not be performed until the PSV process has been completed
- The **Re-assign CC/MSSP/CM** button allows users to turn over custody of the record to another CC/MSSP/CM in their respective facility or unit (refer to [Section 5.5.7](#))
- The **Terminate** button halts the application process immediately. The application may no longer be processed, but CCQAS retains a read-only copy of the terminated application, which may be accessed from the **Applications** tab
- The **Close** button closes the application, which users may reopen later. When users click this button, they are returned to their work list

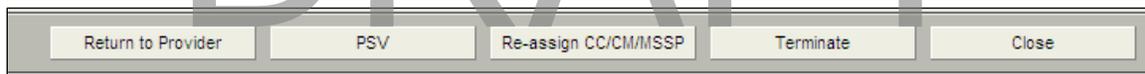


Figure 94: Action Options for E-Applications

5.5.7 Reassigning Ownership of an Application to Another CC/MSSP/CM

If a CC/MSSP/CM has already accepted responsibility for an application and determines that the application should be handled by another CC/MSSP/CM in the same facility or unit, the custody of the application may be transferred to the other individual by clicking the **Re-assign CC/MSSP/CM** button, as depicted in Figure 95 below. A window opens that contains a pick list of all available CMs/MSSPs/CCs in the facility or unit to whom responsibility for the record may be transferred.

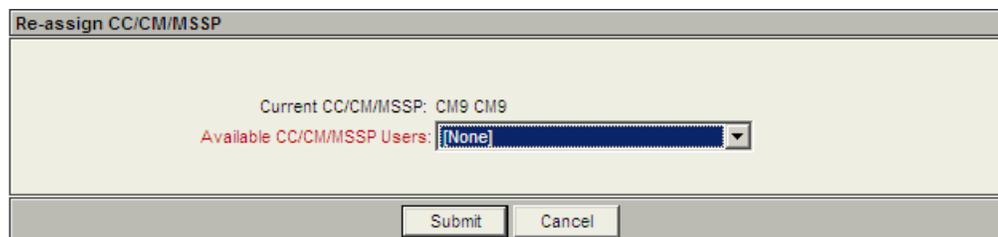


Figure 95: Re-assign Screen

After CC/MSSP/CMs click **Submit**, full custody of the application is transferred to the individual they selected.

CCQAS also allows users that have been granted the “PAC Supervisor” role the ability to reassign applications on behalf of CMs/MSSPs/CCs in their UIC. The “PAC Supervisor” role is explained in more detailed in [Section 5.18](#).

5.5.8 Taking Ownership of an Application from another CC/MSSP/CM

The **Application Reassignment** function may be used in situations where ownership of one or more privilege applications must be transferred to a different CC/MSSP/CM, but the CC/MSSP/CM who is currently responsible for the application(s) is not available to initiate the reassignment. The **Application Reassignment** button is located at the bottom of the work list tab, as depicted in Figure 96 below.

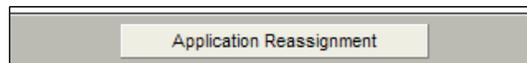


Figure 96: ‘Application Reassignment’ Button

When CC/MSSP/CMs click the **Application Reassignment** button, the **Application Reassignment** screen appears, as depicted in Figure 97 below. This screen displays all applications submitted within the last year that are associated with a user’s facility or unit.

Application Reassignment for WIHHAA , USA LANDSTUHL RMC

This application reassignment process is a backup measure to allows CC/CMSSP users to take over ownership of a privilege application that was originally assigned to another CC/CMSSP user. T CC/CMSSP is not available to reassign the privilege application.

Provider Last Name: Show applications that were submitted between 07/06/2006 and 07/06/2007

Provider	Application Status	Provider Phone	App Submitted	App Effective
▶ HOULIHAN, MARGARET	In Review	(416) 263-8366	07/06/2007	
▶ PIERCE, BENJAMIN	Complete	(915) 569-2800	06/21/2007	06/21/2007
▶ PIERCE, BENJAMIN	Complete	(915) 569-2800	06/28/2007	07/04/2007
▶ POTTER, CHEMUN	Submitted	(454) 098-6746	07/06/2007	

Figure 97: Application Reassignment Screen

The following are important features of the **Application Reassignment** screen:

- Users may search for a particular Provider's application by entering the **Provider Last Name** and clicking the **Go** button at the top of the page
- The **Application** screen defaults to display applications submitted in the past year; the date range for displaying submitted applications may be changed by entering the desired **Start** and **End** dates, and then clicking **Go**
- Users obtain custody of an application by selecting **Reassign to Self** from the hidden menu of actions, as depicted in Figure 97 above

The **Application Reassignment** functionality only allows applications to be reassigned to another CC/MSSP/CM within the facility or unit where the application was submitted. CC/MSSP/CMs may not take custody of a privilege application in a different facility or unit for which they do not have the appropriate permissions to function in the role of a CC/MSSP/CM. An application may be reassigned to another CC/MSSP/CM at any point in the application review and approval process.

5.5.9 Setting an Application as Urgent

In situations where applications require immediate attention by the clinical staff, CCQAS allows CC/MSSP/CMs to flag an application with an urgent status. This action is performed by selecting **Urgent Application** from the hidden menu of actions on the **My Applications** screen, as depicted in Figure 98 below.

Work List				My Applications				Pending Applications				Submitted Applications			
Provider Last Name: <input type="text"/>								Show applications that were submitted between <input type="text"/> to <input type="text"/>							
?	Urgent	Provider		Application Type											
		ALLEN, DAVID		1st E-App											
				1st E-App											
				1st E-App											
				1st E-App											

Figure 98: Urgent Application Menu Item

The **Urgent Application** window opens, as depicted in Figure 99 below. Users select the **Add Urgent Status** radio button, enter **Comments** explaining the details of the urgency, and click **Submit**.

Figure 99: Urgent Application Window

A confirmation message is displayed, as depicted in Figure 100 below.

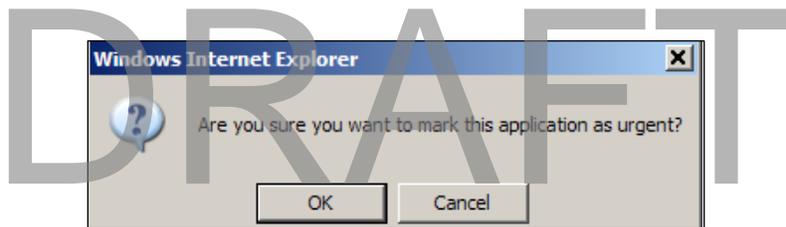


Figure 100: Urgent Application Confirmation Message

After users click **OK**, the work list is refreshed. The application task now appears in red, bold text, with the **Urgent = Yes**. The explanatory comment that was entered may be viewed by selecting **View Urgent Comment** from the hidden menu of actions for the task, as depicted in Figure 101 below.

?	Urgent	Due Date	Task	Role	From (Role)	Provider
	Open		Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	KENT, TRACY (Military)
	Open		Application Ready for Review	CC/CM/MSSP	TAYLOR, JAMES (Provider)	TAYLOR, JAMES (Military)
	No		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	REDDING, OTIS (Military)
	No		Setup PAR	CC/CM/MSSP	N/A	JOBS, STEVE (Military)

Figure 101: Urgent Application Task

If CC/MSSP/CMs wish to remove the urgent status of the application, they may do so at any time during application processing using the same steps listed above. When CC/MSSP/CMs select the **Remove Urgent Status** option and click **Submit** in the **Urgent Application** window (depicted in Figure 99 above), the urgent status is removed.

5.6 Routing a Privilege Application for Primary Source Verification

After CC/MSSP/CMs review the application package and determine that it is ready for processing, they may submit the application for PSV by clicking the **PSV** button located at the bottom of the application screen, as depicted in Figure 94 above. A new window opens, and users select whether the PSV function will be performed in the CC/MSSP/CM or CVO role. After selecting the appropriate option, click **Submit**.

Figure 102: Select PSV Screen

- When users select **PSV by CC/MSSP/CM**, a new work list item is generated for all CC/MSSP/CM personnel in the facility or unit who hold PSV permissions; one of those individuals must then assume responsibility for the application prior to conducting the PSV
- When users select **PSV by CVO**, a new work list item is generated for all individuals who have PSV permissions in the designated CVO unit; one of those individuals in the CVO unit must assume responsibility for the application prior to conducting the PSV
- Users may enter a task due date if the PSV is required by a specific date
- Regardless of who performs the PSV function, the individual conducting the PSV maintains ownership of the application until PSV is completed or the application is returned to the responsible CC/MSSP/CM. The application cannot be routed for review until all required PSVs have been completed

The processes for PSV of the privilege application are addressed in the following sections.

5.7 Primary Source Verification of a Privilege Application by CC/MSSP/CM

When users select **PSV by CC/MSSP/CM** as the means for PSV, a new task is generated for all individuals who have permissions to perform PSV functions for their facility or unit. Figure 103 below depicts the new PSV task that displays when users select this option. Users may view the application from the work list by selecting **Open** from the hidden menu, or by double-clicking anywhere on the record line. The PSV task may also be reassigned to another CC/MSSP/CM by selecting **Reassign Task** from the hidden menu.

WorkList for CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @										
Work List										My Applications
Status: Open Tasks										Role: All
Tasks start date between 10/11/2011 and 10/05/2012										Filter
										Module: CM9, CM9
										User: No Providers
Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv Ex
Yes		PSV Complete/Action Required	CC/CMMSSP	CM9, CM9 (PSV)	KENT, TRACY (Military)	1st E-App	Medical Corps	09/19/2012		
No		Complete PSV	PSV	CM9, CM9 (PSV)	TAYLOR, JAMES (Military)	1st E-App	Medical Service Corps	10/05/2012		
No		PSV Complete/Action Required	CC/CMMSSP	CM9, CM9 (PSV)	REDDING, OTIS (Military)	1st E-App	Dental Corps	09/26/2012		
No		Setup PAR	CC/CMMSSP	N/A	JOBS, STEVE (Military)	1st E-App	Medical Corps	09/17/2012		09/17/2012

Figure 103: Complete PSV Task

A window opens, as depicted in Figure 104 below, with a message asking CC/MSSP/CMs if they accept responsibility for the PSV of the application. This feature was built into CCQAS to accommodate larger facilities and units, in which multiple credentials staff members share the PSV workload.

Assign PAC	
Would you like to take responsibility for the PSV of this application?	
Yes	No

Figure 104: Assign PSV Screen

After CC/MSSP/CMs click the **Yes** button, the application package opens and displays a series of tabs. The first tab is the **Provider PSV Summary** tab, as depicted in Figure 105 below. The **Provider PSV Summary** screen displays expanded sections of the privilege application that require PSV action.

Prime Source Verification (PSV) for JAMES TAYLOR										
Provider PSV Summary										Privileges
										Documents
										Comments
										Expand All Collapse All Print S
[-] Profile										
Name: TAYLOR, JAMES			Gender: Male		Date of Birth: 09/29/1983		No Photo Available			
Branch: F11 - Air Force (USAF)			Rank: GEN - General		Corps: MSC - Medical Service Corps					
AOC/Design/AFSC: 40C0A - Medical Commander - Medical Services			Accession: DA - Direct Accession							
[-] Identification										
Identification Type			Identification Number			State				
Social Security Number			100-55-4444							
[-] State License/Certification/Registration										
Type			State		Number		Field		Status	
License			Illinois		123		School Psychologist		Active	
Expires			Indefinite		ADM Waiver		No		Verified	
									No	
[-] National Certification/Registration [No Data]										
[-] Unlicensed Information										
[-] Drug Enforcement Agency (DEA) / Controlled Dangerous Substances (CDS)										
DEA Number			Type			Expiration				
No Records Found.										
[-] Professional Education										
Degree		Type		Institution		Attended From		Attended To		Completed
Masters in Public Health		Qualifying Degree		Uniformed Services University of Health Sciences		09/29/2008		Yes		Verified
										No
[-] Post Graduate Training [No Data]										
[-] Specialty										
Specialty			Sub Specialty		Specialty Level		Certified Date		Expiration Date	
Occupational Therapist			Ergonomics		Fully Trained				Verified	
									No	
[-] Malpractice Coverage [No Data]										
Print		Complete PSV		Complete PSV by CVO		Return		Print Consent		Close

Figure 105: Provider PSV Summary Screen

Important features of the **Provider PSV Summary** screen include the following:

- Sections of the application which contain no data automatically collapse and display “(No Data)” next to the section header
- All sections of the application may be expanded or collapsed by clicking **Expand All** or **Collapse All**, respectively, in the upper right-hand corner of the screen
- Individual sections of data may be expanded or collapsed by clicking [+] or [-], respectively, to the left of the section header
- Sections of the application which contain data display summary lines for each record entered
- Comments may be associated with each section of the application by clicking the empty notes icon (□); the presence of comments for that section is indicated by the filled notes icon (■)
- The presence of a **Verified** checkbox on the right-hand side of the screen indicates the sections of the application that contain data requiring PSV; after the PSV of that section is complete, CCQAS auto-populates the **Verified** checkbox with a check mark
- When processing the 1st E-application for existing Providers, none of the **Verified** checkboxes are checked, unless the PSV information for previously verified credentials was documented in the Provider’s CCQAS 2.9 credentials record. In most cases, the PSV of the 1st E-application represents the first time this information is fully documented in CCQAS
- A paper copy of the whole application package may be obtained by clicking **Print Summary** in the upper right-hand corner of the **Provider Summary** tab

CC/MSSP/CMs may perform one of several actions using the buttons provided at the bottom of any tab within the application package:

- **Print** sends the **Provider PSV Summary** screen to the printer configured for a user’s workstation
- **Complete PSV** completes the PSV process. This button is only enabled after all PSV requirements have been met for the application package
- **Return** routes the application back to CC/MSSP/CMs who have ownership of the application; the person in the role (whether it is a CVO or CC/MSSP/CM) performing the PSV is required to enter comments explaining why the application is being returned. CC/MSSP/CMs then receive a new work list item indicating that the application has been returned without a completed PSV
- **Print Consent** generates an e-signed *Statement of Consent for Release of Information and Release from Liability* form that may be used, as needed, to verify the accuracy of a Provider’s credentials information
- **Close** closes the application, which may be reopened later

Users may view the details and/or document the PSV information for each credential by selecting **Update** from the hidden menu, or double-clicking the record line.

The **PSV Information** block of each section requiring PSV should be completed as the individual credential is being verified, according to the method of verification that is used. Figure 106 below depicts the **PSV Information** section.

Any unusual circumstances surrounding the credential or the verification of the credential should be noted in the **Remarks** box. Users may edit information pertaining to the credential being verified, but they may not edit information that uniquely identifies the credential. Following PSV of the credential, users click **Save**, and then **Close**, to return to the **PSV Summary** screen. The name and position of the user who conducted the PSV is automatically recorded in the **PSV Information** block after users enter and save all PSV information.

The screenshot shows a web form titled "State License/Certification/Registration". It contains two main sections: "State License/Certification/Registration" and "Prime Source Verification (PSV) Information".

State License/Certification/Registration Section:

- Type:** License (dropdown)
- Number:** 123 (text input)
- Field:** 372 - School Psychologist (dropdown)
- Issue Date:** (calendar icon)
- Expiration Date:** (calendar icon) with a checked "Expiration Indefinite" checkbox.
- Status:** Active (dropdown)
- In Good Standing:** (checkbox)
- Remarks:** (text area)

Prime Source Verification (PSV) Information Section:

- Method:** Radio buttons for Written Correspondence, Telephone, Internet, Email.
- Contact Name:** (text input)
- Email:** (text input)
- Position:** (text input)
- Phone:** (text input)
- Institution:** (text input)
- URL:** (text input)
- Verified Date:** (calendar icon)
- Entered By Name:** JAMES TAYLOR (text input)
- Entered By Position:** (text input)
- Entered By UIC:** CD1CFV/PV (text input)
- PSV Remarks:** (text area)

At the bottom of the form are "Save" and "Close" buttons. A large "DRAFT" watermark is overlaid across the center of the form.

Figure 106: PSV Information Section

Note: In the **PSV Information** block, different data fields are required, depending on which **PSV Method** radio button users select. Users must complete as much of the **PSV Information** block as possible, according to the PSV method used.

The sections of the application that require PSV include the following:

- **State License/Certification/Registration:** All currently-held state licenses/certifications/registrations must undergo PSV each time a privilege application is processed
- **National Certification/Registration:** All currently-held national certifications/registrations must undergo PSV each time a privilege application is processed. If a Provider holds no national certifications/registrations, the **Verified** checkbox is automatically checked
- **Professional Education:** The *Qualifying Degree*, *Qualifying Certificate*, or ECFMG certification, requires a one-time PSV

- **Post-Graduate Training:** All post-graduate training records listed in this section of the application require a one-time PSV
- **Specialty:** CCQAS requires PSV of board certification for physicians and dentists who are American Board of Medical Specialties (ABMS), American Osteopathic Association (AOA), or American Dental Association (ADA) board certified. Specialties with a level of training other than *Board Certified* do not require documentation of PSV in CCQAS
- **References:** All current references listed in a Provider's application must undergo PSV each time a privilege application is processed. If a letter or other written reference was submitted, the document should be scanned into CCQAS and the name and date on the letter should be entered in the **PSV Information** section for the reference with "**Method** = *Written Correspondence*"

Note: If a PSV is performed via email and the email address of the point of contact (POC) is documented in CCQAS, Privacy Act rules dictate that the individual, whose email address is being stored in CCQAS, must be notified of this fact in writing. Until such time as CCQAS provides an automated notification capability, the user should generate an email to the POC, informing him or her that "the POC's email address information is being stored in CCQAS for quality assurance (QA) purposes."

After all required PSVs have been completed in the credentials sections of the application, the **Request Query** box on the NPDB section (refer to Figure 107 below) of the application becomes enabled. The performance of the required NPDB/ Healthcare Integrity and Protection Data Bank (HIPDB) query should then be completed according to established Service and facility procedures. All NPDB/HIPDB queries for Navy facilities are performed centrally every two days by Service-level personnel only. Air Force CVOs also perform queries for Air Force facilities, but Army and Air Force personnel may perform the queries locally. All three Services use the automated **NPDB Batch Query** function, but Army and Air Force personnel may also perform queries without using this function.

If the automated **NPDB Batch Query** function is used to perform NPDB queries, CC/MSSP/CMs must check the **Request Query** box. This action results in the inclusion of a Provider's name and information in NPDB batch queries that are generated by CCQAS to perform NPDB queries. When the system has included the Provider's name in the batch query report, it automatically unchecks **Request Query**, checks the **Query Result Pending** box, and places the corresponding date in the **Last Query Date** field. When the query results are received, CC/MSSP/CMs must manually enter the result for each query by selecting one of the options under the **Adverse Information on File** block for each record. Click the **Save** button, located on the left-hand side of the NPDB section header, to complete the **NPDB** section of the PSV process.

Figure 107: NPDB/HIPDB Section

Army and Air Force users may also perform NPDB queries manually without using the **NPDB Batch Query** function. For manual NPDB queries, Army and AF users should enter the **Last Query Date** and the results of the NPDB query directly onto the **PSV** screen and save the information by clicking the **Save** button in the upper left-hand corner of the section.

Regardless of how the query is performed, the **Last Query Date** must be entered and one of the radio buttons under **Adverse Information on File** must be selected in order to save and complete the NPDB section of the application. Any findings returned from the NPDB query should also be uploaded as a document under the **Documents** tab in the application, according to the Service and facility procedures.

A warning message displays, informing users that the new **Last Query Date** does not match the most recent entry into the Provider's credentials record. Figure 108 below depicts the warning message. Under most circumstances, this situation is expected, and an overwrite of the date in the credentials record is appropriate.

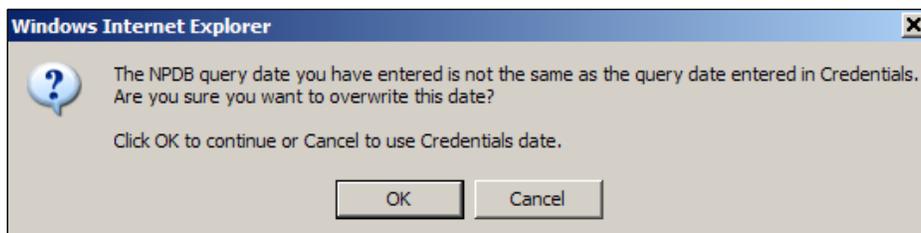


Figure 108: NPDB/HIPDB Update Warning Message

If users click **OK**, CCQAS automatically updates the **Last Query Date** in the credentials record to reflect the most recent query date.

Note: A query to the NPDB automatically initiates the query to the HIPDB. Thus, the **Last Query Date** is generally going to be the same in both the NPDB and HIPDB query sections. The requirement to perform Federation of State Medical Boards (FSMB) queries is generally

limited to Providers working in Air Force facilities with a practice history prior to January 1, 1995. Questions regarding FSMB query requirements should be directed to your supervisor.

The PSV may not be completed until all required credentials have been verified and the results of the NPDB query have been entered and saved on the **PSV** screen.

Note: CCQAS allows any NPDB query performed within the past 90 days to fulfill the NPDB query requirement for the PSV process. Thus, if the **Last Query Date** in the **NPDB** section of the privilege application is less than 90 days old, a new NPDB query is not required by CCQAS. Users may simply click **Save** to accept the previous query information and complete the PSV requirement. A new NPDB query, however, should be performed in accordance with Service policy or if specific questions arise regarding a Provider's competency or performance.

The remaining tabs in the PSV view of the privilege application, **Privileges** tab, **Documents** tab, and **Comments** tab, are similar in form and function to the tabs described in [Section 5.5.3](#), [5.5.4](#), and [5.5.5](#), respectively.

After all PSVs have been completed, and the NPDB query information has been saved, the **Complete PSV** button at the bottom of the screen is enabled. When users click the **Complete PSV** button, a message displays that confirms the completion of the PSV process, as depicted in Figure 109 below.



Figure 109: PSV Complete Message

The completion of the PSV process has the following implications:

- The application is returned to the CC/MSSP/CM who has ownership of the application
- The application is ready for the responsible CC/MSSP/CM to route it through the review process
- The credentials information entered into the electronic application is used to populate or update the Provider's permanent credentials record in CCQAS. If the Provider is newly accessed into military service or employment, the application is used to populate a new credentials record; if the Provider already has an active credentials record in CCQAS, any new information in the privilege application is used to update the credentials records already residing in CCQAS

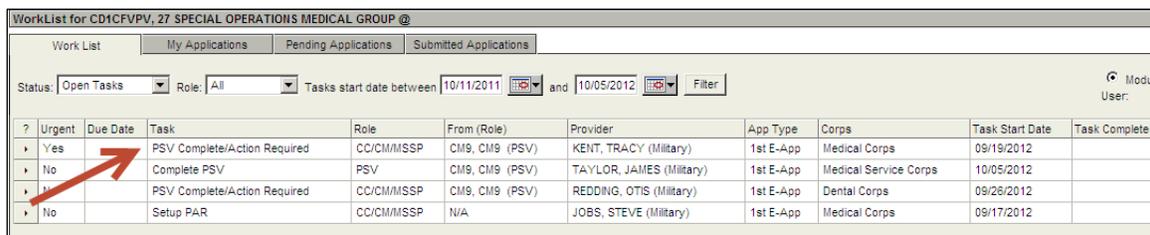
5.8 Primary Source Verification of a Privilege Application by the CVO

The process for PSV by CVOs is identical to the process described in [Section 5.7](#). The only difference is that custody of the record is transferred to the UIC associated with the CVO function for the PSV process. Following completion of the PSV, the privilege application is automatically routed back to the CC/MSSP/CM who has ownership of the application.

If the CVO and the CC/MSSP/CM at the unit share the PSV responsibility, they must do so in a manner that allows only one or the other to have custody of the application at any given time. For example, the CC/MSSP/CM may perform some of the PSV on an application, and then click the **PSV by CVO** button as the bottom of the application to submit the application directly to the CVO. After the CVO performs his or her portion of the PSV, the application may be returned to the CC/MSSP/CM by clicking the **Return** button.

5.9 Building Workflow for Application Review

Following completion of the PSV, the application is returned to CC/MSSP/CMs for routing through the application review process. CC/MSSP/CMs receive a new work list item, “**Task = PSV Complete/Action Required**”, as depicted in Figure 110 below.



Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete
Yes		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	KENT, TRACY (Military)	1st E-App	Medical Corps	09/19/2012	
No		Complete PSV	PSV	CM9, CM9 (PSV)	TAYLOR, JAMES (Military)	1st E-App	Medical Service Corps	10/05/2012	
No		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	REDDING, OTIS (Military)	1st E-App	Dental Corps	09/26/2012	
No		Setup PAR	CC/CM/MSSP	N/A	JOBS, STEVE (Military)	1st E-App	Medical Corps	09/17/2012	

Figure 110: PSV Complete/Action Required Task

Note: If the application was submitted by a CSS member or a Provider that is not requesting privileges, the application is automatically closed by CCQAS. A read-only version of the application is permanently stored in the **Applications** tab as part of the Provider’s historical record, as well as the **My Applications** tab of the responsible CC/MSSP/CM.

If a Provider is requesting clinical privileges with his or her application, CC/MSSP/CMs may initiate application routing by clicking the **Routing** button at the bottom of the screen within the Provider’s application, as depicted in Figure 111. The **Routing** button is only enabled after PSV of the application is completed.

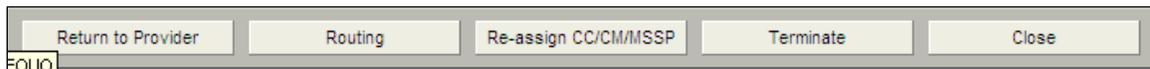


Figure 111: ‘Application Routing’ Button

The **Application Routing** screen is displayed, as depicted below. The **Summary** tab is displayed first, as depicted in Figure 112 below, and then the **UIC** tab, as depicted in Figure 113 below.

Level	Privilege Category	Task Due Date	Reviewers
Level 1 Review	Family Medicine		REVIEWER9, REVIEWER9
Privileging Authority	All Categories		PA9, PA9

Figure 112: 'Application Routing Summary' Tab

Figure 113: 'Application Routing UIC' Tab

Important features of the **Application Routing** screen include the following:

- CCQAS requires a Level 1 and PA review for all applications. CCQAS allows optional use of Levels 2–6, according to the privileging process for the individual facility or unit
- Levels 2–6 may be expanded or collapsed by clicking the [+] or [-], respectively, to the left of the section header
- For each level, the list of all available Reviewers associated with the facility or unit appears in the **Available Reviewers** box
- One or more Reviewers may be selected at each level by clicking the desired Reviewer's name, and then clicking [>] to move the Reviewer's name to the **Selected Reviewers** box. When users double-click the name, it moves to the **Selected Reviewers** box
- A Reviewer's name may be removed from the **Selected Reviewers** box by clicking the desired Reviewer's name, and then clicking [<] to move the Reviewer's name back to the **Available Reviewers** box. When users double-click the name, it moves to the **Available Reviewers** box
- When users click [>>], all Reviewers' names are moved from the **Available Reviewers** box to the **Selected Reviewers** box
- When users click [<<], all Reviewers' names are moved from the **Selected Reviewers** box to the **Available Reviewers** box
- Levels 5 and 6 are committee levels, whereby at least one committee member and one and only one committee chairperson must be selected to participate in the review process
- The names of all individuals who hold PA permissions for the facility or unit are included in the pick list for **Available PAs**
- An application is routed by selecting the appropriate **Route To** radio button, but all routing must be done in chronological order and conclude with the PA review
- The Reviewer's position is shown in parenthesis in the **Available Reviewers** box, if the **Position** field is populated in the user's CCQAS account

The following rules apply to the routing of a privilege application from one level of review to the next (refer to “processing branch clinic UICs” in [Section 16](#)):

- Level 1 review should be assigned to a Provider's clinical supervisor at each corresponding UIC; if the Provider has multiple clinical supervisors (as may be the case with Providers requesting privileging in more than one specialty), each supervisor should be assigned as a Level 1 Reviewer for the application
- An application cannot move to the next level until the current level of review has been completed. If multiple Reviewers are associated with the current level, all Reviewers must complete their review so the application can move forward
- If all Reviewers at the current level take an action of **Recommend**, the application is automatically advanced to the next level of review without being returned to the responsible CC/MSSP/CM

- If any one Reviewer elects to take an action of **Recommend with Modification**, **Do Not Recommend**, or **Return without Action**, the application is returned to the responsible CC/MSSP/CM, who then takes the appropriate action before submitting the application back into the review process
- Levels 5 and 6, the committee levels, require all committee members to complete their reviews before the committee chair renders the committee’s recommendation, and are only assigned at the Parent UIC
- The final committee recommendation for Levels 5 and 6 reflect the recommendation submitted by the committee chair, and are only done at the Parent UIC
- If an application is returned to the responsible CC/MSSP/CM, he or she may reroute the application to the appropriate level following resolution of the issue; Reviewers may be changed, added, or removed from the routing screen prior to rerouting the application

CC/MSSP/CMs select the appropriate Reviewers for Level 1, the PA, and other levels deemed appropriate for their facility or unit’s privileging process. CC/MSSP/CMs may simply click **Submit** to initiate routing. When CC/MSSP/CMs click **Submit**, the application is sent to all individuals who were selected as Level 1 Reviewers. Each Level 1 Reviewer then receives an email notification indicating he or she has a new task in his or her work list that requires action.

5.10 Tracking an Application in Review

Throughout the application review process, CC/MSSP/CMs may view the status of an application at any time without disrupting the workflow process. This is done from the **My Applications** tab. For applications currently in the review process, the “Application Status = *In Review*” is displayed, as depicted in Figure 114 below.

WorkList for CD1CFVVP, 27 SPECIAL OPERATIONS MEDICAL GROUP @								
Work List		My Applications		Pending Applications		Submitted Applications		
Provider Last Name:		Show applications that were submitted between		10/11/2011	and	10/05/2012	Filter	
?	Urgent	Provider	Application Type	Application Status	Provider Phone	App Submitted	Priv Effective	Priv Expiration
▶	Yes	ALLEN, PAUL	1st E-App	Closed	123456	10/01/2012	10/01/2012	09/30/2014
▶	No	JOBS, STEVE	1st E-App	Closed	369852	09/17/2012		09/17/2012
▶	Yes	KENT, TRACY	1st E-App	In Review	(369) 852-1470	09/19/2012		
▶	No	PETERS, ROBERT	1st E-App	Submitted	123-4567	08/27/2012		
▶	No	REDDING, OTIS	1st E-App	In Review	(320) 145-6987	09/26/2012		
▶	No	SMITH, MARK	1st E-App	Closed	1234	09/18/2012	09/18/2012	09/17/2014
▶	No	TAYLOR, JAMES	1st E-App	In Review	123456789	10/05/2012		

Figure 114: In Review Status Indicator

CC/MSSP/CMs may view a detailed summary of actions performed to date on the application by selecting **View Log/Comments** from the hidden menu of actions for the application, as depicted in Figure 115 below.

The **Task Log**, depicted in Figure 115 below, displays a summary line for every completed or pending action associated with the privilege application, in order of completion, with the most recent task listed first. Those tasks with “**Status = Closed**” have been completed. Tasks that have no date in the **Complete Date** column are still pending with “**Status = Open**”.

Provider Application						
Provider Name: TRACY KENT			Application Status: In Review			
SSN: 100-22-4444			Application Submitted: 09/19/2012			
Branch: Air Force (USAF)			Application Effective:			
Rank/Grade: Major General			Application Expiration:			
<div style="display: flex; justify-content: space-between;"> Task Log Comments </div>						
Task	Status	Start Date	Complete Date	Assignee	Role	From (Role)
Application Ready for Review	Open	10/05/2012		REVIEWERS REVIEWERS	Level 1 Reviewer	CM9 CM9 (CC/MSSP)
PSV Complete/Action Required	Closed	09/19/2012	10/05/2012	CM9 CM9	CC/MSSP	CM9 CM9 (PSV)
Complete PSV	Closed	09/19/2012	09/19/2012	CM9 CM9	PSV	CM9 CM9 (PSV)
Application Ready for Review	Closed	09/19/2012	09/19/2012	CM9 CM9	CC/MSSP	TRACY KENT (Provider)
Complete Application	Closed	09/19/2012	09/19/2012	TRACY KENT	Provider	ADMIN ADMIN

Figure 115: 'Task Log' Tab

The **Comments** tab, depicted in Figure 116 below, allows CC/MSSP/CMs to view comments entered at each step during the application process. Recommendations for application approval are also visible from this tab.

Provider Application				
Provider Name: TRACY KENT			Application Status: In Review	
SSN: 100-22-4444			Application Submitted: 09/19/2012	
Branch: Air Force (USAF)			Application Effective:	
Rank/Grade: Major General			Application Expiration:	
<div style="display: flex; justify-content: space-between;"> Task Log Comments </div>				
Role	User	Action	Comment	Date
PAC	CM9, CM9	Add Urgency	dfsdf	10/05/2012 9:55:20 AM CST
Complete	CM9, CM9	Add Urgency	dfsdf	10/05/2012 9:55:20 AM CST
PSV	CM9, CM9	PSV Complete		09/19/2012 4:02:44 PM CST
Provider	KENT, TRACY	Provider Submit		09/19/2012 11:54:40 AM CST

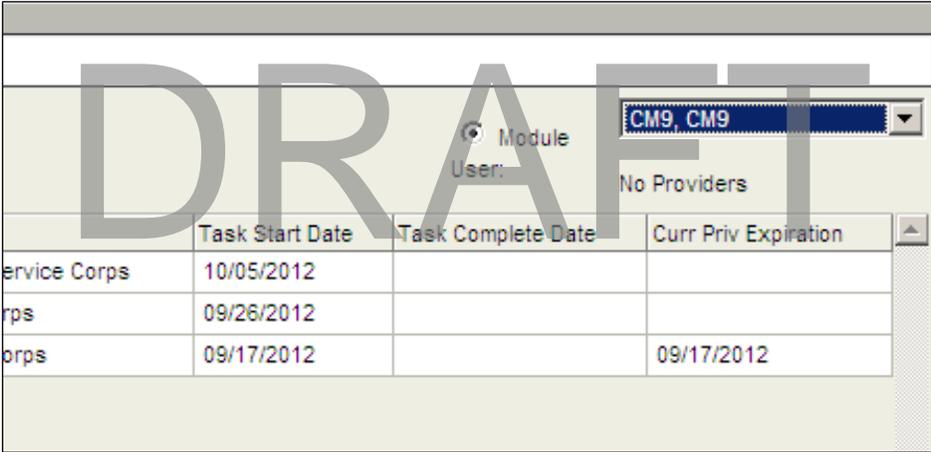
Figure 116: 'Comments' Tab

Any comments entered into CCQAS during the application review process are retained on the **Comments** tab as a permanent part of the historical record. Providers, however, cannot view the **Comments** tab at any time during or after the review process. Comments are not required for all actions made on a privilege application, so some entries on this tab may contain no comments.

5.11 Pulling an Application Out of the Review Process

CC/MSSP/CMs have the ability to retrieve privilege applications currently in the review process. This may be necessary when an application was inadvertently routed to a Reviewer inappropriate for the application, or the assigned Reviewer is unable to take necessary action on the application.

To pull an application out of the review process, CC/MSSP/CMs must first determine where the application is in the review process. CC/MSSP/CMs may determine who currently has custody of the application by examining the **Task Log** tab to identify the Reviewer(s) whose tasks are in an “*Open*” status, as depicted in Figure 114 above. After the Reviewer has been identified, CC/MSSP/CMs can open the Reviewer’s work list by selecting the individual’s name from the **User** pick list, located in the upper right-hand corner of the work list, as depicted in Figure 117 below.



	Task Start Date	Task Complete Date	Curr Priv Expiration
Service Corps	10/05/2012		
Corps	09/26/2012		
Corps	09/17/2012		09/17/2012

Figure 117: Retrieving an Application in Review

The **User** pick list contains the name of all individuals who have been assigned to take some action on the application. By selecting a user’s name, CC/MSSP/CMs gain limited access to that individual’s work list. CC/MSSP/CMs select the specific application that needs to be retrieved, open the active work list item associated with that application, and click the **Return w/out Action** button. This action results in custody of the application going back to the CC/MSSP/CM who originally routed the application for review. CC/MSSP/CMs may then change the assigned Reviewers and re-initiate the routing of the application.

Note: Return w/out Action and **Close** are the only options available to CC/MSSP/CMs when they access the work list of a Reviewer or PA. CCQAS does not permit CC/MSSP/CMs to render a recommendation decision on behalf of the task holder.

5.12 Level 1 Review of an Application

After CC/MSSP/CMs route an application for Level 1 review, each Level 1 Reviewer receives an email notification of a new task in CCQAS and a new task, “Task = *Application Ready for Review*” (depicted in Figure 118 below), is added to his or her work list. The application may be viewed from the work list by selecting **Open** from the hidden menu, or double-clicking anywhere on the record line.

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv Expiration
Yes		Application Ready for Review	Level 1 Reviewer	CM9, CM9 (CC/CM/MSSP)	KENT, TRACY (Military)	1st E-App	Medical Corps	10/05/2012		

Figure 118: Work List for a Level 1 Reviewer

The electronic privilege application is displayed as a series of tabs. Reviewers can see the same tabs and screens that CC/MSSP/CMs see during their initial review of the application, with the following important exceptions:

- A red flag (🚩) alerts Reviewers to any notes entered into the credentials portion of the application (on the **Provider Summary** tab) by a CC/MSSP/CM. Reviewers may view the notes by clicking on the red flag (🚩). Reviewers, however, cannot enter notes into the credentials portion of the application
- All information entered on the **Position** tab is read-only for Reviewers
- The **Privileges** tab contains additional data fields with a pick list, as depicted in Figure 119 below, from which Level 1 Reviewers can select delineations for endorsing each privilege item requested by the Provider

Privilege(s)	Provider	Level 1	Comments
The scope of privileges in Family Medicine includes the evaluation, diagnosis, treatment, and consultation for patients of all ages with any symptom, illness, injury, or condition. Family Medicine physicians may admit and may provide care to patients in the intensive care setting in conformance with MTF policies. They may assess, stabilize, and determine disposition of patients with emergent conditions.	Fully Competent	Not Supported	
Diagnosis and Management (D&M):			
Privilege(s)			
Obstetrical Care	Fully Competent	Fully Competent	
EKG performance and interpretation	Fully Competent	Fully Competent	
Pulmonary function testing and interpretation	Fully Competent	Fully Competent	
Basic synovial fluid analysis	Fully Competent	Fully Competent	
Mechanical Ventilatory support (invasive and noninvasive)	Fully Competent	Fully Competent	
Supervise and/or perform basic spirometry with flow/volume loops and pre/post bronchodilator if needed	Fully Competent	Fully Competent	
Cardiac stress test	Fully Competent	Fully Competent	
D & M Advanced Privileges (Requires Additional Training):			
Privilege(s)			
	Provider	Level 1	Comments

Figure 119: ‘Privileges’ Tab for a Level 1 Reviewer

Level 1 Reviewers are required to select a delineation for each privilege item requested by the Provider for those privileges that are supported at the facility or unit. Reviewers take no action on privilege items that are designated as “Not Supported.” If Reviewers elect to assign a privilege delineation that differs from that which the Provider requested, they are required to enter a comment in the **New Comment** text field, on the **Reviewer Comment** screen, explaining the reason for the difference. Figure 120 below depicts the Reviewer Comment screen.

Reviewer	Level	Date	Recommendation	Comment

Figure 120: Reviewer Comment Screen

The presence of a comment is indicated by the filled notes icon (📝) next to the disputed privilege item. Discrepancies between a Provider’s and a Level 1 Reviewer’s privilege delineation is also noted with a red flag (🚩) to alert subsequent level Reviewers of the change.

Reviewers may also enter a comment against any privilege item without changing the delineation requested by the Provider, by clicking on the empty notes icon (📝) for the item and entering and saving a comment. The entry of a comment by a Reviewer, even if the privilege designation is not changed, results in the **Recommend** option being disabled, and the application must be returned to the responsible CC/MSSP/CM, rather than forwarded in the review process.

Note: If a Provider requests privileges in multiple specialties, several Level 1 Reviewers will likely be assigned to review the requested privileges. In this situation, each Level 1 Reviewer should endorse only the privileges in the specialty that he or she is qualified to review, and leave the remaining privileges for other specialties at the default value (which is the same as that requested by the Provider) for the other Level 1 Reviewer to endorse. Multiple Level 1 Reviewers may also endorse the same set of privileges. Each Reviewer should enter his or her own endorsement and comments, but if the two Reviewers differ in their recommendations regarding a particular privilege item, the privilege item is flagged (🚩) and the privilege delineation field is blank for subsequent levels of review, and the PA will be required to enter a privilege delineation during the Level 7 review.

After reviewing and assigning privilege delineations, each Level 1 Reviewer then submits his or her overall recommendation for the privilege application by selecting one of the following buttons at the bottom of the screen:

- **Recommend** indicates that the Reviewer recommends approval of the Provider's request for privileges with the delineations he or she has entered
- **Recommend with Modification** indicates that the Reviewer has elected to enter a delineation or delineations that may be different from what the Provider has requested, or has entered comments related to individual privileges. If this action is selected, the Reviewer is required to enter general comments explaining the reason for his or her choice of endorsement
- **Do Not Recommend** indicates that the Reviewer does not support the granting of clinical privileges to the Provider, regardless of any changes he or she may have made on the **Privilege** tab. If this action is selected, the Reviewer is required to enter comments explaining his or her reason for not recommending the Provider for privileges. This option has negative repercussions for the Provider and should therefore be selected only after serious, thorough, and thoughtful consideration of all factors related to the Provider and his or her application
- **Return without Action** routes the application back to the responsible CC/MSSP/CM without a recommendation. If this action is selected, the Reviewer is required to enter comments explaining his or her reason for returning the application. This is usually the appropriate choice if a Reviewer, rather than create an *adverse privileging action* with a **Do Not Recommend** action, prefers to return the application to the CM/MSSP/CC, pending satisfaction of issues regarding the application or with the Provider
- **Close** closes the application, which the Reviewer may then reopen at a later time to complete the review

After Reviewers select **Recommend**, **Recommend with Modification**, **Do Not Recommend**, or **Return without Action**, the application is either returned to the CC/MSSP/CM or advanced to the next level of review. Reviewers are given an opportunity to enter comments with their submission, and comments are required if they selected either **Recommend with Modification**, **Do Not Recommend**, or **Return without Action**. All comments entered during the review process became a permanent part of the privileging application. Figure 121 below depicts the **Reviewer Recommendation** screen, where reviews enter their comments.

The screenshot shows a web-based form titled "Reviewer Recommendation". The form has two main sections: "Recommendation:" and "Comments:". The "Recommendation:" section contains the text "Recommend w/ Modification". The "Comments:" section is a text area with the text "Review of training requirements for cardiovascular privileges is required". At the bottom of the form, there are two buttons: "Submit" and "Cancel".

Figure 121: Reviewer Recommendation Screen

Note: CC/MSSP/CMs, other Reviewers, and PAs can view comments entered during a review process, but Providers cannot view these comments either during or after the processing of their application.

If multiple Reviewers are assigned as Level 1 Reviewers, each one must issue a **Recommend** vote on the application for it to advance to the next level of review. If any Level 1 Reviewer issues a **Recommend with Modification**, **Do Not Recommend**, or **Return without Action** vote, the application is returned to the CC/MSSP/CM who holds responsibility for the application. The **Task = Application Returned/Action Required** appears in his/her work list, as depicted in Figure 122 below.

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv Expiration
Yes		Application Returned/Action Required	CC/CM/MSSP	REVIEWER9, REVIEWER9 (Level 1 Reviewer)	KENT, TRACY (Military)	1st E-App	Medical Corps	10/05/2012		
No		Complete PSV	PSV	CM9, CM9 (PSV)	TAYLOR, JAMES (Military)	1st E-App	Medical Service Corps	10/05/2012		
No		PSV Complete/Action Required	CC/CM/MSSP	CM9, CM9 (PSV)	REDDING, OTIS (Military)	1st E-App	Dental Corps	09/26/2012		
No		Setup PAR	CC/CM/MSSP	N/A	JOBS, STEVE (Military)	1st E-App	Medical Corps	09/17/2012		09/17/2012

Figure 122: Application Returned/Action Required Task

After CC/MSSP/CMs open the work list item, they use the **Comments** tab to identify the Reviewer's concerns, as depicted in Figure 123 below.

Role	User	Action	Comment	Date
Level 1 Reviewer	REVIEWER9, REVIEWER9	Return to PAC	The Reviewer selected Recommend with Modification. Please review the issue and re-route to continue processing.	10/05/2012
View Comment	REVIEWER9, REVIEWER9	Recommend w/ Modification		10/05/2012
Recommendation Detail	CM9	Add Urgency	dfsdf	10/05/2012
Recommendation Count	CM9	PSV Complete		09/19/2012
PSV	CM9, CM9	PSV Complete		09/19/2012
Provider	KENT, TRACY	Provider Submit		09/19/2012

Figure 123: 'Comments' Tab of a Returned Application

Comments entered by a Reviewer concerning specific privilege delineations may be viewed by selecting **Recommendation Detail** from the most hidden menu of actions for the Reviewer's recommendation record, as depicted in Figure 124 below.

Credentialing	Privileging	Risk Management	Adverse Actions	Reports	System	Help
Reviewer Recommendations/Comments						
Provider Name: TRACY KENT			Application Status: In Review			
SSN: 100224444			Application Submitted: 09/19/2012			
Branch: Air Force (USAF)			Application Effective:			
Rank/Grade: Major General			Application Expiration:			
Reviewer Name: REVIEWER9, REVIEWER9						
Privilege Location: 27 SPECIAL OPERATIONS MEDICAL GROUP @						
Privilege Category: Family Medicine						
Privilege: Obstetrical Care						
Provider Designation: Fully Competent						
Reviewer Recommendation: With Supervision						
Comments: test						

Figure 124: Recommendation Detail Screen

CC/MSSP/CMs are responsible for facilitating resolution of a Reviewer's concerns to enable the application to move forward. If it is determined that changes need to be made to a Provider's application package, CC/MSSP/CMs return the application to the Provider by clicking the **Return to Provider** button. CC/MSSP/CMs must enter comments or instructions for the Provider as well as unlock the appropriate sections of the application where the Provider needs to make edits, as depicted in Figure 125 below.

Return to Provider	
Select the sections that you wish to unlock for the provider to provide more information:	
<input type="checkbox"/> Profile/Position	<input type="checkbox"/> Continuing Education
<input type="checkbox"/> Identification	<input type="checkbox"/> Contingency Training
<input type="checkbox"/> Contact	<input type="checkbox"/> Practice History
<input type="checkbox"/> License/Certification/Registration	<input type="checkbox"/> Health Status
<input type="checkbox"/> DEA/CDS	<input type="checkbox"/> References
<input type="checkbox"/> Professional Education/Training	<input type="checkbox"/> Work History
<input type="checkbox"/> Specialty	<input type="checkbox"/> Privileges
<input type="checkbox"/> Affiliation	
Comments/Instructions:	
<input type="text"/>	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 125: Return to Provider Screen

The Provider then receives an email notification and a new work list item, indicating that his or her application needs to be edited. The Provider performs the requested edits, and e-signs the application to resubmit it.

CM/MSSP/CCs may then reroute the application through the Level 1 review if these Reviewer(s) wish to see the revised application package. Once a **Recommend** decision has been rendered by all assigned Level 1 Reviewers, the application automatically advances to the next assigned level of review. CM/MSSP/CCs may also reroute the application directly to the next assigned level of review, by selecting the appropriate **Route to** radio button on the **Routing** screen, as depicted in Figure 113 below.

After a Reviewer completes an application review task, the application may be viewed in read-only format from the **Application** tab. The Reviewer, however, may not make further edits to privilege delineations unless the CC/MSSP/CM who is responsible for the application routes it back to him or her for a second review.

5.13 Levels 2, 3, and 4 Review of an Application

After an application has cleared the Level 1 review, it advances to the next level of review assigned to the application. The review process at subsequent levels of review is similar to that described in the previous sections for the Level 1 review, with one exception. Levels 2, 3, and 4 Reviewers do not have the capability to select a delineation for individual privilege items in the electronic application, but they do have full visibility of all comments entered into the application by the CC/MSSP/CM, and the privilege delineations and comments entered by the Level 1 Reviewer.

The red flag (🚩), depicted in Figure 126 below, denotes a change made to a privilege delineation by a Level 1 Reviewer. Reviewers at subsequent levels of review may click on the (📝) to the right of the privilege item to view the Level 1 Reviewer's rationale for changing the privilege delineation. More information regarding how the disputed privilege request was resolved is available by examining the **Comments** tab.

Provider	Level 1	Comments
Fully Competent	Fully Competent	📝
Not Requested	Not Requested	🚩
Not Requested	Not Requested	📝
Not Requested	Not Requested	📝
Not Requested	Not Requested	📝
Not Requested	Not Supported	📝
Not Requested	Not Requested	📝

Figure 126: Red Flag Icon for Review Levels 2-6

Levels 2, 3, and 4 Reviewers may also enter their own comments against any privilege item, by clicking on the empty notes icon (📝) or filled notes icon (📝) for the item. Their comments are then added to other Reviewer comments already entered for the privilege item. The entry of a comment disables the **Recommend** option, and the application must be returned to the CC/MSSP/CM, rather than being forwarded in the review process.

After reviewing the privilege application and comments left by the previous levels of review, the Level 2, 3, or 4 Reviewers submit their recommendation decisions on the application as a whole. If all Reviewers at a given level render a **Recommend** decision, the application automatically advances to the next assigned level of review. If any Reviewer at the assigned level issues a **Recommend with Modification**, **Do Not Recommend**, or **Return without Action** vote, the application is returned to the CC/MSSP/CM who holds responsibility for the application. All Reviewers are given the opportunity to enter comments with their recommendations, which then become a permanent part of the privileging application.

5.14 Levels 5 or 6 (Committee) Review of an Application

Levels 5 and 6 in the review process are reserved for committee review of privilege applications. Levels 5 and 6 consist of two layers of review within each level to accommodate reviews by each of the committee members, followed by a review by the committee chairperson. After an application is routed for committee review, each committee member assigned to review the application receives an email notification and a new task, “**Task = Application Ready for Review.**” After all committee members have performed their review and submitted their individual recommendations, the committee chairperson receives his or her email notification and a new work list item to review the application. The committee chair can view a tally of all recommendation decisions rendered by the committee members and prior levels of review by selecting **Recommendation Count** from the hidden menu of actions on the **Comments** tab, as depicted in Figure 127 below.



Figure 127: Recommendation Count Menu Item

The **Recommendation Count** screen tallies recommendations made at each level of review, as depicted in Figure 128 below.

Reviewer Level	Recommend	Recommend w/Modification	Do Not Recommend
Level 1 Reviewer	1	1	0
Level 2 Reviewer	1	0	0
Level 5 Reviewer	2	0	0
Totals	4	1	0

Figure 128: Recommendation Count Screen

Note: The total count may exceed the number of Reviewers who rendered a recommendation decision on the application. For example, if a Level 1 Reviewer initially selected **Recommend with Modification** during the first review, and then **Recommend** following the Provider's revision of the application, both decisions would be reflected in the final count. The committee chair should carefully review all comments associated with **Recommend with Modification** or **Do not Recommend** decisions prior to rendering a final committee decision to ensure the issues raised with the application are understood and resolved.

After the committee chair evaluates the individual recommendations of the committee members, he or she then submits the final committee recommendation.

The review process at Levels 5 and 6 are similar to that described in the previous section for Levels 2, 3, and 4 in all other respects. Level 5 and 6 Reviewers do not have the capability to enter a delineation for individual privilege items in the electronic application, but they have full visibility of all comments entered into the application by the CC/MSSP/CM, the privilege delineations assigned by the Level 1 Reviewer and his or her comments, and any other comments entered into the electronic application at Levels 2, 3, and 4. They may also enter their own comments against a specific privilege item or when rendering a recommendation decision on the application as a whole. Level 5 or 6 review are complete after the committee chairs submit their recommendation.

5.15 Review of an Application by the PA

The PA performs the final review of the application. PA review is required for all applications. The PA provides the final determination of whether the application is approved or disapproved, and only one PA may be assigned to approve an electronic application.

After an application is routed for PA review, the PA assigned to review the application receives an email notification and a new task, "**Task** = *Application Ready for Review.*" After the PA opens the task, the application is displayed, as depicted in Figure 129 below.

The screenshot displays the 'Provider Application Review' interface for a provider named 'DEANAM PERCE, 27294624'. The interface is divided into several sections:

- Provider Summary:** Shows the provider's name and ID.
- Privilege Category:** Set to 'General Surgery (A)'. A dropdown menu shows 'Cardiovascular Surgery (A)' and 'General Surgery (A)'.
- Privileges List:** A table listing various clinical privileges with columns for 'Privileges', 'Provider', 'Level 1', 'Privileging Authority', and 'Comments'.

Privileges	Provider	Level 1	Privileging Authority	Comments
Category I clinical privileges	Fully Competent	Fully Competent	Fully Competent	
Category II clinical privileges	Fully Competent	Fully Competent	Fully Competent	
Category III clinical privileges	Fully Competent	Fully Competent	Fully Competent	
Category IV clinical privileges	Fully Competent	Fully Competent	Fully Competent	
Statistical Subspecialty	Fully Competent	Fully Competent	Fully Competent	
General Surgery Privileges	Fully Competent	Fully Competent	Fully Competent	
General Surgery	Fully Competent	Fully Competent	Fully Competent	
Cardiac Surgery	Not Requested	Not Requested	Not Requested	
Orthopedic Surgery	Not Requested	Not Requested	Not Requested	
Otolaryngology	Not Requested	Not Requested	Not Requested	
Ophthalmology	Not Requested	Not Requested	Not Requested	
Neurosurgery	Not Requested	Not Requested	Not Requested	
Plastic Surgery	Not Requested	Not Requested	Not Requested	
Thoracic Surgery	Not Requested	Not Requested	Not Requested	
Urology	Not Requested	Not Requested	Not Requested	
Vascular Surgery	Not Requested	Not Requested	Not Requested	
Colorectal Surgery	Not Requested	Not Requested	Not Requested	
Moderate sedation	Fully Competent	Fully Competent	Fully Competent	
- Actions:** Buttons for 'Approve', 'Approve w/ Modification', 'Disapprove', 'Return to Action', and 'Close'.

Figure 129: 'Privileges' Tab for Privileging Authority Review

PAs can see the same tabs and screens that the previous Reviewers saw during their review of the application, with the following differences:

- The **Privileges** tab contains additional data fields with a drop-down pick list of delineations for the PA's use in endorsing each privilege item requested by the Provider
- The PA submits final approval/disapproval of the application

PAs are required to assign a delineation for each privilege item requested by a Provider. For their convenience, however, the delineations are already defaulted to those entered by the Level 1 Reviewer, so keystrokes are generally required only if a PA wishes to override the recommendations previously made. When a delineation field is blank and flagged (resulting from a difference in delineation entered by one or more Level 1 Reviewers), PAs are required to enter the delineation for which the Provider's application will be approved. As is the case with the Level 1 Reviewer, if a PA elects to assign a privilege delineation that differs from that which the Provider requested, the PA is required to enter a comment explaining the reason for the difference. Discrepancies between the Provider's and the PA's privilege delineation are also noted with a red flag (🚩).

Note: PAs may either select a set of privileges from the **Privilege Category** pick list or scroll continuously through the **Privileges** tab to review all privileges from all categories.

PAs have full visibility of all the Reviewers' recommendations and comments entered into the application during the review process. Comments pertaining to specific privilege items may be viewed by clicking the filled note icon (📌) next to the privilege item.

As with previous levels of review, the **Comments** tab provides access to all comments entered during the review process. Application-level comments are displayed directly on the **Comments** tab in abbreviated form, and may also be viewed in their entirety by selecting **View Comment** from the hidden menu. Detailed comments entered for individual privilege items may then be viewed by selecting **Recommendation Detail**, and a tally of all recommendation decisions rendered may be viewed by selecting **Recommendation Count** from the hidden menu of actions.

After reviewing the privilege application, recommendations, and comments from previous levels of review, a PA submits his or her decision by clicking one of the following buttons at the bottom of the screen:

- **Approve** should be selected if a PA wants to approve a Provider's request for privileges with no changes to the delineations, as indicated on the **Privileges** tab
- **Approve with Modification** should be selected if a PA changed a delineation or may have entered comments pertinent to a specific privilege. If this action is selected, the PA is required to enter a general, application-level comment
- **Disapprove** should be selected if a PA wants to disapprove a Provider's application for clinical privileges, regardless of any changes that may have been made on the **Privileges** tab. If this action is selected, the PA is required to enter comments explaining his or her reason for not approving the Provider for privileges

- **Return without Action** returns the application to the CC/MSSP/CM without any approval action by the PA. If this action is selected, the PA is required to enter comments explaining his or her reason for returning the application
- **Close** closes the application, which the PA may then reopen at a later time to complete the review

Since a PA is the last level in the review process, regardless of which action he or she selects, the application is routed back to the CC/MSSP/CM. The only action that may require rerouting of the application back to the PA is **Return without Action**. A PA is given an opportunity to enter comments with his or her submission, and comments are required if **Approve with Modification, Disapprove, or Return without Action** is selected. All comments entered by a PA during the review process become a permanent part of the privileging application. Figure 130 below depicts the **PA Decision** screen.

Reviewed	UIC	Name	Category
<input checked="" type="checkbox"/>	CD1CFVPV	27 SPECIAL OPERATIONS MEDICAL GROUP @	Endodontics

Figure 130: PA Decision Screen

Note: CC/MSSP/CMs and other Reviewers can view comments entered during the review process, but Providers cannot view these comments either during or after the application review process.

After an application has been returned to the assigned CC/MSSP/CM, the PA continues to have access to the application in read-only format from the **Application** tab. The PA, however, cannot make further edits to privilege delineations unless the CC/MSSP/CM routes the application back to him or her for a second review.

5.16 Completing the Application Approval Process

After a PA submits his or her final decision to approve the application for clinical privileges, the application is routed back to the owning CC/MSSP/CM. The CC/MSSP/CM receives a new

work list item, “**Task = PA Decision Complete/Action Required.**” The CC/MSSP/CM completes the approval process by routing approval notifications to the Provider, Level 1 Reviewers, and other individuals involved in the review process that should be notified. The notification process is initiated by opening the task and selecting **Notifications** at the bottom of the screen, as depicted in Figure 131 below.

Note: The automated notification functionality in CCQAS should be used in cases where a Provider’s application for clinical privileges is approved by a PA. In situations where a PA disapproves a Provider’s application, communications with the Provider should be handled outside CCQAS, and Service and MTF protocols should be followed.



Figure 131: 'Notifications' Button

The **Notification Routing** screen appears, as depicted in Figure 132 below.

 A screenshot of a web application window titled "Notification Routing - OTIS REDDING, 100887474". The window has a light beige background and a thin border. At the top, there is a "Provider" section with a "Notify Provider?" label and two radio buttons for "Yes" (selected) and "No". Below this is a text input field for "Acknowledgement Due(days)" containing the number "3". A large, semi-transparent "DRAFT" watermark is overlaid across the center of the screen. Below the acknowledgment field is a section for "Level 1 Reviewers" which is expanded. It contains two columns: "Available Users" and "Selected Users". The "Available Users" column lists "CM9, CM9 REVIEWERS9, REVIEWER9". Between the columns are four arrow buttons: a right arrow (>), a double right arrow (>>), a left arrow (<), and a double left arrow (<<). Below the "Level 1 Reviewers" section are five collapsed sections: "Level 2 Reviewers", "Level 3 Reviewers", "Level 4 Reviewers", "Level 5 Committee Chair", and "Level 6 Committee Chair". At the bottom of the window, there are two buttons: "Submit" and "Cancel".

Figure 132: Notification Routing Screen

Important features of the **Notification Routing** screen include the following:

- CC/MSSP/CMs are required to select the appropriate radio button for **Notify Provider**, but notification at other review levels is not required by CCQAS
- If “**Notify Provider = Yes**” is selected, CC/MSSP/CMs are required to enter the number of days in which the Provider acknowledgment is due
- Levels 2–6 may be expanded or collapsed by clicking the [+] or [-] respectively, to the left of the section header
- For each level, the list of all Reviewers appears in the **Available Reviewers** box
- One or more Reviewers may be selected at each level, by clicking on desired Reviewer’s name, and then clicking [>] to move the Reviewer’s name to the **Selected Reviewers** box. When users double-click the name, it moves to the **Selected Reviewers** box
- A Reviewer’s name may be removed from the **Selected Reviewers** box by clicking the desired Reviewer’s name, and then clicking [<] to move the Reviewer’s name back to the **Available Reviewers** box. When users double-click the name, it moves back to the **Available Reviewers** box
- When users click [>>], all Reviewers’ names move from the **Available Reviewers** box to the **Selected Reviewers** box
- When users click [<<], all Reviewers’ names move from the **Selected Reviewers** box to the **Available Reviewers** box

After CC/MSSP/CMs select the desired recipients for the approval notification, they click **Submit**. A notification email is then distributed to all recipients simultaneously. If a Provider is required to acknowledge the approved application, he or she receives a new work list item with “**Task = Privileging Notification**”, as well as the email notification. Providers should acknowledge the award of privileges within the specified number of days; otherwise, they receive a daily email reminder to do so after the specified number of days have passed. Reviewers are not required to acknowledge the approved application, and will receive only one email notification. They are not required to take any further action regarding the application. To close the notification task in their work list, Providers merely have to open the task, and then select **Close** from the list of options at the bottom of the application record.

When Providers receive a new work list item with “**Task = Privileging Notification**”, they may acknowledge the approved application by first opening the task. At the top of the **Provider Summary** tab is a statement regarding the type of appointment and privileges the Provider has been granted, and instructions on acknowledging the appointment. Figure 133 below depicts the **Summary** tab statement.

Providers may view the list of awarded privileges by clicking the word “**here**” displayed in the acknowledge message as green text.



Figure 133: Provider ‘Acknowledge’ Button on Summary Page

The view-only Privileged Provider Information Report is then displayed, as depicted in Figure 134 below. The Privileged Provider Information Report may be printed by clicking the **Print** button at the bottom of the screen. If Providers click **Close**, the acknowledgement statement is displayed again.

My Applications System Submit Trouble Ticket			
PRIVILEGED PROVIDER INFORMATION REPORT			
SERVICE: Air Force			
UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @			
PROVIDER	SSN	MILITARY/CIVILIAN	
REDDING, OTIS	XXX-XX-7474	Military	
ORGANIZATION UNIT	MILITARY/CIVILIAN	ADMITTING	TYPE OF PRIVILEGES
27 SPECIAL OPERATIONS MEDICAL GROUP @	Military	No	
PRIVILEGE CATEGORY: Endodontics			
Version 1.0			
Dental providers requesting privileges in this specialty must also request privileges in General Dentistry.			
Scope			
PRIVILEGE ITEM (S)		REQUESTED	APPROVED
The scope of privileges in endodontics includes the ability to evaluate, diagnose, consult, manage, and provide therapy and treatment for patients of all ages presenting with conditions or disorders involving the dental pulp and periapical tissues of the teeth. Endodontists may assess, stabilize, and determine disposition of these patients.		Fully Competent	Fully Competent
Diagnosis and Management (D&M):			
Procedures:			
PRIVILEGE ITEM (S)		REQUESTED	APPROVED
Complicated nonsurgical root canal therapy for all permanent teeth		Fully Competent	Fully Competent
Surgical root canal therapy including root-end resection, root-end filling, decompression, root resection, bicuspidization, hemisection, perforation repair, trephination, and incision and drainage		Fully Competent	Fully Competent
Pulpal regeneration (immature permanent tooth with a necrotic pulp)		Fully Competent	Fully Competent
Osseous grafts (intraoral autografts, allografts and alloplasts)		Fully Competent	Fully Competent

Figure 134: Privileged Provider Information Report

When Providers click the **Acknowledge** button (refer to Figure 133 above), a page with all the statements regarding duties and responsibilities, and compliance with Service/MTF regulations and staff by-laws displays, as depicted in Figure 135 below.

Providers must select **I accept**, or **I do not accept**. When either option is selected, the Provider’s work list item is closed.

Acknowledgment

- Based upon the recommendations of the credentials committee, I hereby award you a Medical Staff Appointment with privileges at CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @, CANNON AFB effective, 10/05/2012 and expiring 10/04/2014. As a member of the medical staff, you are expected to participate fully in all accompanying responsibilities, functions and duties within the medical staff IAW Medical Staff Bylaws. You are not authorized to exercise any privileges that were not granted by the Privileging Authority.
- The renewal of privileges is based upon the demonstration of current clinical competency. Quality Improvement/Quality Assessment monitoring and evaluation processes that include data reflecting productivity, peer reviews, medication use, surgical infection rates, element-specific reviews, and timely record completion will be obtained and used in the performance-based privileging process.
- To help maintain the currency of your credentials file, it is your responsibility to forward information to the Credentials Office concerning CPR/ACLS, continuing medical education, changes required in privileges, licensure status, board certification, and malpractice actions. The credentials file is available for your review and periodic review of its contents is encouraged.
- Please acknowledge receipt of this notification by completing the endorsement below within 14 days. If you do not concur with the award of privileges and medical staff appointment, you may submit an appeal as outlined in AFI 44-119, Clinical Performance Improvement.

Accept

I do not concur and will submit an appeal as outlined in AFI 44-119.

Complete Acknowledgment Cancel

Figure 135: Provider “Acknowledgment” Page



Figure 136: Provider Acknowledgement Notification

Reviewers who are included in the notification routing process also receive new work list items for “**Task = Privileging Acknowledgement**”. Reviewers are not required to take action on this task, but the task remains in “*Open*” status on their work list, until they open the task. After they view the awarded privileges and click **Close**, the status of the task changes to “*Completed*”.

A Provider’s acknowledgment is returned to a CC/MSSP/CM in the form of a new work list item with “**Task = Privileging Acknowledgment Received**”. When CC/MSSP/CMs open the work list item, the Provider acknowledgment is visible at the top of the **Provider Summary** page, as depicted in Figure 137 below. CC/MSSP/CMs then click the **Complete** button, which ends the automated processing of the privilege application, regardless of whether the Provider chooses to accept the awarded privileges or not. If the Provider chooses not to accept the PA’s decision and wants to submit an appeal, the appeal process is handled outside of the system.

Provider Application Review - OTIS REDDING, 100887474

Provider Summary Position Privileges Documents Comments [Expand All](#) [Collapse All](#) [Print Summary](#)

Provider Acknowledgment: Accept

Complete

Figure 137: ‘Complete’ Button

After CC/MSSP/CMs click the **Complete** button, the application review process is closed. The assigned CC/MSSP/CM, PA, Reviewers, and Provider may access a read-only version of the approved application from the **Applications** tab at any time, where the **Application Status** is now **Closed**, as depicted in Figure 138 below.

Urgent	Provider	Application Type	Application Status	Provider Phone	App Submitted	Priv Effective	Priv Expiration
Yes	ALLEN, PAUL	1st E-App	Closed	123456	10/01/2012	10/01/2012	09/30/2014
No	JOBS, STEVE	1st E-App	Closed	369852	09/17/2012	09/17/2012	09/17/2012
Yes	KENT, TRACY	1st E-App	In Review	(369) 852-1470	09/19/2012		
No	PETERS, ROBERT	1st E-App	Submitted	123-4567	08/27/2012		
No	REDDING, OTIS	1st E-App	Closed	(320) 145-6987	09/26/2012	10/05/2012	10/04/2014
No	SMITH, MARK	1st E-App	Closed	1234	09/18/2012	09/18/2012	09/17/2014
No	TAYLOR, JAMES	1st E-App	In Review	123456789	10/05/2012		

Figure 138: 'My Applications' Tab with a Closed Application

5.17 The Updated Provider Credentials Record

Following the completion of the PSV process, the credentials information entered into the electronic application is used to populate or update a Provider's permanent credentials record in CCQAS. If the Provider is newly accessed into military service or employment, the application is used to populate a new credentials record. For a Provider who has an active credentials record in CCQAS at the time the PSV was completed, any new credentials information in the application is used to update the credentials record residing in CCQAS. At that point, the updated credentials record is available to any credentials staff member who has appropriate permissions to access the Credentialing module for his or her unit. The Provider's credentials record of CCQAS is explained in detail in [Section 6](#).

The PA's approval of the application results in the update of the **Privileges** section of the Provider's credentials record, as depicted in Figure 139 below. Following this update, the awarded privileges and the assignment information from the **Position** tab of the approved application then appears in the **Privileges** section. The **Privileges** section of a Provider's credentials record contains a summary record line for each privilege application that was approved.

UIC	Status	App Type	Provider Category	Corps	Military/Civilian	Type of Appointment	Type of Privileges	App Date	Effective Date	Expiration Date
CD1CFVPV	Active	1st E-App	Dentist	DC	MIL			09/26/2012	10/05/2012	10/04/2014

Figure 139: Privileges Section in the Credentials Record

Note: Only completed privilege applications approved for this UIC appear in the **Privileges** section of a Provider's credentials record. Past and present privileges awarded at other UICs may be viewed under the **Documents** section of the credentials record, by selecting the **PAR/Snapshots** radio button. [Section 6](#) provides a detailed description of the Provider credentials record.

To view the approved privileges, select **View Privileges** from the hidden menu of actions for the privilege application. This returns the Privileged Provider Information Report, as depicted in Figure 140 below.

Note: Prior to processing a Provider's first E-application, the **Privileges** section of the Provider's credentials record is empty. The **Privileges** section of the credentials record can only be populated by processing electronic privilege applications through the CCQAS workflow.

**** FOUO ****

Name: REDDING, OTIS, Appointment: Priv. Granted Date: 05 Oct 12
 Mil/Civ: Military Corps: DC Privileges: Priv. Expiration Date: 04 Oct 14

PRIVILEGED PROVIDER INFORMATION REPORT

SERVICE: Air Force		
UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @		
PROVIDER REDDING, OTIS	SSN XXX-XX-7474	MILITARY/CIVILIAN Military
ORGANIZATION UNIT 27 SPECIAL OPERATIONS MEDICAL GROUP @	MILITARY/CIVILIAN ADMITTING Military	TYPE OF PRIVILEGES No

PRIVILEGE CATEGORY: Endodontics
 Version 1.0
 Dental providers requesting privileges in this specialty must also request privileges in General Dentistry.
 Scope

PRIVILEGE ITEM (S)	REQUESTED	APPROVED
The scope of privileges in endodontics includes the ability to evaluate, diagnose, consult, manage, and provide therapy and treatment for patients of all ages presenting with conditions or disorders involving the dental pulp and periapical tissues of the teeth. Endodontists may assess, stabilize, and determine disposition of these patients.	Fully Competent	Fully Competent

Diagnosis and Management (D&M):
 Procedures:

PRIVILEGE ITEM (S)	REQUESTED	APPROVED
Complicated nonsurgical root canal therapy for all permanent teeth	Fully Competent	Fully Competent
Surgical root canal therapy including root-end resection, root-end filling, decompression, root resection, bicuspidization, hemisection, perforation repair, trephination, and incision and drainage	Fully Competent	Fully Competent
Pulpal regeneration (immature permanent tooth with a necrotic pulp)	Fully Competent	Fully Competent
Osseous grafts (intraoral autografts, allografts and alloplasts)	Fully Competent	Fully Competent

Other (Facility- or provider-specific privileges only):

Figure 140: Privileged Provider Information Report

Based on the privilege approval date, CCQAS automatically calculates the privilege expiration date for one year for initial appointments, or two years for regular appointments. CC/MSSP/CMs may view and edit these expiration dates in the **Privileges** section of a Provider's credentials record by selecting **Edit** from the hidden menu of actions for the application. The **Provider Position** page opens, as depicted in Figure 141 below.

Click **Generate Reprinted PDF Snapshot** to view the read-only list of approved privileges. Click **Close** to return to the **Privileges** section.

The screenshot shows a web form titled "Provider Privileges". The form contains the following fields and controls:

- Provider Category:** A dropdown menu with "Dentist" selected.
- Duty Section:** A text input field.
- Duty Phone:** A text input field.
- Date Reported to Current Assignment:** A date picker showing a calendar icon.
- Rotation/Permanent Change of Station Date:** A date picker showing a calendar icon.
- Effective Date:** A date picker showing "10/05/2012" and a calendar icon.
- Type of Privileges:** A dropdown menu.
- Type of Appointment:** A dropdown menu.
- Privilege Expiration:** A date picker showing "10/04/2014" and a calendar icon.
- Staff Appointment Expiration:** A date picker showing "10/04/2014" and a calendar icon.

At the bottom of the form, there are three buttons: "Save", "Close", and "Generate Reprinted PDF Snapshot".

Figure 141: Provider Position Screen

In prior versions of CCQAS, the **Privilege Expiration Date** and **Staff Appointment Date** were updated in the **Assignments** section of the credentials record. These fields are now read-only in the **Assignments** section and reflect those dates entered on the **Privileges** tab. The **CSS Review Date** remains active in the **Assignments** section since CSS members are not eligible for privileging. The expiration dates entered on the **Position** screen also dictates when the renewal notices are generated, according to the time period entered on the **Command Parameters** screen (refer to [Section 10](#)).

Note: The **Privileges** section of a Provider's credentials record is only active or visible for Providers who are eligible for privileging. There is no **Privileges** tab in credentials for clinical support staff or non-privileged Providers.

The final menu option available for applications in the **Privileges** section is **Request Civilian Application**. This menu item is intended to allow CC/MSSP/CMs to generate an electronic privilege application for a military Provider and (typically) a reservist or guardsman who also works in the same unit or facility as a contract Provider.

5.18 Managing Privileging Workload: The PAC Supervisor Role

In larger facilities where multiple credentials staff members manage the credentialing and privileging workload for one or more UICs, the "PAC Supervisor" role may be assigned to a CC/MSSP/CM who has oversight responsibility of the credentials staff. The individual assigned the "PAC Supervisor" role has visibility of all the applications submitted to the unit, regardless of processing status, and may reassign responsibility of active applications across staff working

within the UIC. Applications, however, cannot be reviewed, PSV'ed, or routed from the "PAC Supervisor" view. Users must resume their CC/MSSP/CM role to perform these activities.

Note: CCQAS also has a "CVO Supervisor" role that functions in a similar manner. The "CVO Supervisor" has visibility of all the applications submitted to the CVO and may reassign responsibility of active applications across staff working within the CVO.

The "PAC Supervisor" role is listed on the **Privileging** tab in the **Permissions** section of the user account, as depicted in Figure 142 below. In most cases, Service-level CCQAS Administrators assign the "PAC Supervisor" role to the appropriate facility personnel.

Update User -- CM9, CM9

Demographics MTF Roles/Permissions

*** This is the MTF for these specified Permissions *** CD1CFVPV

Privileging Module	System Admin
PAC	<input type="radio"/> No <input checked="" type="radio"/> Yes
PAC Supervisor	<input type="radio"/> No <input checked="" type="radio"/> Yes
CVO	<input type="radio"/> No <input checked="" type="radio"/> Yes
CVO Supervisor	<input checked="" type="radio"/> No <input type="radio"/> Yes
Reviewer	<input type="radio"/> No <input checked="" type="radio"/> Yes
Privileging Authority	<input type="radio"/> No <input checked="" type="radio"/> Yes
PAR Evaluator	<input checked="" type="radio"/> Yes
PAR Reviewer	<input checked="" type="radio"/> Yes
CLP Administrator	<input checked="" type="radio"/> Yes
State License Waiver Endorser	<input checked="" type="radio"/> Yes

Message from webpage

By making this user a PAC Supervisor, this user will inherit all the permissions of the PAC role.

OK

Note: Permissions are cumulative.
INSERT includes UPDATE and READ
DELETE includes INSERT, UPDATE, and READ

Save Close

Figure 142: PAC Supervisor Role on the 'Permissions' Tab

CCQAS requires individuals who are assigned the "PAC Supervisor" role to also have the "PAC" role. If an individual is assigned the "PAC Supervisor" role and does not already have "PAC" role permission, CCQAS automatically assigns that user the "PAC" role.

Users who have "PAC Supervisor" permissions can see an additional tab labeled **Submitted Applications** when they access the Privileging module, as depicted in Figure 143 below.

Provider	Status	Application Status	App Submitted	Resp. CC/CM/MSSP	Took Ownership	PA Decision	PA Decision Date	# of D
KENT, TRACY	Closed	In Review	09/19/2012	CM9, CM9	10/05/2012			
PETERS, ROBERT	Complete	Submitted	08/27/2012	CM9, CM9				
TAYLOR, JAMES	Non-Compliant	In Review	10/05/2012	CM9, CM9	10/05/2012			

Figure 143: Submitted Applications Screen

The following are important features of the **Submitted Applications** screen:

- Users may search for a particular application by entering **Provider Last Name** in free text, and then selecting a value from the **Status** or **Assigned CC/CM/MSSP** pick lists
- If no **Provider Last Name** is specified, CCQAS displays all Providers whose applications are in the selected **Status** or **Assigned CC/CM/MSSP**
- If no **Provider Last Name** or **Status** is specified, CCQAS displays all Providers whose applications are assigned to the selected **Assigned CC/CM/MSSP**
- If no **Provider Last Name** or **Assigned CC/CM/MSSP** is specified, CCQAS displays all Providers whose applications are assigned to the selected **Status**
- The date range defaults to display applications for the past 12 months; the date range for displaying work list items may be changed by entering the desired **Start** and **End** dates, and then clicking the **Filter** button.

To reassign an application from one CC/MSSP/CM to another, click **Application Reassignment** at the bottom of the page. The **Application Reassignment** screen appears, as depicted in Figure 144 below.

Urgent	Due Date	Task	Application	Returned/Action Required	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Co
Yes		Complete PSV	Complete PSV		PSV	CM9, CM9 (PSV)	TAYLOR, JAMES (Military)	1st E-App	Medical Service Corps	10/05/2012	
Open		Complete PSV	Complete PSV		CC/CM/MSSP	N/A	JOBS, STEVE (Military)	1st E-App	Medical Corps	09/17/2012	

Figure 144: Application Reassignment Screen

Users are given the choice of **Available CC/CM/MSSP Users**, as depicted in Figure 145 below. Click **Submit**.

Re-assign Task

**Please note that this will not reassign the application to the selected CC/CM/MSSP only this specific task. If you want to reassign the application, you must use the button 'Application Reassignment' located on the bottom of your worklist listing.

Current PSV: CM9 CM9

Available PSV(s):

Figure 145: Re-Assign CC/CM/MSSP Screen

A message displays in a pop-up window, as depicted in Figure 146 below. Users must confirm or deny their intent to take responsibility of the record by clicking either **OK** or **Cancel**.

After one of these two options is selected, the screen refreshes. Users click **Close** to return to the **Submitted Applications** screen.

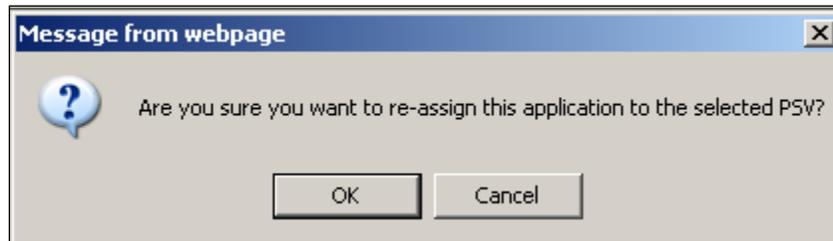


Figure 146: Reassign Confirmation Screen

6 Managing Provider Credentials Records

While a Provider's privilege application is only "active" during the submission, review, and approval process, his or her credentials record is active at all times while the Provider is assigned to a facility or unit. The credentials record functions as the permanent repository for the Provider's credentials, assignment history, and past and present privileges held. [Section 5](#) of this manual describes how a Provider's credentials record may be created or updated through the processing of his or her application for clinical privileges. This section addresses the creation and management of a Provider's credentials record by the custodial facility's credentials staff using the CCQAS Credentials module.

6.1 Creation of a New Record by the Credentials Staff

Credentials records are created and populated using data submitted by Providers on their online application. This is the preferred method for creating new credentials records for Providers who do not already have one. Occasionally, it may be necessary for CC/MSSP/CMs to create and populate credentials record themselves, as was done under previous versions of CCQAS.

The process of adding a new credentials Provider record by CC/MSSP/CMs is initiated from the **Credentials Provider Search** screen. CC/MSSP/CMs may access this screen by selecting **Credentialing** from the main menu bar, and then selecting **Provider Search** from the menu, as depicted in Figure 147 below.

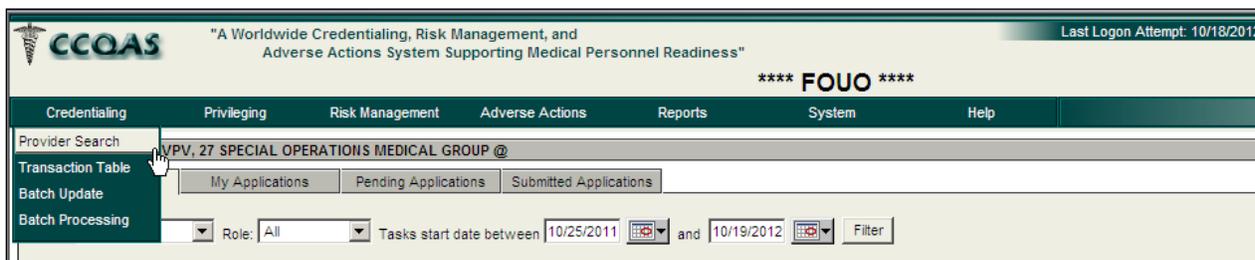


Figure 147: Provider Search Menu Item

The resulting screen contains three tabs, the first two of which enables users to search for existing credentials records (refer to [Section 6.2](#)). The third tab, **Add Credentials Provider**, allows users to create a new credentials record. CC/MSSP/CMs may also create a new credentials record by clicking **Add Provider** at the bottom of the screen.

The **Add Provider** screen appears, as depicted in Figure 148 below. CC/MSSP/CMs are required to populate all data fields on this screen (except **Middle Initial** and **Suffix**) to create a new credentials record.

Figure 148: Add Provider Screen

Important features of the **Add Provider** screen include the following:

- **U.S. Issued SSN** is automatically checked; if users uncheck this box, CCQAS automatically assigns a pseudo-SSN to the credentials record
- The **Country** refers to the Provider's country of origin
- Users are required to enter the Provider SSN twice to ensure the correct number is entered
- The value selected for **Provider Type** should be selected to best describe the position or assignment held by the Provider at this unit or facility
- The **Status** should reflect the individual's position or assignment at this unit or facility

After all required information is entered into the **Add Provider** screen, users click **Add** to create the new record. CCQAS first checks its database to ensure that no record exists for this Provider. If a record does not exist, a new credentials record is returned for the Provider. This new record is unpopulated, with the exception of the demographic information entered to create the record.

If a record already exists with the same unique combination of **First Name Last Name**, and **Date of Birth**, CCQAS alerts users by displaying a "Similar Person Found" message. If this message displays, users must not proceed with the creation of a new credentials record until they have confirmed that a new Provider record is needed and the data used to create the record is correct.

If a record already exists in CCQAS with the entered **SSN**, a "Matching SSN" message displays with information regarding the UIC to which the Provider with the matching SSN is currently assigned. If this message displays, users must not proceed with creating a new credentials record. Instead, contact the credentials personnel where the Provider is assigned to discuss the appropriate course of action.

Note: Users should consult with their Service CCQAS Administrator for guidance regarding the management of dual status Providers in CCQAS 2.10.0.0. Dual status Providers are Providers who work in both a military status as a reservist or guardsmen, and a civilian status as a contract Provider in a military facility.

6.2 Searching for a Provider's Credentials Record

The ability to query the CCQAS database to locate credentials records for one or multiple Providers using user-specified search criteria is a core feature of the CCQAS application. CCQAS offers the following mechanisms for locating a Provider's credentials record:

- Credentials Provider Search (basic search)
- Advanced Search
- Provider Locator

Each of these search functions is described in detail in this section. Users must understand that database searches utilize the data that is entered into each Provider's record. If credentials records are incomplete or populated with inaccurate data, a user's ability to locate the desired record(s) may be diminished.

6.2.1 Searching for Records within the Facility/Unit

Permissions in CCQAS are structured to limit users' access to only those credentials records that they are responsible for tracking. Most facility-based users only have access to Provider credentials records associated with a single facility or unit. Reserve and Guard personnel may have access to credentials records associated with multiple units. The **Basic** and **Advanced Search** functions only query the subset of the CCQAS database that users have permission to access.

6.2.1.1 Using the Basic Search Function

The **Credentials Provider Search** screen allows users to query the database to retrieve a specific record and/or group of records, as depicted in Figure 149 below.

The screenshot shows the 'Credentials Provider Search' screen in the CCQAS application. The page header includes the CCQAS logo and the tagline 'A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness'. The user is logged in as '**** FOUO ****' with ID 'W00074'. The navigation menu includes 'Credentiaing', 'Privileging', 'Risk Management', 'Reports', 'System', and 'Help'. The search interface has three tabs: 'Provider Search' (selected), 'Advanced Credentials Search', and 'Add Credentials Provider'. The search form contains the following fields and options:

- Last Name: [Text Input]
- First Name: [Text Input]
- SSN: [Text Input]
- Alias Last Name: [Text Input]
- Alias First Name: [Text Input]
- NPI: [Text Input]
- Branch: [Dropdown Menu]
- Corps: [Dropdown Menu]
- Civilian Role: [Dropdown Menu]
- Primary UIC: [Text Input]
- Assignment UIC: [Text Input]
- Other UIC: [Text Input]
- Department: [Text Input]
- Work Center: [Text Input]
- File Manager: [Text Input]
- Provider Type: [Dropdown Menu]
- Sort By: [Dropdown Menu, set to 'Last Name']

Search filters include:

- Assignment Status: Inactive, Current, Pending
- Search Type: All (Primary UIC or Assignment UIC), Primary UIC, Assignment UIC, ICTB, Provider Locator

At the bottom, there are buttons for 'Search', 'Clear Screen', and 'Add Provider'. A 'Record Count' field is empty, and a 'Record Limit' is set to 100.

Figure 149: Credentials Provider Search Screen

The key features of searches conducted on the **Credentials Provider Search** screen include the following:

- Users may populate any of the data fields shown on the **Credentials Provider Search** screen as criteria for their search
- Users may enter one or many characters in free text data fields as search criteria. For example, users may enter **Last Name** = *pierce* to search for all Providers with this last name, or they may enter **Last Name** = *pie* to search for all Providers whose last name begins with the letters 'pie'
- Search criteria entered into free text data fields are not case sensitive
- If data fields that are populated from pick lists are used for querying CCQAS, users must select one of the pick list values; free text or partial values are not accepted
- Users may sort the list of retrieved records using any of the data fields available on the **Credentials Provider Search** screen using the **Sort by** pick list
- Users may query records of different **Record Status** and **Record Type**
- Users may specify the number of records returned when querying the database by adjusting the **Record Limit**
- Only Providers assigned to the UIC listed in the upper right-hand corner of the **Credentials Provider Search** screen are included in the query
- If a search is conducted for a specific Provider, and that Provider is assigned to a UIC other than the UIC being searched, CCQAS will not find the record. In this instance, users should use the **Provider Locator** function to gain access to that Provider's credentialing information

The process for conducting a basic search of the CCQAS database consists of the following steps:

- Selecting the criteria for the search
- Selecting the Record Status
- Selecting the Record Type
- Setting the Record Limit
- Clicking **Search** to produce search results

Step 1: Selecting Search Criteria

The data fields available for use as search criteria are shown in the top half of the **Credentials Provider Search** screen, as depicted in Figure 149 above. These data fields are associated primarily with Provider demographic and assignment information. If users wish to conduct a search based on other types of Provider information such as specialties or licensure data, they need to conduct their query using the **Advanced Search** tab (refer to [Section 6.2.2](#)). The data fields available on this screen consist of a combination of free text fields (**Last Name**, **First Name**, **SSN**, etc.) and pick lists (**Branch**, **Corps**, **Civilian Role**, etc.). Search criteria entered in

the free text fields are compared to records in the database, and those records that are populated with the value for the selected data field that match or begin with the same characters are retrieved. For example, if users enter “**Work Center** = *ped*”, CCQAS retrieves all records where the **Work Center** is populated with a value beginning with the letters ‘ped’, such as *pediatrics*, *pediatric clinic*, *pediatric oncology*, etc. Search criteria entered in the pick list fields is compared to the database, and records are only returned if there is an exact match. For example, if **Civilian Role** = *Physician* is selected, only credential records for civilian physicians are retrieved.

Users can specify search criteria in multiple fields to further refine their search. For example, if users select **Civilian Role** = *Physician* and **Provider Type** = *Contractor*, CCQAS only retrieves those records that match both criteria (e.g., civilian physicians who are contractors, rather than government employees). Using multiple search criteria allows users to better focus their queries and has the added advantage of potentially improving overall system performance and response time, since CCQAS is required to retrieve a smaller volume of records. Care must be taken, however, when selecting multiple query criteria to ensure that the criteria may logically be used together.

Step 2: Selecting the Record Status

Record Status options allow users to search for Provider records based on the Provider’s status at their facility/unit. The default value is **Record Status** = *Current*, which indicates that only records for Providers who are currently performing duty at the facility/unit are included in the query (e.g., only Providers whose assignment records at that facility/unit have no end date). The **Record Status** = *Inactive* indicates records associated with Providers who performed duty at the facility/unit in the past, but their assignment at that facility/unit has ended. **Record Status** = *Pending* indicates records for Providers who are projected to begin performing duty at the facility/unit at some future date (e.g., a scheduled incoming ICTB or Permanent Change of Station [PSC] that has not yet commenced). The **Record Status** = *All* results in all records, regardless of status, being included in the system query.

Step 3: Selecting the Record Type

Record Type options allow users to search for records based on the nature of the Provider’s assignment at their facility/unit. The default value of **Record Type** = *All* includes all Provider records in the query, regardless of whether the Provider is permanently assigned to the facility/unit or just working there as a result of an ICTB. Users may elect to limit the search to **Record Type** = *Credentialing* if only permanently assigned Providers are queried. If users elect to limit the search to **Record Type** = *ICTB*, both incoming ICTBs (i.e., coming into the facility from another location) and outgoing ICTBs (i.e., sent out to another facility) are included in the query.

Step 4: Setting the Record Limit

The **Record Limit** located in the lower right-hand corner allows users to specify a maximum number of records to be returned from a search of the CCQAS database. This feature was built into CCQAS to ensure that system performance is not degraded by returning inordinately large numbers of records. The default value is **Record Limit** = 100. Users should attempt to set the **Record Limit** to a value slightly higher than the anticipated number of records that will be returned from a typical database query. The **Record Count** listed in the lower left hand-hand corner of the **Search Results** tab indicates the actual number of records returned in the search, as depicted in Figure 150 below. If the **Record Count** < **Record Limit**, users may be assured that all records meeting the query criteria were returned on the **Search Results** screen. If the **Record Count** = **Record Limit**, the query should be repeated using a higher **Record Limit**.

Step 5: The Search Results

After users enter all search criteria on the **Credentials Provider Search** screen, they select the **Search** radio button in the **Action** section of the screen (i.e., the default value), and then click **Search** at the bottom of the screen to execute the query. The results of the query are returned on a newly-created **Search Results** tab.

?	Name	SSN	Primary MC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
Open		100-4488888	N00074	09/18/2012	F11	MC	Dual	Active		2
Initiate Custody Transfer		082-52-0122	N00074	08/25/2012			CV	Active		1
Deactivate Provider		082-72-0123	N00074	08/27/2012	N13	MC	ML	Active		1
Letters		082-42-0121	N00074	08/24/2012	N13	MSC	ML	Active		1
Change SSN		082-52-0121	N00074	08/25/2012	N13	MSC	ML	Active		1
Grant Module Access		082-72-0122	N00074	08/27/2012			ML	Active		1
•	KENT, TRACY	100-22-4444	CD1CFVPV	09/19/2012	F11	MC	Dual	Active		2
•	NEWTON, SAMANTHA	777-66-5555	N00074	10/18/2012	N11	MC	Dual	Active		2
•	PETERS, JESSICA	100-99-3232	N00074	10/19/2012			ML	Active		1
•	SMITH, MARK	200-55-9999	N00211	10/15/2012	F11	MC	Dual	Active		3

Figure 150: Search Result screen

Each Provider record that meets the query criteria is listed as a row on the **Search Results** tab. From this screen, users may open a selected credentials record by double-clicking anywhere on the record line, or single-clicking the small arrow to the left of the selected record, to open a menu of Provider actions, and then selecting **Open**. The other menu options are discussed in other sections of this manual.

In addition to the **Search** button, two other buttons are available at the bottom of the **Credentials Provider Search** screen, **Clear Screen** and **Add Provider**. Following the execution of the query, users click **Clear Screen** to refresh the search screen, remove any previously entered criteria, and reset all fields to their default values. Users click **Add Provider** to initiate the

process of adding a new Provider credentials record to the CCQAS database (refer to [Section 6.1](#)).

6.2.2 Using the Advanced Search Function

Users may use the **Advanced Search** screen to query the CCQAS database using criteria that are not available on the **Credentials Provider Search** screen. This functionality allows users to query the database using any combination of data fields in the electronic credentials file. Users may access the **Advanced Search** screen by clicking the **Advanced Credentials Search** tab from the **Credentials Provider Search** screen, as depicted in Figure 151 below.

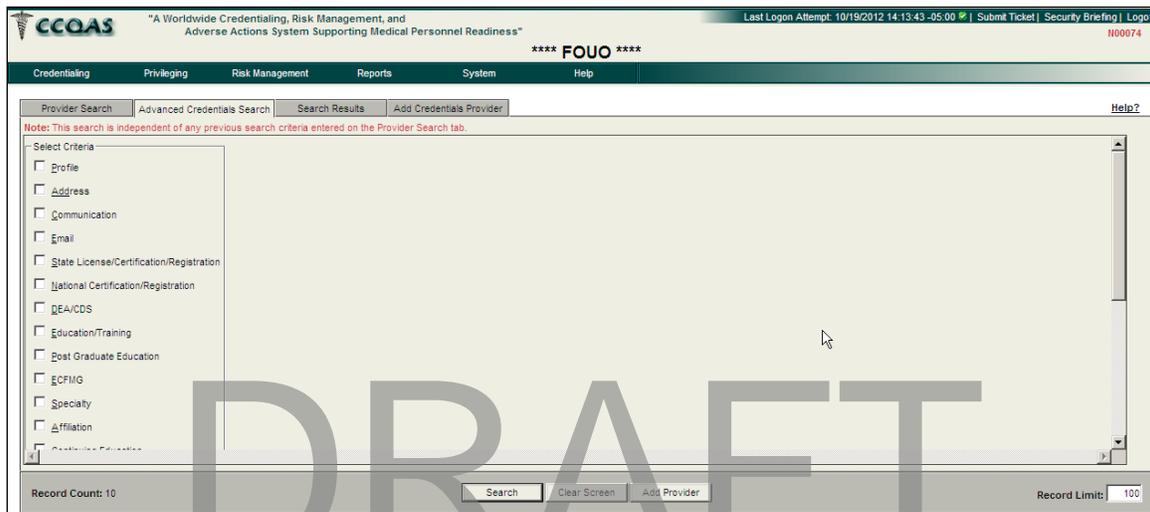


Figure 151: Advanced Search Screen

The **Advanced Search** screen functions in a manner very similar to the CCQAS ad-hoc reporting tool. Like the ad-hoc tool, mastery of the **Advanced Search** functionality requires a good working knowledge of CCQAS data, an understanding of the limitations of the tool, and practice. Users are encouraged to review the discussion and sample problems in [Section 14](#) prior to using the **Advanced Search** functionality to perform system queries.

The process for conducting an advanced search of the CCQAS database consists of the same steps required to perform a basic search:

- Selecting the criteria for the search
- Selecting the **Record Status**
- Selecting the **Record Type**
- Setting the **Record Limit**
- Clicking **Search** to produce search results

Step 1. Selecting Search Criteria

The selection of criteria for an advanced search is a two-step process. First, users select the categories of data that will be used as criteria for their query in the **Select Criteria** section on the left-hand side of the **Advanced Search** screen. The categories listed are similar, but not identical, to the tabs and sections in the electronic credentials record. The selection of data categories on this screen determines which data fields will be made available for use as query criteria. The following mapping between categories of data in the electronic credentials record and the categories list on this screen may aid users in identifying the categories to select on this screen. Table 2 below lists the mapping of data from the credentials file to the **Advanced Search** function.

Table 2: Mapping of Data from the Credentials File to the Advanced Search Function

Credentials File Section	Credentials File Tab or Subsection	Example Data Fields	Advanced Search Category
Profile	all	Name	Provider Search
Civ/Mil	all	Branch, Rank, Corps, Role	Provider Search
Identification	all	SSN	Provider Search
Contact Information	all	Home Address, Phone, Email	Address, Phone, Email
Lic/Cert/Reg	State Licensure/Cert/Reg	Number, State, Field	License/Cert/Reg
	National Cert/Reg	Number, Field, Agency	License/Cert/Reg
DEA/CDS	all	Number, Expiration Date	DEA/CDS
Education/Training	Primary Education	Degree, Institution	Education/Training
	Prof Ed/ECFMG	ECFMG	Education/Training
	Other Education	Type, Field of Study	Education/Training
Specialty	all	Specialty, Board Certification	Specialties
Affiliation	Malpractice Insurance	Insurance Contractor, Address	Affiliations
	Clinical Affiliations	Facility Name, Approval Date	Affiliations
	Academic Appointments	Facility Name	Affiliations
	Organization Memberships	Facility Name	Affiliations
Continuing Education	all	Type, Course, Credits	Continuing Education
Contingency Training	all	BLS, ACLS, CBRNE, C4	Contingency Training
References	all	Reference Type, current	References
Readiness	all	Mob UIC/UTC, MRT Date	Readiness
NPDB/HIPDB/FSMB	NPDB/HIPDB/FSMB	Last Query Date	NPDB/HIPDB/FSMB
Reserve Training	all	Reserve UIC, Annual Training Location Name	Reserve Training
Assignments	Assignment	Assigned UIC	Assignment

Credentials File Section	Credentials File Tab or Subsection	Example Data Fields	Advanced Search Category
Remarks	all	Type, Remarks Text	Remarks

When users select a category of data, a window opens, allowing them to select the desired data field, operator, and value for their query. A listing and description of available operators is provided in Table 3 below.

Table 3: Operators for Advanced Search Function

Operator	Data Types	Description
Equal to	All	To query all records with a specified value
Not Equal to	All	To query all records other than those with a specified value
Less Than	Numeric, Dates	To query all records with a value less than a specified number or earlier than a specified date
Less Than or Equal to	Numeric, Dates	To query all records with a value less than or equal to a specified number or earlier than or equal to a specified date
Greater Than	Numeric, Dates	To query all records with a value greater than a specified number or later than a specified date
Greater Than or Equal to	Numeric, Dates	To query all records with a value greater than or equal to a specified number or later than or equal to a specified date
Between	Numeric, Dates	To query all records with a value between (or equal to) a specified range of numbers or dates.
Is Null	All	To query all records that contain no data in the data field, e.g., the field is empty
Is Not Null	All	To query all records that contain data for the data field, e.g., the field is not empty
Begins with	Alphanumeric	To query all records in which the value for the data field begins with a specified letter or number
Ends with	Alphanumeric	To query all records in which the value for the data field ends with a specified letter or number
Contains	Alphanumeric	To query all records in which the value for the data field includes a specific sequence of one or more letters or numbers
Like (wildcard = %)	Alphanumeric	To query all records in which the value for the data field includes a specific sequence of one or more letters or numbers and any additional characters where the % is placed
Not Like (wildcard = %)	Alphanumeric	To query all records except those in which the value for the data field includes a specific sequence of one or more letters or number and any additional characters where the % is placed

If users wish to use more than one data field to query the CCQAS database, they may add other query criteria from a different category by checking the second category. User may add another query criterion from the same category by clicking **Add Criteria**. In order to combine query criteria from the same category, users must specify how the two criteria are related. If users select **AND**, only those Providers who meet both criteria will be selected for inclusion on the report. If users select **OR**, those Providers who meet one or the other of the criteria will be included on the report.

Note: Users must specify **AND** or **OR** when combining query criteria from the same category. If users apply query criteria from different categories, CCQAS automatically applies **AND** logic for the query.

The following example illustrates the advanced search functionality:

Example: Robert, an experienced CCQAS user, wishes to query CCQAS for all dentists and oral surgeons in his facility who hold a state license that is due to expire in the next 30 days. Robert needs to query CCQAS for Providers who hold specialties of “Dentist” or “Oral & Maxillofacial Surgery” and whose state license expires within a defined date range. For the purposes of this example, assume that the current date is January 1, 2008.

Robert needs to use multiple query criteria to generate this query. He wants to identify Providers with a state license due to expire within a specified date range. After he enters the criteria, Robert selects the **AND** operator to add more criteria from a different section. He then selects **Specialty**, and then selects the HIPAA Provider Taxonomy Code (HPTC) Specialties of interest. He selects **OR** to query Providers who have specialties of “Dentist” OR “Oral & Maxillofacial Surgery”. Since the license expiration information is on the **State License** tab, **AND** is automatically applied, as depicted in Figure 152 below.

The screenshot shows the CCQAS Advanced Search interface. The top navigation bar includes tabs for Credentiaing, Privileging, Risk Management, Reports, System, and Help. The main search area is titled "Provider Search" and contains a "Select Criteria" sidebar on the left and a search criteria table on the right. The sidebar has checkboxes for various criteria categories, with "State License/Certification/Registration" and "Specialty" checked. The search criteria table is divided into two sections: "State License/Certification/Registration Criteria" and "Specialty Criteria".

Column	Operator	Value
State Lic. Expiration Date	Between	01-01-2008 And 01-01-2008
HPTC Specialty	Equal to	Dentist
HPTC Specialty	Equal to	Oral & Maxillofacial Surgery

The "Specialty Criteria" section also includes an "OR" operator between the two specialty rows. At the bottom of the interface, there are buttons for "Search", "Clear Screen", and "Add Provider", along with a "Record Count: 10" and "Record Limit: 100" indicator.

Figure 152: Example Query using Advanced Search Functionality

Written as a parenthetical expression, Robert’s query would display as follows:

State License expires 30 days after January 1 AND (Dentist OR Oral Surgeon)

Note: Robert could also run two separate queries to access the desired records. He could run one query to retrieve all dentists whose licenses are expiring, and then a query all oral surgeons whose licenses are expiring.

Step 2 & 3. Selecting the Record Status and Record Type

Users select the desired **Record Status** and **Record Type** option for the “Advanced Search” query on the **Credentials Provider Search** screen.

Note: Any criteria that users enter on the **Credentials Provider Search** screen before they click the **Advanced Search** tab is automatically applied to the “Advanced Search” query using **AND** logic.

Step 4. Setting the Record Limit

Users may set the **Record Limit** for the query on either the **Credentials Provider Search** screen or the **Advanced Search** screen.

Step 5: The Search Results

After users enter all desired search criteria on the **Credentials Provider Search** screen and **Advanced Search** screen, they click **Search**, at the bottom of the screen, to execute the query. Each Provider record that meets the query criteria is listed as a row on the **Search Results** screen. From this screen, users may then access each of the credentials files individually. Following the execution of an advanced query, users should click **Clear Screen** to refresh the search screen, remove any previously entered criteria, and reset all fields to their default values.

6.2.3 Locating Provider Records at Other Facilities or Units

CCQAS does not permit CC/MSSP/CMs to access a Provider’s credentials file unless that Provider is currently assigned or performing ICTB duty at their location. CCQAS does, however, permit CC/MSSP/CMs to perform a search across all CCQAS locations to identify if a Provider’s credentials record exists, and, if so, where it is located. The **Provider Locator** function allows users to search the entire CCQAS database for one or more Provider’s credentials records using the basic search criteria available on the **Credentials Provider Search** screen.

6.2.3.1 Using the Provider Locator Function

Searches for Provider credentials records may also be conducted using the **Provider Locator** function. The **Provider Locator** function does not allow users to access the credentials record for a given Provider, but it does provide contact information for the CCQAS POC who currently has custody of the credentials record. To use the **Provider Locator** function, CCQAS users enter the appropriate search criteria on the **Credentials Provider Search** screen, select the **Provider Locator** radio button in the **Action** section, and then click Search. Figure 153 below depicts the **Provider Locator** function.

The screenshot displays the CCQAS web application interface. At the top, the CCQAS logo is on the left, and the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" is in the center. To the right of the tagline, it says "**** FOUO ****". Below this is a navigation bar with tabs for "Credentialing", "Privileging", "Risk Management", "Reports", "System", and "Help".

The main content area is titled "Provider Search" and contains several tabs: "Advanced Credentials Search", "Search Results", and "Add Credentials Provider". The "Advanced Credentials Search" tab is active. It features a form with the following fields:

- Last Name: [Text Input]
- First Name: [Text Input]
- Alias Last Name: [Text Input]
- Alias First Name: [Text Input]
- Branch: [Dropdown Menu]
- Corps: [Dropdown Menu]
- Primary UIC: [Text Input]
- Assignment UIC: [Text Input]
- Department: [Text Input]
- Work Center: [Text Input]
- Provider Type: [Dropdown Menu]
- Sort By: [Dropdown Menu, currently set to "Last Name"]

Below the form are two sections:

- Assignment Status:**
 - Inactive
 - Current
 - Pending
- Search Type:**
 - All (Primary UIC or Assignment UIC)
 - Primary UIC
 - Assignment UIC
 - ICTB
 - Provider Locator

A red arrow points to the "Provider Locator" radio button. At the bottom of the form, there is a "Record Count: 10" label and three buttons: "Search", "Clear Screen", and "Add Provider".

Figure 153: Provider Locator Function

The **Provider Locator** screen appears, listing all Provider records in CCQAS that meet the search criteria. Multiple credentialing and ICTB records are displayed if they exist for the Provider.

Note: Users may obtain the POC information provided to them on the **Provider Locator** function from the **MTF Contacts** screen in CCQAS. It is important that users update their own contact information on the **MTF Contacts** screen, so that other CCQAS users are able to contact them as needed.

The **Provider Locator** function also allows gaining facilities to request an ICTB or PCS transfer from the location where a Provider is currently assigned. This is explained in detail in Sections [8](#) and [9](#).

6.2.3.2 Updating the MTF Contacts Screen

Users may update the **MTF Contacts** information for a unit by clicking the **System** main menu, and then selecting the **MTF Contacts**, as depicted in Figure 154 below.

Note: If **MTF Contacts** is not an available menu item, users have not been granted the permissions necessary to edit MTF Contact information, and should contact their CCQAS Administrator for further assistance.

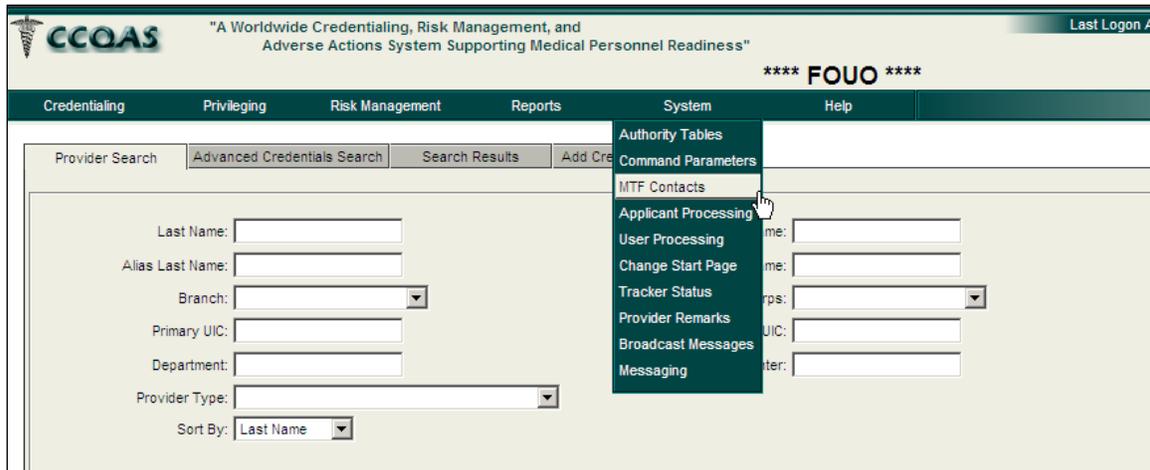


Figure 154: MTF Contacts Menu Item

A list of MTF contact records displays according to the Service affiliation of the UIC for which the user is responsible, as depicted in Figure 155 below. Users are only permitted to change contact information for the UICs to which they have access; the contact information for all other UICs is read-only. Users may edit the contact information by double-clicking the contact record for the appropriate UIC. Contact information should be complete and accurate so that other CCQAS users may easily contact you as necessary.

After all contact information has been updated, users should enter the date in the **Remarks** field so that others know when the contact information was last verified. All information is entered and viewable to others when users click **Save** to close the record.

The screenshot shows the 'Update MTF Contact' screen. It includes the following sections:

- MTF Information:**
 - UIC: N00074, Privileging: Yes, Service: Navy
 - Activate Privileging Module: Privileging Module Activated
 - MTF Name: NAVAL SPECIAL WARFARE COMMAND
 - Address 1: 2000 TRIDENT WAY
 - Address 2: BLDG 624
 - City: SAN DIEGO
 - State: CA - California
 - Zip: 92155-5599
 - Country: United States - US
 - DMIS: [Empty]
 - Head Officer: CAPT Gary S. Gluck - For
- Branch Clinics:**

UIC	Name	Location
N00160	WALTER REED NATIONAL MILITARY MEDICAL CENTER	BETHESDA, MD
N00183	NAVAL MEDICAL CENTER	PORTSMOUTH, VA
- Credentials Coordinator:**
 - Name: Ms. Jocelyn Fonseca
 - Commercial Phone: (619) 537-1171
 - DSN Phone: [Empty]
 - Fax Phone: (619) 437-0927
 - Email Address: Jocelyn.Fonseca@navsoc.socom.m
- Risk Manager:**
 - Name: [Empty]
 - Commercial Phone: [Empty]
 - DSN Phone: [Empty]
 - Fax Phone: [Empty]
 - Email Address: [Empty]
- Remarks:**
 - Alternate MSSP is HMC Oscar Tanjuaquo E-mail Oscar.Tanjuaquo@navsoc.socom.mil phone number (619) 537-1168

Buttons: Save, Cancel

Figure 155: Update MTF Contact Screen

6.3 The Provider Credentials Record

The CCQAS credentials record functions as the permanent repository for a Provider's credentials, assignment history, and past and present privileges granted. To access a Provider's credentials record, CC/MSSP/CMs must perform a search for the desired record using the **Basic** or **Advanced** Provider search functionality (refer to Sections [6.2.1](#) or [6.2.2](#)). CC/MSSP/CMs may open the desired Provider record by selecting **Open** from the menu of available actions, as depicted in Figure 156 below. CC/MSSP/CMs may also open the record by double-clicking anywhere on the summary record line.

Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
ALLEN, PAUL	100-44-8888	N00074	09/18/2012	F11	MC	Dual	Active		2
	082-52-0122	N00074	08/25/2012			CIV	Active		1
	082-72-0123	N00074	08/27/2012	N13	MC	ML	Active		1
	082-42-0121	N00074	08/24/2012	N13	MSC	ML	Active		1
	082-52-0121	N00074	08/25/2012	N13	MSC	ML	Active		1
	082-72-0122	N00074	08/27/2012			ML	Active		1
NEWTON, SAMANTHA	100-22-4444	CD1CFVPV	09/19/2012	F11	MC	Dual	Active		2
	777-88-5555	N00074	10/18/2012	N11	MC	Dual	Active		2
PETERS, JESSICA	100-89-3232	N00074	10/19/2012			ML	Active		1
SMITH, MARK	200-55-9999	N00211	10/15/2012	F11	MC	Dual	Active		3

Figure 156: Opening a Credentials Record

The credentials record is organized into sections that are accessible by clicking the section name in the navigation bar on the left-hand side of the screen, as depicted in Figure 157 below.

Provider Summary:

- Name: PAUL ALLEN
- SSN: 100-44-8888
- Branch: F11
- Primary UIC: N00074
- Rank: Lt Gen
- Cred Status: Active
- Corps: MC
- Input Clerk: MSSP154
- AOC/Desig/AFSC: 40C0

Navigation Bar (Left):

- Profile
- Identification
- Contact Information
- Lic/Cert/Reg
- DEA/CDS
- Education/Training
- Specialty
- Affiliation
- Continuing Education
- Contingency Training
- References
- Databank Queries
- Custody History
- Work History
- Privileges
- Documents
- Remarks

Form Fields:

- First Name: PAUL
- Person ID: 100-44-8888
- Date of Birth: 09/01/1984
- Citizenship: [Dropdown]
- NPI: [Field]
- Source DIMHRS: [Field]
- Digitized Date: [Field]
- Force (USAF): [Dropdown]
- Leutenant General: [Dropdown]
- Medical Corps: [Dropdown]
- AOC/Desig/AFSC: 40C0 - Medical Commander
- Accession: DA - Direct Accession

Figure 157: Navigation Bar

Summary information about the Provider is listed in the header portion of the credentials record. This header is read-only and viewable from any section within the record. Though the header cannot be edited directly, changes made to associated fields in the credentials record will be

reflected in the header after users save, close, and then re-open the record. Each section of the credentials record is explained in the following sections. The reader is also referred to the [Credentialing & Privilege Data Dictionary](#) for definitions and business rules associated with individual data elements within each section of the record.

Note: Per the CCQAS convention, all fields labeled in red text denote required fields, that is, fields that must be populated so the information on the screen can be saved.

6.3.1 The Profile Section

The **Profile** section in the credentials record contains a Provider's personal demographic information, as depicted in Figure 158 below.

The screenshot shows the CCQAS Profile Section for a provider named Paul Allen. The form is pre-populated with the following information:

- Provider Information:** Name: PAUL ALLEN, SSN: 100-44-8888, Branch: F11, Rank: Lt Gen, Corps: MC, AOC/Desig/AFSC: 40C0.
- Personal Information:** Last Name: ALLEN, First Name: PAUL, Date of Birth: 09/01/1964, Gender: Male, Marital Status: (empty), File Mgr: (empty).
- Military Information:** Branch: F11 - Air Force (USAF), Rank: Lt Gen - Lieutenant General, Corps: MC - Medical Corps, AOC/Desig/AFSC: 40C0 - Medical Commander, Accession: DA - Direct Accession.
- Alias Information:** No records returned.

A large "DRAFT" watermark is overlaid on the form. The "No Photo Available" message is also visible.

Figure 158: Profile Section

All required data fields on the **Profile** screen were pre-populated when the credentials record was first created, and changes to required data fields are generally not needed. This screen also includes optional fields to document any alias or other names that Providers have used during their professional career and free text fields to describe their working location or assignment in the hospital or clinic. It is recommended that each facility or unit develop its own convention for standardizing the use of the **Dept Code** and **Work Center** fields. Applying standard values in these fields makes them a useful field for performing Provider searches and running standard and ad-hoc credentialing reports.

If credentials management is divided among two or more credentials staff members in a facility or unit, use of the **File Mgr** field is highly recommended. Users should populate the **File Mgr** field with their name, or their designated alias, to identify the record as one for which they are responsible. Standard and ad-hoc reports may then be run that may help individual staff

members manage their workload. Users may then save all information entered in the **Profile** section by clicking **Save** in the upper left-hand corner of the screen.

Note: the **NPI** field is imported from an authoritative source for this information, the Defense Medical Human Resource System – internet (DMHRSi). After it is imported, this field may not be edited. If changes are needed to the NPI, they must be performed in DMHRSi.

6.3.2 The Military Section

CCQAS requires every Provider to be assigned a status of **Military** or **Civilian**. **Military** information is captured on the **Profile** page, as depicted in Figure 159 below. Civilian information is captured on the **Work History** screen, as part of the civilian assignment information. Active duty personnel and guard/reserve personnel on active duty assignments should be designated as military Providers. Civilian employees and contractors should be designated as civilian Providers. Dual-status Providers (e.g., guard/reserve personnel who are also contract Providers) must fill out the **Military** section of the profile page, and have a separate **Civilian** assignment per the location where they work. Users are directed to consult their Service policy for guidelines on documenting dual-status Providers who work at different locations under their military and civilian assignments.

The screenshot shows the 'Provider' profile page in CCQAS. At the top, there are navigation tabs: Credentialing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. The main content area is titled 'Provider' and includes a 'Close Pro' button. Below this, there is a 'Profile' section with a 'Save' button. The 'Profile' section contains a 'Provider' sub-section with the following fields: Last Name (CAROLLA), First Name (ADAM), MI, Suffix, Title, Person ID Type (Social Security Number), Person ID (100-55-7474), Date of Birth (09/02/1990), Citizenship, Gender (Male), Marital Status, File Mgr, and NPI. Below the 'Provider' section is the 'Military Information' section, which is checked. It contains fields for Branch, Rank, Corps, AOC/Desig/AFSC, and ASI. The 'Civilian Information' section is unchecked. A 'No Photo Available' message is displayed on the right side of the form.

Figure 159: Figure 6.3-4. Military Section of Profile

When users enter a checkmark for **Military**, the fields for that status are activated. For Providers designated as **Military**, data fields must be populated in the following order: **Branch**, **Rank**, **Corps**, **AOC/DESIG/AFSC**, and then **ASI** (Army Providers only), since the value selected for each field creates the pick list for subsequent fields. For civilian Provider assignments, the **Role** is required to designate the Provider's practitioner type. The **Accession** is required for both types of Provider to capture the pathway by which the Provider began working for the DoD.

Users may save all information entered by clicking **Save** in the upper left-hand corner of the screen.

6.3.3 The Identification Section

Users may create a record of a Provider's SSN or Foreign Identification Number (FIN) in the **Identification** section at the time the credentials record is first created, as depicted in Figure 160 below. This number is used to uniquely identify each credentials record in CCQAS. After users create the credentials record, the SSN or FIN associated with the record may not be edited.

The screenshot shows the CCQAS interface for a provider's identification section. The header includes the CCQAS logo, the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness", and a "FOUO" (For Official Use Only) warning. The navigation menu includes Credentiaing, Privileging, Adverse Actions, Reports, System, and Help. The provider information is displayed as follows:

Name: ADAM CAROLLA	Branch: Primary UIC: CD1CFVPV	Rank: Cred Status: Active	Corps: Input Clerk: CM9	AOC/Desig/AFSC:
--------------------	-------------------------------	---------------------------	-------------------------	-----------------

The Identification section is active, showing a table with the following data:

Identification Type	Identification Number	State
Social Security Number	100-55-7474	

Figure 160: Identification Section

Additional forms of personal identification, however, may be documented in CCQAS. To document another form of personal identification, click **Add**. The **Identification** screen appears, as depicted in Figure 161 below.

Both the **Identification Type** and **Identification Number** are required. Users may then save the information by clicking **Save** at the bottom of the screen. With the exception of the SSN or FIN, other forms of personnel identification entered in CCQAS may be edited or deleted later, as appropriate.

If it is discovered that a SSN or FIN for an existing credentials record is incorrect, consult your Service CCQAS Administrator for further guidance.

The screenshot shows the "Add Identification" screen in the CCQAS interface. The provider information is the same as in Figure 160. The Identification section is empty, and the "Add" button is visible. The "Identification Type" dropdown menu is open, showing the following options:

- Foreign Drivers License
- U.S. Certificate of Naturalization
- U.S. Drivers License
- U.S. Military Identification Card
- U.S. Resident Alien Card

Figure 161: Add Identification Screen

6.3.4 The Contact Information Section

The **Contact Information** section consists of three tabs to document address, email, and phone information for a Provider, as depicted in Figure 162 below. CCQAS requires that one, and only one, home address, work address, email address, and phone number be designated as “primary” for the purposes of communicating with the Provider.

Provider																							
Name: ADAM CAROLLA		Branch:	Rank:																				
SSN: 100-55-7474		Primary UIC: CD1CFVPV	Cred Status: Active																				
		Corpe:	AOC/Desig/AFSC:																				
		Input Clerk: CM9																					
<table border="1"> <thead> <tr> <th colspan="3">Address</th> <th>Email</th> <th>Phone</th> </tr> </thead> <tbody> <tr> <td colspan="5">Add</td> </tr> <tr> <td>?</td> <td>Address Type</td> <td>Full Address</td> <td></td> <td>Primary</td> </tr> <tr> <td>v</td> <td>Home</td> <td>64 MAPLE AVE FAIRFAX VA</td> <td></td> <td>Yes</td> </tr> </tbody> </table>				Address			Email	Phone	Add					?	Address Type	Full Address		Primary	v	Home	64 MAPLE AVE FAIRFAX VA		Yes
Address			Email	Phone																			
Add																							
?	Address Type	Full Address		Primary																			
v	Home	64 MAPLE AVE FAIRFAX VA		Yes																			

Figure 162: Contact Information Section

The extent to which this information is already populated in the credentials record depends, in part, on the extent to which the Provider has been integrated into the CCQAS electronic privileging process, as follows:

- The primary email address and phone number in a Provider’s credentials record is auto-populated with the data used to create the Provider’s CCQAS user account. If the Provider has not yet been issued a user account, these tabs may be empty unless the assigned CC/MSSP/CM enters the contact information directly into the Provider’s credentials record
- Providers are required to include a primary home address to E-sign and submit their 1st E-application. If Providers have not yet had their 1st E-application processed, the **Address** tab is empty unless the CC/MSSP/CM enters the contact information directly into the Provider’s credentials record
- Providers may also enter a primary local work address on the 1st E-application, but they are not required to do so. If a primary local work address has not been entered, the CC/MSSP/CM should enter the information directly into the Provider’s credentials record (**Note:** use of the automated NPDB query function in CCQAS requires that Providers have a documented local work address to be included in an NPDB query)

The **Add** button in the upper left-hand corner of each tab allows the addition of a new contact record, as appropriate. CCQAS supports multiple contact records of each type, but only one of each type may be designated as primary. Over time, it is likely that primary contact information for a Provider will change. It is imperative that these changes be made in CCQAS as soon as possible to ensure that communications with the Provider are not disrupted.

The most direct method for updating primary contact information in a Provider’s record is to add the new record, designate it as **Primary**, and then click **Save**. For example, if a Provider’s primary phone number needs to be changed, users may enter a new primary number by clicking **Add**. When users enter the **Type** and **Phone Number** and select the “**Primary Phone = Yes**” radio button, the new number is automatically designated as the primary phone number when

users click Save. Figure 163 below depicts the screen to update a Provider’s primary phone number.

The screenshot shows the CCOAS interface for updating a provider's contact information. The provider's name is ADAM CAROLLA (SSN: 100-55-7474). The form is titled 'Contact Phone' and includes a dropdown for 'Type', a text input for 'Phone Number', and radio buttons for 'Primary Phone' (Yes/No). The 'No' option is selected. The interface also shows a 'Save' button and a 'Close' button.

Figure 163: Updating a Primary Phone Number

Users may designate existing contact records as “primary” by selecting **Update** from the hidden menu, selecting the “**Primary = Yes**” radio button, and then saving the record. The **Update** function also allows users to make changes to the contact information, but it should only be used if corrections or additions to an existing contact record are needed. Users should create a new contact record for each unique physical address, email address, or phone number associated with the Provider.

6.3.5 The License/Certification/Registration (Lic/Cert/Reg) Section

The **Licensure/Certification/Registration** section contains **State** and **National** tabs to support the documentation of state and national licenses, certifications, or registrations held by a Provider. It also contains a third tab, **Unlicensed information**, to document circumstances where a Provider does not currently hold an active U.S. license. Figure 164 below depicts the **Licensure/Certification/Registration** section.

The screenshot shows the 'Lic/Cert/Reg' section with the 'State' tab selected. A table lists the provider's licenses. A context menu is open over the first row, showing options: Add, Renewal Letter, Update, Delete, and Verification Letter.

Type	State	Number	Field	Status	Expires	ADM Waiver
License	Arizona	123	Dentists	Active	10/01/2014	No

Figure 164: Lic/Cert/Reg Section

Users should document all past and present state and national credentials held by the Provider in his or her credentials record. In general, Providers should update this information each time a new E-application for privileges is submitted. Occasionally, however, CC/MSSP/CMs may need to add or edit this information between privileging cycles.

6.3.5.1 Documenting State Licenses, Certifications, or Registrations

Every Provider who is subject to licensing at the state-level must hold at least one current, valid state license to render care to patients in DoD facilities. This includes physicians, dentists, physician assistants (PAs), nurse practitioners, and registered nurses. Dental hygienists are not state-licensed, but they may be required to be state-registered. In general, civilian and contract Providers are required to comply with all licensing requirements imposed by the state or country in which they are practicing. Military Providers may render care in any DoD facility worldwide as long as they hold one current and valid license from any U.S. state. Under specific circumstances, however, Providers may require a waiver in cases where state requirements cannot be practically applied to DoD Providers. These exceptions are discussed below.

Users may view or update existing state license records by selecting **Update** from the hidden menu of actions for the record. Users may create state-level licenses, certifications, and registrations by clicking **Add** on the **State** tab, as depicted in Figure 165 below.

The screenshot displays the CCQAS interface for documenting state licenses. At the top, the header includes the CCQAS logo, the mission statement "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness", and a security notice "**** FOUO ****". The navigation menu includes Credentiaing, Privileging, Adverse Actions, Reports, System, and Help. The main content area is titled "Provider" and shows details for ADAM CAROLLA, including his branch (F11), rank (Lt Gen), and corps (DC). Below this, the "State License/Certification/Registration" form is visible. It contains fields for Type (License), Number (123), Field (030 - Dentists), State (AZ - Arizona), Issue Date, Status (Active), and Expiration Date (10/01/2014). There is also a checkbox for "Expiration Indefinite" and a checked box for "In Good Standing". A large "DRAFT" watermark is overlaid on the form. Below the license form is the "Prime Source Verification (PSV) Information" section, which includes a "Current" tab and a "History" tab. It contains fields for Method (Written Correspondence, Telephone, Internet, Email), Contact Name (JESSICA), Position, Institution, and Verified Date (10/15/2012). At the bottom of the form are "Save" and "Close" buttons.

Figure 165: State License/Certification/Registration Screen

Users are required to enter the **Number**, **State**, **Field**, **Status**, and **Type** for each state license, certification, or registration record created.

Hint: The **Field** field includes an A–Z sort function  that allows users to display the pick list in numerical order by field code or alphabetic order by field descriptions.

The remaining fields on the screen should be populated with information provided on the Provider's license/certification/registration certificate. In the few cases where the license has no associated expiration period or date, users should check **Expiration Indefinite** in lieu of entering an **Expiration Date**. When a license's expiration date is earlier than the current date, the license is flagged as expired.

The **PSV Information** section at the bottom of the screen displays the pertinent information from the most recent PSV of the credential. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** section with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position of the individual who performed the original PSV is then populated in the PSV record history.

After an active license has been verified and deemed to be in good standing, users must select the **In Good Standing** checkbox. If the **In Good Standing** checkbox is not checked, users must enter explanatory **Remarks** to save the record. Users then click **Save** to return to the **State** tab.

Note: Each time the license record is saved, CCQAS automatically updates the **Entered by Name** and **Entered by Position** fields in the **PSV Information** section of the screen. If users opening a record for viewing, but not editing, they should close the record by clicking the **Close** button, rather than clicking the **Save** button.

Depending on the state(s) in which they hold an active medical license, military physicians may require an administrative waiver. PAs may also require a state license waiver, depending on their practice circumstances. Waiver requirements for military physicians and PAs are explained in detail in Sections [6.3.5.2](#) and [6.3.5.4](#), respectively.

Foreign National Local Hires (FNLH) and other foreign-trained Providers who hold active licenses issued in the country where they practice should be documented on both the **State** tab (by selecting **State** = issuing country) and the **Unlicensed Information** tab. The **Unlicensed Information** tab is explained in Section [6.3.5.5](#).

6.3.5.2 Administrative Waivers for Military Physicians

DoD has a requirement that all physicians must be state licensed and fulfill all of the state's requirements for practice unless this provision is expressly waived. In order to provide health care services independently as a health care professional in the MHS, physicians must hold at least one current, unrestricted state medical license. A physician's military physician's license must meet all the clinical and administrative requirements and be no different than his or her civilian counterpart's license. Renewal fees are not subject to waiver. The Assistant Secretary of Defense for Health Affairs (ASD(HA)) reviewed all state medical board requirements and identified the following five states as having administrative licensure requirements that do not comply with DoD policy, and thereby making licensees of these states eligible for a request for a waiver:

- Florida: Malpractice insurance requirement and Neurological Injury Compensation Association (NICA) (risk pool)
- Kansas: Malpractice insurance and Healthcare Stabilization Fund (risk pool)
- Massachusetts: Malpractice insurance
- Oregon: Actual practice within the State
- Pennsylvania: Malpractice insurance and Medical Professional Liability Catastrophe Loss Fund (CAT Fund) (risk pool)

Waiver requests are considered on a case-by-case basis and must be requested for each period of license renewal.

CCQAS allows users to document whether or not a waiver has been granted by activating the **Admin Waiver** field on their state license record when a physician is licensed in one of these five waiver states. Figure 166 below depicts the **Admin Waiver** field.

The screenshot displays the 'State License/Certification/Registration' form for a provider named ADAM CAROLLA. The form includes fields for License Type (License), Number, Field, Issue Date, Status, and Remarks. A red arrow points to the 'Admin Waiver' dropdown menu, which is currently set to 'Yes'. Other fields include State (OR - Oregon), Expiration Date (No), and an 'In Good Standing' checkbox. The top navigation bar includes tabs for Credentialing, Privileging, Adverse Actions, Reports, System, and Help. The provider's information at the top includes Name, Branch (F11), Rank (Lt Gen), Corps (MC), SSN (100-55-7474), Primary UIC (CD1CFV/PV), Cred Status (Active), and Input Clerk (CM9).

Figure 166: Admin Waiver Field

If a physician has only one active license and the state of licensure is a waiver state, DoD policy requires him or her to have a valid waiver for that state. If a physician holds an active, unrestricted medical license in a non-waiver state, waivers are not required for active licenses held in waiver states, unless the license from the non-waiver status loses its active status. If a physician holds active licenses from multiple waiver states, only one of those licenses requires a waiver.

6.3.5.3 Documenting National Certifications or Registrations

Every Provider who is subject to certification at the national level must hold at least one current, valid national certification to render care to patients in DoD facilities. This includes PAs, nurse practitioners, and allied health professionals.

Note: ABMS, AOA, or ADS board certification information for board-certified physicians and dentists is documented on the **Specialties** tab (refer to [Section 6.3.8](#)), and **not** on the **Licensure/Certification/Registration** tab.

Users may view or update existing national records by selecting **Update** from the hidden menu of actions for the record. Users may create National-level certifications and registrations by clicking **Add** on the **National** tab, as depicted in Figure 167 below.

The screenshot shows the 'National Certification/Registration' screen. At the top, there is a header with the CCQAS logo and the text 'A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness'. Below this is a navigation bar with tabs for 'Credentialing', 'Privileging', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area is divided into two sections: 'National Certification/Registration' and 'Prime Source Verification (PSV) Information'.

The 'National Certification/Registration' section contains the following fields:

- Type:** A dropdown menu with 'Certification' and 'Registration' options.
- Number:** A text input field.
- Status:** A dropdown menu with 'Registration' selected.
- Issue Date:** A date picker.
- Field:** A dropdown menu with a sort function icon (A-Z and Z-A).
- Specialty:** A dropdown menu with 'No Specialty Code' selected.
- Agency:** A dropdown menu with 'No Agency' selected.
- Expiration Date:** A date picker.
- In Good Standing:** A checkbox.
- Remarks:** A large text area.

The 'Prime Source Verification (PSV) Information' section is divided into 'Current' and 'History' tabs. The 'Current' tab is active and contains the following fields:

- Method:** Radio buttons for 'Written Correspondence', 'Telephone', 'Internet', and 'Email'.
- Contact Name:** A text input field.
- Position:** A text input field.
- Source:** A dropdown menu.
- Verified Date:** A date picker.
- Institution:** A text input field.
- URL:** A text input field.
- Entered By Name:** A text input field.
- Entered By Position:** A text input field.
- Entered By UIC:** A dropdown menu.
- PSV Remarks:** A large text area.

At the bottom of the screen, there are 'Save' and 'Close' buttons.

Figure 167: National Certification/Registration Screen

Users are required to enter the **Number**, **Field**, **Specialty**, **Agency**, **Type**, and **Status** for each national certification or registration record created. To ensure data consistency, the pick list values for the **Specialty** and **Agency** are driven by the value selected for **Field**.

Hint: The **Field** field includes an A–Z sort function  that allows users to display the pick list in numerical order by field code or alphabetic order by field descriptions.

The remaining fields on the screen should be populated with information provided on the Provider's certification/registration certificate. In the few cases where the certification has no associated expiration period or date, users must select **Expiration Indefinite** in lieu of entering an **Expiration Date**. When a license's expiration date is earlier than the current date, the license is flagged as expired.

The **PSV Information** section at the bottom of the screen displays the pertinent information from the most recent PSV of the credential. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position of the individual who performed the original PSV is then populated in the PSV record history.

After an active license has been verified and deemed to be in good standing, users must select the **In Good Standing** check box. If users do not select the **In Good Standing** checkbox, they must enter explanatory **Remarks** to save the record. Users then click **Save** to return to the **State** tab.

Depending on the circumstances of their employment, some PAs may require an **Admin Waiver**. The administrative waiver requirement for military PAs is explained in detail in [Section 6.3.5.4](#). PAs who require an administrative waiver should be documented on both the

National tab and the **Unlicensed Information** tab. The **Unlicensed Information** tab is explained in [Section 6.3.5.5](#).

6.3.5.4 Waivers of Licensure Requirements for Qualified Military PAs

PAs may be licensed by state medical boards and also certified by several national organizations as competent to practice medicine. Joint Commission on Accreditation of Healthcare Organizations (JCAHO) requires that PAs be licensed by the state in which they practice. Most state licensing boards, however, require that PAs practice under the tutelage of a physician who is licensed by the same state. Compliance with this requirement is not practical for the military. The DoD has established the Health Affairs (HA) Policy 04-001 to waive the state licensure requirement for qualified PAs employed by the DoD under other than non-personal services contracts.

If a PA has a valid, unexpired national certification and the appropriate privileging authority finds the individual qualified to be privileged, CCQAS automatically generates a PA waiver. After a PA has been formally granted his or her privileges, CCQAS creates an administrative waiver sub-record in lieu of the JCAHO-required state license on the **State Licensure/Certification/Registration** tab of the PA's record. In order for CCQAS to generate the PA waiver, all of the following conditions must be met:

- PAs may not have the **Accession** = *NPSC – Non Personal Service Contract* on the **Profile** tab
- PAs' National Certification records must include the following:
 - **Field** = 642 – *Physician Assistants* or 645 – *Physician Assistants, Osteopathic*
 - **Specialty** = *Physician Assistant*
 - **Agency** = *NCCPA – National Commission On Certification of PA's*
 - **Expiration Date** that has not expired
- The **Priv-Cat** (expiration) **Date** must not be expired

If these conditions are met, CCQAS automatically generates a PA waiver sub-record on the **State Licensure/Certification** screen, which has the following characteristics:

- **Number** = *PA Waiver*
- **Field** = the value enter for **Field** on the PA's national certification record
- **Status** = *Active*
- **Expiration Date** = the lesser of National Certification/Registration **Expiration Date** and the **Priv-Cat** (expiration) **Date**
- **In Good Standing** = *Yes*
- **ADM Waiver** = *Yes*

The waiver record is available as a summary record only and cannot be opened, edited or deleted. The waiver remains current and valid as long as the national certification and privilege expiration dates are not expired. The PA waiver automatically expires when either (or both) a PA's privileges or national certification expire(s) or are revoked. The PA waiver is

automatically renewed as privileges and the national certification is renewed and will continually reflect the lesser of these two expiration dates. The PA waiver is automatically transferred during an ICTB transaction in the same manner as other license or certification records. The PA waiver, however, is not transferred for a PCS transaction, since a new waiver must be generated based on privileging at the new location. PAs who are contracted under non-personal services contracts are not eligible for a PA waiver, and must hold a valid state license.

6.3.5.5 Unlicensed Information Screen

The **Unlicensed Information** screen, depicted in Figure 168 below, is used to document any situation where Providers do not hold an active state license in the U.S. or one of its territories. This includes Providers who do not hold any active licenses, as well as those whose only active licenses are held outside the U.S.

The screenshot shows the 'Unlicensed Information' screen for Provider ADAM CAROLLA. The provider's details include Name: ADAM CAROLLA, SSN: 100-55-7474, Branch: F11, Rank: Lt Gen, Corps: MC, and Cred Status: Active. The screen has a 'Reason' dropdown menu with the following options: 'I am currently involved in the licensure application process.', 'I have let my license lapse and am currently unlicensed in any U.S. jurisdiction.', 'I am an active duty physician assistant utilizing the PA licensure waiver.', 'I am currently enrolled in an internship program. (i.e. medical, dietetic, social worker, etc...)', 'I am currently enrolled in medical post-graduate training that does not require licensure. (PG-1 & PG-2 ONLY)', 'I have not yet completed my doctoral degree and am ineligible for licensure. (i.e. clinical psychologists)', 'I am currently enrolled in a health profession education program and am ineligible to apply for licensure. (i.e. medical/dental school)', and 'I am a Foreign National Local Hire'. There is also a 'Remarks' field and a 'Save' button.

Figure 168: Unlicensed Information Screen

Users are required to select one of the explanations from the **Reason** pick list. If users select **Reason = I am currently involved in the licensure application process**, they are required to enter the **Available State**, and then click **Add** to have the state included in the **Licensure State** list. The selection of **Reason = "I have let my license lapse"** requires users to enter explanatory **Remarks**.

As a Provider's situation changes, the information maintained on this screen should be updated. For example, when a previously unlicensed Provider obtains an active, U.S. license, he or she is no longer considered 'unlicensed', and users may delete the information on the screen by clicking **Delete** in the upper left-hand corner of the tab.

6.3.6 The Drug Enforcement Agency/Controlled Dangerous Substances Section

The **Drug Enforcement Agency/Controlled Dangerous Substances (DEA/CDS)** section supports the documentation of all federal and state certifications issued to Providers, allowing them to prescribe or dispense medications to patients. All past and present DEA or CDS certifications issued to Providers should be documented in their credentials record. In general, Providers should update this information each time a new E-application for privileges is

submitted. Occasionally,, however, CC/MSSP/CMs may need to add or edit this information between privileging cycles.

Users may view or update existing DEA/CDS records by selecting **Update** from the hidden menu of actions for the record. Users may create new DEA/CDS records by clicking **Add** in the upper left-hand corner of the tab, as depicted in Figure 169 below.



Figure 169: DEA/CDS Section

Users are required to enter the **Number**, **Expiration Date**, and select **Type** for each DEA or CDS record created. When documenting a fee-exempt DEA number obtained by a military Provider, use **Type** = *DEA (fee exempt)*. A fee-exempt DEA certification may only be used when the individual is functioning in the capacity of a military Provider. It is not valid for use when a Provider is rendering care during off-duty employment or functioning in another non-military capacity. For all other (i.e., fee-paid) DEA numbers, use **Type** = *Federal*. CDS numbers should be documented with **Type** = *State*. Any records with **Type** = *Other* should be accompanied by explanatory text in the **Remarks** section. The **Verified Date** should reflect the date when the number is PSV'ed. In the few cases where the registration has no associated expiration period or date, user should check **Expiration Indefinite** in lieu of entering the **Expires** date, as depicted in Figure 170 below.

A button to access the DEA website is provided for reference purposes at the bottom of the screen. After users enter all information, click **Save** to save the data entered and return to the **DEA/CDS Summary** screen.

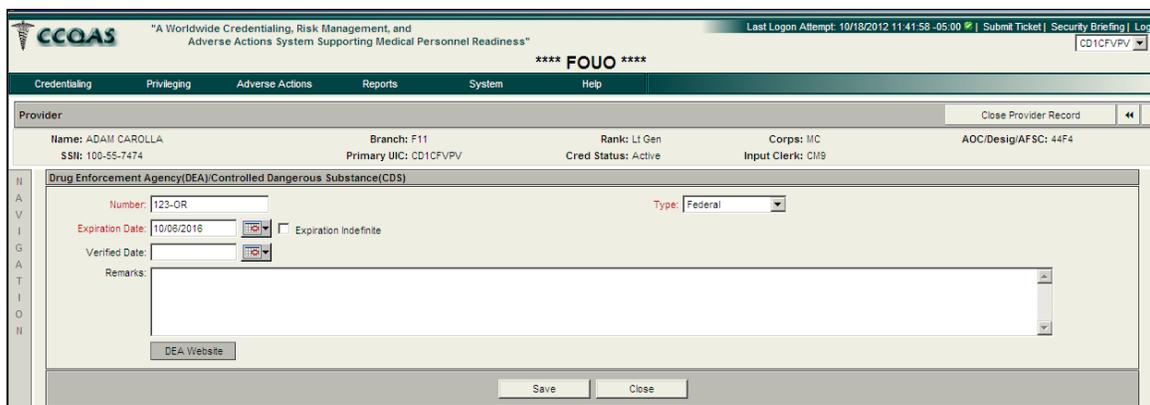


Figure 170: DEA/CDS Screen

6.3.7 The Education/Training Section

The **Education/Training** section supports the documentation of the academic and practical educational credentials for Providers. This section consists of three tabs to document a Provider's professional education, ECFMG certification (if applicable), and post-graduate training.

In general, Providers should update all new education and training information each time they submit an E-application for privileges. Occasionally, CC/MSSP/CMs may need to add new credentials to a Provider's record between privileging cycles. CC/MSSP/CMs may add a new record to the appropriate screen by clicking the **Add** button in the upper left-hand corner of the screen, as depicted in Figure 171 below.

?	Degree	Type	Institution	Attended From	Attended To	Completed
	Doctor of Dental Surgery	Qualifying Degree	Uniformed Services University of Health Sciences		10/15/2007	Yes

Figure 171: Education/Training Section

6.3.7.1 Documenting Professional Education

The **Professional Education** tab is designed to capture a Provider's academic credentials. Providers may only have one Qualifying education entry. Depending on the type of Provider, this primary academic credential may either be a degree (e.g., physician, nurse, etc.) or a certificate (e.g., Licensed Vocational Nurse [LVN]/ Licensed Practical Nurse [LPN]), where **Type** = *Qualifying Degree* or **Type** = *Qualifying Certificate*, respectively. The qualifying degree or certificate is required for submission of an E-Application, so most credentials records will already have this information documented and verified, as depicted in Figure 172 below.

The screenshot displays the CCQAS interface for a provider's record. At the top, the header includes the CCQAS logo, the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness", and a "FOUO" (For Official Use Only) warning. The navigation menu includes Credentiaing, Privileging, Adverse Actions, Reports, System, and Help. The provider information section shows: Name: ADAM CAROLLA, Branch: F11, Rank: Lt Gen, Corps: MC, AOC/Design/AFSC: 44F4, and Primary UIC: CD1CFVPV. The Professional Education tab is active, showing a record for a Qualifying Degree in Surgery from Services University of Health Sciences, completed on 10/15/2007. The PSV Information section is also visible, showing the verification method as Written Correspondence, verified on 10/09/2012, with contact name LESLIE.

Figure 172: Qualifying Degree Record

The *Qualifying Degree* or *Qualifying Certificate* is the only professional education record for which full PSV documentation is required by CCQAS. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** section with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position are captured in the PSV entry history. After CC/MSSP/CMs document the PSV of this degree or certificate in CCQAS, the PSV does not have to be repeated during future privileging actions.

Additional academic degrees obtained by Providers should also be entered into CCQAS as **Type** = *Other Degree* or *Other Certificate*. Each unique degree or certificate held by Providers should be documented in a separate record on the **Professional Education** tab.

Example: The primary education record for a PA should be **Type** = *Qualifying Degree* and **Degree/Cert** = *MPAS – Masters of Physician Assistant Studies*. This is the degree that qualifies Providers to function as PAs. Providers also have a bachelor's degree that was obtained as a prerequisite for the advanced degree. The bachelor's degree would be created as a second primary education record with **Type** = *Other Degree*.

Note: Users may enter a new *Qualifying Degree* at any time by selecting **Type** = *Qualifying Degree*, the previously marked *Qualifying Degree* is defaulted to *Other Degree*.

For all professional education records, the **Type**, **Degree**, **Institution Name**, **Date Attended to**, and **Completed** fields are required. The value that users select for **Type** determines the list of values available in the pick list for **Degree**. If Providers are currently obtaining the degree/certification, or never completed it, they should mark **Completed** as *No*, and should enter explanatory **Remarks**.

If the academic credentials were obtained at the Uniform Services University of Health Sciences (USUHS), users should click **USUHS** to populate **Institution**, as depicted in as depicted in Figure 173 below. If they were obtained elsewhere, users should enter the institution where the degree or certificate was obtained into CCQAS using the **Search** function .

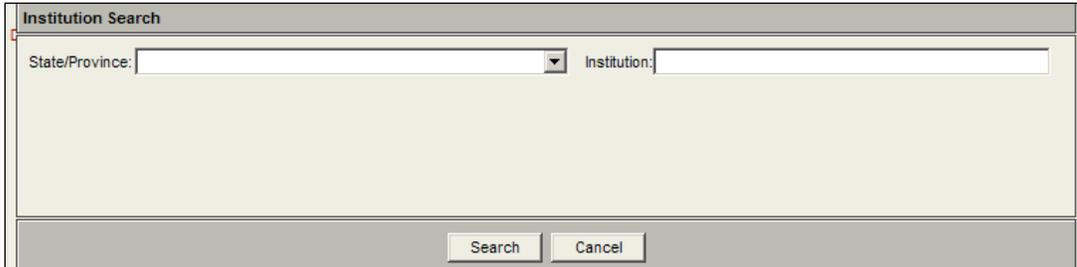


Figure 173: Institution Search Screen

To ensure data consistency, users should use the search function  to enter the name of all educational institutions. The search function allows users to search for a board by entering a **State/Province** in which the institution is located, or by institution name.

Hint: When searching for institutions by name, enter a key word or phrase to locate the correct institution. For example, if users enter “*Harvard*”, the search returns *Harvard Medical School*, *Harvard University Medical School*, etc. Users may then select the value that best matches the institution description on the Provider’s diploma or certificate.

When users click **Search**, a list of institutions that meet the search criteria displays. Users may then select the appropriate institution from the list, and then click **OK**. The **Professional Education** tab appears with the **Institution** populated with the value selected. In most cases, **City** and **State** auto-populate the location of the institution selected. If the **City** and **State** are not auto-populated by the **Search** function, users should verify and manually enter the city and state associated with the institution.

Note: If several search attempts have failed to find the correct institution name, users should select the **Check Here if Institution not Found** checkbox and enter the name of the institution.

After the **Professional Education** screen has been populated, users click **Save** to save the information and return to the **Professional Education** tab.

6.3.7.2 Documenting Post Graduate Training

The **Post Graduate Training** tab is designed to capture the practical education and training for Providers, as depicted in Figure 174 below. This tab pertains primarily to Providers who are required to complete internships, residencies, or fellowships as part of their formal training (i.e., physicians and dentists).

The screenshot shows the 'Post Graduate Training' tab for provider ADAM CAROLLA. The table contains one record:

Field of Study	Training Type	Institution	Attended From	Attended To	Completed
Cardiology	Residency (PGY-2)	Uniformed Services University of Health Sciences	10/06/2005	10/02/2006	Yes

Buttons for 'Add', 'Update', and 'Delete' are visible at the bottom of the table.

Figure 174: 'Post Graduate Training' Tab

Unless they are currently in their internship (i.e., Post-graduate year 1 [PGY-1]), most physicians and dentists should have multiple “Other Education” records in the CCQAS credentials file. Each professional year of post graduate medical study should be documented as a separate training record in CCQAS, as depicted in Figure 175 below.

The screenshot shows the 'Post-Graduate' form for provider ADAM CAROLLA. The form fields are as follows:

- Type:** Residency (PGY-2)
- Field of Study:** Cardiology
- Institution:** USUHS Uniformed Services University of Health Sciences
- Address 1:** 123 Main Street
- City:** Eugene
- State:** OR - Oregon
- Attended From:** 10/06/2005
- Attended To:** 10/02/2006
- Completed:** Yes
- Remarks:** (Empty text area)

Below the form is the 'Prime Source Verification (PSV) Information' section, which includes fields for Contact Name, Position, Email, Phone, URL, and Entered By Name/Position/UIC.

Figure 175: Post Graduate Training Record

Note: When users enter a new training record, they should select **Type** = *Internship (PGY-1)*, *Residency (PGY-2)*, etc. instead of **Type** = *Internship* or **Type** = *Residency*. The non-specific values of *Internship* and *Residency* are used for importing historical data from older versions of the CCQAS application where the post graduate year was not specified.

The **Field of Study** is a free text field to enter the most appropriate description of training that took place. The **Institution** should be entered in the same manner as described in the previous section. If the **City** and **State** are not auto-populated by the **Search** function, users should verify and manually enter the city and state associated with the institution. A **Remarks** section is available to include additional information that is pertinent to the education credential being

entered into the Provider's credentials record. **Remarks** are required if **Completed** = *No* or **Completed** is *null*.

Users should document complete PSV information for each post graduate training record in CCQAS. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** section with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position are captured in the PSV entry history. After the PSV of the completed training is documented in CCQAS, the PSV does not have to be repeated during future privileging actions.

6.3.7.3 Documenting Foreign Trained Providers

If Providers received their medical training outside the U.S., users should check **Foreign Trained** on the **Qualifying Degree** record under the **Professional Education** tab. This activates the **Fifth Pathway** checkbox and the **ECFMG** tab. If foreign-trained Providers are rendering patient care in a facility in the U.S. or its territories, they are required to have one of these two certifications. If Providers are working exclusively outside the U.S. (for example, they are local national foreign hires), they may not be required to have either certification. In both cases, the details of a Provider's qualifying degree and other training should then be documented as completely as possible on the **Professional Education** and **Post Graduate Training** tabs.

The Fifth Pathway program is a program whereby foreign-trained physicians may attend a fifth year of medical school in the U.S. prior to moving into their residency programs. If a Provider completed an extra year of medical school under the Fifth Pathway program, users should select the **Fifth Pathway** checkbox and enter the details of the Provider's Fifth Pathway training on the **Post Graduate Training** tab as a separate training record, with "**Type** = *Fifth Pathway*".

Alternatively, foreign-trained Providers who wish to work in the U.S. may also obtain ECFMG certification. If a Provider holds ECFMG certification, users should enter the information printed on his or her ECFMG certificate into the **ECFMG** tab in CCQAS, as depicted in Figure 176 below.

The screenshot displays the 'Professional Education' tab in the CCQAS system. At the top, the provider's name is TONYA WILLIAMSON, with SSN: FBB-00-0001. The branch is F11, primary UIC is CD1CFVPV, rank is CAPT, and corps is NC. The credential status is Active, and the input clerk is KELLYR. The AOC/Design/AFSC is 46N3E. The form is for a 'Qualifying Certificate' (Type) from the 'University of Barbados' (Institution Name). The certificate is 'F - Bachelor of Medical Science'. The provider is a 'Foreign Medical Graduate' and has checked 'Check here if institution not found'. The degree was attended from an unspecified date to 10/04/2010. The completion status is 'Yes'. Below this is the 'Prime Source Verification (PSV) Information' section, which includes fields for 'Method' (Written Correspondence, Telephone, Internet, Email), 'Contact Name', 'Position', 'Phone', 'Email', 'Entered By Name', 'Entered By Position', 'Entered By UIC', 'Source', 'Verified Date', 'Institution', and 'URL'. There is also a 'PSV Remarks' field.

Figure 176: ECFMG Tab

Users should document complete PSV information for an ECFMG certification in CCQAS. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** section with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position are captured in the PSV entry history. After the PSV of the ECFMG certification is documented in CCQAS, the PSV does not have to be repeated during future privileging actions.

The Fifth Pathway and ECFMG certifications apply only to physicians and should be left blank for all other types of Providers who are trained outside the U.S.

6.3.8 The Specialty Section

The **Specialty** tab in the credentials record describes the medical or dental specialties in which Providers have been trained to practice. Every Provider record in CCQAS should have at least one specialty record in the **Specialty** section. All specialties and subspecialties held by a Provider should be documented in his or her credentials record, and each specialty should be documented as a separate record in CCQAS. In general, Providers should update this information each time a new E-application for privileges is submitted. Occasionally, CC/MSSP/CMs may need to add or edit this information between privileging cycles.

Users may edit an existing specialty record by selecting **Update** from the hidden menu of options. Users may add a new specialty record by clicking **Add** in the upper left-hand corner of the screen, as depicted in Figure 177 below.

Specialty	Sub Specialty	Specialty Level	Certified Date	Expiration Date
No Subspecialty	No Subspecialty	Fully Trained		

Figure 177: Specialty Section

The **Specialty** screen appears, as depicted in Figure 178 below. Users are required to enter the **Specialty**, **Sub-Specialty**, and **Level** of training to create a new specialty record.

Figure 178: Adding a Specialty

The pick list of values for **Specialty** reflects Health Insurance Portability and Accountability Act (HIPAA) health care provider taxonomy codes. The pick list of values for **Sub-Specialty** is driven by the choice of **Specialty**. These field dependencies are designed to maintain the consistency and integrity of information within the credentials record. The **Level** of training pertains directly to the **Specialty** and **Sub-Specialty** reported on this screen. The highest level of training achievable for physicians and dentists is *Board Certification*. User should only enter "**Board Certification**" for physicians and dentists who have been board-certified by a board belonging to the ABMS, AOA, or ADA. If physicians or dentists have completed all required professional training and licensure, but have not been board certified, then **Level** = *Fully Trained*.

The highest level of training that is achievable for all other practitioner types is *Fully Trained*. Providers who have not completed their required professional training should be designated as *In Training*.

Note: Users must document National certifications and registrations for allied health professions and other Providers on the **Licensure/Certification/Registration** tab (refer to [Section 6.3.5](#)). In the **Specialties** section, the term ‘Board Certification’ applies only to board-certified physicians and dentists.

6.3.8.1 Documenting Board Certification for Physicians and Dentists

When physicians or dentists have been designated as board-certified, additional data fields are presented that capture the information contained on the Provider’s certificate of board certification, as depicted in Figure 179 below.

Figure 179: Board Certification Section

To ensure data consistency, users should activate the search function to enter the name of the certifying board. The search function allows users to search for a board by entering a partial board name (e.g., enter “**surg**” to search for *American Board of Surgery* or a board affiliation (i.e., *ABMS*, *AOA*, or *ADA*), as depicted in Figure 180 below.

When users click **Search**, a list of boards that meet the search criteria displays on the screen. Users may then select the appropriate board from the list and click **OK**. The **Specialty** screen appears with the **Board** populated with the board name selected. **Certifying Board** is auto-populated with the correct board affiliation (i.e., *ABMS*, *AOA*, or *ADS*).

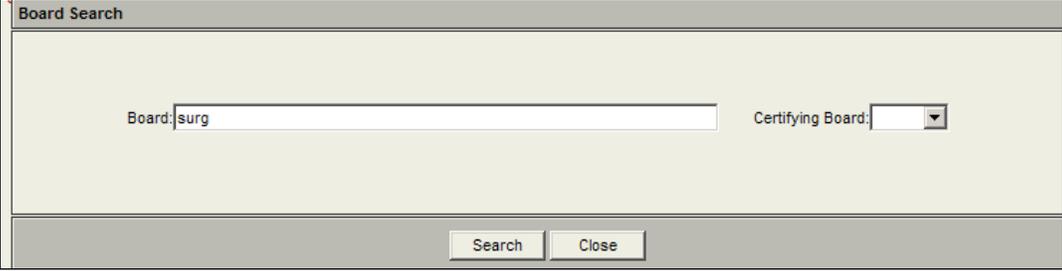


Figure 180: Board Search Screen

Note: If several search attempts have failed to find the correct board name, users should consult their Service CCQAS representative for further assistance.

The remaining fields in the **Board Certification** section should be populated with the **Certification Number**, **Certified Date**, and **Expiration Date** indicated on the Provider's certificate and the **Verified Date** when the certificate was PSV'ed. In the few cases where the certification has no associated expiration period or date, users should check **Expiration Indefinite** in lieu of entering an **Expiration Date**.

CCQAS requires full PSV documentation for board-certified specialties. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** section with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position are captured in the PSV entry history. PSV is required each time the board certification is renewed.

6.3.8.2 Designating Privileges

The privileging status of Providers should be designated by selecting the most appropriate radio button in the **Privileges** section of the **Specialty** screen. **Privileged** indicates that Providers currently hold privileges in their specialty. **Unprivileged** indicates that Providers are subject to privileging, but do not currently hold privileges in their specialty. **Written Plan of Supervision** indicates that Providers currently hold supervised privileges in their specialty. Navy and Coast Guard units/facilities use **Core**, **Core w/ Supplemental**, and **Itemized** in lieu of **Privileged** to assign privileging status to privileged Providers. Users should select a status of **Not Applicable** for any Provider who is not eligible for privileging (e.g., registered nurses, technicians, hygienists, etc.).

6.3.9 The Affiliation Section

The **Affiliation** section supports the documentation of a Provider's affiliations with other health care organizations. The **Affiliation** section consists of two tabs to document the Provider's Academic Affiliations and Organizational Memberships, as depicted in Figure 181 below. In general, Providers should update this information each time a new E-application for privileges is submitted. Occasionally, however, CC/MSSP/CMs may need to add or edit this information between privileging cycles.

Figure 181: Affiliation Section

6.3.9.1 The Academic Affiliations Tab

Users should create an **Academic Affiliation** to document any academic appointments or other professional associations with academic institutions, as depicted in Figure 182 below.

CCQAS requires the entry of the **Institution Name** and **Position** to save an academic affiliation record. A search function is provided to assist with the entry of the **Institution Name**. The **Institution Name** may also be typed directly on the screen as a free-text entry. The remainder of the fields on the screen should be populated to the extent appropriate to fully document a Provider's affiliation.

Figure 182: 'Academic Affiliations' Tab

6.3.9.2 The Organizational Memberships Tab

An **Organization Membership** refers to a Provider's membership in professional societies, associations, or other organizations, as depicted in Figure 183 below.

CCQAS requires the entry of the **Institution** and **Position** to save an organizational membership record. A search function is provided to assist with the entry of the **Institution**. The **Institution** may also be typed directly on the screen as a free-text entry. The remainder of the fields on the screen should be populated to the extent appropriate to fully document the Provider's membership.

The screenshot shows the 'Organizational Memberships' tab for provider ADAM CAROLLA. The page includes a navigation menu with options like 'Credentiaing', 'Privileging', 'Adverse Actions', 'Reports', 'System', and 'Help'. The provider's details are listed at the top: Name: ADAM CAROLLA, SSN: 100-55-7474, Branch: F11, Rank: Lt Gen, Corps: MC, and AOC/Desig/AFSC: 44F4. The main section is titled 'Organizational Memberships' and contains a form with fields for 'Institution Name' (with a dropdown menu showing 'UBHS'), 'Position', 'Address 1', 'Address 2', 'City/Town', 'State', 'Postal Code', 'Phone', 'Membership Dates' (From and To), 'POC Name', and 'POC E-mail'. There are also checkboxes for 'Military Facility', 'Civilian Facility', and 'Lifetime Member'. 'Save' and 'Close' buttons are at the bottom.

Figure 183: 'Organizational Memberships' Tab

6.3.10 The Continuing Education Section

The **Continuing Education** section supports the documentation of the continued medical and dental education that Providers have completed. In general, Providers should update this information each time a new E-application for privileges is submitted. Occasionally, CC/MSSP/CMs may need to add or edit this information between privileging cycles.

Users may edit an existing education record by selecting **Update** from the hidden menu of options. Users may create a new education record by clicking **Add** in the upper left-hand corner of the screen, as depicted in Figure 184 below.

The screenshot shows the 'Continuing Education' section for provider ADAM CAROLLA. It features a table with the following data:

Course Type	Credit Hours	Course Number / Sponsor	Training Description	Started	Completed
Dental Safety	3		Dental Safety	10/01/2012	10/05/2012

Buttons for 'Add', 'Update', and 'Delete' are visible on the left side of the table. A 'Help?' link is in the top right corner of the table area.

Figure 184: Continuing Education Section

The **Continuing Education** screen displays, as depicted in Figure 185 below. The **Type** of continuing education determines the other fields on the screen that are required to be filled out. The remaining fields on the screen should be completed according to the information provided on the training certificate and official course documentation.

After the screen has been populated with the required information, users click **Save**. The **Continuing Education** section displays, showing a summary of the new or updated training record.

The screenshot shows the 'Continuing Education' form for Provider ADAM CAROLLA. The form includes fields for Type (CDE), Course Title (CDE), Start Date, Course No. / Sponsor, Credits (MIL/ED, Other, RSRV / GRD, Unknown), Training Location (Skyline), Completion Date (10/05/2012), and Credit Category (2). A dropdown menu is open over the 'Credits' field, showing options: MIL/ED, Other, RSRV / GRD, and Unknown. The form also has 'Save' and 'Close' buttons at the bottom.

Figure 185: Continuing Education Record

CCQAS can accommodate as many training records as are required to completely document a Provider's training history. The "Additional Training" standard report allows users to report a summary of all continuing education completed by one or multiple Providers within a selected time period.

6.3.11 The Contingency Training Section

The **Contingency Training** section supports the documentation of the one-time and on-going medical and military training courses completed by Providers. In general, Providers should update this information each time a new E-application for privileges is submitted. Occasionally, CC/MSSP/CMs may need to add or edit this information between privileging cycles.

Users may edit an existing training record by selecting **Update** from the hidden menu of options, as depicted in Figure 186 below. Users may add a new training record by clicking **Add** in the upper left-hand corner of the screen.

The screenshot shows the 'Contingency Training' section for Provider ADAM CAROLLA. It features an 'Add' button and a table with columns for Type, Completion Date, Expiration Date, and Instructor. A dropdown menu is open over the 'Type' column, showing options: Add, Update, and Delete. The table contains one record: CBRNE - Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons, with a Completion Date of 9/4/2012 and no instructor listed.

Figure 186: Contingency Training Section

The Contingency Training screen appears, as depicted in Figure 187 below. Each contingency training record includes the **Training Type** and **Expiration Date** or **Completion Date**, depending on whether the course is a one-time or ongoing training requirement. In general, all Providers should hold a current Basic Life Support (BLS) certification, since BLS certification is a requirement for all health care providers. The other types of training generally only apply to specific groups of Providers.

Figure 187: Contingency Training Record

If the Provider is an instructor for any of the on-going courses being documented, check **Check here if you are an instructor**, and enter the expiration date of the Provider’s instructor certificate in the **Expiration Date** field. If the Provider is an instructor for a one-time training course, enter the expiration date of the instructor certificate in the **Remarks** section of the training record.

After the screen has been populated with the required information, users click **Save**. The **Contingency Training** section displays, showing a summary of the new or updated training record. CCQAS flags any expiration dates that are past the current date by displaying the date in red text and an exclamation point (!) to the right of the date field. Users may run the “Training Expiration” standard report to identify all Providers who have expired training certifications.

6.3.11.1 The References Section

The **References** section supports the documentation of individuals named as professional references. Providers are required to submit current references with their E-Application, which are then PSV’ed prior to application review. Occasionally, CC/MSSP/CMs may need to add or edit reference information directly into the Provider’s credentials record.

Users may edit an existing reference record by selecting **Update** from the hidden menu of options. Users may create a new reference record by clicking **Add** in the upper left-hand corner of the screen, as depicted in Figure 188 below.

?	Current	Name	Title/Position	Address	City	State
		DAVE	Clinical Supervisor			
		JESSICA	Clinical Supervisor			

Figure 188: References Section

The **Reference Name** and **Title/Position** are required on every reference record, as depicted in Figure 189 below. Although they are not displayed in red text, either an **Email**, **Phone #**, or **Fax #** are also required so that the reference may be contacted. Additional contact information should be entered, as available.

The screenshot shows the CCQAS Reference Record form for Adam Carolla. The form is divided into several sections:

- Provider Information:** Name: ADAM CAROLLA, SSN: 100-55-7474, Branch: F11, Primary UIC: CD1CFVPV, Rank: Lt Gen, Cred Status: Active, Corps: MC, Input Clerk: CM9, AOC/Desig/AFSC: 44F4.
- References:** Current Reference: Yes No. Reference Name: DAVE, Title/Position: Clinical Supervisor.
- Address:** Address 1: 123 address, Address 2: , Address 3: , Address 4: , City: Smalltown, State: OR, Province: , Zip: .
- Contacts:** Email: , Phone #: 123234 EXT. 56, Fax #: .
- Prime Source Verification (PSV) Information:** Current tab selected. Method: PSV Not Required, Written Correspondence, Telephone, Internet, Email. Source: E-Application. Verified Date: , Institution: , URL: . Entered By Name: MSSP152/MSSP152, Entered By Position: , Entered By UIC: N00080 (Non-Primary).

Figure 189: Reference Record

CCQAS requires full PSV documentation for current references submitted by Providers on their E-application. In general, the information displayed in the **PSV Information** section of this screen reflects the PSV information entered when a Provider's most recently submitted E-Application was processed. If the credential has not been previously PSV'ed, CC/MSSP/CMs should complete the PSV and document the details in the **PSV Information** section of the screen. If the PSV was previously performed, but not documented in CCQAS, CC/MSSP/CMs should populate the **PSV Information** section with the verification date and method indicated in the Provider's paper credentials file. The name, UIC, and position are captured in the PSV entry history. PSV of current references is required with each E-Application submitted.

6.3.11.2 The Databank Queries Section

The **Databank Queries** tab, depicted in Figure 190 below, supports the documentation of the results of NPDB, HIPDB, FSMB queries, and Other Reporting Agency Information. This section allows users to view the date and status of the last query made to each of the data banks and request a new data bank query, when needed.

In general, the **Last Query Date** in the NPDB and HIPDB sections of the screen should reflect the date when a Provider's last E-application was PSV'ed. The **Last Query Date** is updated in the Provider's credentials record each time the PSV of a privilege application is performed. CC/MSSP/CMs may also request a query anytime it is outside the normal privileging cycle by checking the **Request Query** box and clicking **Save**.

The screenshot displays the CCQAS interface for the Databank Queries section. At the top, it shows the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". The user is logged in as "CD1CFVPV" and the system is marked as "FOUO". The provider information for ADAM CAROLLA is shown, including SSN, Branch, Rank, Corps, and AOC/Design/AFSC. The interface is divided into sections for NPDB/HIPDB and FSMB/Other. The NPDB/HIPDB section includes a "Save" button, a "National Practitioner Data Bank (NPDB) Information" section with a "Request Query" checkbox, a "Query Results Pending" checkbox, and radio buttons for "Adverse Information On File" (Yes, No, No, but was previously Yes). Below this is a "National Practitioner Data Bank (NPDB) Query History" section with a table for query results. The HIPDB section has a similar layout with "Healthcare Integrity and Protection Data Bank (HIPDB) Information" and "Healthcare Integrity and Protection Data Bank (HIPDB) Query History".

Figure 190: Databank Queries Section

6.3.11.3 NPDB/HIPDB Query Requirements

The NPDB is primarily an alert system intended to restrict the ability of physicians, dentists, and other health care practitioners to move from state to state without disclosure or discovery of previous medical malpractice payment and adverse action history. Adverse actions can involve licensure, clinical privileges, professional society membership, and exclusions from Medicare and Medicaid.

The HIPDB is an alert system developed by HIPAA to combat fraud and abuse in health insurance and health care delivery. It serves to alert users that a comprehensive review of a practitioner's, Provider's, or supplier's past actions may be prudent. A query to the HIPDB is automatically generated when the NPDB is queried.

DoD Directive 6025.13 states that NPDB/HIPDB queries should be performed at a minimum of every two years, upon initial granting or renewal of clinical privileges at each privileging location, or in response to a specific concern, as appropriate. The NPDB/HIPDB requirement applies to all licensed practitioners who have the right to receive privileges. Users should consult Service policy if questions arise concerning the requirements and procedures associated with queries in the NPDB/HIPDB database.

There is a charge associated with performing NPDB/HIPDB queries, so not all users of CCQAS are authorized to perform them. Users are referred to their Service's privileging policy for further guidance requesting and obtaining NPDB and HIPDB query results.

6.3.11.4 FSMB Query Requirements

The FSMB maintains the Federation Physician Data Center, a central repository for formal actions taken against physicians by state licensing and disciplinary boards, Canadian licensing authorities, the U.S. Armed Forces, the U.S. Department of Health and Human Services, and other regulatory bodies. To be included in the Data Center, an action must be a matter of public

record or be legally releasable to state medical boards or other entities with recognized authority to review physician credentials. Actions fall into two categories: prejudicial (e.g., revocations, probations, suspensions, or consent orders) and non-prejudicial (e.g., reinstatements of licensure, replacement of lost or destroyed licenses, or license denials). After an action is reported to the Federation, it becomes part of a physician's permanent record. FSMB queries are made to the NPDB and HIPDB independently of queries.

Within DoD, FSMB requirements may vary according to Service regulations. The Army and Navy do not have a requirement for queries against the FSMB at this time. The Air Force requires a one-time FSMB query requirement for any practitioner with a practice history prior to January 1995. Additional queries may be requested if specific concerns regarding a Provider's practice history arise. All Air Force queries are performed centrally by Service personnel. If a query is needed, the CM should check the **Request Query** box and click **Save**. Air Force Service personnel enter query results into CCQAS after the query is performed and results are obtained.

6.3.12 The Custody History Section

The **Custody History** section in the credentials record is designed to display a complete history of a Provider's credentials custody, as depicted in Figure 191 below. This tab contains UIC, POC, Reason, Effective Date and End Date information for each facility that has had custody of the Provider's record. This information is read-only for informational purposes, and cannot be edited.

UIC	POC	Reason	Effective Date	End Date
27 SPECIAL OPERATIONS MEDICAL GROUP @ CANNON AFB (CD1CFVPV)	Mrs. Karen Bair (SGHC) Phone: 575.784.8608 DSN: 681.9609 Fax: Comm: 575.784-8608 DSN: 681.6028 Email: JESSICA.NEWTON@AMR.COM	Provider has been assigned to this UIC	09/25/2012	

Figure 191: Custody History Section

6.3.13 The Work History Section

The **Work History** section in the credentials record is designed to manage all current and past Assignments (MIL/CIV or Other) for Providers, their Work History, and their Malpractice Insurance, as depicted in Figure 192 below.

UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date	Transferred From	Dept	Work Center	Primary Specialty	Primary Sub-Specialty	Privilege Status	Privilege Type	PAR Expected	PA
N00060	Civil Service Employee			CV	CRED	Current	10/15/2012									No	
CD1CFVPV	Administrative			MIL	CRED	Current	09/25/2012									No	

Figure 192: Work History Section

6.3.13.1 The Assignments Tab

The **Assignments** tab, within the **Work History** section, is designed to capture a Provider's assignment history in DoD facilities (refer to Figure 193 below). The UIC, Provider Type, Reported Date, Planned Rotation, MIL/CIV, Type, Status, Start Date, End Date, Transferred From, Dept, Work Center, Primary Specialty, Primary Sub-Specialty, Privilege Status, PAR Expected, PAR Date, and Type of Duty information for each permanent and temporary duty assignment is documented as a separate assignment record. CCQAS automatically creates a new assignment record each time an ICTB or PCS transaction is performed on a Provider's credentials record. CC/MSSP/CMs are responsible for populating the assignment record pertaining to a Provider's duty at his or her location.

UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date	Transferred From	Dept	Work Center	Primary Specialty	Primary Sub-Specialty	Privilege Status	Privilege Type	PAR Expected	PA
N00060	Civil Service Employee			CV	CRED	Current	10/15/2012									No	
CD1CFVPV	Administrative			MIL	CRED	Current	09/25/2012									No	

Figure 193: 'Assignment' Tab

The assignment record that pertains to a CC/MSSP/CM's own location is displayed in bold text on the **Assignments** screen, as depicted in Figure 194 below. This is the only assignment record CC/MSSP/CMs are able to edit. Information entered for all other assignment locations is presented as view-only.

CC/MSSP/CMs may enter or edit assignment information by selecting **Open** from the menu of available actions for the appropriate assignment record. CC/MSSP/CMs may also open the desired record by double-clicking anywhere on the summary record line.

The screenshot displays the 'MTF Assignment Record' for provider ADAM CAROLLA. The interface includes a navigation menu (Credentiaing, Privileging, Adverse Actions, Reports, System, Help) and a header with the CCOAS logo and 'FOUO' marking. The record details include:

- Provider Information:** Name: ADAM CAROLLA, SSN: 100-55-7474, Branch: F11, Rank: Lt Gen, Corps: MC, AOC/Design/AFSC: 44F4.
- Assignment Section:** Assignment UIC: CD1CFVPV, Start Date: 09/25/2012, End Date, Dept Code, Work Center, Planned Rotation, Last Perf. Appraisal, and Provider Type: ADM - Administrative.
- Military/Civilian Section:** Branch: F11 - Air Force (USAF), Rank: Lt Gen - Lieutenant General, Corps: MC - Medical Corps, Accession: *- Unknown.
- Primary Business Address:** Fields for Address 1, 2, 3, City/Town, State, Country, Province, Postal Code, POC Name, and POC Phone.
- Privileges Table:**

Primary	Specialty	SubSpecialty	Privilege Type	Status	Comment
C	Endodontics	No Subspecialty	Unpriviledged	Unpriviledged	

Figure 194: MTF Assignment Record

The **Assignment** section of an “MTF Assignment” record is designed to capture the location and dates associated with the assignment, as depicted in Figure 194 above. The value for **Assigned UIC** is prepopulated with the UIC listed in the upper right-hand corner of the screen, but may be edited, if appropriate. **Other UIC** is provided to document other locations where Providers may also work, as part of their assigned duties to this location. This value may be edited, as appropriate. The search function should be used to edit or enter the **Assigned UIC** or **Other UIC**, to ensure the code is entered correctly.

The **Dept Code** and **Work Center** reflect the values entered (if any) on the **Profile** tab for the assignment record associated with a Provider’s permanent work location. In other words, the values of **Dept Code** and **Work Center** on the two tabs are always synchronized for the current permanent assignment. For ICTB assignment records, CC/MSSP/CMs should enter the appropriate information corresponding to the ICTB location. The **Provider Type** is a required field for all assignment records to describe the specific situation under which a Provider is performing duty at the assignment location. The **Reported** and **Planned Rotation** date field define the start and end date of the assignment, respectively. The **Last Perf Appraisal** refers to the clinical performance assessment specifically associated with the Provider’s duties while at that assignment.

The **Primary Business Address** section of an assignment record is view-only and auto-populated with primary work address information entered in the **Contacts** section of the Provider’s credentials record. If work address information needs to be added or edited, all changes must be made in the **Contacts** sections. After the address changes are entered and saved, the new information will be reflected on the assignment record.

The **Privileges** tab of the assignment record, depicted in Figure 195 below, summarizes the Provider's privileging status at that assignment. The **Staff Appoint**, **Priv-Cat**, and their respective **Expires** dates are view-only and auto-populated from information entered in the **Privileges** section of the credentials records (refer to [Section 6.3.14](#)). CC/MSSP/CMs should enter the **Position Title**, any appropriate **PCM** information, and select the appropriate checkboxes and radio buttons in the **Privileges** section to indicate the specialties in which the Provider is privileged at this assignment. Pertinent explanatory remarks may be entered in the **Remarks** section of the record. This is also where CC/MSSP/CMs can add offline privileges to an assignment.

UIC	Status	App Type	Provider Category	Corps	Military/Civilian	Type of Appointment	Type of Privileges	App Date	Effective Date	Expiration Date
CD1CFVPV	Inactive	1st E-App	Dentist	DC	MIL					

Figure 195: 'Work History Privileges' Tab

The **Tracker Status** tab of the **Work History** section, depicted in Figure 196 below, is designed to display and add **Assignment Status**, **Assignment Status Date**, and **Assignment Status Remarks** data.

Assignment Status	Assignment Status Date	Assignment Status Remarks
No Records Returned		

Figure 196: 'Tracker Status' Tab

6.3.14 The Privileges Section

The **Privileges** section in the credentials record maintains a repository of all privileges granted to Providers at all privileging locations, via the CCQAS electronic privileging process, or the offline privileging process. Each approved privilege application is documented as a separate record on this screen. CCQAS automatically adds a new privileging record each time a privilege application is approved for a Provider. If the Provider has not yet been privileged via the online privileging process, this section of his or her credentials record is empty. If the Provider is not eligible for privileging, the **Privileges** section of his or her credentials record is not enabled. Figure 197 below depicts the **Privileges** section.

The screenshot shows the CCQAS interface for the Privileges section. At the top, it displays the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". The user is logged in as CD1CFVPV. The main header includes "Credentiaing", "Privileging", "Adverse Actions", "Reports", "System", and "Help". The provider information for Samantha Newton is shown, including her SSN, Branch (N11), Rank (ADM), Corps (MC), and AOC/Design/AFSC (2100). Below this, there is a table of privileges with columns for UIC, Status, App Type, Provider Category, Corps, Military/Civilian, Type of Appointment, Type of Privileges, App Date, Effective Date, and Expiration Date. The "Open" option is highlighted in the table.

UIC	Status	App Type	Provider Category	Corps	Military/Civilian	Type of Appointment	Type of Privileges	App Date	Effective Date	Expiration Date
Open	Active	Transfer (PCS)	Physician	MC	ML			10/11/2012	10/11/2012	10/10/2014
View Privileges	Active	1st E-App	Physician	MC	ML			08/27/2012	08/27/2012	10/18/2012
N00000	Inactive	Modification	Physician	MC	ML			08/27/2012	08/27/2012	10/18/2012

Figure 197: Privileges Section

Each privileging record provides a hidden menu of options. The **Open** option opens the **Provider Privileges** screen, as depicted in Figure 198 below.

This screen is auto-populated from the information contained in the **Position** tab of the approved privilege application. For current privileging records, CC/MSSP/CMs may edit the information on this screen, as needed, to reflect the Provider's assignment information accurately. CCQAS automatically calculates the staff appointment and privilege expiration dates using the date that the PA used to approve the privilege application. CC/MSSP/CMs may edit the type of appointment and privileges requested, as well as their respective expiration dates, as long as the appointment and privileging periods do not exceed the 12 months for initial appointments, or 24 months for regular appointments. After all edits are made, click **Save** to save the information and return to the **Privileges** section.

The screenshot shows the CCQAS interface for the Provider Privileges screen. At the top, it displays the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". The user is logged in as CD1CFVPV. The main header includes "Credentiaing", "Privileging", "Adverse Actions", "Reports", "System", and "Help". The provider information for Joshua Peters is shown, including his SSN, Branch (F11), Rank (Lt Gen), Corps (MC), and AOC/Design/AFSC (4000). Below this, there is a form for editing provider privileges. The form includes fields for Provider Category (Physician), Duty Section, Duty Phone, Date Reported to Current Assignment, Rotation/Permanent Change of Station Date, Effective Date (10/15/2012), Type of Privileges, Type of Appointment, Privilege Expiration (10/14/2014), and Staff Appointment Expiration (10/14/2014). The "Edit" option is highlighted in the form.

Figure 198: Provider Privileges Screen

Note: The **Edit** option for privileging records that are no longer current allows users to view, but not edit, the **Provider Privileges** screen.

A view-only listing of any approved privileges is displayed by selecting **View Privileges** from the hidden menu of actions for the privileging record. The “Privileged Provider Information” Report then displays, as depicted in Figure 199 below.

**** FOUO ****

Name: GRISWALD, CLARK, Appointment: Priv. Granted Date: 25 Oct 12
 Mil/Civ: Military Corps: MC Privilegas: Priv. Expiration Date: 24 Oct 14

PRIVILEGED PROVIDER INFORMATION REPORT

SERVICE: Air Force UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @		
PROVIDER GRISWALD, CLARK	SSN XXX-XX-7171	MILITARY/CIVILIAN Military
ORGANIZATION UNIT 27 SPECIAL OPERATIONS MEDICAL GROUP @	MILITARY/CIVILIAN ADMITTING Military	TYPE OF PRIVILEGES No
PRIVILEGE CATEGORY: Aerospace Medicine Version 1.0		
Physicians requesting privileges in this specialty must also request privileges in their primary discipline and/or General Medical Officer privileges. Physicians requesting privileges in this specialty must also request Flight Surgeon privileges.		
Scope		
PRIVILEGE ITEM (S)	REQUESTED	APPROVED
The scope of privileges for Aerospace Medicine physicians includes the evaluation, diagnosis, treatment and consultation on an outpatient basis of pilots, aircrew and patients who are transported by rotary or fixed-wing aircraft. Aerospace Medicine physicians are responsible to discover and prevent various adverse physiological responses to hostile biologic and physical stresses encountered in the aerospace environment, perform aeromedical evacuation and patient transport evaluations as well as special operational evaluations, perform evaluation and initial management of decompression illness, investigate disaster/mishap response, perform deployment and travel requirements evaluations, and apply operational medicine education to individuals and groups under their care.	Fully Competent	Fully Competent
Aerospace Medicine Physicians may assess, stabilize, and prepare for aeromedical transport of patients with stable or emergent conditions, consistent with medical staff policy.		

Figure 199: Privileged Provider Information Report

This report provides a listing of all privileges requested by a Provider and approved by the PA. If a requested privilege is not supported at the facility or unit, **Not Supported** is displayed in the **Approved** column of the report. Users may print this report by clicking **Print**. Users then click **Close** to return to the **Privileges** section.

6.3.15 The Provider Photo Section

The **Photo** section allows CC/MSSP/CMs to upload and store a photograph of a Provider in his or her credentials record, as depicted in Figure 200 below. The addition of a photo to the credentials record is important to support visual confirmation of a Provider’s identity. A **Photo** section is not present in a Provider’s E-Application. It is the responsibility of CC/MSSP/CMs to upload an authenticated photo of a Provider into this section of the Provider’s credentials record in accordance with Service guidance.



Figure 200: Photo Section

The photograph must be 1 megabyte (MB) or less in size to be uploaded to CCQAS; have a .pdf, .jpeg, or .gif file extension; and already be loaded onto a user's workstation or electronically accessible on a local network. To upload the photo, users click the **Browse** button and enter the file pathway that describes the photo's location on their hard drive or network. After the file pathway is specified, click **Upload Photo**. Depending on the computer and network speed, the photo may take several minutes to upload.

A Provider's photo should be updated periodically. To update a photo, the existing photo should first be deleted by clicking the **Delete Photo** button. A new photo may then be uploaded using the process described above.

6.3.16 The Documents Section

The **Documents** section stores all documents that Providers or CC/MSSP/CMs have uploaded to CCQAS to date. It also stores "PAR" documents and privilege, application, and Appendix Q "Snapshots" that CCQAS automatically generates. The **Provider Documents** and **PAR/Snapshots** radio buttons allow users to toggle between these different types of documents.

The process of adding Provider documents to a privilege application is explained in [Section 5.5.4](#) in this manual. All documents uploaded during the application process are listed in the **Documents** section of the credentials record, following application approval and closure. CC/MSSP/CMs may download, rename, delete, or send a message regarding existing documents in the **Documents** section of a Provider's credentials record at any time by selecting the appropriate option from the hidden menu of actions for each document record, as depicted in Figure 201 below.



Figure 201: Documents Section

New documents may be added to a Provider's credentials record at any time by clicking the **Add** button. In order to be uploaded into CCQAS, each individual document must be 5MB or less in size and have a .pdf, .jpeg, or .gif file extension.

Other important features of the **Provider Documents** screen include the following:

- Users may search the list of documents associated with the application by selecting the desired document type from the **Filter by File Type** pick list
- The summary line for each uploaded document includes the type of document, when it was uploaded and by whom, and the name of the file that was uploaded
- Users may view the document by selecting **Download** from the hidden menu of actions for the document record
- The **User's Name** and **User's UIC** reflect the individual who uploaded the document to the application and the **Upload Date** reflects the date and time the document was originally uploaded

CCQAS automatically generates a PDF file at various points in time during the processing of an E-application or electronic PAR form. Users may view these PDF files by selecting the **PARs/Snapshots** radio button at the top of the screen, as depicted in Figure 202 below. A PAR PDF file is generated each time PAR Evaluators, PAR Reviewers, or Providers complete their electronic review of the PAR. "Snapshots" are CCQAS-generated PDF files of the privilege application created each time a Provider or PA E-signs the E-application or Appendix Q, and when PSV of the E-application has been completed. Thus, several PDF files for each E-Application and PAR may be listed on the screen.

Application Type	File Type	Description	Created Date
1st E-App	Application Packet	PA Review Complete	10/1/2012 5:08:00 PM
1st E-App	Application Packet	PSV Complete	10/1/2012 5:01:28 PM
1st E-App	Application Packet	E-Signature Complete	10/1/2012 4:58:32 PM
1st E-App	Application Packet	E-Signature Complete	10/1/2012 4:54:28 PM
1st E-App	Application Packet	E-Signature Complete	10/1/2012 4:51:56 PM
1st E-App	Application Packet	PSV Complete	9/18/2012 12:27:40 PM
1st E-App	Application Packet	E-Signature Complete	9/18/2012 12:24:37 PM

Figure 202: PARs/Snapshots listing

The time and date that each PDF file is generated is documented on the right-hand side of the screen to assist users in identifying the most recently generated PDF file of the desired document. The PDF file may be viewed by selecting **Download** from the hidden menu of actions for the record.

Note: All previously submitted E-Applications, Appendix Q documents, and PAR forms, regardless of privileging location, are displayed on this screen.

6.3.17 The Remarks Section

The **Remarks** section is the final listed section of the of a Provider's credentials record, as depicted in Figure 203 below. The **Remarks** functionality is a customizable feature of CCQAS that allows each Service and facility to decide if and how it should be used. There is no **Remarks** section in the Provider's E-Application that populates the **Remarks** section of the credentials record. It is the responsibility of CC/MSSP/CMs to use this functionality in accordance with Service guidance and facility practice.

Type	Remarks	Entered By	Date Entered	Modified By	Date Modified	Global
No Records Returned						

Figure 203: Remarks Section

The **Remarks** section remains empty until the **Provider Remarks Type** pick list is configured. Any user may perform this configuration, as long as he or she has permission to access the **Provider Remarks** menu item under the **System** main menu. Figure 204 below depicts the **Provider Remarks** section.

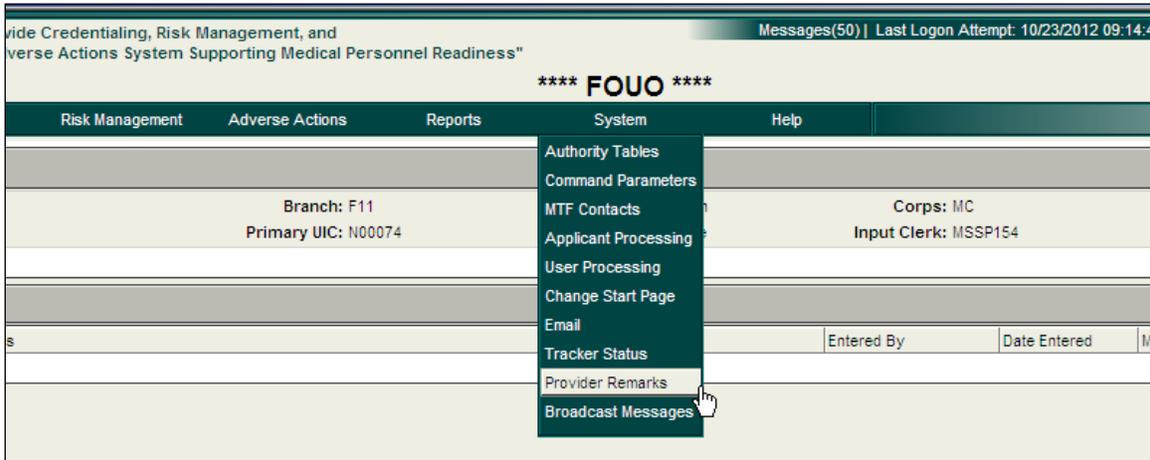


Figure 204: Provider Remarks Section

The **Provider Remarks Type** window opens, as depicted in Figure 205 below. The pick list options for **Provider Remarks** are created when CC/MSSP/CMs click **Insert** in the upper left-hand corner of the screen.

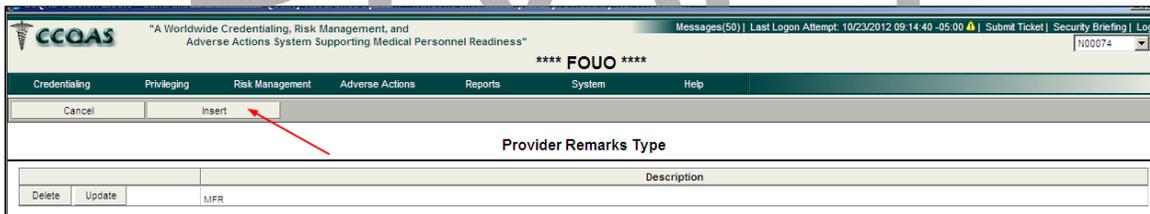
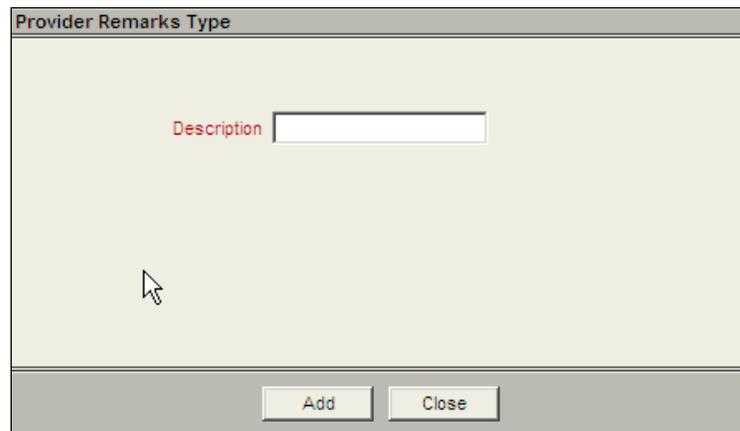


Figure 205: Provider Remarks Window

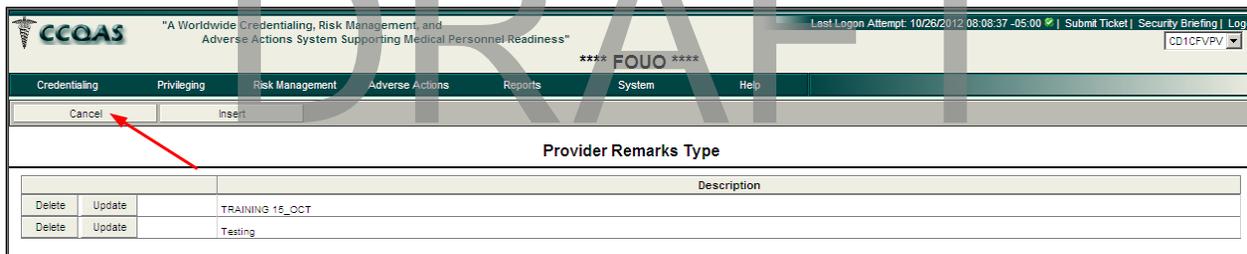
After CC/MSSP/CMs enter a free-text **Description** and click **Add**, the **Provider Remarks Type** displays one new entry. Figure 206 below depicts the **Provider Remarks Type** screen.



The screenshot shows a window titled "Provider Remarks Type". Inside the window, there is a text input field with the label "Description" in red text to its left. Below the input field, there are two buttons: "Add" and "Close". A mouse cursor is visible over the input field.

Figure 206: Provider Remarks Type Screen

Additional remarks types may be entered by repeating this process until the complete list of pick list values have been created, as depicted in Figure 207 below. After all desired values have been created, CC/MSSP/CMs click **Cancel** to complete the configuration process.



The screenshot shows the CCQAS application interface. At the top, there is a header with the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". Below the header is a navigation menu with options: Credentialing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. The main content area is titled "Provider Remarks Type" and contains a table with two entries. A red arrow points to the "Cancel" button in the top left corner of the table area.

		Description
Delete	Update	TRAINING 15_OCT
Delete	Update	Testing

Figure 207: Provider Remarks Type Screen

After the **Provider Remarks** pick list has been configured, CC/MSSP/CMs may enter remarks into the credentials record, as depicted in Figure 208 below.

Figure 208: Provider Remarks Type Screen

CC/MSSP/CMs enter the **Type** of remark and text in the **Remarks** field, and then click **Save**, as depicted in Figure 209 below. The **Remarks** section displays, showing the remark that was just entered, the name of the individual who entered it, and the date it was entered. Another new remark may be entered by clicking **Add Provider Remarks** in the upper left-hand corner of the screen.

Type	Remarks	Entered By	Date Entered	Modified By	Date Modified	Global
	User guide section 6	ADMIN	10/23/2012			Yes

Figure 209: Provider Remarks Menu Options

CC/MSSP/CMs may edit a remark by selecting **Update** from the hidden menu, or delete it by selecting **Delete**. The name of the user and the date of editing is documented each time a remark is updated. The content of the **Remarks** Section may be printed in one of several ways. Individual remarks may be printed by selecting **Print** from the hidden menu of options. To print all remarks on this screen, click **Print Preview**. In both cases, the document to be printed appears in a separate browser window. Users have the options to change the font style and size, print the document, or save it to their hard drive or network.

6.4 Updating Credentials Records Using Batch Processing

At any point in time, CC/MSP/CMs may access a Provider's credentials record to update training information or perform a variety of transactions on an individual record. Updates and transactions may also be "batch" processed, which enables users to update multiple records with the same data, without having to edit each Provider's record individually. Since batch processing results in the same action being performed on multiple records, the update must be exactly the same for all records involved. For example, a **Batch Training** action is only appropriate if all of the records included in the batch need to be updated to reflect completion of the same class or course. Other actions that may be batched include ICTB and PCS transactions (ICTB and PCS transactions are discussed in Sections 8 and 9, respectively), deactivation and reactivation of credentials records (see sections below), and a variety of letters.

All batch actions are initiated from the **Credentialing > Batch Processing** menu, as depicted in Figure 210 below.



Figure 210: Credentialing Batch Process Menu

Provider records may be batch-processed by selecting the appropriate radio button in the **Batch Job Type** section of the screen, as depicted in Figure 211 below. Notice that the sample screenshot below illustrates the **Batch Training** radio button as selected. **Batch Training** supports the addition of training information to the **Continuing Education** and **Contingency Training** sections of Providers' credentials records.

Users may enter additional search criteria in the upper portion of the **Credentials Provider Search** screen if they wish to limit the batch action to only certain groups of records (e.g., only Providers in a specific department, work center, corps, or unit). After all appropriate search criteria are entered and the desired batch action is selected, users click **Search**.

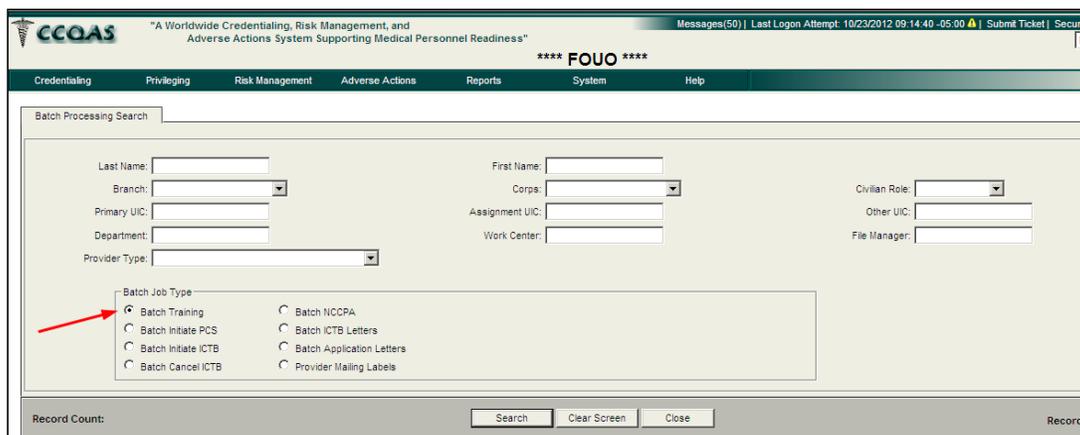


Figure 211: Action Section of the Credentials Provider Search Screen

A list of Providers that meet the search criteria specified is displayed on the **Batch Training** tab, as depicted in Figure 212 below. Users may check which Providers from the search list should be included in the transaction, enter the appropriate training information, and then click **Submit Batch**. Other batch actions may be performed in the same manner as the example above.

The screenshot shows the CCQAS interface with the 'Batch Training' tab selected. A table lists providers with columns for Name, SSN, UIC, Type, Brch, Crps, Start Date, and End Date. Below the table, there is a 'Training' section with radio buttons for 'Continuing Education' (selected) and 'Contingency Training'. A dropdown menu for 'Type' is open, showing options: CDE, CEU, CHE, CME, CNE, MIL ED, Other, RSRV / GRD, and Unknown. Other fields include 'Course Title', 'Start Date', 'Course No. / Sponsor', 'Training Location', 'Completion Date', and 'Credit Category'. At the bottom, there are 'Submit Batch' and 'Cancel' buttons, and a 'Record Limit' of 100.

Name	SSN	UIC	Type	Brch	Crps	Start Date	End Date
<input type="checkbox"/> ALLEN, PAUL	100-44-8868	CD1CFV/PV	CRED	F11	MC	10/01/2012	
<input type="checkbox"/> ANG, Civil Registration	082-52-0122	N00074	CRED			08/25/2012	
<input type="checkbox"/> AS, APPENDIX Q NC	082-72-0123	N00074	CRED	N13	MC	08/27/2012	
<input type="checkbox"/> ASI, UMI educ	082-42-0121	N00074	CRED	N13	MSC	08/24/2012	
<input type="checkbox"/> CRED, NC AVDERSE	082-72-0122	N00074	CRED			08/27/2012	
<input type="checkbox"/> CRED, NC PRIV app	082-52-0121	N00074	CRED	N13	MSC	08/25/2012	
<input type="checkbox"/> NEWTON, SAMANTHA	777-86-5555	CD1CFV/PV	CRED	N11	MC	10/11/2012	
<input type="checkbox"/> PETERS, JESSICA	100-99-3232	N00074	CRED			10/19/2012	

Figure 212: Continuing Education Batch Training Screen

After the batch is submitted, all Provider records included in the batch are automatically updated to include the new training course information in the appropriate section of the Provider's credentials record.

Records that are updated or transacted through batch processing remain independent of each other after the batch action has been completed. For example, if a **Batch ICTB** transaction is performed, and then one or more Providers in the batch do not perform the ICTB as planned, individual ICTB transactions may be cancelled or ended without impacting the ICTB transactions for the remainder of the batch.

6.5 Deactivating a Credentials Record

When a Provider's record is deactivated, the record status in CCQAS changes from *Current* to *Inactive*. This action may be appropriate when military Providers retire from active duty service or for civilian or contract employees whose employment arrangement has ended. Not all users have the necessary permissions to deactivate a Provider's record. For those who do have the necessary permissions, users should consult Service policies prior to deactivating any Provider credentials records.

In order to deactivate an individual Provider's record that is currently in active status, users must perform a search for the record, using record **Status** = *Active* (the default setting). An individual Provider may be deactivated by selecting **Deactivate Provider** from the menu of Provider actions, as depicted in Figure 213 below.

The screenshot shows the CCQAS web application interface. At the top, there is a header with the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". Below this is a navigation bar with tabs for Credentiaing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. The main content area displays a table of providers with columns for Name, SSN, Primary UIC, Start Date, Branch, Corps, Status, Cred Status, NPI, and Active Assignments. A context menu is open over the first row (ALLEN, PAUL), with the "Deactivate Provider" option highlighted. The table contains 11 records.

Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
ALLEN, PAUL	100-44-8888	N00074	09/18/2012	F11	MC	Dual	Active		2
	082-52-0122	N00074	08/25/2012			CV	Active		1
	082-72-0123	N00074	08/27/2012	N13	MC	MIL	Active		1
	082-42-0121	N00074	08/24/2012	N13	MSC	MIL	Active		1
	082-52-0121	N00074	08/25/2012	N13	MSC	MIL	Active		1
	082-72-0122	N00074	08/27/2012			MIL	Active		1
KENT, TRACY	100-23-4444	CD1CFVPV	09/19/2012	F11	MC	Dual	Active		2
NEWTON, SAMANTHA	777-66-5555	N00074	10/18/2012	N11	MC	Dual	Active		2
PETERS, JESSICA	100-99-3232	N00074	10/19/2012			MIL	Active		1
ROSS, TERRY	100-99-2727	CD1CFVPV	10/23/2012			Dual	Active		2
SMITH, MARK	200-55-9999	N00211	10/15/2012	F11	MC	Dual	Active		3

Figure 213: Deactivate Provider Menu Item

Users then enter the **End Date** and **Disposition**, indicating when and why the record should be deactivated, as depicted in Figure 214 below.

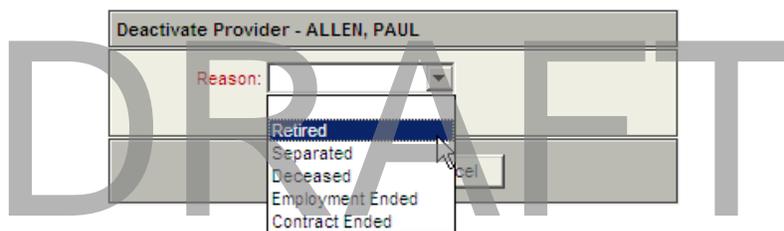


Figure 214: Deactivate Provider Screen

If the current date is set as the **End Date**, the Provider's record is placed in inactive status directly after the record is deactivated. If the **End Date** is set to a future date, the record becomes inactive at midnight (Central Time) on the day before the effective date. The inactive record will not be included in system queries or reports unless users include inactive records as part of their search and reporting criteria.

6.6 Generating Provider Mailing Labels

CCQAS supports the generation of mailing labels for any Provider or set of Providers with a CCQAS credentials record. Complete instructions for generating mail labels are available from the **Help** menu (**Instructions > Mailing Labels**), as depicted in Figure 215 below.

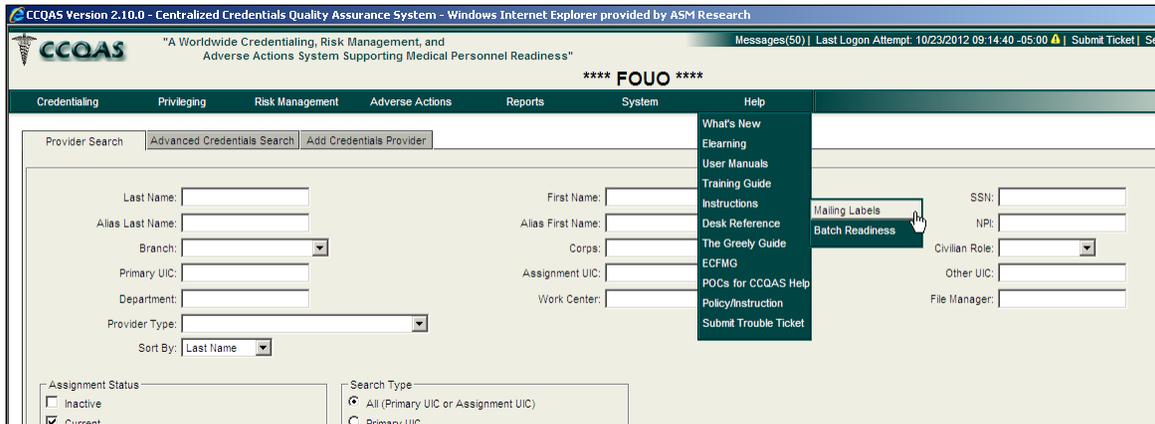


Figure 215: Mailing Labels Menu Item

The generation of mailing labels is initiated from the **Credentialing > Batch Processing** screen by selecting **Provider Mailing Labels** in the **Batch Job Type** section of the screen, as depicted in Figure 216 below.

CC/MSSP/CMs may enter additional search criteria in the upper portion of the **Credentials Provider Search** screen if they wish to generate mailing labels for only certain groups of Providers (e.g., only Providers in a specific department, work center, corps, or unit). After all appropriate search criteria are entered and the desired batch action is selected, click **Search**.

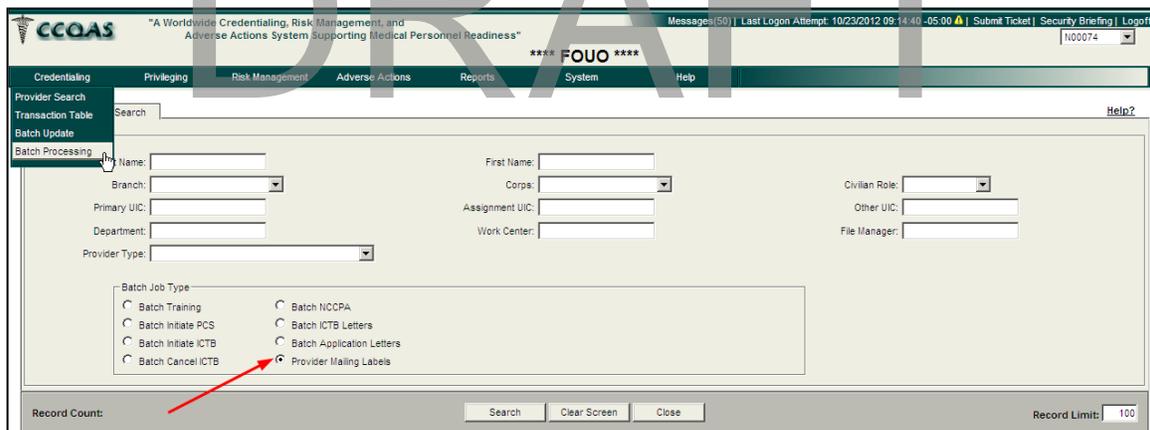
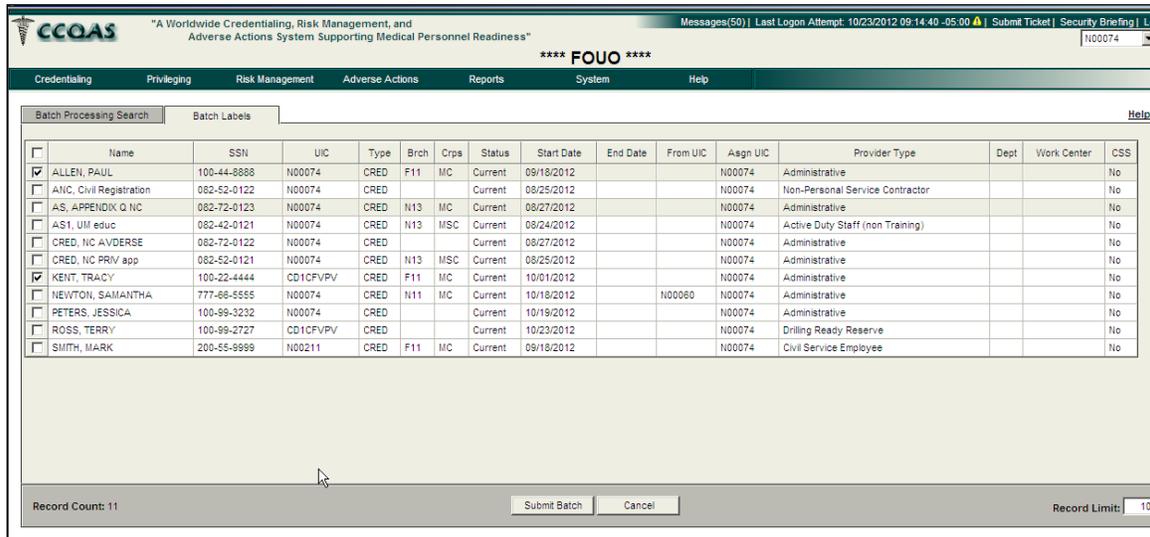


Figure 216: 'Provider Mailing Label' Radio Button

A list of Providers that meet the search criteria specified displays on the **Batch Labels** tab, as depicted in Figure 217 below. CC/MSSP/CMs may check which Providers for whom mailing labels should be generated, and then click **Submit Batch**.



The screenshot shows the 'Batch Labels' tab in the CCQAS application. At the top, there is a navigation menu with options: Credentiaing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. Below the menu, there are two tabs: 'Batch Processing Search' and 'Batch Labels'. The 'Batch Labels' tab is active, displaying a table with 11 records. The table columns are: Name, SSN, UIC, Type, Brch, Crps, Status, Start Date, End Date, From UIC, Asgn UIC, Provider Type, Dept, Work Center, and CSS. The records are as follows:

Name	SSN	UIC	Type	Brch	Crps	Status	Start Date	End Date	From UIC	Asgn UIC	Provider Type	Dept	Work Center	CSS
<input checked="" type="checkbox"/> ALLEN, PAUL	100-44-8888	N00074	CRED	F11	MC	Current	09/18/2012			N00074	Administrative			No
<input type="checkbox"/> ANIC, Civil Registration	082-52-0122	N00074	CRED			Current	09/25/2012			N00074	Non-Personal Service Contractor			No
<input type="checkbox"/> AS, APPENDIX Q NC	082-72-0123	N00074	CRED	N13	MC	Current	09/27/2012			N00074	Administrative			No
<input type="checkbox"/> ASI, Ull educ	082-42-0121	N00074	CRED	N13	MSC	Current	09/24/2012			N00074	Active Duty Staff (non Training)			No
<input type="checkbox"/> CRED, NC AVDERSE	082-72-0122	N00074	CRED			Current	09/27/2012			N00074	Administrative			No
<input type="checkbox"/> CRED, NC PRIV app	082-52-0121	N00074	CRED	N13	MSC	Current	09/25/2012			N00074	Administrative			No
<input checked="" type="checkbox"/> KENT, TRACY	100-22-4444	CD1CFVPV	CRED	F11	MC	Current	10/01/2012			N00074	Administrative			No
<input type="checkbox"/> NEWTON, SAMANTHA	777-86-5555	N00074	CRED	N11	MC	Current	10/18/2012		N00060	N00074	Administrative			No
<input type="checkbox"/> PETERS, JESSICA	100-99-3232	N00074	CRED			Current	10/19/2012			N00074	Administrative			No
<input type="checkbox"/> ROSS, TERRY	100-99-2727	CD1CFVPV	CRED			Current	10/23/2012			N00074	Drilling Ready Reserve			No
<input type="checkbox"/> SMITH, MARK	200-55-9999	N00211	CRED	F11	MC	Current	09/18/2012			N00074	Civil Service Employee			No

At the bottom of the table, there is a 'Record Count: 11' and a 'Record Limits: 10' field. Below the table, there are two buttons: 'Submit Batch' and 'Cancel'.

Figure 217: 'Batch Labels' Tab

CC/MSSP/CMs are then given options for the types of mailing labels they wish to generate for the selected Providers, as depicted in Figure 218 below.

After the desired mailing label option is selected, CCQAS copies all of the applicable data to the **Clipboard** function on the user's desktop. The contents of the clipboard then need to be downloaded to a Microsoft Word® or Excel® file for editing and printing. Users are referred to the instructions provided from the CCQAS **Help** menu for additional assistance in editing and printing the mailing labels.

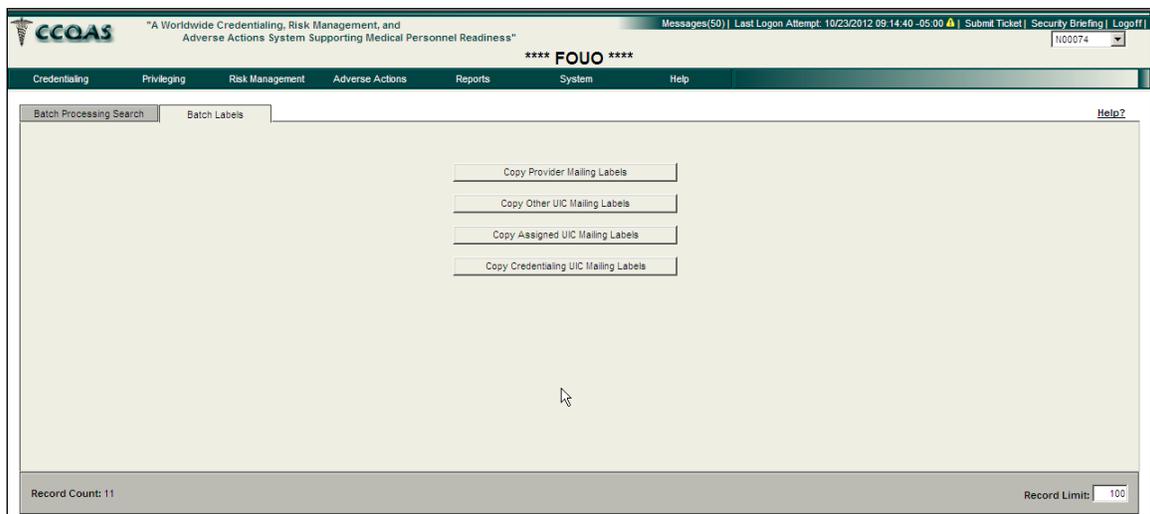


Figure 218: Batch Labels Options

7 Modification of Provider Credentials and Clinical Privileges

Changes in a Provider's professional credentials should be updated in CCQAS in a timely manner. The method for updating CCQAS with new credentialing information depends on whether or not a Provider wishes to request a change in clinical privileges commensurate with the new credentials. If the new credentials do not warrant a change in the Provider's current privileging status, or the Provider does not wish to change his or her current privileges, the credentials record may be updated in one of the following ways:

- CC/MSSP/CMs may enter the new information directly into the Provider's CCQAS credentials record, based on the appropriate documentation received from the Provider or other trusted source. This process does not change the Provider's current clinical privileges; it only ensures that the most recent credentials information is available in CCQAS (refer to [Section 6](#)), or
- The Provider may add the new credentials information to his or her next application for renewal of clinical privileges (refer to [Section 10](#)) or an application for privileges at a new duty station (refer to [Section 9](#))

If the change in credentials supports a change to the Provider's current clinical privileges, then the Provider may wish to request modification of privileges before the next privilege renewal cycle. In this case, the Provider may submit an application for modification or augmentation of privileges and include any new credential(s) with that application. An application for modification or augmentation of clinical privileges may also be appropriate when a facility or unit has begun to support one or more privilege items that the Provider previously requested, but was not granted on the basis of the facility not having the resources to support the privilege(s).

7.1 Generating an Application for Modification or Augmentation of Privileges

After Providers are granted clinical privileges at a facility via the CCQAS online privileging process, a modification or augmentation of the current, approved privileges may be requested at any time. An application for modification of privileges can be initiated by a Provider or the PAC.

To generate the application as a Provider, users in this role simply log in to CCQAS, click the **Applications** tab, and select "**Request Modification**" from the hidden menu of actions for the most recently approved privilege application. The hidden menu can be viewed by either right-clicking the privilege application record or by clicking the **Hidden Menu** icon  to the left of the record, as depicted in Figure 219 below.

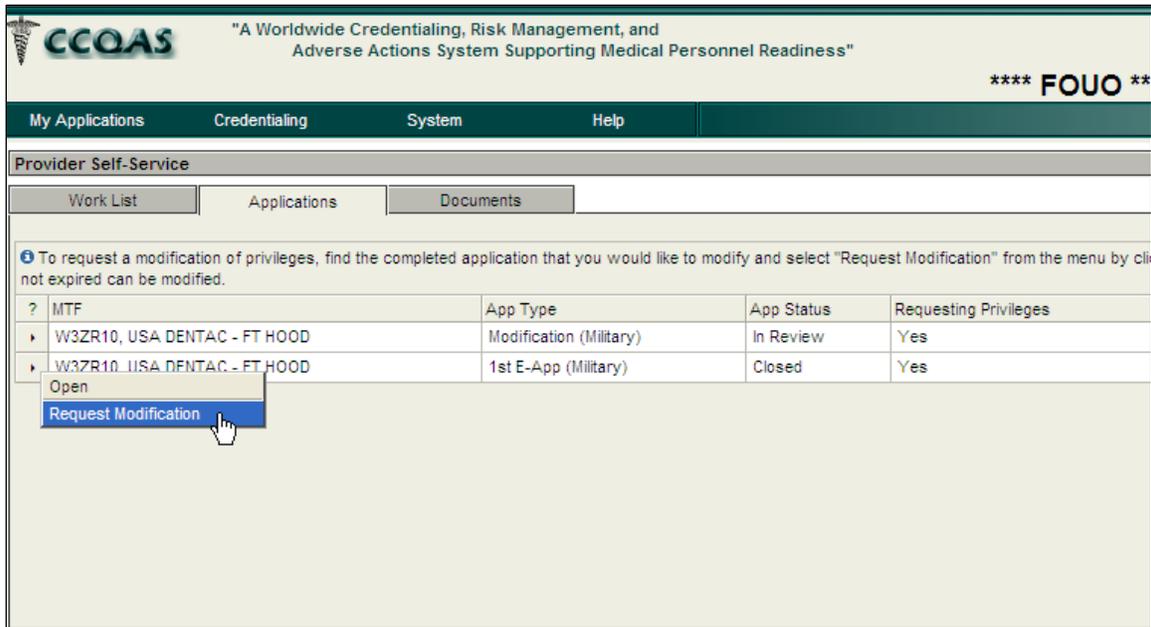


Figure 219: Request Modification Menu Item

CCQAS only permits Providers to request a modification of the most recently approved application at their facility or unit. The **Request Modification** menu item is not active or enabled for applications that are currently in the review process, for approved applications that are not current, or for applications associated with other facilities or units.

When Providers select **Request Modification**, the **Application Modification Instructions** screen appears, as depicted in Figure 220 below. Providers may print these instructions by clicking **Print**, or they may cancel the request and return to the **Applications** tab by clicking **Cancel**.

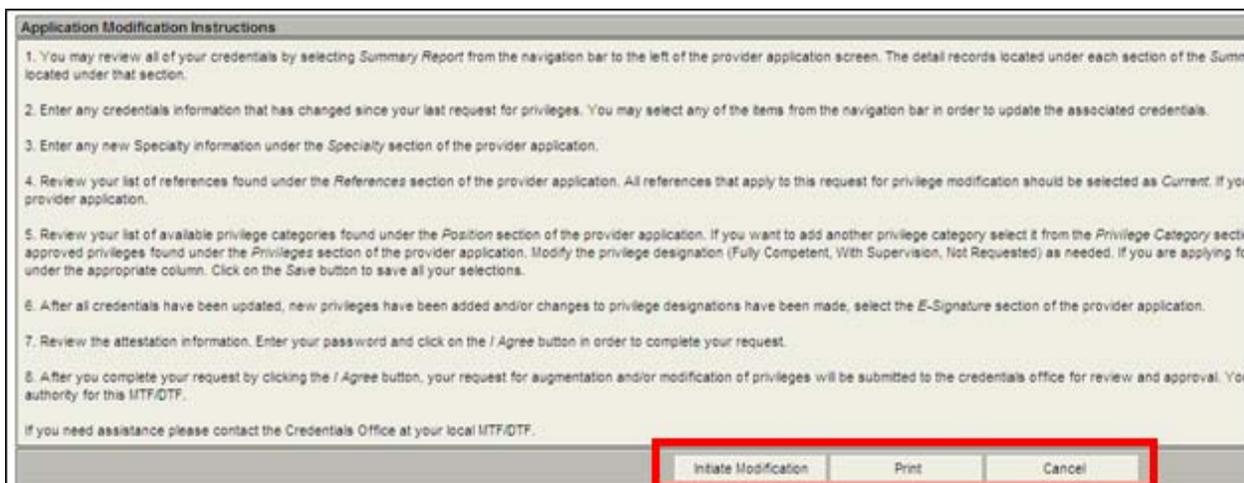


Figure 220: Application Modification Instructions Screen

When Providers click **Initiate Modification**, a new application for modification of privileges appears, as depicted in Figure 221 below. Providers must proceed with the application process, according to the instructions provided.

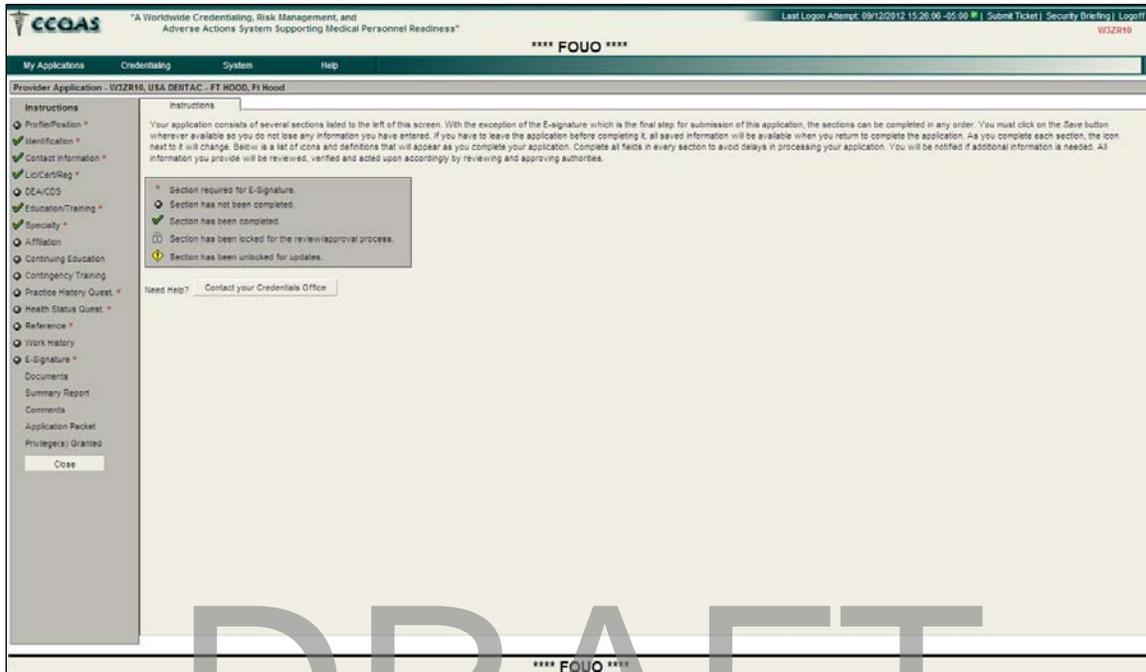


Figure 221: Provider Application (Modification)

The following are important features of the application for modification of privileges:

- The application is pre-populated with a Provider's most current credentials information from his or her CCQAS credentials file
- Providers may not edit existing credentials information that has already been verified via the PSV process, except to update expiration or renewal dates
- Providers may add to the application new credentials that are supported by appropriate documentation
- The application reflects the list of clinical privileges that were granted during the most recent privileging action by a Provider's current privileging unit or facility
- The section of the application containing the "Practice History" questions must be completed prior to submitting the application. If a "Yes" response was submitted on a prior online privilege application, the modification application pre-populates with the Provider's previous entries
- The section of the application containing the "Health Status" questions of the application must be completed prior to submitting the application. If a "Yes" response was submitted on a prior online privilege application for questions 5, 6 or 7, the modification application pre-populates with the Provider's previous entries

- All references listed on the original application are listed on the Modification Application, with a status of “**Current = No**”. Providers should edit the **References** section to indicate which references are still current or add new references
- Currently, approved privileges are displayed in the **Privileges** section. Providers simply need to change the privilege delineation that is driving the modification

Note: Providers should enter sufficient information on the modification application to support the request for additional clinical privileges. For example, if privileges are requested on the basis of those same privileges being newly supported by the facility, Providers should include a comment on the application indicating that the application is being submitted for privileges on that basis.

When Providers create the application for modification of privileges, the system generates an email notification for them and a new work list item on their “Work List” entitled, “App Type = *Modification*”. Figure 222 below depicts a sample modified application.

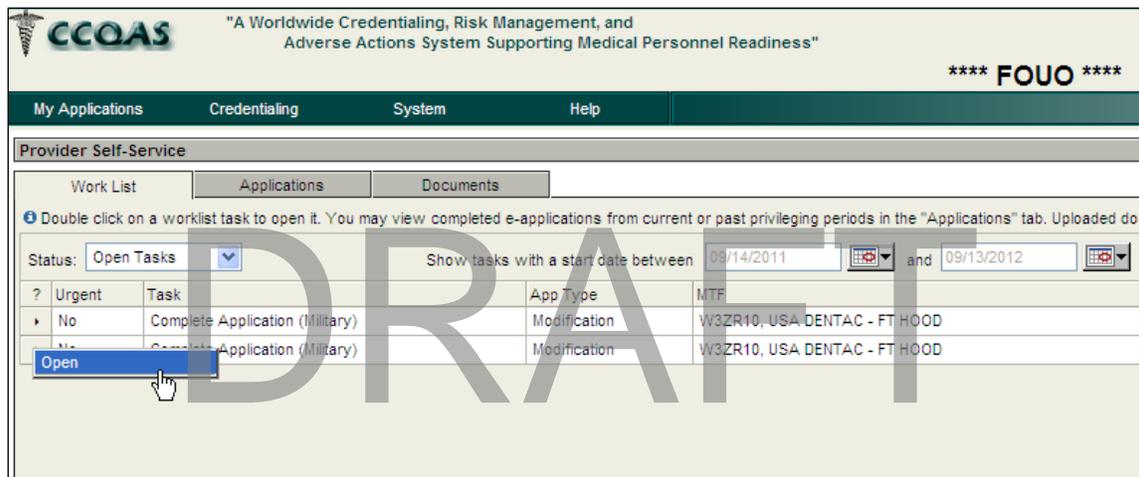


Figure 222: Provider Task – Complete Application, Modification

The work list item to complete the Modification Application remains active until either the Provider completes and submits the application, or 90 days pass without submitting the application. After the application is submitted, it is locked and cannot be edited by the Provider, unless the CC/MSSP/CM returns the application to him or her with instructions to modify it.

7.2 Processing an Application for Modification or Augmentation of Privileges

After the Provider signs and submits the Modification Application, the system forwards it to the CC/MSSP/CM. The CC/MSSP/CM receives a new work list item with “App Type = *Modification*”, as depicted in Figure 223 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Credentiaing Privileging Reports System Help

WorkList for W3ZR10 , USA DENTAC - FT HOOD

Work List My Applications Pending Applications

Status: Open Tasks Role: All Tasks start date between 09/19/2011 and 09/13/2012 Filter

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type
No		Application Ready for Review	CC/CM/MSSP	CROSS, GIDEON (Provider)	CROSS, GIDEON (Military)	Modification

Figure 223: CC/MSSP/CM Task – Application Ready to Review, Modification

From this point, the PSV and review processes are similar to those of the original application upon which the modification is based, with a few exceptions. For a modification of approved privileges, only the Provider's license(s), certification(s) or registration(s) and those credentials that require verification but were not previously verified need to undergo the PSV process. A new NPDB query must also be performed in accordance with Service policy.

Note: CCQAS will accept a **Last Query Date** within the past 90 days as fulfillment of the PSV requirement, but a new NPDB/Healthcare Integrity and Protection Data Bank (HIPDB) query should be performed in accordance with Service or facility protocol, or any time concerns or questions arise regarding the Provider's recent practice. Regardless of the value entered for the **Last Query Date**, the CC/MSSP/CM or CVO clicks **Save** in the upper left corner of the NPDB Query section of the **PSV Summary** screen so that CCQAS can complete the PSV process. The **PSV Summary** screen is depicted in Figure 224 below.

Prime Source Verification (PSV) for NICK DUNNE

Provider PSV Summary Privileges Documents Comments

NPDB / HIPDB / FSMB

Save

National Practitioner Data Bank (NPDB) Information

Last Query Date : 09/03/2012 Result Date : 09/19/2012

Request Query Query Results Pending

NPDB Website

Adverse Information On File:
 Yes
 No
 No, but was previously Yes

Healthcare Integrity and Protection Data Bank (HIPDB) Information

Last Query Date : Result Date :

Request Query Query Results Pending

Adverse Information On File:
 Yes
 No
 No, but was previously Yes

Figure 224: NPDB/HIPDB/FSMB Provider Summary

Sections of the application that were modified by the Provider are flagged so that the CC/MSSP/CM, CVO, and Reviewers may easily identify what information has been changed or added since the original application was approved. Icons appear next to each data element that was changed from the original application, indicating that the section needs to be verified on the basis of new or modified information. If the “Verified” box on the right-hand side of the screen is checked, the information in that section does not require re-verification. Figure 225 below depicts the flagged credentials on the Modification Application.

Prime Source Verification (PSV) for GIDEON CROSS		
Provider PSV Summary		Privileges
? DEA Number		
No Records Found.		
[-] Professional Education []		
? Degree	Type	Institution
▶ Doctor of Medicine	Qualifying Degree	Uniformed
+ Post Graduate Training [No Data] []		
[-] Specialty []		
? Specialty	Sub Specialty	
▶ Family Practice	Addiction Medicine	
+ Malpractice Coverage [No Data] []		

Figure 225: Flagged Credentials on the Modification Application

The CC/MSSP/CM and Reviewers are able to see the original privileges granted to the Provider, as well as the changes to privileges being requested by the Provider, as depicted in Figure 226 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Credentialing Privileging Reports System Help

Prime Source Verification (PSV) for GIDEON CROSS

Provider PSV Summary Privileges Documents Comments

W3ZR10

Privilege Category: Allergy and Immunology Sort by: Core

Core Privileges

Allergy and Immunology

- Version 1.0
- Physicians requesting privileges in this subspecialty must also request privileges in their primary discipline
- Scope

Privilege(s)

The scope of privileges in Allergy and Immunology includes the evaluation, diagnosis, consultation, management, and provision of therapy and treatment for conditions or disorders. This scope also includes the consultation, management, education, and provision of therapy and treatment for events. Physicians may admit and may provide care to patients in the intensive care setting.

This privilege was added to this application.

nc

Privilege(s)

Knee Pain nc

Diagnosis and Management:

Privilege(s)

- Performance and interpretation of diagnostic testing for immediate hypersensitivity disease (skin testing, challenges)
- Performance and interpretation of diagnostic testing for delayed hypersensitivity
- Performance and interpretation of diagnostic testing for reactive airway disease and asthma (e.g., spirometry with flow-volume loops)

Figure 226: Flagged Privileges on the Modification Application

Under most circumstances, the application for modification of privileges is routed through the same Reviewers for the original application upon which the modification was made. After the PA reviews and approves the Modification Application, the CC/MSSP/CM issues the appropriate notifications and completes the application process.

After the application is approved, the system imports the modified privileges into the **Privileges** section of the Provider's credentials record. The **Staff Appointment Expiration** and **Privilege Expiration** dates are not updated by the system as a result of an approved application for modification of privileges. These dates, however, may be changed by the CC/MSSP/CM in the **Privileges** section of the Provider's credentials record (refer to [Sections 5–17](#)). Any edits made to these expiration dates in the **Privileges** section of the Provider's credentials record are displayed in read-only format in the current assignment record in the **Assignments** section.

The approved Modification Application then becomes a read-only record accessible to the Provider from the **Applications** tab. Additional modifications of clinical privileges may be requested by initiating a second Modification Application from the previously approved application. Or, the Provider may simply wait to request additional privileges when the privilege renewal cycle begins again.

8 ICTB Process

Providers who perform temporary duty at locations other than those to which they are assigned may require privileging at a temporary location. The process by which the appropriate credentials information is supplied to the temporary facility or unit (i.e., gaining location) is referred to as the ICTB process. ICTBs are commonly used for Providers engaging in training activities, temporary duty assignments, and deployments.

CCQAS supports the ICTB process in the following ways:

- CCQAS enables CC/MSSP/CMs at gaining facilities to electronically request an ICTB transfer for any Provider from their parent, or 'sending' location (i.e., the facility or unit to which the Provider is currently assigned)
- When the sending location initiates an ICTB, CCQAS transfers a copy of the Provider's credentials record to the gaining location. In general, this copy is view-only and referred to as the ICTB record
- When the sending location initiates an ICTB, CCQAS also generates a new electronic privilege application for the Provider to request privileges at the ICTB location. This application is referred to as an ICTB application. An Appendix Q form may also be generated for Navy Providers who are not requesting supplemental privileges for their ICTB duty at another Navy location
- Following the completion of ICTB duty that is longer than 4 days in duration, CCQAS automatically initiates the online PAR process at the gaining location

These processes are described in the following sections.

8.1 Requesting an ICTB at the Gaining Location

Through its Credentialing module, CCQAS 2.10.0.0 allows CC/MSSP/CMs at gaining locations to request an ICTB transaction for a specific Provider. To locate the Provider's credentials

record, select **Provider Search** from the Credentialing drop-down menu. Enter the last name of the Provider, select the **Provider Locator** radio button, and then click **Search**. If the Provider name and other attributes indicate that this is the Provider CC/MSSP/CMs are searching for, click **Assignment** from the hidden menu of actions on the **Search Results** tab, as depicted in Figure 227 below.

Note: CC/MSSP/CMs must select the **Provider Locator** radio button for the search function to locate Providers outside of the user's UIC. If CC/MSSP/CMs select the default **Search** radio button, CCQAS only searches for the Provider among those who are already performing duty at the user's location.

Provider Search	Advanced Credentials Search	Search Results	Add Credentials Provider				
▶ Earth, Leo K	796-03-1125	W07CAA	09/07/2012	A11	MC	MIL	Active
▶ Flack, Roberta Sylvia	122-33-4444	N68094	09/07/2012	N11	MC	Dual	Active
▶ Foreman, Chuck	300-09-8765	EB1MFNDQ	08/29/2012	F11	MC	MIL	Active
▶ Fred, Cox	100-01-2345	EB1MFNDQ	08/31/2012			CIV	Active
▶ Grams, Don	219-99-1111	W0Q1AA	09/24/2012			MIL	Active
▶ Greenway, Chad	300-01-2345	EB1MFNDQ	09/12/2012			CIV	Active
▶ Grey, Jean L	333-44-5555	W1MLAA	09/18/2012			CIV	Active
▶ HEBBURN, AUDREY	569-48-2536	W3ZR20	09/27/2012	A11	MC	MIL	Active
▶ Assignment	796-88-8888	W07CAA	09/26/2012			CIV	Active
▶ Request Custody Transfer	222-34-1234	CL1LFC0F	09/15/2012	F11	MC	MIL	Active
▶ Deactivate Provider	111-22-3333	N00183	08/29/2012			Dual	Active
▶ Letters	444-55-4444	CL1LFC0F	09/21/2012			CIV	Active
▶ Change SSN	222-33-4444	N00183	09/12/2012			Dual	Active
▶ Grant Provider Access							
▶ JOBS, STEVE	100-79-8888	AM0JFQCL	09/17/2012	F11	MC	MIL	Active
▶ Johnson, Brad	400-01-2345	W2DNAA	09/14/2012			Dual	Active
▶ Jones, George	218-11-2222	S30MFLRY	09/21/2012			MIL	Active
▶ Jones, Davey e	123-88-4567	N68093	09/17/2012	A11	MC	MIL	Active
▶ Jones, Davey	999-33-8758	N00183	09/07/2012			CIV	Active

Record Count: 100 Search

Figure 227: Assignment Menu Item on the Search Results Tab

When the **Assignment** screen of the Provider's credential record appears, CC/MSSP/CMs select the **Request ICTB** option from the hidden menu next to the assignment in which the ICTB will be created, as depicted in Figure 228 below.

Name: AUDREY HEPBURN					Branch: A11				
SSN: 569-48-2536					Primary UIC: W3ZR20				
Assignments			Work History			Malpractice Insurance			
Add Assignment									
?	UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date
	W3ZR20	Active Duty Staff (non Training)			MIL	CRED	Current	09/27/2012	
Request ICTB									
Request PCS									

Figure 228: Request ICTB action on Assignment Screen

CC/MSSP/CMs must enter the **ICTB Begin Date** and **ICTB End Date**, and then click **Send**, as depicted in Figure 229 below. A message displays, which indicates that the request was sent.

CCQAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 10/04/2012 10:14:00-05:00 Submit Ticket Security Briefing Log

**** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Provider Name: BRIAN ADAMS Branch: F11 Rank: COL Corps: MC AOC/Design/AFSC: 44A1
 SSN: 091-82-0121 Primary UIC: DW1CFDN9 Cred Status: Active Input Clerk: CM2013

Broadcast Message to DW1CFDN9

Subject: ICTB Transfer Requested

ICTB Begin Date: 10/03/2012

ICTB End Date: 10/19/2012

Type of Duty: Duty

Message Preview: DAWSON RICHARD is requesting that the credentialing record for ADAMS, BRIAN (091-82-0121) be ICTB'd to BB1CFDPR, 0002 MEDICAL GROUP, Barksdale AFB with a beginning date of 10/03/2012 and ending date of 10/19/2012.

My contact information is as follows:
 Username: CM2013!
 Email: nchernyavskaya@asmr.com
 Phone: (111) 222-3333 (Home)

Send Close

Figure 229: Request ICTB Screen at Gaining Location

The responsible CC/MSSP/CM at the sending location receives the request through the **Broadcast Messages** function within the application. The next time the CC/MSSP/CM at the sending location logs in to CCQAS, he or she is alerted to a new incoming broadcast message for the unit, as depicted in Figure 230 below.



Figure 230: New Incoming Broadcast Message Alert for Sending Location

To view incoming messages, select **Broadcast Messages** from the **System** drop-down menu, as depicted in Figure 231 below.

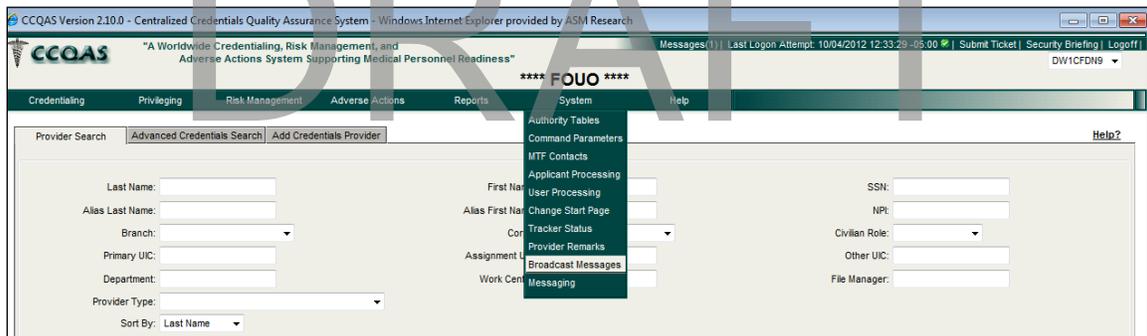


Figure 231: Broadcast Messages Menu Item at the Sending Location

An automatic notification is sent to the primary PAC whenever a non-primary UIC performs an ICTB transaction on one of his or her assignments. The Broadcast Message for an ICTB includes the name of the requested Provider, the dates for the ICTB duty, and POC information for the gaining facility or unit. Figure 232 below depicts the Broadcast Message menu item.

After the primary PAC reads the message, he or she may close it by clicking **Close**, or print it by clicking **Print Selected Message(s)**. To delete the message, select **Delete Selected Message(s)** from the hidden menu of actions for the message.

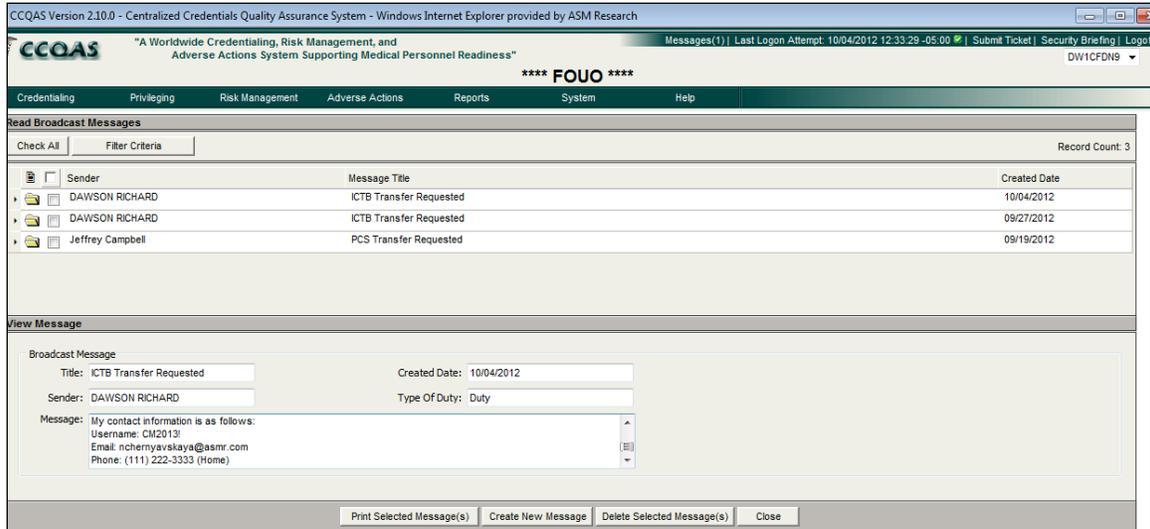


Figure 232: Broadcast Message Menu Item

In all instances, it is the responsibility of the sending facility or unit to initiate the ICTB transaction. The gaining unit can only request the ICTB transaction, but cannot initiate it.

Note: The **Create New Message** button allows CC/MSSP/CMs to write a message for broadcasting to other CCs/MSSPs/CMs. The message is not limited to any one particular topic. The **Broadcast Message** functionality, therefore, can be viewed as email functionality within the CCQAS system only.

8.2 Initiating the ICTB at the Sending Location

CC/MSSP/CMs at sending locations may initiate an ICTB transaction, regardless of whether or not the gaining location submits a Broadcast Message requesting the ICTB. The location that owns the Provider's credentials record is the only facility that may initiate an ICTB transaction. The sending facility, however, may initiate multiple ICTB transactions on the same Provider record as the situation and facility and Service protocol dictate.

Sending facility CC/MSSP/CMs initiate an ICTB transaction through the Credentiaing module. To initiate an ICTB transaction, select **Provider Search** from the **Credentiaing** drop-down menu. Enter the last name of the Provider, select the **All (Primary UIC or Assignment UIC)** radio button, and then click **Search**.

On the **Search Results** tab, select **Open** from the hidden menu of actions for the Provider's record. After the Provider's credentials record is opened, click **Work History** on the **Navigation** bar on the left-hand side of the screen, as depicted in Figure 233 below.

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Provider

Name: HART CRANE Branch: F11 Rank: Lt Gen
SSN: 101-92-0123 Primary UIC: DW1CFDN9 Cred Status: Active

Work History Malpractice Insurance

Profile Identification Contact Information Lic/Cert/Reg DEA/CDS Education/Training Specialty Affiliation Continuing Education Contingency Training References Databank Queries Custody History Work History Privileges

NAVI GATION	Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date	Transferred From	Dept	Work Center	Primary Special
	Administrative			MIL	CRED	Current	10/19/2012					

Figure 233: Work History Section on Navigation Menu

From the hidden menu of actions, next to the assignment record, click **Initiate ICTB** in the menu. CC/MSSP/CMs then enter the appropriate information for the ICTB transaction and submit the ICTB transaction, as depicted in see Figure 234 below.

CCOAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Provider

Name: HART CRANE Branch: F11 Rank: Lt Gen
SSN: 101-92-0123 Primary UIC: DW1CFDN9 Cred Status: Active

Assignments Work History Malpractice Insurance

Add Assignment

NAVI GATION	? UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date	Transferred From	Dept	Work Center	Primary Sp
	DMSSP	Administrative			MIL	CRED	Current	10/19/2012					

Open
Initiate PCS
Initiate ICTB
End Assignment
Cancel Assignment
Letters
Initiate Application
Reactivate Privileges

Figure 234: Initiate ICTB Menu Option

CC/MSSP/CMs then enter the **To Command**, **Start Date**, **End Date**, and other appropriate information for the ICTB transaction, and then click **Submit** to initiate the ICTB transaction. Figure 235 below depicts the ICTB form.

The screenshot shows a web-based form for initiating an ICTB transaction. The form is titled "Initiate ICTB - HART, CRANE". At the top, it displays "To Command: BB1CFDPR". The form is organized into several sections:

- ICTB Information:** Contains "Start Date: 10/19/2012" and "End Date: 10/27/2012". There is a checkbox for "Evaluation (PAR/OER)".
- Provider Information:** Includes "Type of Duty: Active Duty Special Work (ADSW)", "Current PED: 10/18/2014", and "ICTB Duty Status: Military" (selected).
- Credential Signature Authority Information:** Lists fields for Name, Position, Command, Location, and Phone, all populated with specific text.
- Additional Information:** A section for "Select the additional text for paragraph 13:" with a dropdown menu showing "No additional information in Credentials File" (selected), "Additional license information in Credentials File", and "Additional information in Credentials File - Please Call". Below this is a field for "Additional comments for paragraph 14:" with a radio button for "None" selected.
- Final Options:** At the bottom, there are two radio button options: "Suppress ICTB E-Application" (set to "No") and "Generate ICTB Letter" (set to "Yes").

Figure 235: ICTB Form

Note: The required fields (red field labels) to initiate an ICTB are common to all Services. The **Initiate ICTB** screen contains additional text fields that are auto-populated with information that users have entered on the **Command Parameters** screen, but these fields are editable on the **Initiate ICTB** screen.

Note: There is an option to **Suppress ICTB E-Application**, which suppresses an electronic privileging application from being generated as part of the Initiate ICTB function. There is another option to **Generate ICTB Letter**, in which users can designate **Yes** or **No** as part of the transaction.

The **Initiate ICTB** screen appears differently if Providers have not yet submitted their 1st E-application using CCQAS. If the ICTB application is the first E-application Providers complete in CCQAS, and they do not yet have a user account (i.e., user ID and password) when the ICTB transaction is initiated, *the system also automatically generates a new user account for Providers*. Additional data fields are present on the **Initiate ICTB** screen to capture a Provider's primary email address and phone information, as depicted in Figure 236 below. The primary email address and phone information are required to create the new user account for the Provider.

The screenshot shows a web form titled "Provider Information". It contains the following fields and options:

- Type of Duty: [Dropdown menu]
- Current PED: [Text input field]
- Provider's AKO Email: [Text input field]
- Provider's Phone Type: [Dropdown menu with "Home" selected]
- Provider's Phone Number: [Text input field]
- Projected Provider Category: [Dropdown menu]
- ICTB Duty Status: Military Civilian

Figure 236: Email Address and Phone Number Fields for User Account

Provider then receive their user ID and temporary password information needed to access CCQAS via an email message sent to the email address entered on the **Initiate ICTB** screen. Providers must provide an accurate email address on the **Initiate ICTB** screen to receive the necessary information to access CCQAS.

After a sending facility initiates an ICTB transaction, the following actions automatically occur:

- CCQAS generates a copy of the Provider's credentials record that the gaining facility may use to document assignment and other details of the duty performed by the Provider at the ICTB location
- CCQAS generates a privilege application for the Provider to request privileges at the gaining location (unless users selected **Yes** for the **Suppress ICTB E-Application**)

8.3 The ICTB Assignment Record

An ICTB transaction is the only situation where duplicate copies of a Provider's credentials record are active at multiple locations. Although the two copies are identical in content, they are not identical in function. Sending CM/MSSP/CCs retain full access to, and responsibility for, maintaining a Provider's primary credentials record, while gaining facility personnel have mostly view-only access to their copy of the Provider's credentials data.

If the ICTB is scheduled to be effective as of the current date, a new assignment record with **Status = Current** and **Type = ICTB** is created at the sending facility, with the start date being the current date, as depicted in Figure 237 below. In a Provider's **Work History** section, new assignment information is read-only at the sending facility, but any changes made to the current credentials record (e.g., **Type = Credentialing**) is automatically applied to the current ICTB record to maintain synchronization between the two records.

The screenshot shows the CCQAS search results screen for the sending location. The provider information is as follows:

- Name: HART CRANE
- SSN: 10140-0123
- Branch: F11
- Primary LIC: DW1CF0R9
- Rank: Lt Gen
- Corp: MC
- Cad Status: Active
- Input Clerk: CM2113
- ADC/Design/AFSC: 4000

The table below shows the assignments for this provider:

7	LIC	Provider Type	Reported Date	Planned Rotation	M/L/C/V	Type	Status	Start Date	End Date	Transferred From	Dept	Work Center	Primary Specialty	Primary Sub-Specialty	Privilege Status	Privilege Type	PAK Expected	PAK Date	Type of Duty
1	DW1CF0R9	Administrative			ML	CRE3	Current	10/19/2012									No		
2	DW1CF0R9	Administrative			ML	ICTB	Current	10/19/2012	10/27/2012	DW1CF0R9 (ICTB)							No		Active Duty Special Work (ADSW)

Figure 237: Search Results Screen for the Sending Location

The hidden menu of actions for the ICTB record differs from that of the Credentials record. The ICTB record may be viewed at the sending location, but may not be edited. Any changes to a Provider's credentials during the ICTB duty period should be entered into the Credentials record. The menu options enable the sending location to generate letters pertinent to the ICTB duty or reset the Provider's password as necessary. The sending location also uses this menu to cancel the ICTB transaction or end the ICTB if the end date occurs earlier than originally expected.

At the same time the ICTB record is created at the sending facility, the same ICTB record with **Status = Current** and **Type = ICTB** becomes available to the gaining location, as depicted in Figure 238 below. The sections in this record are read-only, with the exception of the newly-created assignment record for the ICTB location in the **Assignment** section. Gaining CC/MSSP/CMs may enter the ICTB assignment information directly into this assignment record. They may also access all documents, PARs, and snapshots listed in the **Documents** section.

UIC	Provider Type	Reported Date	Planned Rotation	M/LC/V	Type	Status	Start Date	End Date	Transferred From	Dept	Work Center	Primary Specialty	Primary Sub-Specialty	Privilege Status	Privilege Type	PAR Expected	PAR Date	Type of Duty
DW1CF09	Administrative			ML	CHED	Current	10/19/2012									No		
BB1CF09	Administrative			ML	ICTB	Current	10/19/2012	10/27/2012	DW1CF09 (ICTB)							No		Active Duty Special Work (ADSW)

Figure 238: Search Results Screen for the Gaining Location

The other options from the hidden menu of actions for the ICTB record at the gaining facility allow gaining CC/MSSP/CMs to generate letters pertinent to the ICTB duty and reset a Provider's password, as necessary.

If the ICTB is scheduled to be effective as of the current date, the ICTB credentials record will be visible at the sending facility, directly after the ICTB transaction is initiated. If the ICTB transaction was completed using a future date as the effective date, the Provider's ICTB record remains in pending status at the sending facility until midnight (Central Time) on the day before the effective date. The ICTB transaction is classified as a pending transaction until the effective date is reached. After the effective date has passed, the ICTB record will be included in system queries or reports run at the sending and receiving facilities unless users include only records of **Type = Credentialing** in their search and reporting criteria.

8.4 The Transaction Table

A transaction is written to the Transaction Table at both the sending facility and gaining facilities each time an ICTB is initiated. Although CCQAS does not require it, gaining CM/MSSP/CCs should acknowledge receipt of the ICTB transaction in the Transaction Table. This acknowledgment allows the sending facility to know that the transaction was received and accepted. CC/MSSP/CMs are alerted to a new entry in the Transaction Table by a message window that appears each time they access the Credentials module, as depicted in Figure 239 below.

Acknowledgement of the transaction also eliminates the appearance of this message window, which appears each time CM/MSSP/CCs access the Credentials module.

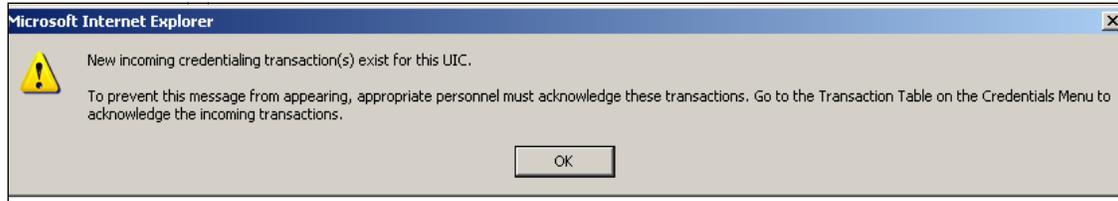


Figure 239: New Incoming Credentials Transaction Window

The Transaction Table may be viewed by clicking the **Credentialing** main menu bar across the top of the screen, and then selecting **Transaction Table**, as depicted in Figure 240 below.

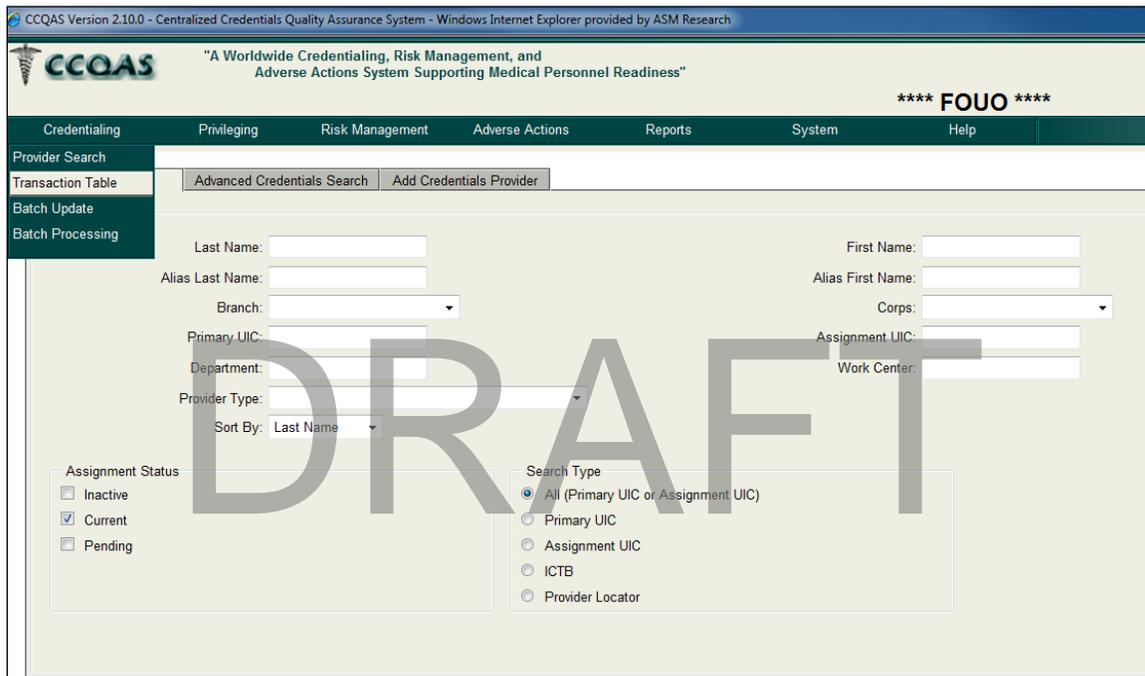


Figure 240: Accessing the Transaction Table

The **Provider Transactions** screen displays, as depicted in Figure 241 below. Users may then select the **Type** and **Direction** of the transactions they wish to view.

The gaining facility may acknowledge incoming ICTB transactions by selecting the **Direction** = *Incoming*, **Status** = *Unacknowledged* or *Both* and **Action** = *ICTB*, and then clicking **Search**. A list of incoming transactions is displayed, as depicted in Figure 241 below.

Users may then acknowledge the desired transaction by clicking the **Acknowledged** checkbox next to the record, and then clicking **Save**. The transaction is then changed to **Status** = *Acknowledged*. Users may close the Transaction Table by clicking **Close**.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

Provider Transactions

Direction: Incoming, Outgoing, Primary MTF

Status: Unacknowledged, Acknowledged, Both

Action: PCS, ICTB, All, Update of Credentials Requested, Non-Primary Assignment Created, Custody Transfer

Acknowledged	From MTF	To MTF	Primary MTF	Action	Initiated	Provider Name	SSN	Sender's Name	Sender's Phone
<input type="checkbox"/>	CD1CFV/PV	CD1CFV/PV	N00060	Non-Primary Assignment Created	10/11/2012	SAMANTHA NEWTON	777-66-5555	CM9 CM9	((111) 222-3333
<input type="checkbox"/>	CD1CFV/PV	CD1CFV/PV	N00074	Non-Primary Assignment Created	10/01/2012	PAUL ALLEN	100-44-8888	CM9 CM9	((111) 222-3333
<input type="checkbox"/>	AM0JFQCL	CD1CFV/PV	AM0JFQCL	ICTB	09/17/2012	WILL TEST112233554	112-23-3554	CM1 CM1	((111) 222-3333

Search Save Close Results showing last 6 months of history

Figure 241: The Provider Transactions Screen for an Incoming ICTB

Sending CM/MSSP/CCs may then perform a query on the Transaction Table to view the acknowledgement status of the ICTB transaction. For example, a user at a sending location can find outgoing ICTB transactions by selecting the **Direction = Outgoing**, **Status = Both** and **Action = ICTB**, and then clicking **Search**. A list of outgoing ICTB transactions displays, with an indicator of whether the ICTB has been acknowledged by the gaining location.

If CCQAS users at a gaining location are not expecting the ICTB, or have concerns about the transaction, they should contact the sending location prior to acknowledging the transaction. POC information for the sending location is included for each record listed in the Transaction Table.

8.5 The Transfer (ICTB) Application for Clinical Privileges

After an ICTB transaction has been initiated, the system automatically sends an email notification to Providers, and an active task is placed in their work list, with “**Task = Complete Application**” and “**App Type = Transfer (ICTB)**”, as depicted in Figure 242 below.

CCQAS Version 2.10.0 - Centralized Credentialing Query Assurance System - Windows Internet Explorer provided by ASM Research

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" **** FOUO ****

My Applications System Submit Trouble Ticket

Provider Self-Service

Work List Applications Documents

Double click on a worklist task to open it. You may view completed e-applications from current or past privileging periods in the "Applications" tab. Uploaded documents, performance assessments and PDF files of completed e-applications may be viewed in the "Documents" tab.

Status: Open Tasks Show tasks with a start date between 10/20/2011 and 10/19/2012 Filter

Urgent	Task	App Type	MTF	CC/CMSSP	CC/CMSSP Phone	Task Start Date
Open	Complete Application (Military)	Transfer (ICTB)	BB1CFDPR_0002 MEDICAL GROUP			10/19/2012

Figure 242: Provider Task – Complete Application, Transfer (ICTB)

Providers may then open, complete, and submit the Transfer Application according to the instructions provided. Figure 243 below depicts the Transfer (ICTB) Application for privileges.

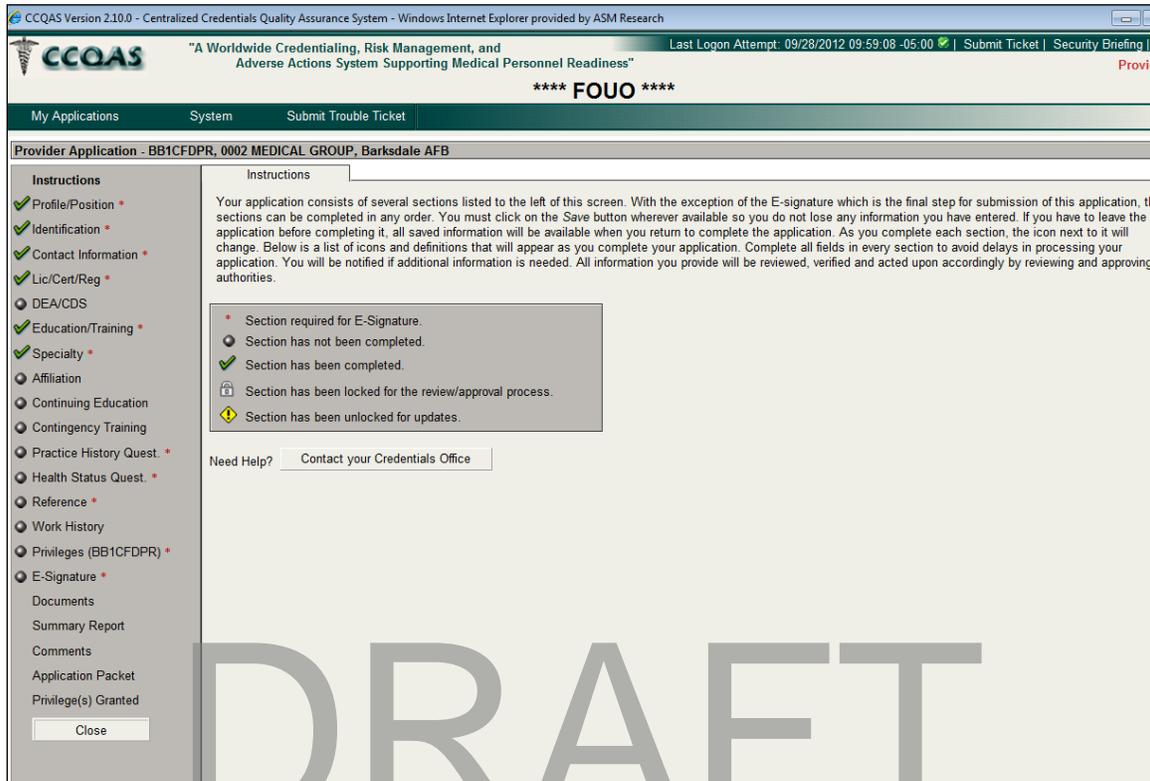


Figure 243: Transfer (ICTB) Application for Privileges

The following are important features of the Transfer (ICTB) Application:

- The application pre-populates with a Provider's most current credentials information from his or her CCQAS credentials record
- Providers may edit or add credentials to an ICTB Transfer Application
- The section of the application containing the "Practice History" questions must be completed prior to submitting the application. If a **Yes** response was submitted on a prior online privilege application, the modification application is pre-populated with the Provider's previous entries
- The section of the application containing the "Health Status" questions of the application must be completed prior to submitting the application. If a **Yes** response was submitted on a prior online privilege application for questions 5, 6 or 7, the modification application is prepopulated with the Provider's previous entries
- All references listed on the original application are listed on the Modification Application, with a status of "**Current = No**". Providers should edit the **References** section to indicate which references are still current, or add new references

- The application reflects the list of clinical privileges granted by a Provider's current privileging unit or facility during the most recent privileging action. However, Providers are able to edit the delineations to coincide with their current competencies and (updated) credentials pertinent to this ICTB privilege application
- Providers may still scan and upload documents to the application, as appropriate

The Transfer (ICTB) email notification is sent to Providers only once, but the work list item to complete the ICTB Transfer Application remains active, either until Providers complete and submit the application, or 90 days pass without submitting the application. After Providers submit the application, it is locked and cannot be edited by them, unless the responsible CC/MSSP/CM at the ICTB location returns the application to them with instructions to modify it.

8.6 Processing an ICTB Transfer Application for Clinical Privileges

When CC/MSSP/CMs at a parent facility initiate the ICTB transaction, CCQAS adds a Provider's pending application to the *gaining* CC/MSSP/CM's **Pending Applications** tab list, as depicted in Figure 244 below. With the listing on this tab, CC/MSSP/CMs at gaining locations can have visibility of the number of days Providers take to accomplish their privilege application after the system generates the task.



Figure 244: Gaining CC/MSSP/CM's Pending Applications Tab

After Providers e-sign and submit the application, their Transfer (ICTB) application disappears from the **Pending Applications** listing for the gaining facility CC/MSSP/CM, who then receives a new email notification of a task pending in CCQAS. A new work list item with "App Type = *Transfer (ICTB)*" is added to his or her work list, as depicted in Figure 245 below.



Figure 245: Gaining CC/MSSP/CM Task – Transfer (ICTB) Application

The PSV requirements for an ICTB application are limited to re-verification of all Provider licenses, certifications, and registrations, and a new NPDB query in accordance with Service policy. The remaining sections of the ICTB application package are view-only, since maintenance and validation of these credentials are the responsibility of the CM/MSSP/CC at the location where the Provider is permanently assigned. Figure 246 below depicts the **Provider PSV Summary** screen for the ICTB application.

The screenshot shows the 'Provider PSV Summary' screen in the CCQAS system. The browser title is 'CCQAS Version 2.0.0 - Centralized Credentialing, Quality Assurance System - Windows Internet Explorer provided by ADM Research'. The page has a navigation menu with options like 'Credentialing', 'Privileges', 'Task Management', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area is titled 'Prime Source Verification (PSV) for IMRT CBAC' and contains a form for a provider named 'COURT, KAREN'. The form includes sections for:

- Personal Information:** Name (COURT, KAREN), Gender (Female), Date of Birth (10/19/1988), Social Security Number (101-80-0123), and State (Alabama).
- Identification:** Identification Type (Social Security Number) and Identification Number (101-80-0123).
- State License/Certification/Registration:** License Type (Alabama), License Number (123), Field (Allopathic Physician), Status (Active), Expiration (11/19/2012), and ACME Status (No).
- National Certifications/Registration:** Includes a section for Drug Enforcement Agency (DEA) / Controlled Dangerous Substances (CDS).
- Education:** Degree (Doctor of Medicine), Institution (Uniformed Services University of Health Sciences), and Graduation Date (09/05/02).
- Specialty:** Specialty (Allopathic Technology Practitioner) and Specialty Level (Fully Trained).
- Other Sections:** Academic Appointments, Organizational Memberships, Continuing Education, and Contingency Training.

 At the bottom, there is a 'National Practitioner Data Bank (NPDB) Information' section with a 'Last Query Date' of 10/19/2012 and a 'Request Query' button. A large 'DRAFT' watermark is overlaid across the center of the screen.

Figure 246: Provider PSV Summary Screen for the ICTB Application

Note: CCQAS will accept a **Last Query Date** within the past 90 days as fulfillment of the PSV requirement, but a new NPDB/HIPDB query should be performed in accordance with Service or facility protocol or any time concerns or questions arise regarding a Provider's recent practice. Regardless of the value entered for the **Last Query Date**, CC/MSSP/CMs or CVOs must click **Save** in the upper left-hand corner of the **NPDB Query** section of the **Provider PSV Summary** screen for CCQAS to complete the PSV process.

After these PSV requirements are met, the ICTB application may be routed for review and approval at the ICTB facility or unit, according to the processes discussed in detail in [Section 5](#).

After the ICTB application is approved, the system imports the new privileges into the **Privileges** section of a Provider's ICTB record. The system automatically calculates new **Privilege Expiration** and **Staff Appointment Expiration** dates for the Provider, based on the end date for the ICTB duty. CC/MSSP/CMs, however, may change these dates in the **Privileges** section of the Provider's ICTB record. Any edits made to these expiration dates in the **Privileges** section will be displayed in read-only format in the current assignment record in the **Assignments** section of the ICTB record.

8.7 Cancelling an ICTB

It may be necessary to cancel an ICTB transaction in cases where a Provider does not report to the ICTB location, as scheduled. An ICTB may be cancelled at any time after it has been initiated, as long as the ICTB is still in active status (e.g., the end date for the ICTB has not yet been reached). CCQAS users at sending locations may manually cancel an ICTB transaction by selecting **Cancel ICTB** from the menu of actions for the ICTB record on the **Search Results** screen, as depicted in Figure 247 below.



Figure 247: Cancel ICTB Menu Item

When the ICTB is cancelled, the ICTB record at both locations is deleted and will not be available in system queries or reports. An ICTB record may not be recovered after it has been cancelled. An ICTB can only be cancelled by the sending location.

8.8 Ending an ICTB

The end date for an ICTB transaction is selected at the time that the ICTB is initiated by the issuing facility. When the end date is reached, CCQAS automatically ends the ICTB transaction; the status of the ICTB record at the sending and receiving facilities is changed from *Active* to *Inactive*, and is not included in system queries or reports run at either facility unless users include only records of **Status = Inactive** in their search and reporting criteria. The inactive ICTB record also becomes a read-only record at both locations.

If the ICTB ends prior to the end date established when the ICTB record was created, CCQAS users at issuing facilities may manually end the ICTB transaction by selecting **End ICTB** from the menu of actions on the **Search Results** screen, as depicted in Figure 248 below.



Figure 248: End ICTB Menu Item

When the ICTB is manually terminated, the ICTB record at both locations is changed from *Active* to *Inactive*. An ICTB can only be terminated by the issuing facility.

8.9 PAR for ICTB Duty

CCQAS automatically initiates the PAR process for any ICTB duty that is greater than four days. When the ICTB duty ends, a new work list item for CC/MSSP/CMs at ICTB units is created with “Task = *Setup PAR*”, as depicted in Figure 249 below.



Figure 249: Gaining CC/MSSP/CM Task – Setup PAR

The ICTB PAR should reflect a Provider’s performance while on ICTB duty. A PAR Evaluator should complete a PAR, with an optional review by one or more PAR Reviewers, as soon as is reasonably possible following the end of the ICTB duty. The PAR process is explained in detail in [Section 11](#).

Although the exception rather than the rule, CC/MSSP/CMs may cancel a PAR due to certain conditions (e.g., a Provider coming back from a remote deployment where no PAR evaluators were on hand). Mechanisms are in place for the system to allow the application to move forward when a scenario such as this occurs. Also, CC/MSSP/CMs who received the “*Setup PAR*” work list item may replace the electronic PAR process in CCQAS with a paper-based PAR process (i.e., “*Offline PAR*”) that occurs outside the CCQAS application. This process is explained in greater detail in [Section 11](#).

8.10 The ICTB Process for Navy Facilities

Unlike the Army and Air Force, the Navy has adopted core privileging, which allows Navy Providers, under most circumstances, to render patient care at an ICTB location without undergoing the ICTB application process described in the sections above.

Core privileging allows Navy Providers with approved privileges at one facility to exercise those same privileges at other Navy facilities. Instead of an ICTB application for privileges, Navy Providers use their **Appendix Q – Request to Exercise Clinical Privileges**. The Appendix Q is a letter requesting to exercise at the gaining facility the privileges they hold at the parent facility. If Providers request privileges that were not supported at their parent facility, and therefore, are not covered by the Appendix Q, they must complete an application for modification of their parent facility-granted privileges, or proceed through the ICTB application process, previously explained in this section.

Note: Navy Providers who perform ICTB duty at Army or Air Force facilities still need to submit completed ICTB applications, since their Navy core privileges do not “transfer” to Army or Air Force locations. Navy Providers who are requesting additional supplemental privileges at

a Navy ICTB location must also submit completed ICTB applications, since the Appendix Q document does not cover privileges not awarded at the assigned location.

The generation of the Appendix Q letter begins with the initiation of an ICTB transaction on a Provider's credentials record. After an ICTB transaction has been initiated, the system automatically sends an email notification to Providers, and an active task is placed in their work list, with "**Task = Complete Application**" and "**App Type = Transfer (ICTB)**". When Providers open the new task, the **ICTB Privilege Request** screen appears, as depicted in Figure 250 below.

Figure 250: ICTB Privilege Request Screen

If Providers select the **Privilege Application** radio button, and then click **Submit**, an ICTB privilege application opens, as described in [Section 8.5](#).

If Providers select the **Appendix Q** radio button, and then click **Submit**, the **Appendix Q** form displays, as depicted in Figure 251 below.

Figure 251: Appendix Q Letter

The Appendix Q letter consists of a series of tabs. The **Appendix Q** tab contains explanatory text that describes the conditions under which privileges are granted at an ICTB location. Providers must E-sign and click **I agree** to submit the request for privileges. The remaining tabs

of the Appendix Q letter mirror those displayed in an E-application, but all information is displayed in view-only format.

After users E-sign and submit the Appendix Q letter, gaining facility MSSPs receive a new email notification of a task pending in CCQAS. A new work list item with “App Type = *Transfer (ICTB)*” is added to their work list. After a gaining MSSP takes responsibility for the task, the E-signed Appendix Q is displayed, as depicted in Figure 252 below.

Figure 252: E-Signed Appendix Q

A formal PSV process is not required under the terms of the Appendix Q, thus no **PSV** option appears at the bottom of the screen. The remainder of the routing and approval processes, however, are identical to the processes for review and approving an E-application. MSSPs click the **Routing** button to select the appropriate clinical staff to review and approve the Appendix Q. After it is approved, the Appendix Q is permanently stored as a PDF file in the **Documents** section of the Provider’s credentials record.

9 Permanent Changes of Station Process

A PCS is the permanent transfer of an active duty Provider from one duty location to another. Within the CCQAS application, PCS is the electronic transaction that permanently transfers responsibility for a Provider’s hard copy credentials file from the old duty location (i.e., the sending location) to the new duty location (i.e., the gaining location). Military Providers who receive orders for a PCS are required to re-apply for clinical privileges to render patient care at the new duty station.

CCQAS supports the PCS process in the following ways:

- CCQAS allows CC/MSSP/CMs at gaining facilities to electronically request a PCS transfer for any Provider from their parent, or ‘sending’ location (the facility or unit to which the Provider is currently assigned)

- When a PCS is initiated by the sending location, CCQAS generates a new electronic privilege application for the Provider to request privileges at the new duty location. This application is referred to as a PCS application
- When a PCS is initiated by the sending location, CCQAS automatically initiates the online PAR process at the sending location to document the Provider's performance over the past privileging period
- When a PCS date becomes effective, CCQAS permanently transfers the Provider's credentials record to the gaining location
- When a PCS transaction is performed, the primary PAC is given the option to transfer custody of the credentials record
- When users elect to perform a custody transfer concurrently with the PCS, the PCS transfer and the custody transfer have the same date

These processes are described in more detail in the following sections.

9.1 Requesting a PCS at the Gaining Location

CCQAS 2.10.0.0 allows CC/MSSP/CMs at gaining facilities or units to request a PCS transaction for a specific Provider using the **Provider Locator** function in the Credentialing module. To request a PCS transaction, select **Credentials Provider Search** from the **Credentialing** main menu, as depicted in Figure 253 below. Enter the last name of the Provider, select the **Provider Locator** radio button, and then click **Search**. If the Provider name and other attributes indicate that this is the Provider you are searching, select **Assignment** from the hidden menu of actions on the **Provider Locator** tab.

Note: CC/MSSP/CMs must select the **Provider Locator** radio button for the search function to locate Providers outside of the user's UIC. If the default **Search** radio button is selected, CCQAS only searches for the Provider among those that are already performing duty at the user's location or if there is an active assignment at that UIC.

Provider Search	Advanced Credentials Search	Search Results	Add Credentials Provider				
▶ Earth, Leo K	796-03-1125	W07CAA	09/07/2012	A11	MC	MIL	Active
▶ Flack, Roberta Sylvia	122-33-4444	N68094	09/07/2012	N11	MC	Dual	Active
▶ Foreman, Chuck	300-09-8765	EB1MFNDQ	08/29/2012	F11	MC	MIL	Active
▶ Fred, Cox	100-01-2345	EB1MFNDQ	08/31/2012			CIV	Active
▶ Grams, Don	219-99-1111	W0Q1AA	09/24/2012			MIL	Active
▶ Greenway, Chad	300-01-2345	EB1MFNDQ	09/12/2012			CIV	Active
▶ Grey, Jean L	333-44-5555	W1MLAA	09/18/2012			CIV	Active
▶ HEPBURN, ANDREY	569-48-2536	W3ZR20	09/27/2012	A11	MC	MIL	Active
▶ Assignment	796-88-8888	W07CAA	09/26/2012			CIV	Active
▶ Request Custody Transfer	222-34-1234	CL1LFC0F	09/15/2012	F11	MC	MIL	Active
▶ Deactivate Provider	111-22-3333	N00183	08/29/2012			Dual	Active
▶ Letters	444-55-4444	CL1LFC0F	09/21/2012			CIV	Active
▶ Change SSN	222-33-4444	N00183	09/12/2012			Dual	Active
▶ Grant Provider Access							
▶ JOBS, STEVE	100-79-8888	AM0JFQCL	09/17/2012	F11	MC	MIL	Active
▶ Johnson, Brad	400-01-2345	W2DNAA	09/14/2012			Dual	Active
▶ Jones, George	218-11-2222	S30MFLRY	09/21/2012			MIL	Active
▶ Jones, Davey e	123-88-4567	N68093	09/17/2012	A11	MC	MIL	Active
▶ Jones, Davey	999-33-8758	N00183	09/07/2012			CIV	Active

Record Count: 100 Search

Figure 253: Assignment Menu Item on the 'Provider Locator' Tab

DRAFT

The Provider's assignment section of his or her credentials record displays, as depicted in Figure 254 below. CC/MSSP/CMs then click the hidden menu of actions and select **Request PCS** on the Provider's current Credentials record.

The screenshot shows the CCQAS interface for a provider's assignment. The provider's name is AUDREY HEPBURN, SSN: 569-48-2536, Branch: A11, and Primary UIC: W3ZR20. The screen displays a table of assignments with a dropdown menu open over the first row, showing 'Request PCS' as an option.

UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date
W3ZR20	Duty Staff (non Training)			MIL	CRED	Current	09/27/2012	
W3ZR20	Duty Staff (non Training)			MIL	ICTB	Current	09/28/2012	10/31/2012

A large 'DRAFT' watermark is visible across the bottom of the screen.

Figure 254: Request PCS Screen

CC/MSSP/CMs must enter the **PCS RNLT Date** (i.e., Report No Later Than), and then click **Send**. A message displays, which indicates the request was sent, as depicted in Figure 255 below.

The screenshot shows a message preview window with the following content:

Subject: PCS Transfer Requested

PCS RNLT Date: 10/31/2012

Message Preview: CC201 CC201 is requesting that the credentialing record for HEPBURN, AUDREY (569-48-2536) be PCS'd to W3VYAA, USA MEDCOM, Ft Sam Houston NLT 10/31/2012.

My contact information is as follows:
 Username: CC201
 Email: KARA.HUGHES@ASMR.COM
 Phone:

Buttons: Send, Close

Figure 255: Request PCS Message Screen

CC/MSSP/CMs at sending (i.e., losing) facilities or units receive the request through the **Broadcast Message** function within the application. The next time the CC/MSSP/CM at the sending facility or unit logs into the system, he or she will receive a new incoming broadcast message for the unit, as depicted in Figure 256 below.



Figure 256: New Incoming Broadcast Message Alert

To view incoming broadcast messages, select **Broadcast Messages** from the **System** drop-down menu, as depicted in Figure 257 below.

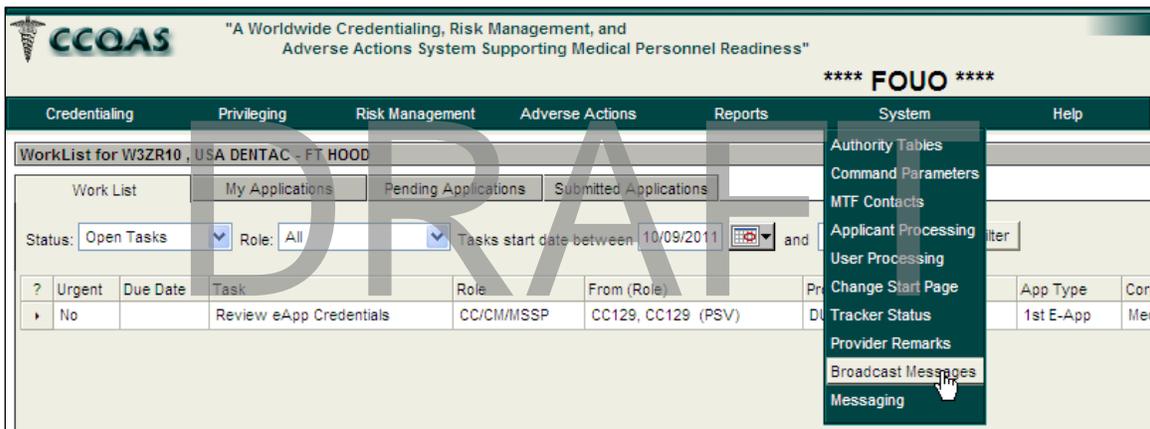


Figure 257: Broadcast Message Menu Item

The Broadcast Message for a PCS includes the name of the requested Provider, the dates for the PCS duty, and POC information for the gaining location, as depicted in Figure 258 below.

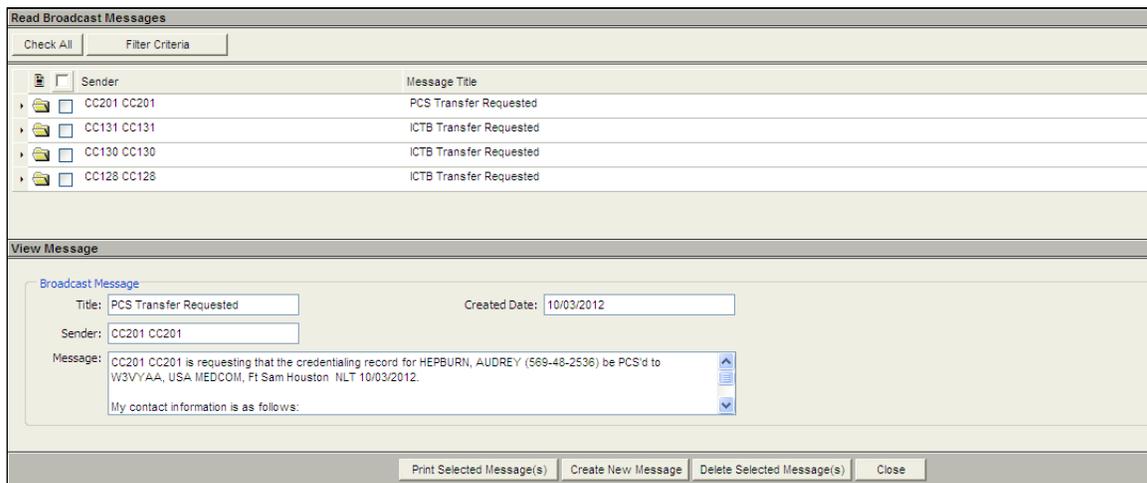


Figure 258: Broadcast Message Menu Item

After CC/MSSP/CMs read the message, they may close it by clicking **Close**, or print it by clicking **Print Selected Message(s)**, at the bottom of the screen. To delete the message, select **Delete** from the hidden menu of actions for the message. In all instances, it is the responsibility of the sending location to initiate the PCS transaction. The gaining location can request the PCS transaction, but cannot initiate the PCS transaction.

Note: The **Create New Message** button allows CC/MSSP/CMs to write a message for broadcasting to other CCs/MSSPs/CMs. The message is not limited to any one particular topic. The **Broadcast Message** functionality, therefore, can be viewed as email functionality within the CCQAS system only.

9.2 Initiating the PCS at the Sending Location

Sending CC/MSSP/CMs may initiate a PCS transaction, regardless of whether or not the gaining location submits a Broadcast Message requesting the PCS.

Note: The location that owns the Provider's credentialing record is the only location that may initiate the PCS transaction. A Provider's record may not be PCS'ed if the Provider is on an active ICTB.

A PCS transaction is initiated through the Credentialing module. To initiate a PCS transaction, select **Provider Search** from the **Credentialing** drop-down menu. Enter the last name of the Provider, select the **All (Primary UIC or Assignment UIC)** radio button, and then click **Search**.

On the **Search Results** tab, select **Open** from the hidden menu of actions for the Provider's record, as depicted in Figure 259 below.

Provider Search		Advanced Credentials Search		Search Results		Add Credentials Provider	
?	Name	SSN	Primary UIC				
▶	CROSS, GIDEON	234-64-3256	W3ZR10				
▶	DUNNE, NICK	237-65-8365	W3ZR10				
▶	HEPBURN, AUDREY	569-48-2536	W3ZR20				

Open
Initiate Custody Transfer
Deactivate Provider
Letters
Change SSN
Grant Module Access

Figure 259: Open Menu Item

Navigate to the **Work History** section of the credentials record by selecting **Work History** from the **Navigation** menu on the left. Select the hidden menu of actions, and then select **Initiate PCS**, as depicted in Figure 260 below.

Provider				
Name: AUDREY HEPBURN				
SSN: 569-48-2536				
Primary UIC: W3ZR20				
Assignments		Work History		Malpractice Insurance
Add Assignment				
?	UIC	Provider Type	Reported Date	Planned Rotation
▶	W3ZR20	Active Duty Staff (non Training)		
		Active Duty Staff (non Training)		

Open
Initiate PCS
Initiate ICTB
End Assignment
Cancel Assignment
Letters
Initiate Application
Reactivate Privileges

Figure 260: Initiate PCS Screen

CC/MSSP/CMs enter the **Gaining UIC**, **Effective Date**, and then select either **Yes** or **No** for **Transfer Custody**. Click **Submit** to initiate the PCS transaction, as depicted in Figure 261 below.

Figure 261: Initiate PCS Prompts Screen

The **Initiate PCS** screen, depicted in Figure 262 below, appears differently if Providers have not yet submitted their 1st E-application using CCQAS. If the PCS application is the first E-application Providers will complete in CCQAS, and they do not yet have a user account (i.e., user ID and password) when the PCS transaction is initiated, *the system will also automatically generate a new user account for them*. Additional data fields are present on the **Initiate PCS** screen to capture a Provider's primary email address and phone information, both of which are required to create the new user account for Providers.

Figure 262: Initiate PCS Screen for 1st E-Application

Providers then receive their user ID and temporary password information, which are required to access CCQAS, via an email message sent to the address entered on the **Initiate PCS** screen. It is critical that Providers enter an accurate email address on the **Initiate PCS** screen to receive the necessary information to access CCQAS.

Immediately after the sending location initiates a PCS transaction, the following actions automatically occur:

- CCQAS generates a privilege application for the Provider to request privileges at the gaining location
- The PAR process is initiated to document the Provider's performance at the sending location over the prior privileging period

CCQAS permanently transfers custody of the Provider's credentials record to the gaining location on the **Effective Date**. The transferred credentials record is explained in more detail in the next section.

9.3 The Transferred Provider Credentials Record

The Primary UIC (i.e., sending UIC) for a PCS has the ability to update and maintain a Provider's credential record if custody transfer is not initiated. However, if transfer of custody is initiated with the PCS, the gaining UIC has custody of the Provider's credential record. If users select **No** for transfer custody when the PCS is submitted, then the gaining UIC is not able to update or maintain the Provider's credential record. If the PCS is scheduled to be effective as of the current date and transfer of custody is requested, the following actions occur within the CCQAS application as soon as the transaction is submitted:

- The current assignment record is removed from the Provider's credential record
- The Provider's module access for the sending UIC is removed
- The complete Provider credentials record with **Status = Current** is transferred to the gaining facility. All previously entered data is retained in the credentials record when it is transferred. CCQAS automatically creates a new assignment record in the **Assignments** section of the credentials record, with the start date being the current date. This new assignment record is populated by the gaining CC/MSSP/CM to document the Provider's assignment information at the gaining facility
- Information from the Provider's assignment at the losing facility is maintained as a read-only record in the **Assignments** section of the credentials record
- A transaction is written to the Transaction Table at both the sending and gaining facility. The Transaction Table is explained in Section 9.4

If the PCS transaction was completed using a future date as the effective date, the Provider's record remains in active status at the sending facility until midnight (Central Time) on the day before the effective date. The PCS transaction is classified as a "pending transaction" until the effective date is reached.

9.4 Transaction Table for Incoming PCS Transactions

The Transaction Table may be viewed by clicking the **Credentialing** main menu bar across the top of the screen, and then selecting **Transaction Table**, as depicted in Figure 263 below.

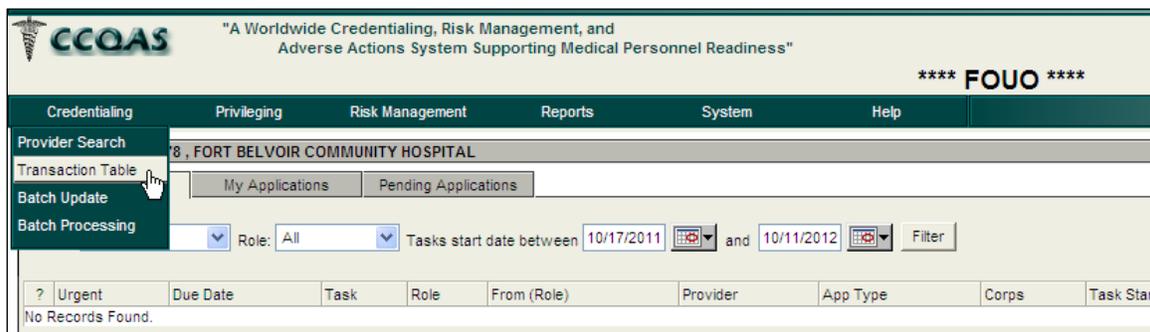


Figure 263: Accessing the Transaction Table

The **Provider Transactions** screen appears, as depicted in Figure 264 below. User may then select the **Type** and **Direction** of the transactions they wish to view.

The gaining location may acknowledge incoming ICTB transactions by selecting the **Direction** = *Incoming*, **Status** = *Unacknowledged* or *Both*, and **Action** = *PCS*, and then clicking **Search** at the bottom of the screen. A list of incoming transactions is displayed.

Users may then acknowledge the desired transaction by clicking the **Acknowledged** checkbox next to the record, then and clicking **Save**. The transaction is then changed to **Status** = *Acknowledged*. Close the Transaction Table by clicking **Close** at the bottom of the screen.

The screenshot shows the 'Provider Transactions' window. It has three filter sections: 'Direction' with radio buttons for 'Incoming' (checked), 'Outgoing', and 'Primary MTF'; 'Status' with radio buttons for 'Unacknowledged', 'Acknowledged', and 'Both'; and 'Action' with radio buttons for 'PCS', 'ICTB', 'All', 'Update of Credentials Requested', 'Non-Primary Assignment Created', and 'Custody Transfer'. Below these is a table with columns: Acknowledged, From MTF, To MTF, Primary MTF, Action, Initiated, Provider Name, SBN, Sender's Name, and Sender's Phone. Two rows are visible, both with 'PCS' action and 'Incoming' direction. At the bottom are 'Search', 'Save', and 'Close' buttons, and a note 'Results showing last 6 months of history'.

Acknowledged	From MTF	To MTF	Primary MTF	Action	Initiated	Provider Name	SBN	Sender's Name	Sender's Phone
<input type="checkbox"/>	W07CAA	W20H4A	W07CAA	PCS	10/11/2012	GREEN OLIVE	796-81-8001	CC91 CC91	(111) 222-3333
<input type="checkbox"/>	W20H7S	W20H4A	W20H10	PCS	10/10/2012	CHANNING TATUM	684-12-3668	CC100 CC100	(111) 222-3333

Figure 264: Provider Transactions Screen for Incoming PCS

Sending CC/MSSP/CMs may then perform a query on the Transaction Table to view the acknowledgement status of the PCS transaction. For example, the user at the sending location may find outgoing PCS transactions by selecting the **Direction** = *Outgoing*, **Status** = *Both* and **Action** = *PCS*, and then clicking **Search** at the bottom of the screen. A list of outgoing PCS transactions displays with an indicator of whether the PCS has been acknowledged by the gaining location.

If CCQAS users at a gaining location are not expecting the PCS, or have concerns about the transaction, they should contact the sending location prior to acknowledging the transaction. POC information for the sending location is included for each record listed in the Transaction Table.

9.5 The Transfer (PCS) Application for Clinical Privileges

After a PCS transaction is initiated, the system automatically sends an email notification to Providers, and an active task is placed in their work list with “Task = *Complete Application*” and “App Type = *Transfer (PCS)*”, as depicted in Figure 265 below.

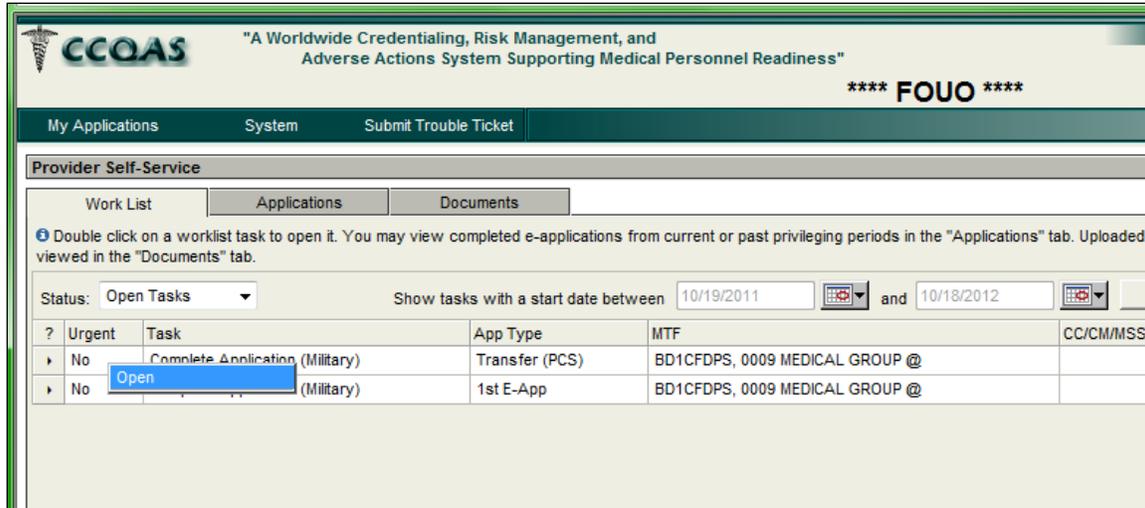


Figure 265: Provider Task – Complete Application, Transfer (PCS)

Providers may then open, complete, and submit the Transfer (PCS) Application according to the instructions provided, as depicted in Figure 266 below.

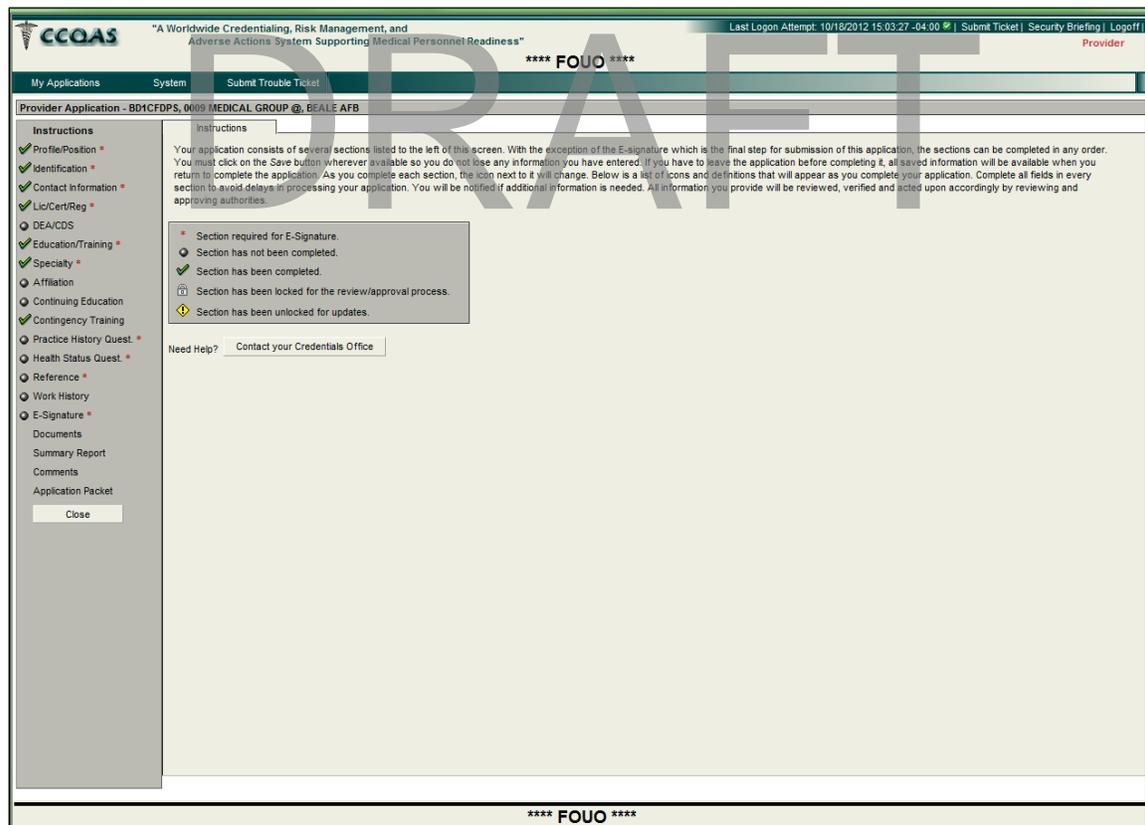


Figure 266: Transfer (PCS) Application for Privileges

The following are important features of the Transfer (PCS) application:

- The application is pre-populated with a Provider's most current credentials information from his or her CCQAS credentials file
- Providers may not edit existing credentials information that has been previously PSV'ed, except to update expiration or renewal dates
- Providers may add new credentials that are supported by appropriate documentation
- The application reflects the list of clinical privileges granted by a Provider's current privileging unit or facility during the most recent privileging action. Providers, however, are able to edit the delineations to coincide with their current competencies and (updated) credentials pertinent to this PCS privilege application
- The section of the application containing the "Practice History" questions must be completed prior to submitting the application. If a **Yes** response was submitted on a prior online privilege application, the modification application is pre-populated with the Provider's previous entries
- The section of the application containing the "Health Status" questions of the application must be completed prior to submitting the application. If a **Yes** response was submitted on a prior online privilege application for questions 5 ,6 or 7, the modification application is pre-populated with the Provider's previous entries
- All references listed on the original application are listed on the Transfer Application with a status of "**Current = No**". Providers should edit the **References** section to indicate which references are still current, or add new references

The Transfer (PCS) email notification is sent to Providers only once, but the work list item to complete the Transfer Application remains active, either until Providers complete and submit the application, or 90 days pass without submitting the application. The email notification contains contact information for the credentials staff at the gaining location, in case Providers encounter problems completing their application. After the application is e-signed and submitted, it is locked and cannot be edited by Providers, unless the CC/MSSP/CM at the gaining location returns the application to Providers with instructions to modify it.

9.6 Processing a PCS Transfer Application for Clinical Privileges

When CC/MSSP/CMs at sending locations initiate a PCS transaction, CCQAS adds a Provider's pending application to a *gaining* CC/MSSP/CM's **Pending Applications** tab list, as depicted in Figure 267 below. With the listing on this tab, CC/MSSP/CMs at gaining locations can see the number of days Providers take to complete and submit their privilege application after the system generates the task.

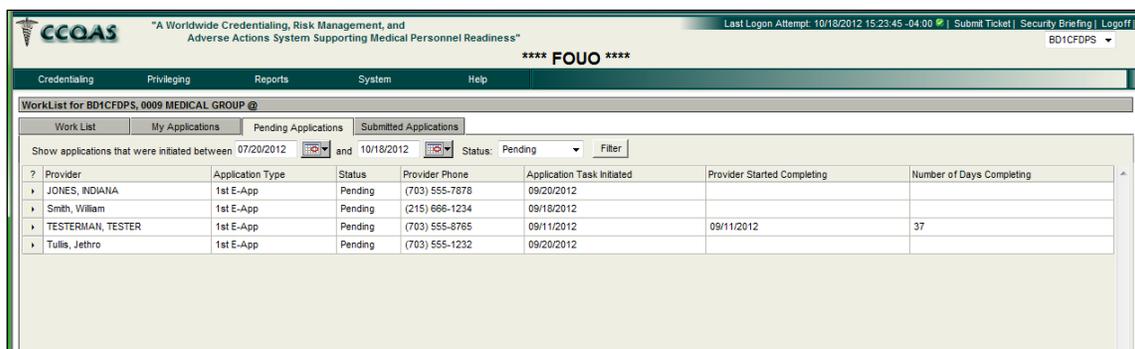


Figure 267: Gaining CC/MSSP/CM's 'Pending Applications' Tab

After a Provider's Transfer (PCS) application is e-signed and submitted, it disappears from the **Pending Applications** listing for gaining facility CC/MSSP/CMs, who then receives a new email notification of a task pending in CCQAS. A new work list item with "App Type = *Transfer (PCS)*" is added to their work list, as depicted in Figure 268 below.

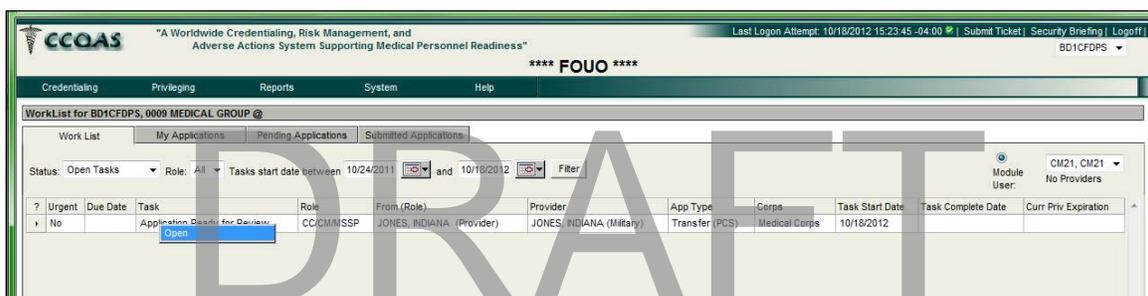


Figure 268: Gaining CC/MSSP/CM Task – Application Ready for Review, Transfer (PCS)

From this point, the PSV and review processes are similar to those for the 1st E-application, with the following exceptions:

- All Provider licenses, certifications, and/or registrations must be re-verified
- New credentials that require PSV, but were not previously verified, undergo the PSV process. Professional education and other static credentials which generally are not updated over time do not have to undergo PSV if they have already been PSV'ed in CCQAS
- A new NPDB query must also be performed

Note: CCQAS will accept a **Last Query Date** within the past 90 days as fulfillment of the PSV requirement, but a new NPDB/HIPDB query should be performed in accordance with Service or facility protocol, or any time concerns or questions arise regarding a Provider's recent practice. Regardless of the value entered for the **Last Query Date**, CC/MSSP/CMs or CVOs must click **Save** in the upper left-hand corner of the **NPDB Query** section of the **PSV Summary** screen for CCQAS to complete the PSV process.

- A minimum of one PAR from the sending location must be completed (already available in the **PARs/Snapshots** folder of the **Documents** Tab) before the application can be routed for review at the PCS location

These requirements must be met prior to routing the Transfer (PCS) application for review and approval.

Sections of the application edited by Providers are flagged so that CC/MSSP/CMs, CVOs, and reviewers may easily identify what information has been changed since the last application was approved. Icons appear next to each record that was added or changed from the original application, indicating that data within that section may need to be verified. If the **Verified** box on the right-hand side of the screen is checked, the information in that section does not have to be verified again, as depicted in Figure 269 below.

The screenshot displays the CCOAS Prime Source Verification (PSV) interface for Indiana Jones. The 'State License/Certification/Registration' section contains the following data:

Type	State	Number	Field	Status	Expires	ADM Waiver	Verified
License	Virginia	1234	Pharmacist	Active	Indefinite	No	<input type="checkbox"/>

The 'Verified' checkbox is unchecked, indicating that this section is flagged for verification. The interface also includes sections for National Certification/Registration (Completed), Unlicensed Information, and Drug Enforcement Agency (DEA) / Controlled Dangerous Substances (CDS) information.

Figure 269: Flagged Section for State License/Certification Registration Screen

After the PCS application for privileges is approved, the system imports the new privileges into the **Privileges** section of a Provider's credentials record for the assignment associated with the gaining UIC. Based on the privileges approval date, the system automatically calculates new **Privilege Expiration** and **Staff Appointment Expiration** dates for the Provider, for one-year periods for initial appointments, and two-year periods for regular appointments.

CC/MSSP/CMs, however, may change these dates in the **Privileges** section of the Provider's credentials record. Any edits made to these expiration dates in the **Privileges** section will be

displayed in read-only format in the new assignment record in the **Assignments** section of the credentials record.

9.7 PAR for the PCS Application

When the “Complete Application” task is created for a Provider, a new work list item for CC/MSSP/CMs at the sending location is created with “**Task = Setup PAR**”, as depicted in Figure 270 below.

The screenshot shows the CCQAS application interface. At the top, there is a header with the CCQAS logo and the text: "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". Below the header, there are navigation tabs: "Credentialing", "Privileging", "Reports", "System", and "Help". The main content area is titled "WorkList for BD1CFDPS, 0009 MEDICAL GROUP @". There are three sub-tabs: "Work List", "My Applications", and "Pending Applications". Below the sub-tabs, there are filters: "Status: Open Tasks", "Role: CC/CMMSSP", and "Tasks start date between 10/24/2011 and 10/18/2012". A table below the filters shows a single row for a task:

Task	Role	From (Role)	Provider	App Type	Corps	Ta
Setup PAR	CC/CMMSSP	N/A	JONES, INDIANA (Military)	1st E-App	Medical Corps	06

Figure 270: Sending CC/MSSP/CM Task – Setup PAR

The PCS PAR should reflect a Provider’s performance during the current or most recent privileging period at the sending location. PAR Evaluators should complete a PAR, with an optional review by one or more PAR Reviewers, prior to routing the PCS Transfer Application through the review process. The PAR process is explained in [Section 11](#).

Note: In Figure 270 above, “**App Type = 1st E-App**” indicates that the period of evaluation for this PAR corresponds to the privileges granted and performed under the last privilege application approved for the Provider at this location. In this example, the Provider’s last approved privilege application was his or her 1st E-Application. A PAR task always references the previous privileging period and privilege application, since past performance is being assessed.

Although the exception rather than the rule, CC/MSSP/CMs may cancel a PAR as appropriate (e.g., a Provider coming back from a remote deployment where no PAR evaluators were on hand). Also, CC/MSSP/CMs who received the “*Setup PAR*” work list item may replace the electronic PAR process in CCQAS with a paper-based PAR process (i.e., “*Offline PAR*”) that occurs outside CCQAS. These processes are explained in greater detail in [Section 11](#).

9.8 Cancelling a PCS

Administrator-level permissions to the CCQAS application are necessary to cancel a PCS transaction. If a PCS transaction was initiated in error and needs to be cancelled, a Service-level CCQAS Administrator should be contacted for assistance.

9.9 Changes to the CCQAS User Account after a PCS Transaction

Upon initiation of a PCS transaction, CCQAS automatically generates a new E-application so that Providers may request clinical privileges in advance of arrival at a gaining location. This new application is indicated on the **MTF** tab in a Provider’s user account. Providers should also continue to view and open tasks generated by the sending facility, such as tasks to review and

acknowledge the electronic PAR, generated to assess their performance over the prior privileging period at the losing facility.

A Provider's access to the Privileging module (and any other CCQAS module to which a user was granted access) at a sending facility, however, is removed, since the individual is no longer a member of the medical staff at the sending facility. If a Provider has open work list items associated with the Privileging module tasks at the sending location at the time that the PCS transaction is initiated, a warning message is displayed, as depicted in Figure 271 below.

If users click **Cancel**, the PCS transaction is cancelled. If users click **OK**, the PCS transaction proceeds. If the **PCS Effective Date** is one or more days in the future, CCQAS sends an automated email notification, instructing Providers to complete their tasks prior to the PCS date. This email notification is not generated if the **PCS Effective Date** is the current date.

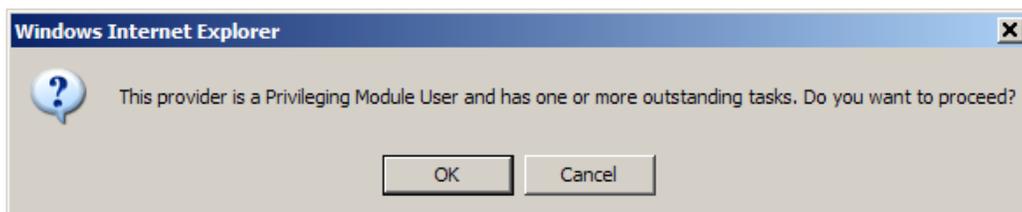


Figure 271: Outstanding Tasks Warning Message

As long as open tasks remain on a user's work list (user refers to the individual who was PCS'ed), his or her name should appear in the User list on the assigned CC/MSSP/CM's work list screen. After open work list items are cancelled or reassigned, CCQAS automatically removes the user's name from the User list.

No Privileging module access is automatically granted to a user's account at a gaining facility. CC/MSSP/CMs at gaining facilities must add **Module User** access if and when access is required, so that users can perform their new jobs.

10 Renewal of Clinical Privileges

As a Provider's privilege expiration date approaches, a new application for renewal of clinical privileges must be completed and submitted for review. Unlike the application for modification of privileges (refer to [Section 7](#)), Providers are not required to take any action to generate the application for renewal of privileges. At the designated time, the system will automatically generate the renewal application and send a notification to Providers indicating that a new task has been placed in their work list in CCQAS. CC/MSSP/CMs may also initiate the renewal application process manually, if needed.

10.1 Auto-Generating an Application for Renewal of Clinical Privileges

In order for CCQAS to automatically generate a renewal application for a Provider, the CC/MSSP/CM at each facility or unit must set the length of the application renewal period on the **Command Parameters** screen. Providers can access this screen by clicking the **System** main menu, as depicted in Figure 272 below.

Note: CC/MSSP/CMs are responsible for ensuring the **Command Parameters** screen is populated with current and complete information about the command and contact personnel. CCQAS uses the information on this screen to generate credentialing and privileging letters and forms. Refer to [Section 12](#) for detailed information on the letter generation process.

The screenshot shows the CCQAS web application interface. At the top, there is a header with the CCQAS logo and the tagline: "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". To the right of the header, it says "**** FOUO ****". Below the header is a navigation bar with tabs for "Credentiaing", "Privileging", "Reports", "System", and "Help". The "System" tab is selected, and a dropdown menu is open, showing options: "Authority Tables", "Command Parameters" (highlighted with a mouse cursor), "MTF Contacts", "Applicant Processing", "User Processing", "Change Start Page", "Tracker Status", "Provider Remarks", "Broadcast Messages", and "Messaging". The main content area contains a "Provider Search" section with fields for "Last Name", "Alias Last Name", "Branch" (dropdown), "Primary UIC", "Department", "Provider Type", and "Sort By" (dropdown). To the right of the search fields are fields for "First Name", "Alias First Name", "Corps" (dropdown), "Assignment UIC", and "Work Center".

Figure 272: Command Parameters Menu Item

On the right-hand side of the **Command Parameters** screen, under the **Privileging** section, two data fields are available to designate the **Active Renewal Notice Days** and **Reserve/Guard Renewal Notice Days**, as depicted in Figure 273 below.

The screenshot shows the "Command Parameters" screen. It is divided into two sections: "Certification Authority" and "Privileging". Under "Certification Authority", there are two text input fields: "Official" with the value "COL Alexander Smith" and "Title" with the value "Commander". Under "Privileging", there are several fields: "Privileging Module Activated" with the value "Yes", "Privileging Authority UIC" with the value "W2H810" and a small icon, "Active Renewal Notice Days" with the value "30", and "Reserve/Guard Renewal Notice Days" with the value "90".

Figure 273: Renewal Days Parameters on the Command Parameters Screen

CC/MSSP/CMs should enter the desired number of days in advance of a Provider's privilege expiration date when they want the system to generate the renewal application for active duty and civilian Providers, or reserve/guard Providers, respectively. The number of days entered should allow sufficient lead time for the Provider to complete and submit his or her renewal application prior to the expiration of current privileges.

Example: If CC/MSSP/CMs want to have their privileged active duty Providers start their renewal application one month before the privilege expiration date, they should set the “**Active Renewal Notice Days = 30.**” The **Reserve/Guard Renewal Notice Days** typically sets a longer period of time according to facility or unit privileging practice and Service guidance.

Only one number may be entered in each field, and this number applies for both initial and regular appointment expirations. After these parameters are saved, a renewal application is generated for each Provider at the established number of renewal days prior to the **Privilege Expiration Date** entered into the Provider’s credentials record. When the renewal application is generated, the system sends an email notification to the Provider, and an active task is placed in the Provider’s work list entitled “Task = *Complete Application*” and “App Type = *Renewal*”, as depicted in Figure 274 below.

The screenshot shows the 'Provider Self-Service' interface. At the top, there are tabs for 'Work List', 'Applications', and 'Documents'. Below the tabs, there is a help icon and text: 'Double click on a worklist task to open it. You may view completed e-applications from current or past privileging periods in the "Applications" tab. U in the "Documents" tab.' Below this, there is a 'Status' dropdown menu set to 'Open Tasks' and a search filter 'Show tasks with a start date between' with two date pickers: '10/06/2011' and '10/05/2012'. Below the search filters is a table with the following data:

?	Urgent	Task	App Type	MTF
▶	No	Complete Application (Military)	Renewal	W2DH78, FORT BELVOIR COMMUNITY HOSPITA

Figure 274: Provider Work List Item – Complete Renewal Application

10.2 Manually Generating a Renewal Application for Clinical Privileges

There may be times when CC/MSSP/CMs need to initiate the privilege renewal process outside of the established privilege renewal cycle, as discussed in [Section 10.1](#). A renewal application may be manually generated within the **Credentials** module. To do so, CC/MSSP/CMs search for the desired Provider, and then select **Open** from the hidden menu of options on the **Search Results** tab, as depicted in Figure 275 below.

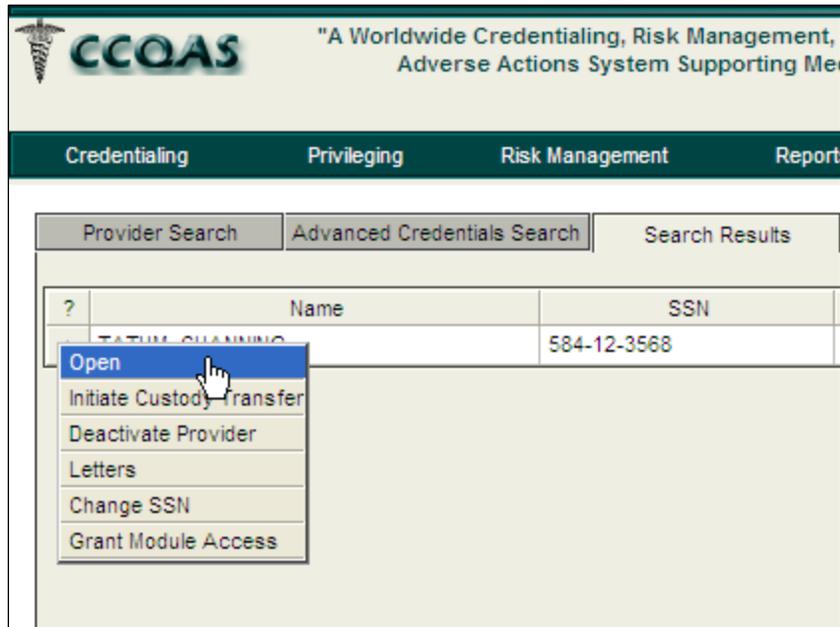


Figure 275: Open Credentials Record

After CC/MSSP/CMs open the record, they select the **Work History** section from the navigation menu. When the **Assignment** screen is displayed, CC/MSSP/CMs can initiate the application by selecting the hidden menu of actions from the assignment, and then selecting **Initiate Application**, as depicted in Figure 276 below.

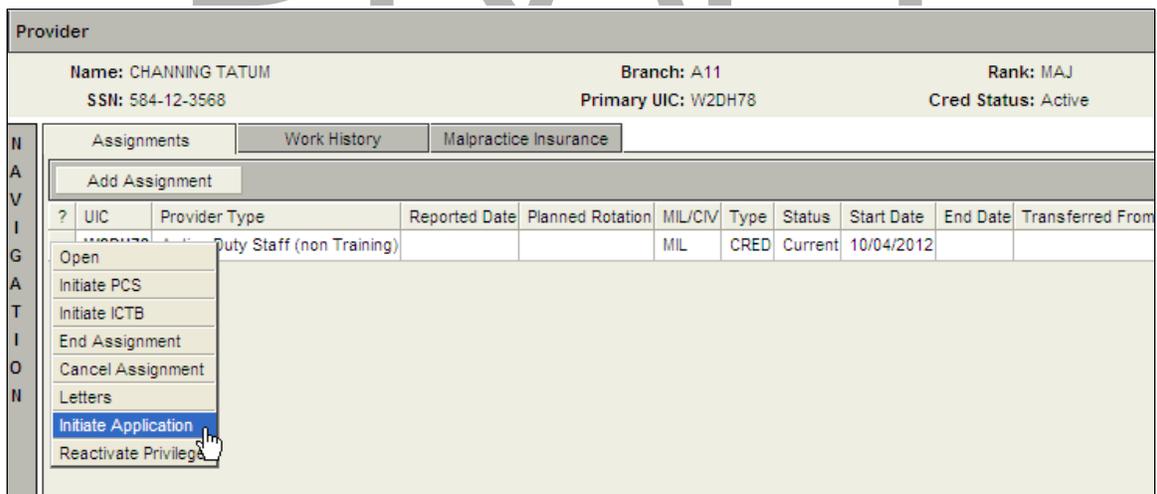


Figure 276: Initiate Renewal Application

CC/MSSP/CMs then select **Renewal** from the **Privilege Application Type** drop-down list, and then click **Submit**, as depicted in Figure 277 below.

Figure 277: Initiate Renewal Screen

This action generates the renewal application for the Provider. CCQAS then sends an email notification to the Provider, and an active task is then placed in his or her work list entitled “Task = *Complete Application*” and “App Type = *Renewal*”.

10.3 The Renewal Application

After a renewal application is generated for them, Providers may open, complete, and submit the Renewal Application, according to the instructions provided, as depicted in Figure 278 below.

Figure 278: Provider Application (Renewal)

The following are important features of the Renewal Application:

- The application is prepopulated with a Provider's most current credentials information from his or her CCQAS credentials file
- Providers may not edit existing credentials information that has been previously PSV'ed, except to update expiration or renewal dates
- Providers may add new credentials that are supported by appropriate documentation
- The application reflects the list of clinical privileges granted by a Provider's current privileging unit or facility during the most recent privileging action. Providers, however, are able to edit the delineations to coincide with their current competencies and (updated) credentials pertinent to this renewal application
- The section of the application containing the "Practice History" questions must be completed prior to submitting the application. If a "Yes" response was submitted on a prior online privilege application, the modification application is pre-populated with a Provider's previous entries
- The section of the application containing the "Health Status" questions of the application must be completed prior to submitting the application. If a "Yes" response was submitted on a prior online privilege application for questions 5 ,6 or 7, the modification application is prepopulated with a Provider's previous entries
- All references listed on the original application are listed on the Transfer Application with a status of "**Current = No**". Providers should edit the **References** section to indicate which references are still current or add new references

The renewal email notification is sent to a Provider only once, but the work list item to complete the renewal application remains active, either until the Provider completes and submits the application, or 90 days pass without submitting the application. After it is submitted, the application is locked and cannot be edited by the Provider, unless the CC/MSSP/CM returns the application to the Provider with instructions to modify it.

10.4 Processing an Application for Renewal of Clinical Privileges

When the renewal application is generated for a Provider, CCQAS adds his or her pending application to the CC/MSSP/CM's **Pending Applications** tab list. With the listing on this tab, CC/MSSP/CMs can view the number of days Providers take to complete and submit their privilege application after the system generates the task.

After the application is e-signed and submitted, the Provider's renewal application disappears from the **Pending Applications** tab and the CC/MSSP/CM then receives a new email notification of a task pending in CCQAS. A new work list item with "**App Type = Renewal**") is added to his or her work list, as depicted in Figure 279 below.

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps
No		Application Ready for Review	CC/CMMSSP	TATUM, CHANNING (Provider)	TATUM, CHANNING (Military)	Renewal	Medical Corps
No		Setup PAR	CC/CMMSSP	N/A	TATUM, CHANNING (Military)	1st E-App	Medical Corps

Figure 279: CC/MSSP/CM Task – Renewal Application Ready for Review

From this point, the PSV and review processes are similar to those for the 1st E-application, with the following important exceptions:

- All Provider licenses, certifications, and/or registrations must be re-verified
- New credentials that require PSV, but were not previously verified, undergo the PSV process. Professional education and other static credentials, which generally are not updated over time, do not have to undergo PSV if they have already been PSV'ed in CCQAS
- A new NPDB query must also be performed if the **Last Query Date** is greater than 90 days old

Note: CCQAS will accept a **Last Query Date** within the past 90 days as fulfillment of the PSV requirement, but a new NPDB/HIPDB query should be performed in accordance with Service or facility protocol if concerns or questions arise regarding a Provider's recent practice. Regardless of the value entered for the **Last Query Date**, CC/MSSP/CMs or CVOs must click **Save** in the upper left corner of the **NPDB Query** section of the **PSV Summary** screen in order for CCQAS to complete the PSV process.

- A minimum of one PAR covering the prior privileging period must be completed (already available in the "PARs/Snapshots" folder of the **Documents** tab) before the Renewal Application can be routed for review

These requirements must be met prior to routing the renewal application for review and approval.

Sections of an application edited by Providers are flagged so that CC/MSSP/CMs, CVOs, and Reviewers may easily identify what information has been changed since the last application was approved. Icons appear next to each record that was added or changed from the original application, indicating that data within that section may need to be verified. If the **Verified** box on the right-hand side of the screen is checked, the information in that section does not have to be re-verified, as depicted in Figure 280 below.

Type	State	Number	Field	Status	Expires	ADH Waiver	Verified
License	Colorado	234234	Anatomic Physician	Training	12/31/2013	No	<input checked="" type="checkbox"/>

Figure 280: Modified Section for State License/Certification/Registration

After the renewal application for privileges is approved, the system imports the new privileges into the **Privileges** section of a Provider's credentials record. Based on the privileges approval date, the system automatically calculates new **Privilege Expiration** and **Staff Appointment Expiration** dates for the Provider, for one-year periods for initial appointments, and two-year periods for regular appointments. These dates, however, may be changed by CC/MSSP/CMs in the **Privileges** section of the Provider's credentials record. Any edits made to these expiration dates in the **Privileges** section will be displayed in read-only format in the new assignment record in the **Assignments** section of the credentials record.

10.5 PAR for the Renewal Application

When the **Complete Application** task is created for a Provider, a new work list item is also created for the CC/MSSP/CM entitled, "Task = *Setup PAR*", as depicted in Figure 281 below.

The screenshot shows the CCQAS WorkList interface. At the top, there is a header with the CCQAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". Below this is a navigation bar with tabs for Credentiaing, Privileging, Risk Management, Reports, System, and Help. The main content area is titled "WorkList for W20H78, FORT BELVOIR COMMUNITY HOSPITAL". It features a "Work List" tab and a "My Applications" tab. Below the tabs, there are filters for Status (Open Tasks), Role (All), and Tasks start date between 10/11/2011 and 10/05/2012. A table of tasks is displayed below the filters. The table has columns for Urgent, Due Date, Task, Role, From (Role), Provider, and App Type. The first row of the table is highlighted with a red box, showing a task named "Setup PAR" with Role "CC/CM/MSSP", From (Role) "N/A", Provider "TATUM, CHANNING (Military)", and App Type "1st E-App".

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type
No		Setup PAR	CC/CM/MSSP	N/A	TATUM, CHANNING (Military)	1st E-App

Figure 281: CC/MSSP/CM Task – Setup PAR

The renewal PAR should reflect a Provider’s performance during the current or most recent privileging period at the Provider’s current assignment location. A PAR Evaluator should complete a PAR, with an optional review by one or more PAR Reviewers, prior to routing the PCS Transfer Application through the review process. The PAR process is explained in [Section 11](#).

Note: In Figure 281, “App Type = 1st E-app” indicates that the period of evaluation for this PAR corresponds to the privileges granted and performed under the last privilege application approved for the Provider at this location. In this example, the Provider’s last approved privilege application was his or her 1st electronic application. A PAR task always references the previous privileging period and privilege application, since past performance is being assessed.

Although the exception rather than the rule, CC/MSSP/CMs may cancel a PAR due to certain conditions (e.g., a Provider coming back from a remote deployment where no PAR evaluators were on hand). Mechanisms are in place for the system to allow the application to move forward when a scenario such as this occurs. Also, CC/MSSP/CMs who received the “Setup PAR” work list item may replace the electronic PAR process in CCQAS with a paper-based PAR process (“Offline PAR”) that occurs outside CCQAS. This process is explained in greater detail in [Section 11](#).

11 The PAR

CCQAS allows users to generate, complete, and review a PAR online for a privileged Provider for every privileging period in every duty assignment. CCQAS automatically initiates the PAR process to document the Provider’s performance prior to the renewal of clinical privileges at the same location, or the award of privileges at a PCS location, or following the completion of duty at an ICTB location. The PAR process may also be manually initiated independent of these privileging events for any Provider who has an approved electronic application in CCQAS.

Although the exception rather than the rule, CC/MSSP/CMs may cancel the automated PAR and replace it by initiating the offline PAR process that occurs outside the CCQAS application. The PAR process, after it is initiated, may also be reassigned or terminated, when appropriate. These processes are addressed in [Sections 11.7 through 11.9](#).

11.1 Automated Initiation of the PAR Process

CCQAS was designed to initiate the PAR process in support of upcoming privileging actions for a Provider. CCQAS automatically initiates the PAR process under the following circumstances:

- When a Renewal application is created for a Provider (refer to [Section 10](#)), the automated PAR process initiates for the current privileging period that is about to expire
- When a PCS transaction is initiated for a Provider (refer to [Section 9](#)), the automated PAR initiates for the most recent privileging period at the sending facility
- When a period of ICTB duty ends for a Provider (refer to [Section 8](#)), and the ICTB duty was greater than 3 days in duration, the automated PAR process initiates for the work performed at the ICTB location

When CCQAS generates a Renewal application or a Transfer (i.e., PCS) application for a Provider, it also generates a new work list item for the CC/MSSP/CM entitled, “Task = *Setup PAR*”, as depicted in Figure 282 below.

Note: Figure 282 depicts the *Setup PAR* task for a Provider where the “App Type = *Transfer(PCS)*” but the *PAR* task was generated at the same time this Provider’s renewal application was generated. In this example, the last E-Application the Provider completed was his or her PCS application for privileges when the Provider initially transferred into this unit. The *PAR* task pertains to the privileging period established when this Provider’s PCS application was approved.

The screenshot shows the CCQAS application interface. At the top, it displays 'CCQAS Version 2.10.0 - Centralized Credentialing, Quality Assurance System - Windows Internet Explorer provided by ASM Research'. The main header includes 'A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness' and '**** FOUO ****'. Below the header, there are navigation tabs: 'Credentialing', 'Privileging', 'Risk Management', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area is titled 'Work List for BB1CFDPR, 0002 MEDICAL GROUP'. It shows a table with columns: 'Urgent', 'Due Date', 'Task', 'Role', 'From (Role)', 'Provider', 'App Type', 'Coops', 'Task Start Date', 'Task Complete Date', and 'Curr Priv Expiration'. A single row is visible with the following data: 'No', 'Setup PAR', 'CC/MSSP', 'N/A', 'Anderson, Blaine (Military)', 'Transfer (PCS)', 'Medical Corps', '09/21/2012', and '09/21/2012'. The user 'RICHARD DAWSON' is logged in.

Figure 282: CC/MSSP/CM Work List Item – Setup PAR

It is the responsibility of the CC/MSSP/CM at the facility or unit where the Provider was privileged to assign one or more PAR Evaluators to complete the PAR form for the applicable privileging period. The *Setup PAR* task that is generated for a Renewal application is sent to the CC/MSSP/CM at the current location of assignment, but the CC/MSSP/CM at the sending location receives the *Setup PAR* task for Transfer (i.e., PCS) applications. The *Setup PAR* task that is generated for ICTB duty is sent to the CC/MSSP/CM at the ICTB location.

The completion of a PAR is required by CCQAS so the CC/MSSP/CM can route a Renewal application or PCS application for review and approval. Completion of future privileging actions may also be contingent upon the completion of any ICTB PARs due on a Provider who performed temporary duty at one or more MTFs between privileging cycles.

CCQAS provides the option to route the completed PAR to one or more PAR Reviewers, who may then review the completed PAR and provide their concurrence or non-concurrence with its content. The inclusion of PAR Reviewers in the PAR process is not required by CCQAS, but should be performed according to Service policy. The routing, completion, and review of the PAR are discussed in Section [11.3](#) and [11.4](#).

Note: At the time of publication of this user guide, only the Navy required the inclusion of a PAR Reviewer in the PAR routing process.

11.2 Manual Initiation of the PAR Process

The PAR process may also be initiated manually for any Provider as long as he or she has an approved electronic application in CCQAS. CC/MSSP/CMs may initiate a PAR manually by selecting **Work List** from the **Privileging** main menu, and then clicking the **My Applications** tab. A list of all applications processed for all Providers during the default date range are returned, as depicted in Figure 283 below. A PAR may be initiated manually for any completed application that is listed on the **Applications** screen.



Figure 283: Initiate PAR Menu Item

CC/MSSP/CMs select **Initiate PAR** from the list of options in the hidden menu for the Provider's selected application coinciding with the privileging period for the PAR. If the Provider has multiple, completed applications in CCQAS, it is important for CC/MSSP/CMs to select the application associated with the privileging period that requires a PAR. This is because the PAR form that is generated by CCQAS reflects the awarded privileges associated with the application from which the PAR was initiated manually.

11.3 Routing of the PAR

The PAR routing, completion, and review process is the same regardless of whether the **Setup PAR** task was initiated automatically by CCQAS or initiated manually by a CC/MSSP/CM. When CC/MSSP/CMs open the **Setup PAR** task, or initiate the PAR manually, the **PAR Routing** screen appears, as depicted in Figure 284 below.

Figure 284: PAR Routing Screen

Important features of the **PAR Routing** screen include the following:

- The Provider’s demographic information is displayed in read-only format on the screen header
- The **Period of Evaluation** should auto-populate, displaying the time period over which the awarded privileges apply. The dates are editable by CC/MSSP/CMs
- The **Purpose of Evaluation** auto-populates if the *Setup PAR* task was generated automatically by CCQAS. If the PAR was initiated manually, then CC/MSSP/CMs should make the appropriate selection from the pick list
- The Provider’s performance for each specialty in which he or she was privileged must be reported on a separate PAR, and a PAR Evaluator must be selected for each specialty in which the Provider was privileged
- Branch clinics are displayed in separate tabs on this screen, if the Provider possesses privileges at that *UIC PAR* task
- The names of all individuals who have the “PAR Evaluator” role assigned to their user account should appear in the **PAR Evaluator** pick list
- If the Provider was privileged in more than one specialty, then one PAR Evaluator should be assigned for each specialty in which the Provider was privileged during the evaluation period
- The names of all individuals who have the PAR Reviewer role assigned to their user account should appear in the PAR Reviewer box

- Assignment of one or more PAR Reviewers is optional; assignment of PAR Reviewers should be according to Service or facility policy

CC/MSSP/CMs may perform one of the following actions on the **PAR Routing** screen:

- CC/MSSP/CMs may cancel the **PAR** task by selecting **Cancel PAR**. This results in the removal of the **Setup PAR** task from the work list and cancel the PAR completion requirement for the associated application
- CC/MSSP/CMs may populate all required fields on the **PAR Routing** screen and click **Submit** to send the electronic PAR to the assigned PAR Evaluator
- If the online PAR process is replaced by a paper-based PAR process, the radio button for **Offline PAR** should be selected prior to clicking **Submit**. The offline PAR process is discussed in [Section 11.7](#)
- CC/MSSP/CMs may close the **PAR Routing** screen and return to the work list by clicking **Close**. The **Setup PAR** task remains open in the work list

After CC/MSSP/CMs enter all required information on the **PAR Routing** screen and click **Submit**, each assigned PAR Evaluator receives an email notification indicating the presence of a new task in his or her work list that requires action.

11.4 Completing the PAR – The PAR Evaluator Role

After CC/MSSP/CMs submit the routing for the PAR, each assigned PAR Evaluator receives a new work list item with “Task = *Complete PAR*”, as depicted in Figure 285 below.

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Sta
• No		Complete PAR	PAR Evaluator	CM2013, CM2013 NC DO NOT change (CC/CM/MSSP)	Anderson, Barney (Military)	1st E-App	Medical Corps	09/19/20
• No		Complete PAR	PAR Evaluator	CM2013, CM2013 NC DO NOT change (CC/CM/MSSP)	Anderson, Barney (Military)	1st E-App	Medical Corps	09/18/20
• No		PA Decision Complete/Action Required	CC/CM/MSSP	CM2013, CM2013 NC DO NOT change (Privileging Authority)	ADAMS, BRIAN (Military)	1st E-App	Medical Corps	09/18/20
• No		PA Decision Complete/Action Required	CC/CM/MSSP	CM2013, CM2013 NC DO NOT change (Privileging Authority)	Anderson, Barney (Military)	1st E-App	Medical Corps	09/14/20
• No		Complete PSV	CVO	CM2013, CM2013 NC DO NOT change (PSV)	AF, FIRST NC CRED (Military)	1st E-App	Medical Officer	09/04/20

Figure 285: PAR Evaluator Work List Task – Complete PAR

When PAR Evaluators open the *Complete PAR* task, the **Profile** section of the **Performance Assessment Report** is displayed, as depicted in Figure 286 below.

The **Profile** section provides demographic information about the Provider and the location, time period, and Provider’s privilege category (i.e., specialty) that require evaluation. PAR Evaluators may navigate between different sections of the application by clicking the desired section of the form listed down the left side of the screen.

Note: All documents that are associated with the privilege application, on which the PAR evaluation period is based, are viewable by selecting **Documents** from the navigation bar that runs vertically on the left side of the screen.

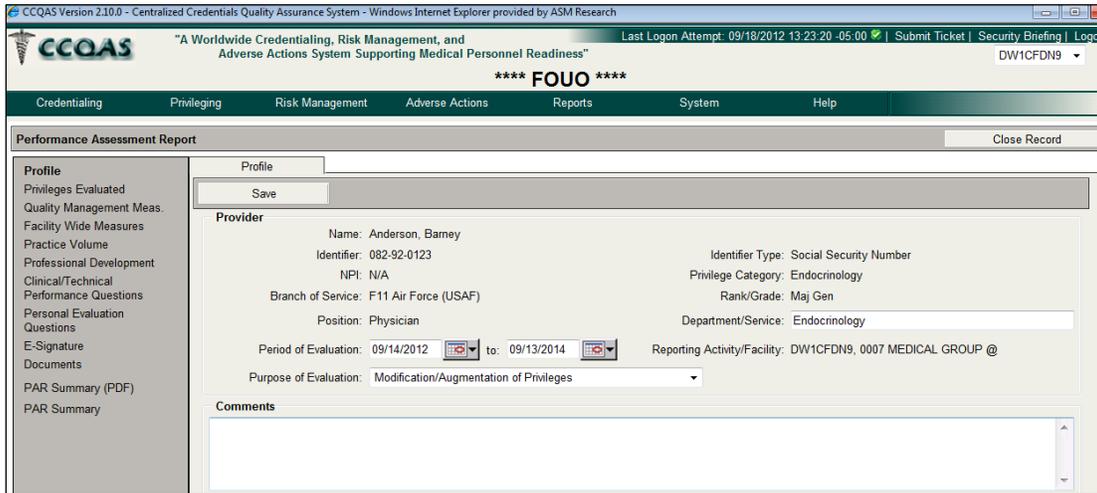


Figure 286: Profile Section of the PAR

DRAFT

The next section of the PAR form is the **Privileges Evaluation** section, as depicted in Figure 287 below.

The screenshot shows the 'Privileges Evaluated' section of a Performance Assessment Report. The interface includes a navigation menu on the left with options like Profile, Privileges Evaluated, Quality Management Meas., Facility Wide Measures, Practice Volume, Professional Development, Clinical/Technical, Performance Questions, Personal Evaluation Questions, E-Signature, Documents, PAR Summary (PDF), and PAR Summary. The main content area is titled 'Privileges Evaluated' and has a 'Save' button. Below the button, the 'Privilege Category' is set to 'Dermatology'. The table below lists various dermatology privileges and their evaluation status.

Privilege(s)	Evaluation	Acceptable	Unacceptable	Not Observed	Comments
The scope of privileges in Dermatology includes the evaluation, diagnosis, and provision of consultation, and surgical treatment of patients with diseases of the skin and adjacent mucous membranes, cutaneous appendages, hair, nails, and subcutaneous tissue. Dermatologists may admit and may provide care to patients in the intensive care setting or the operating room in accordance with MTF policies. Privileges also include the ability to assess, stabilize, and determine the disposition of patients with emergent conditions in accordance with medical staff policy.	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Diagnosis and Management (D&M):					
Fungal cultures	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Knee Pain nc	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Oil preparation of scabies	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Patch testing for delayed hypersensitivity	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Photopatch testing	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Wood's light examination	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Wright's stain (Tzanck test)	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Procedures:					
Advanced Cryotherapy	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Cryosurgical removal of skin lesions	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Curettage	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Electrosurgical removal of skin lesions	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Figure 287: Privileges Evaluated Section for the Army PAR

In Army and Navy facilities, PAR Evaluators should indicate their assessment of the Provider's performance for each privilege granted to the Provider. If PAR Evaluators select **"Unacceptable"** for any of the privilege items, a comment is required to save the information entered on the screen, as depicted in Figure 288 below.

PAR Evaluators may also add a comment for any item by clicking the empty note icon (📝), as depicted in Figure 289 below. After a comment is added, the empty note icon (📝) becomes a filled note icon (📝). After all items have been evaluated, click **Save**.

CCOAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/19/2012 15:12:07 -05:00 Submit Ticket | Security Briefing | Logout

**** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Performance Assessment Report Close Record

Profile Privileges Evaluated Quality Management Meas. Facility Wide Measures Practice Volume Professional Development Clinical/Technical Performance Questions Personal Evaluation Questions E-Signature Documents PAR Summary (PDF) PAR Summary

Privileges Evaluated Save

Privilege Category: Endocrinology

- Physicians requesting privileges in this subspecialty must also request Internal Medicine privileges.
- Scope

Privilege(s)	Evaluation	Acceptable	Unacceptable	Not Observed	Comments
The scope of privileges in endocrinology, diabetes, and metabolism includes the evaluation, diagnosis, treatment, and provision of consultation to patients (including critically ill patients) with injuries or disorders of the endocrine glands (e.g., thyroid and adrenal glands), metabolic and nutritional disorders, diabetes in pregnancy or gestational disorders, pituitary diseases, and menstrual and gonadal problems. Privileges include the performance of history and physical exams. Practitioners may admit and may provide care to patients in the intensive care setting in accordance with MTF policies. Specialists in endocrinology, diabetes, and metabolism assess, stabilize, and determine disposition of patients with emergent conditions in accordance with medical staff policy.	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
- nc

Privilege(s)	Evaluation	Acceptable	Unacceptable	Not Observed	Comments
Knee Pain nc	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
- Diagnosis and Management (D&M):

Privilege(s)	Evaluation	Acceptable	Unacceptable	Not Observed	Comments
Interpretation of bone mineral density measurements	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Management of hormone delivery systems, including continuous subcutaneous insulin infusion via insulin pump	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Performance and interpretation of static and dynamic (stimulation and suppression) endocrine function tests	Fully Competent	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
- Procedures:

Privilege(s)	Evaluation	Acceptable	Unacceptable	Not Observed	Comments
Fine needle thyroid biopsy	Fully Competent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
- Other (Facility- or provider-specific privileges only):

Figure 288: Privileges Evaluated Section for the Navy PAR with Unacceptable

CCOAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 09/18/2012 13:23:20 -05:00 Submit Ticket | Security Briefing | Logout

**** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Performance Assessment Report Close Record

Profile Privileges Evaluated Quality Management Meas. Facility Wide Measures Practice Volume Professional Development Clinical/Technical Performance Questions Personal Evaluation Questions E-Signature Documents PAR Summary (PDF) PAR Summary

Privileges Evaluated

Privilege Category: Endocrinology

- Endocrinology
 - Version 1.0
 - Physicians requesting privileges in this subspecialty must also request Internal Medicine privileges.
 - Scope

Privilege(s)	Evaluation
The scope of privileges in endocrinology, diabetes, and metabolism includes the evaluation, diagnosis, treatment, and provision of consultation to patients (including critically ill patients) with injuries or disorders of the endocrine glands (e.g., thyroid and adrenal glands), metabolic and nutritional disorders, diabetes in pregnancy or gestational disorders, pituitary diseases, and menstrual and gonadal problems. Privileges include the performance of history and physical exams. Practitioners may admit and may provide care to patients in the intensive care setting in accordance with MTF policies. Specialists in endocrinology, diabetes, and metabolism assess, stabilize, and determine disposition of patients with emergent conditions in accordance with medical staff policy.	Fully Competent
 - nc

Privilege(s)	Evaluation
Knee Pain	Fully Competent
 - Diagnosis and Management (D&M):

Privilege(s)	Evaluation
Interpretation of bone mineral density measurements	Fully Competent
Management of hormone delivery systems, including continuous subcutaneous insulin infusion via insulin pump	Fully Competent
Performance and interpretation of static and dynamic (stimulation and suppression) endocrine function tests	Fully Competent
 - Procedures:

Privilege(s)	Evaluation
Fine needle thyroid biopsy	With Supervision
 - Other (Facility- or provider-specific privileges only):

Figure 289: Privileges Evaluated Section for the Air Force PAR

In Air Force facilities, this section of the PAR presents a read-only listing of the privileges awarded to the Provider, and no action on each privilege is required on the part of PAR Evaluators. PAR Evaluators, however, must render a general assessment of the Provider's competency at the end of the PAR form.

The next section of the PAR form is the **Quality Management Measures** section, as depicted in Figure 290 below. When PAR Evaluators first open the PAR, this screen contains no data. To add a measure, click **Add**.



Figure 290: Quality Management Measures Section of the PAR

A screen appears with a pick list of different types of measures to select, as depicted in Figure 291 below. For each type of measure selected, different data fields are enabled to collect the appropriate information for the measure.

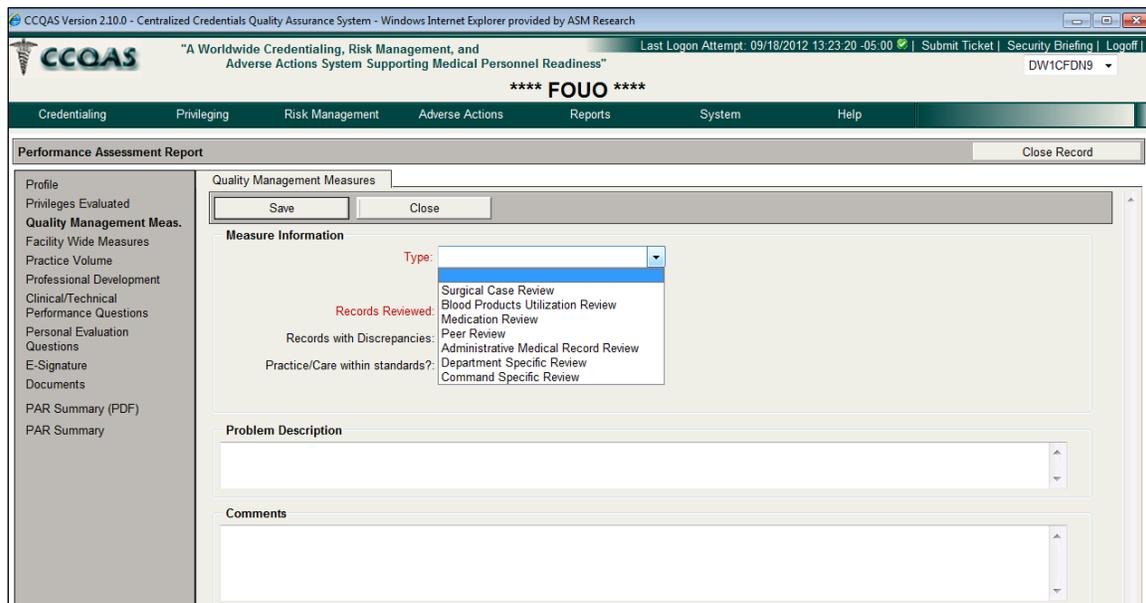


Figure 291: Types of Quality Management Measures

In general, a comment in the **Comments** section of the screen is required, if “**Practice/Care within standards? = No**” is entered for any of the documented measures.

As each measure is assessed, PAR Evaluators click **Save**. Multiple measures, as many as are appropriate to paint as complete a picture as possible of the Provider’s performance, may be assessed and entered in the **Quality Management Measures** section of the PAR.

The **Quality Management Measures** and **Practice Volume** metrics (described below) differ, depending on the Provider category. Physicians, allied health Providers, and nurse practitioners have a different set of measures than those for dentists; preventive medicine physicians and dental hygienists have their own unique sets of measures.

The next section of the PAR form is the **Facility Wide Measures** section, as depicted in Figure 292 below. The information entered into this section of the PAR depends on the measures being monitored over the period of evaluation or the standard measures used by the Service or facility for performing PARs. When PAR Evaluators first open the PAR, this screen contains no data. To add a measure, click **Add**.



Figure 292: Facility-Wide Measures Section of the PAR

A screen appears with a pick list of different types of measures to select, as depicted in Figure 293 below. For each type of measure selected, different data fields are enabled to collect the appropriate information for the measure.

As each measure is assessed, PAR Evaluators click **Save**. Multiple measures, as many as are appropriate to paint as complete a picture as possible of the Provider’s performance, may be assessed and entered in the **Facility Wide Measures** section of the PAR.

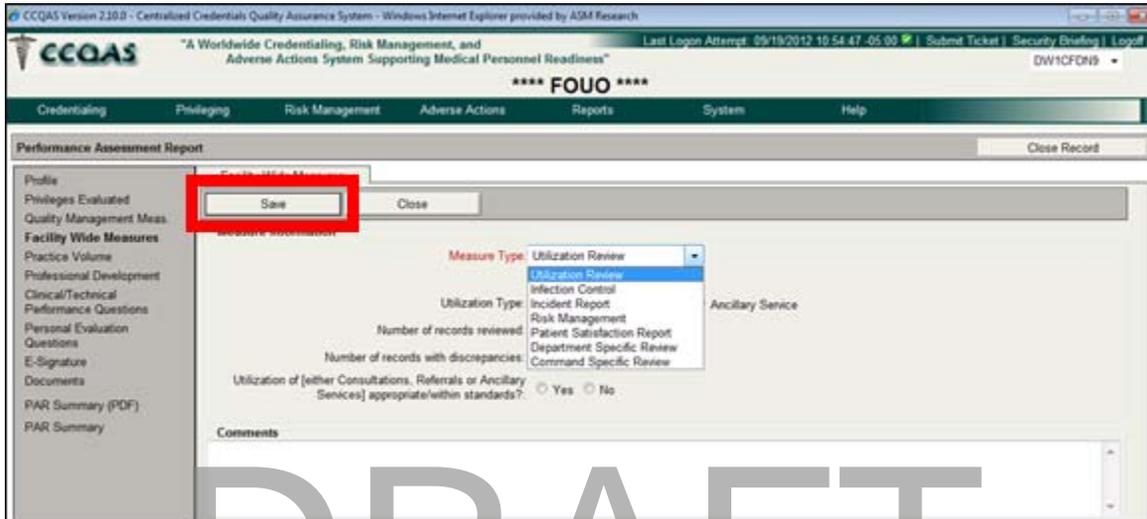


Figure 293: Types of Facility-Wide Measures

The next section of the PAR form is the **Practice Volume** section, as depicted in Figure 294 below. CCQAS automatically calculates the **Total Number of Procedures** and the **Total Number of Days Unavailable** as the PAR Evaluator enters data for the individual metrics.

As already mentioned above, **Practice Volume** metrics differ depending on Provider category. Physicians, allied health Providers, and nurse practitioners have a different set of measures from those for dentists, while preventive medicine physicians and dental hygienists have their own unique sets of measures.

The screenshot displays the 'Practice Volume' section of the PAR form within the CCQAS application. The interface includes a navigation menu with options like 'Credentiaing', 'Privileging', 'Risk Management', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area is titled 'Performance Assessment Report' and contains a 'Practice Volume' tab. A 'Save' button is located at the top of the form. The form is divided into several sections: 'Procedures', 'Monthly Data', 'Leave/Absence Data', and 'Comments'. Each section contains input fields for various metrics, such as 'Number of Diagnostic Procedures in Radiology', 'Average Monthly Admissions', and 'Total Number of Days Unavailable'. A large 'DRAFT' watermark is overlaid across the center of the form.

Figure 294: Practice Volume Section of the PAR

The next section of the PAR is the **Professional Development** section, as depicted in Figure 295 below. This section is pre-populated using data from the **Continuing Education** section of the Provider’s credentials record. The sum of credits accrued in each credit category is displayed for the PAR evaluation period and over the past three years. A summary of the associated continuing education courses is listed on the bottom half of the screen.

PAR Evaluators should enter the number of papers published, presentations given, etc., in the center of the screen, provide any pertinent supporting comments, and then click **Save**.

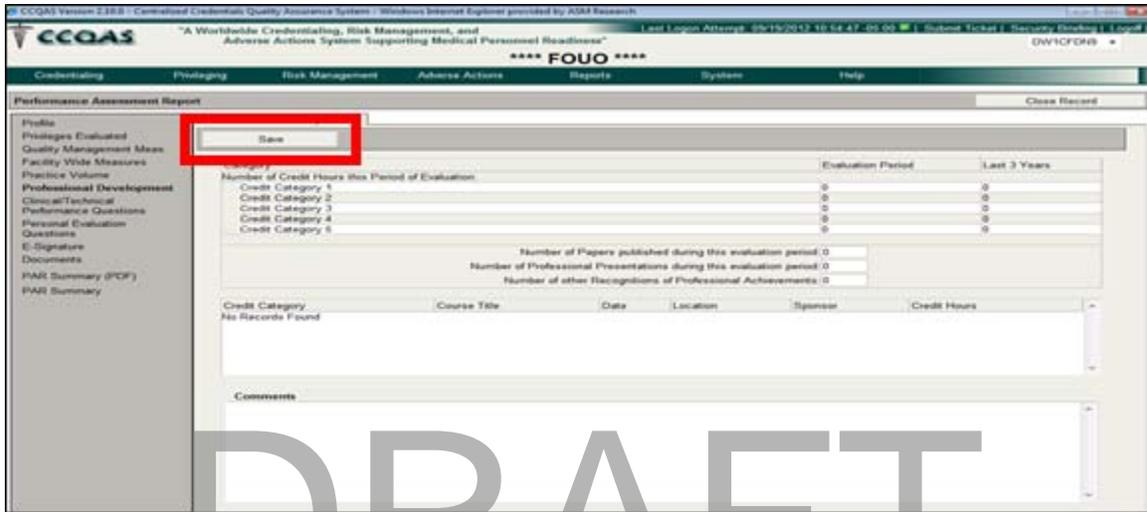


Figure 295: Professional Development Section of the PAR

The next section of the PAR form is the **Clinical/Technical Performance Questions** section, as depicted in Figure 296 below. If PAR Evaluators select “*Unsatisfactory*” for any of the questions, a comment is required to save the information entered on the screen. PAR Evaluators may also add a comment for any item by clicking the empty note icon (📄). After a comment is added, the empty note icon becomes a filled note icon (📄). After all items have been evaluated, click **Save**.

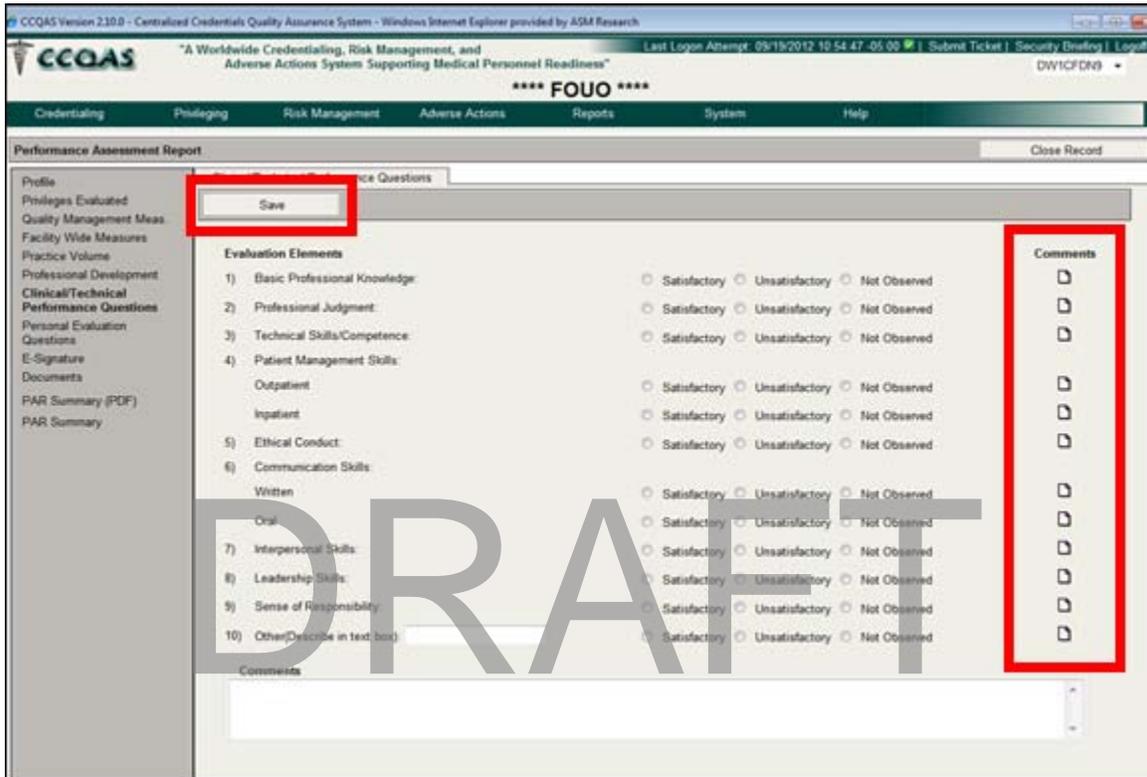


Figure 296: Clinical/Technical Performance Questions Section of the PAR

The next section of the PAR form is the **Personal Evaluation Questions** section, as depicted in Figure 297 below. If PAR Evaluators select “**No**” in answer to question #2, and “**Yes**” in answer to the other questions, a comment is required to save the information entered on the screen. PAR Evaluators may also add a comment for any response by clicking the empty note icon (📄). After a comment is added, the empty note icon becomes a filled note icon (📄). After all questions have been answered, click **Save**.

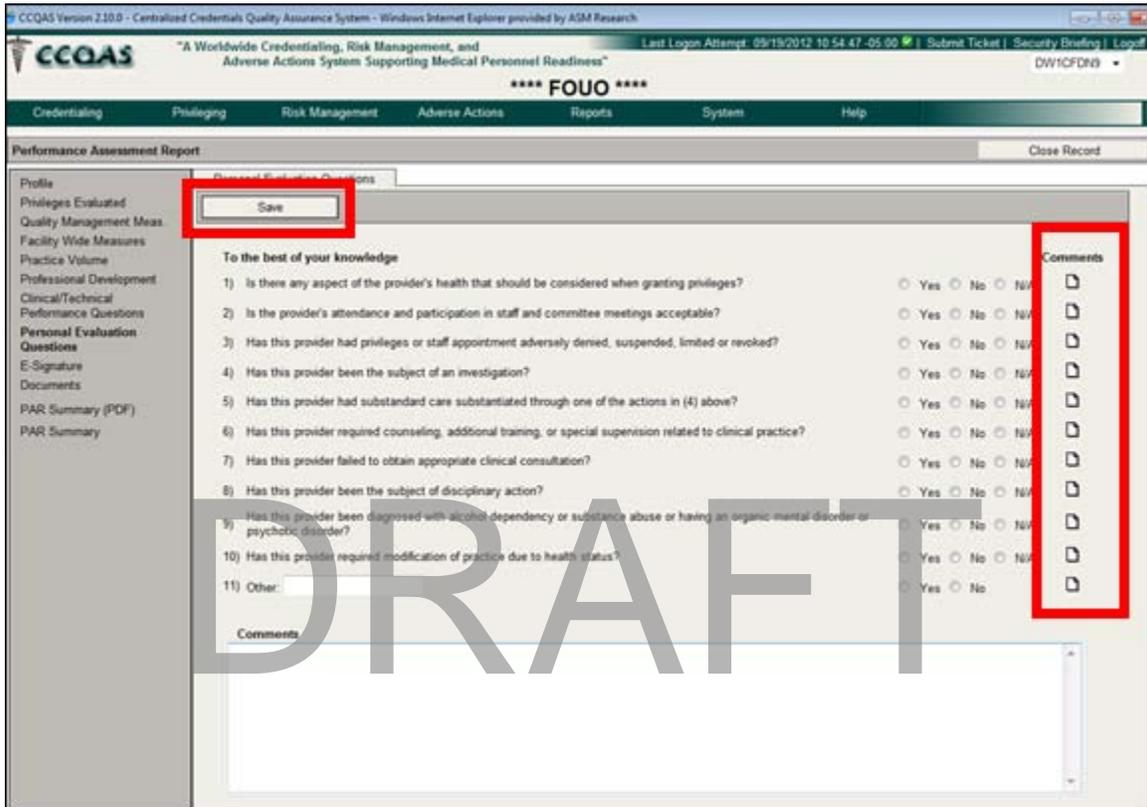


Figure 297: Personal Evaluation Questions Section of the PAR

At any time during the completion of the PAR, PAR Evaluators may review all information entered into the PAR form. The PAR form may be viewed by selecting **PAR Summary** from the navigation bar. When this option is selected, CCQAS returns a read-only version of the PAR form, as depicted in Figure 298 below, which contains all information that was entered to date by the PAR Evaluator.

CCQAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Login Attempt: 09/19/2012 10:54:47 -05:00 | Submit Ticket | Security Briefing | Logout | DW1CFD98

**** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Performance Assessment Report Close Record

PERFORMANCE ASSESSMENT REPORT

Profile
Privileges Evaluated
Quality Management Meas.
Facility Wide Measures
Practice Volume
Professional Development
Clinical/Technical
Performance Questions
Personal Evaluation
Questions
E-Signature
Documents
PAR Summary (PDF)
PAR Summary ←

SECTION I - PROFILE

NAME (Last, First MI)	RANK/GRADE	NPI
Anderson, Barney	Maj Gen	N/A
POSITION	SPECIALTY	DEPT/SERVICE
Physician	Medical Commander - Medical	Allergy and Immunology
REPORTING ACTIVITY/FACILITY		
DW1CFD98, 0007 MEDICAL GROUP @		
PURPOSE OF EVALUATION	PERIOD OF EVALUATION	
Notification/Augmentation of Privileges	09/14/2012 to 09/13/2014	
Comments		
SECTION II - PRIVILEGES BEING EVALUATED		
Version 1.0		
Physicians requesting privileges in this subspecialty must also request privileges in their primary discipline		
Scope		
PRIVILEGE ITEM (S)	REQUESTED	APPROVED
The scope of privileges in Allergy and Immunology includes the evaluation, diagnosis, consultation, management, and provision of therapy and treatment for patients presenting with hypersensitivity and immunologic conditions or disorders. This scope also includes the consultation, management, education, and provision of therapy and treatment for patients presenting for immunization healthcare including routine prevention, travel, education, military readiness and adverse events. Physicians may admit and may provide care to patients in the intensive care setting in accordance with MTF policies.	Fully Competent	Fully Competent
nc		
PRIVILEGE ITEM (S)	REQUESTED	APPROVED

Figure 298: PAR Summary Form

The same form may be generated as a read-only portable document format (PDF) file by selecting **PAR Summary (PDF)**. The PDF file may be printed or electronically downloaded to the user's computer hard drive or some other memory device.

PAR Evaluators click the **E-Signature** section of the PAR to open the **E-signature** tab after all other sections have been completed and reviewed, as depicted in Figure 299 below. PAR Evaluators then enter an overall assessment of the Provider's performance, add any supporting comments, and then click **Submit** to complete the **PAR** task.

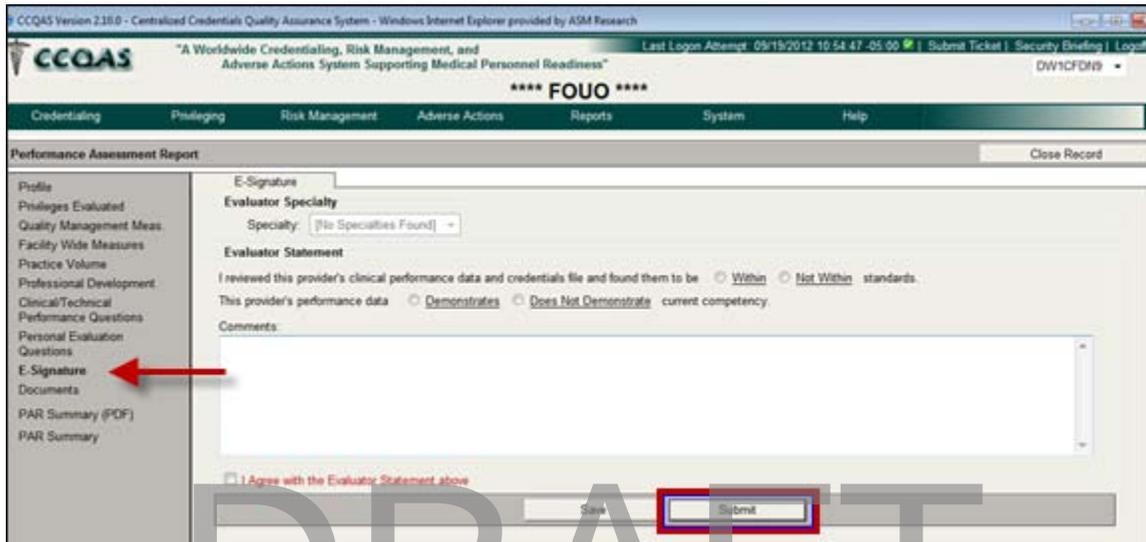


Figure 299: E-Signature Section of the PAR

A confirmation screen appears, as depicted in Figure 300 below. PAR Evaluators must ensure that all sections of the PAR have been reviewed. When PAR Evaluators click **OK**, the screen refreshes to display the work list. The **Complete PAR** task closes. After PAR Evaluators complete the PAR, CCQAS sends email notifications to the PAR Reviewers (if any were assigned) and the Provider, indicating the presence of a new task in their work list.

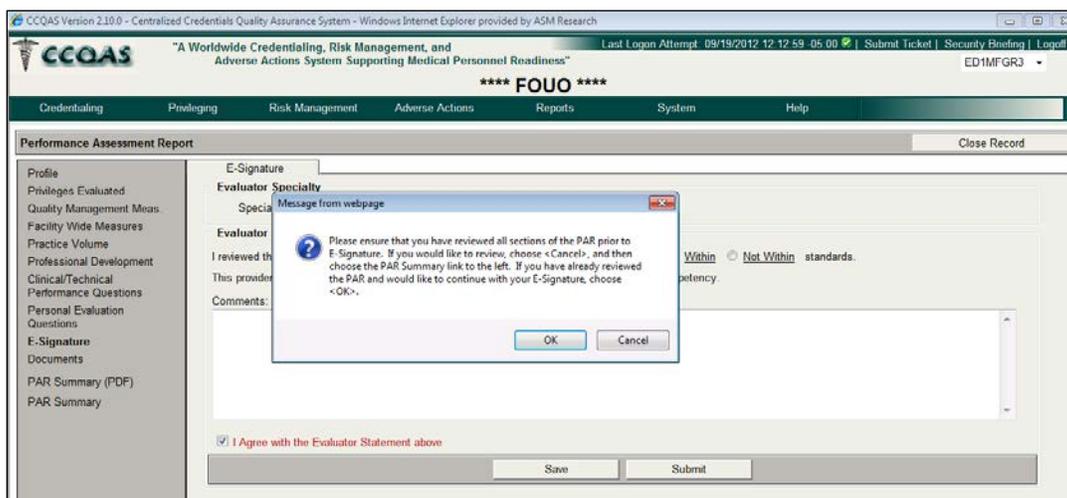


Figure 300: E-Signature Confirmation Screen

After the PAR has been submitted, CCQAS allows CC/MSSP/CMs to proceed with routing the Renewal or PCS application for review and approval. Neither the assigned PAR Reviewers nor the Provider need to review the PAR to route a Renewal or PCS privilege application.

11.5 Reviewing the PAR-The PAR Reviewer Role

After PAR Evaluators submit a completed PAR, each assigned PAR Reviewer receives a new work list item with “Task = *Review PAR*”, as depicted in Figure 301 below.

Note: The Provider and any PAR Reviewer(s) who were assigned by the CC/MSSP/CM during the routing of the PAR receive their *Review PAR* tasks simultaneously.

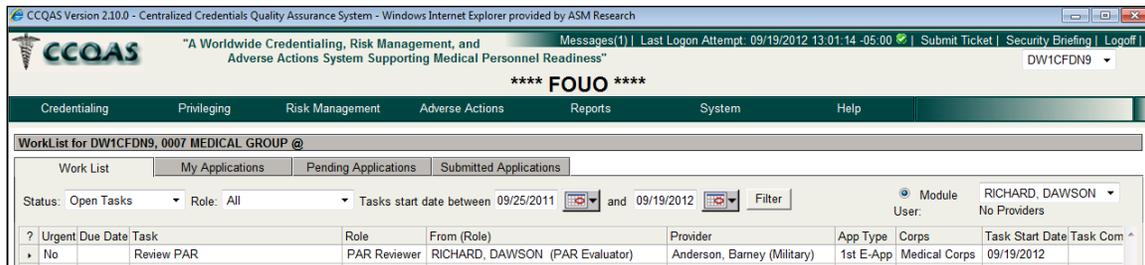


Figure 301: PAR Reviewer Work List Task – Review PAR

When PAR Reviewers open the *Review PAR* task, the PAR displays in read-only format. PAR Reviewers may review the **PAR** section by section or by using one of the **PAR Summary** options, but they may not edit any of the PAR content. When their review is complete, PAR Reviewers select the **E-Signature** section, as depicted in Figure 302 below.

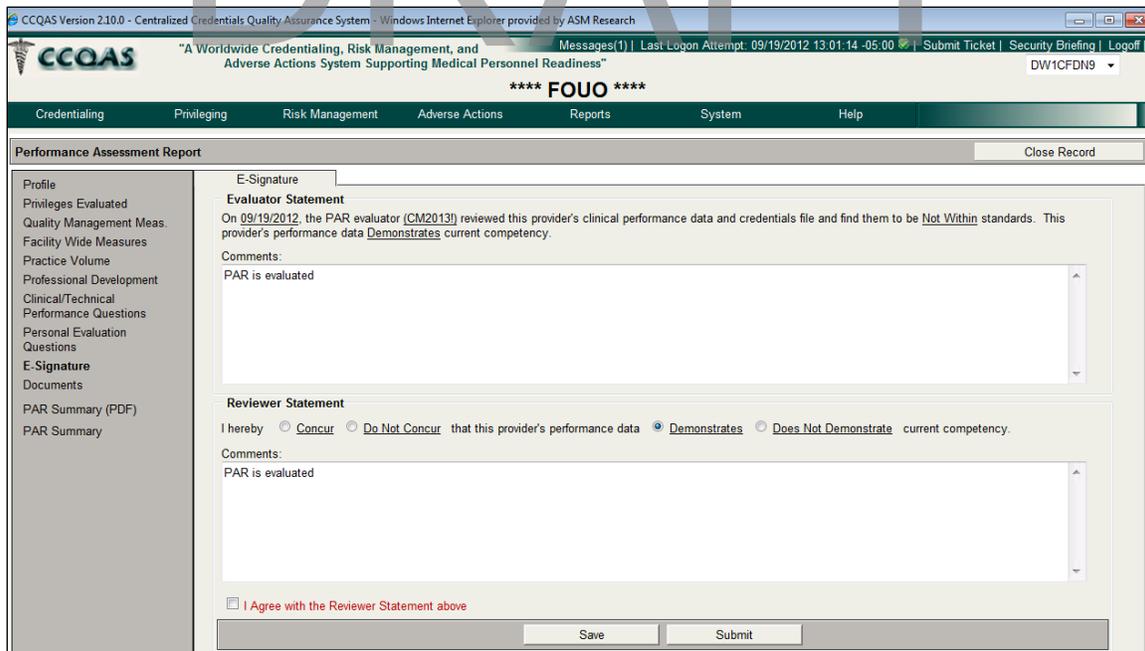


Figure 302: PAR Reviewer E-Signature Screen

On the **E-Signature** screen, the overall evaluation and comments rendered by the PAR Evaluator are presented. The Reviewer enters his or her assessment of the PAR and optional comments in a second **Comments** box, and then clicks **Submit** to enter his or her concurrence or non-concurrence with the PAR. After the Reviewer E-signs the PAR form, the screen refreshes to display the work list. The **Review PAR** task then closes. The Reviewer's concurrence with the PAR is not required for a Renewal or PCS application to be routed for review and approval.

11.6 Reviewing the PAR-The Provider Role

After PAR Evaluators submit a completed PAR, the Provider receives a new work list item with "Task = *Review PAR*", as depicted in Figure 303 below.

Note: A Provider and any PAR Reviewer(s) who were assigned by the CC/MSSP/CM during the routing of the PAR receive their **Review PAR** tasks simultaneously.

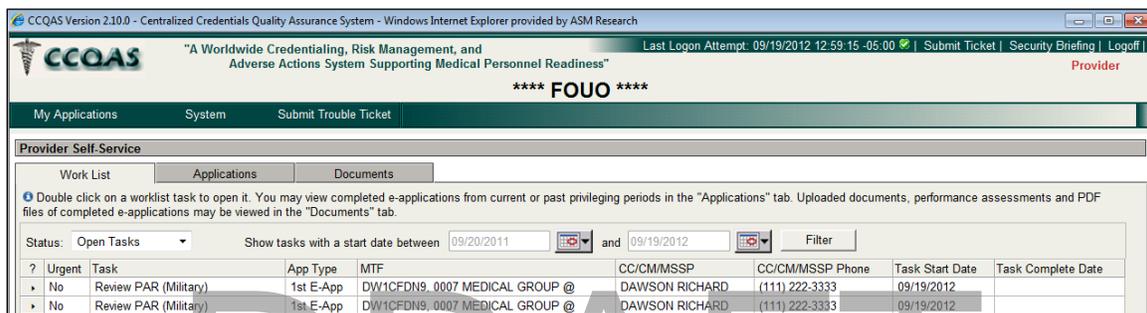


Figure 303: Provider Work List Task – Review PAR

When Providers open the **Review PAR** task, the PAR displays in read-only format. Providers may review the **PAR** section by section or by using one of the **PAR Summary** options, but they may not edit any of the PAR content. When the review is complete, PAR Reviewers select the **E-Signature** section, as depicted in Figure 304 below.

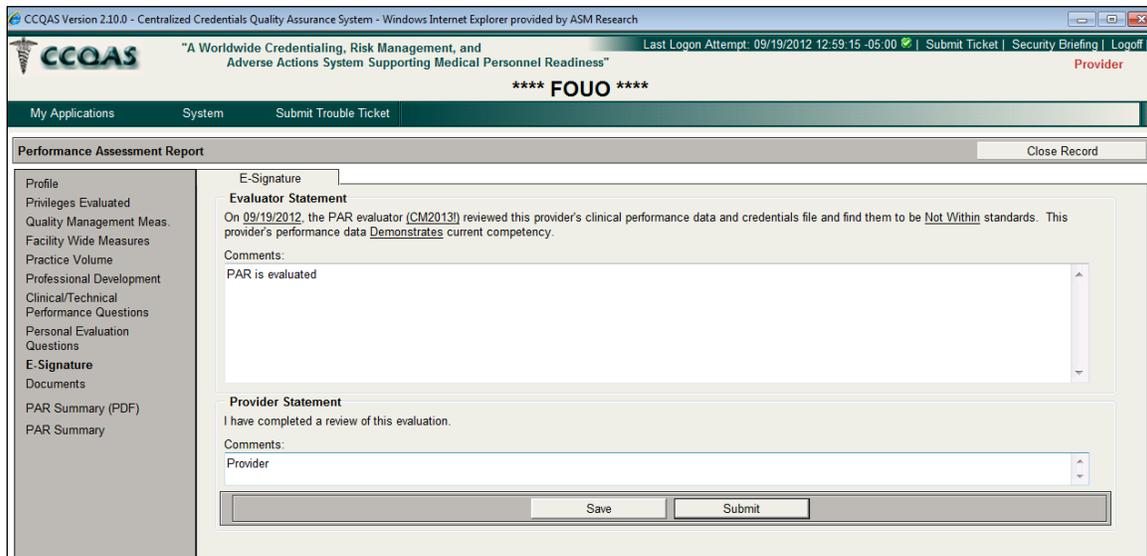


Figure 304: Provider E-Signature Screen

On the **E-Signature** screen, the overall evaluation and comments rendered by the PAR Evaluator and PAR Reviewer (if one was assigned) are presented. Providers may enter optional comments in a second **Comments** box, and then click **Submit** to acknowledge that they have reviewed the PAR. After Providers E-sign the PAR form, the screen refreshes to display the work list. The **Review PAR** task then closes. A Provider’s acknowledgement of the PAR is not required in order for a Renewal or PCS application to be routed for review and approval.

11.7 Bypassing the Automated PAR Process

If it is determined that an offline, paper PAR process should be performed in lieu of the electronic PAR, CC/MSSP/CMs should select the radio button corresponding to **“Offline PAR”** on the top portion of the PAR Routing screen, as depicted in Figure 305 below, and then click **Submit**. [RJ2]

The screenshot shows the CCQAS PAR Routing screen. The header includes the CCQAS logo and navigation links: Messages(1), Last Logon Attempt: 09/18/2012 13:17:11 -05:00, Submit Ticket, Security Briefing, Logoff. The main content area displays provider information for BOARD, Jeff (SSN: 091320127, Rank/Grade: General, Privileges Effective: 9/17/2012). The 'Type' section shows 'Electronic PAR' and 'Offline PAR' radio buttons, with 'Offline PAR' selected. The 'Purpose of Evaluation' is set to 'Modification/Augmentation of Privileges'. The 'Period of Evaluation' is from 09/17/2012 to 09/16/2014. The 'Dermatology' specialty is listed at the bottom.

Figure 305: ‘Offline PAR’ Radio Button

CCQAS sends PAR Evaluators an email message that they have a PAR to complete, and a new task, **“Task = Complete Offline PAR”**, is also be added to the evaluator’s work list, as depicted in Figure 306 below.

The screenshot shows the CCQAS WorkList for WZDHAA, Walter Reed National Military Medical Center. The 'Status' is set to 'Completed Tasks'. The 'Role' is 'All'. The 'Tasks start date between' is from 09/25/2011 to 09/19/2012. The 'User' is CC2007, CC2007 NC. The 'Provider' is BOARD, Jeff (Military). The table below shows a task to complete an offline PAR.

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date
No		Complete Offline PAR	PAR Evaluator	Campbell, Jeffrey (CC/CM/MSSP)	BOARD, Jeff (Military)	1st E-App	Medical Corps	09/19/2012	09/19/2012

Figure 306: Evaluator Work List Task – Complete Offline PAR

When PAR Evaluators open the **Complete Offline PAR** task, the **Offline PAR Notification** screen opens, as depicted in Figure 307 below. The **Offline PAR Notification** screen includes the information about the Provider, PAR duty location, and time period for the PAR. PAR Evaluators can print the information by selecting **Print**, close the screen and return to the work list by clicking **Cancel**, or acknowledge receipt of the notification by clicking **Acknowledge PAR Requirement**. After the notification is acknowledged, PAR Evaluators should proceed with completion of the offline PAR.



Figure 307: Offline PAR Notification

Electing to perform an offline PAR does not remove the requirement for a PAR to be completed prior to processing a Renewal or Transfer (i.e., PCS) application in CCQAS. However, since an “Offline PAR” means a paper report, CC/MSSP/CMs must ensure that before routing a renewal or PCS privilege application, the paper PAR is completed and available to the Reviewers by scanning and uploading it into the Provider’s privilege application. The offline PAR should be uploaded as a “Provider Document” as **Type = Clinical Performance Evaluation/Performance Assessment Reports**. Individuals wishing to view the paper-based PAR may then access it via the **Provider Documents** screen, rather than the **PAR/Snapshots** screen in the **Documents** sections of the E-application.

11.8 Cancelling the Setup PAR Task

If it is determined that a PAR is not required or a PAR cannot be completed, CC/MSSP/CMs may cancel the **PAR** task by clicking **Cancel PAR** at the bottom of the **PAR Routing** screen, as depicted in Figure 308 below.



Figure 308: ‘Cancel PAR’ Button

This action closes the **Setup PAR** task in the CC/MSSP/CM's work list, and removes the system requirement to have the PAR completed and submitted prior to the routing of a renewal or PCS application. If it is later decided that a PAR is required, CC/MSSP/CMs may initiate the **PAR** task manually, as described in [Section 11.2](#). If a PAR has already been routed and it is decided that the completion of the PAR is no longer needed, the PAR process must be terminated (refer to Section 11.9 below)

11.9 Terminating or Reassigning a PAR In-Process

Occasions may arise when a PAR needs to be reassigned or terminated after the task has already been assigned to a PAR Evaluator, particularly in situations when the assigned PAR Reviewer is no longer available to complete the **PAR** task. CCQAS allows CC/MSSP/CMs to reassign or terminate a **PAR** task that has already been initiated, as long as the task is still active in the PAR Evaluator's work list.

In order to reassign or terminate an in-process PAR, CC/MSSP/CMs must access the assigned PAR Evaluator's work list by selecting his or her name from the **User** list in the upper right-hand corner of the work list screen. On the PAR Evaluator's work list, CC/MSSP/CMs select **Cancel PAR** from the hidden menu of items for the **Complete PAR** task, as depicted in Figure 309 below.

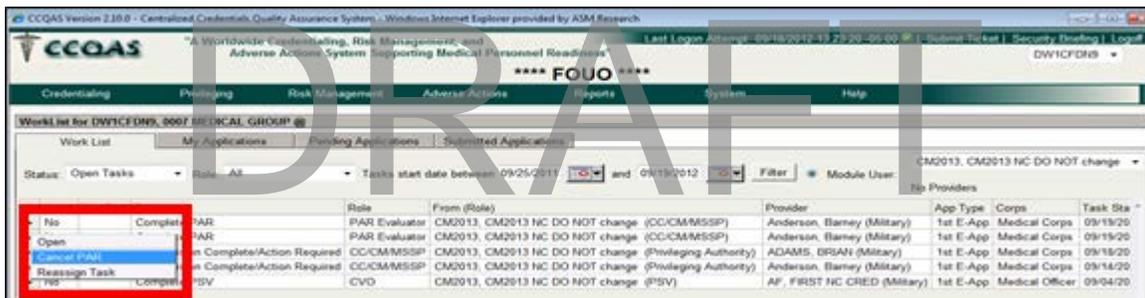


Figure 309: Complete PAR Task Menu Options

A warning message displays, asking CC/MSSP/CMs to confirm their intent to cancel the PAR, as depicted in Figure 310 below.

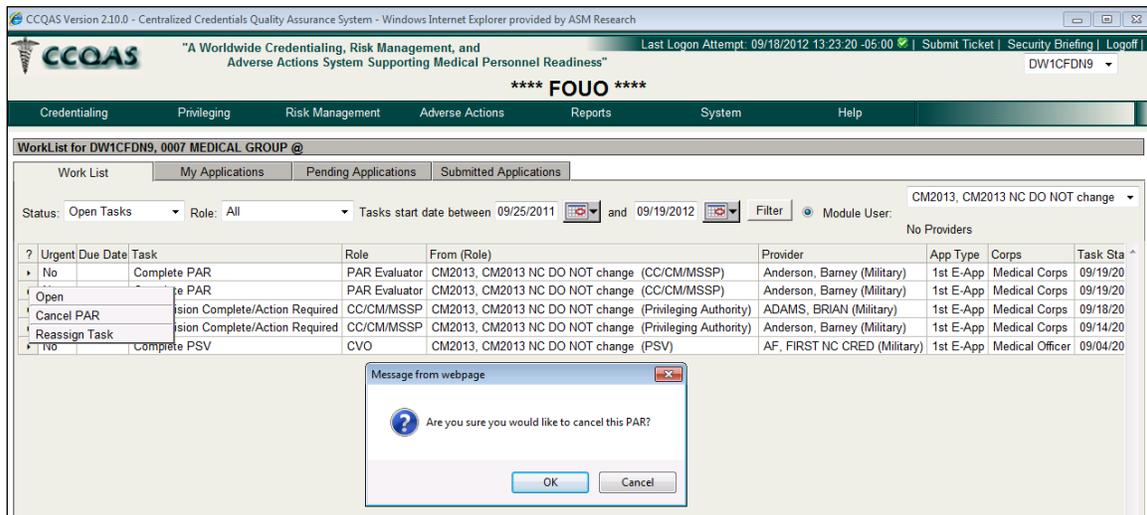


Figure 310: Cancel PAR Warning Message

When CC/MSSP/CMs click **OK**, the **PAR** task is terminated. If the **PAR** task should be assigned to a new PAR Evaluator, CC/MSSP/CMs select **Reassign Task** from the hidden menu of options, as depicted in Figure 309 above. The **Re-assign Task** window opens, as depicted in Figure 311 below.

When CC/MSSP/CMs select a new PAR Evaluator from the pick list and click **Submit**, the **Complete PAR** task is removed from the old PAR Evaluator's work list and added to the new PAR Evaluator's work list.

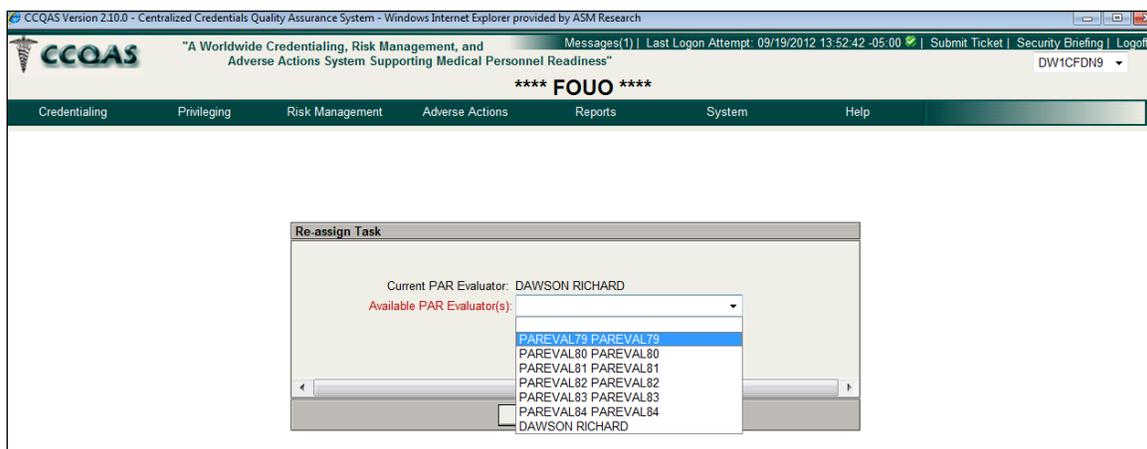


Figure 311: Re-assign Task Window

Only CC/MSSP/CMs may cancel a **PAR** task that has already been assigned to a PAR Evaluator. The **Cancel PAR** and **Reassign Task** menu options are not available in the PAR Evaluator's work list.

12 Generating Credentialing and Privileging Letters

Credentialing staff are frequently required to generate written letters for the purpose of communicating with a variety of entities both inside and outside the DoD. CCQAS supports the automated generation of a number of standard letters by which information is drawn from Providers' electronic credentials files and other locations in the CCQAS database to create a pre-formatted, pre-populated letter that may then be printed or saved for editing by users. CCQAS may generate letters in several different ways and for individual Providers or groups of Providers in batch mode.

Proper use of this functionality, however, requires that the information in both the electronic credentials file and the **Command Parameters** screens in the CCQAS application be accurate and up-to-date.

12.1 Command Information for Letter Generation

The **Command Parameters** screen must contain complete and accurate information about the command that is responsible for Provider credentialing and privileging actions so that users realize the benefits of automated letter generation in CCQAS. The **Command Parameters** screen may be accessed by clicking **System** on the main menu, then and selecting **Command Parameters**, as depicted in Figure 312 below.

Note: If the **Command Parameters** feature is not an available item from this menu, users have not been granted the permissions necessary to edit command information for their facility or unit, and should contact the CCQAS Administrator for further assistance.

?	Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
▶	ADAMS, BRIAN	091-82-0121	DW1CFDN9	09/18/2012	F11	MC	Dual	Active		2
▶	AF_TERM_REC	083-92-0121	DW1CFDN9	08/29/2012	C11	MO	MIL	Active		1
▶	AF_NC INC NPI	090-72-0121	DW1CFDN9	09/07/2012			MIL	Active		1
▶	Anderson, Barn	082-92-0123	DW1CFDN9	08/29/2012	F11	MC	MIL	Active		1
▶	Brooks, Tom	092-02-0121	W2DHAA	09/20/2012	A13	MC	Dual	Active		2
▶	FORD, JOE	291-42-0121	DW1CFDN9	09/14/2012			MIL	Active		1

Figure 312: Command Parameters Menu Item

CCQAS pulls information from the **Command Parameters** screen to populate the body and signature line of the letters that are generated, as depicted in Figure 313 below.

CCQAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness"

Last Logon Attempt: 09/25/2012 12:33:59 -05:00 | Submit Ticket | Security Briefing | Logout | DW1CFDN9

**** FOUO ****

Credentialing Privileging Risk Management Adverse Actions Reports System Help

Command Parameters
Local MTF: 0007 MEDICAL GROUP @

Credentials Signature Authority
Command: MEDICAL GROUP
Location: TEXAS
Office: Professional Group
Name: Renee Marie Hutchison
Position: Credentials Coordinator
Phone: (916) 465-1232

Risk Management Signature Authority
Command: MEDICAL GROUP
Location: TEXAS
Office: Professional Group
Name: Renee Marie Hutchison
Position: Risk Management Coordinator
Phone: (916) 465-1300

POC for FCOMS/ECONS
Name: Barbara Green
Phone: (916) 465-1200

Certification Authority
Official: COL
Title: Commander

Privileging
Privileging Module Activated: Yes
Privileging Authority UIC: DW1CFDN9
Active Renewal Notice Days: 30
Reserve/Guard Renewal Notice Days: 30

Authority Address
Address 1: 2020 Main Street
Address 2:
City: Fairfax
State: CA Zip: Country: United States

Credentials
Exp. Credentials 1st Notice Days: 0
Exp. Credentials 2nd Notice Days: 0

Points of Contact
First: Renee Marie Hutchison
Second: Barbara Green
Third: Lisa Gibson

Save Close

**** FOUO ****

Figure 313: Command Parameters Screen

Users may then add or edit command and contact information according to the following guidelines:

- The **Credentials Signature Authority**, **Risk Management Signature Authority**, and **Certification Authority** are the authorities who are authorized to sign letters having to do with function
- The **Position** of individuals pertains to the function they perform with that Authority, not military rank
- The **Phone** field should include any area codes and special prefixes that are necessary for individuals in another location to contact the POC. Telephone numbers should be grouped by periods or spaces (e.g., 202.767.4144)
- The **Certifying Authority Official** should contain the name of the individual under whose authority the Certification would be signed
- The **Privileging Authority UIC** is automatically filled in with the UIC for the MTF, but may be edited if appropriate
- The **Authority Address** should be the mailing address for the office

- The **Points of Contact** should be the names of individuals who should be contacted for more information

All updated command information will be available after users click **Save**, and then click **Close** to return to the **Credentials Provider Search** screen.

12.2 Generating Letters for Individual Providers

This section describes the process of generating letters for individual providers.

12.2.1 Generating a Letter from Letters Menu

Users may access letters either from the Provider search or work history. Letters may be generated for an individual Provider by searching for the Provider's record and selecting **Letters** from the menu of available Provider actions on the **Search Results** screen, as depicted in Figure 314 below.

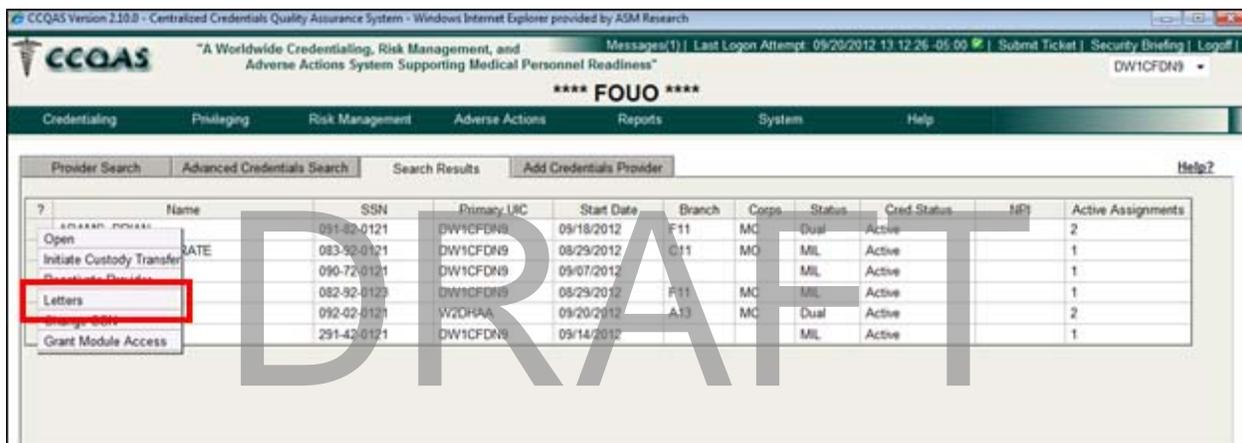


Figure 314: Letters Menu Item Provider Search

Users may then view the complete list of letters, as depicted in Figure 315 below.

Generate Letter - ADAMS, BRIAN (DW1CFDN9)	
DEA / DoD Provider Multi-Purpose Administration Form	
Consent and Release	
Staff Appointment Notification	
Staff Appointment Renewal	
Expiring Credentials	
Status Sheet (Snapshot)	
Pre-Populated Privileging Application (off-line privileging event)	
ICTB	
Cancel	

Figure 315: List of Provider Letters

Staff Appointment Notification Letter, Staff Appointment Renewal Letter, Expiring Credentials Letter, ICTB Letter, and Status Sheet (Snapshot) Letter contain assignment-specific information and must be generated from the work history section by selecting the appropriate assignment. If users have access to these letters from the Provider search, they are notified about assignment-specific information associated with these letters, and the system prompts them if they want to be transferred to the work history. Figure 316 below depicts the **Work History Letters** menu.

CCQAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research

***** FOUO *****

Provider: BRIAN ADAMS, Branch: F11, Rank: COL, Corps: MC, AOC/Design/AFSC: 44A1

Work History Letters Menu:

- Open
- Initiate PCS
- Initiate ICTB
- End Assignment
- Cancel Assignment
- Letters
- Initiate Application
- Reactivate Privileges

Figure 316: Work History Letters Menu

Users may run the desired letter by clicking the report name. Most letters are automatically generated after they are selected, and then pre-populated with data from the Provider’s current credentials record.

The Drug Enforcement Administration (DEA)/ DoD Multi-purpose Administration Form consist of a set of 3 letters, as depicted in Figure 317 below. Select the **Initial Application** letter from the drop-down menu.

The screenshot shows a window titled "Generate DEA Letter - ADAMS, BRIAN (DW1CFDN9)". Below the title bar, the text "Select section of the DEA Multi-purpose form to populate:" is displayed. A dropdown menu is open, showing three options: "Initial Application" (highlighted in blue), "Notification of Change of Station", and "Return of Military DEA Registration Certificate".

Figure 317: DEA Multi-Purpose Letters

The **Letter Initiation** screen appears, as depicted in Figure 318 below. Select the radio button next to the appropriate license, and then click **Submit**.

The screenshot shows the same window as Figure 317, but now the dropdown menu is set to "Initial Application". Below the dropdown is a table with the following data:

	State	License Number	Expiration Date	Status
<input checked="" type="radio"/>	AK	1343 AF	09/18/2011	Active
<input type="radio"/>	AK	army 13	07/15/2012	Active

Below the table are two buttons: "Submit" and "Cancel". The "Submit" button is highlighted with a red box.

Figure 318: DEA Initial Application Form State Selection

The **Initial Application Letter** result screen appears, as depicted in Figure 319 below. Notice that the top section of the letter is now populated with the user's information.

DoD Provider Administration Form - Windows Internet Explorer provided by ASM Research

Print Close Save Electronic Copy

**** For Official Use Only (FOUO) ****

Drug Enforcement Administration (DEA) Registration Number
DoD Provider Multi-purpose Administrative Form

(X) Statement of Understanding **(Required for New Applications Only)**

I understand that the DEA number assigned to me is to be used only for official duty in the care of DoD beneficiaries and may not be used for any other category of patients, except as allowed by official military duties. I understand that the number will be used for prescribing and administering only and cannot be used for purchasing or storing of controlled substances. I understand that the DEA number will be voluntarily surrendered upon separation from military service and a separate DEA number is required for work outside of official military duty.

Applicant Name: BRIAN ADAMS RANK/SERIES _____
Unit/Facility: 0007 MEDICAL GROUP
Unit Address: 7 MDG 697 Louisiana Drive DYESS AFB TX 79607-1367
Social Security Number: XXX-XX-0121
Medical/Dental License Number: 1343 AF State of: AK Expiration Date: 09/18/2015

Applicant Signature: _____
Credentiaing Authority Signature: _____ Date: _____
Name: Ms. Renee Marie Hutchison (SGQ)
Title: Credentials Authority
Address: 2020 Mail Street
Fairfax, CA
Phone Number (Commercial): (325) 696-4262

Figure 319: Initial Application Letter Result

Before a **Notification of Change of Station** letter can be generated, users must select the **Notification of Change of Station** letter from the **Generate DEA Letter** drop-down menu (refer to Figure 317 above), and then select the radio button next to the appropriate DEA information, as depicted in Figure 320 below.

Generate DEA Letter - ADAMS, BRIAN (DW1CFDN9)

Select section of the DEA Multi-purpose form to populate:

Notification of Change of Station

To Command: _____

	DEA Number	DEA Type	Expiration Date
<input checked="" type="radio"/>	234	DEA (Fee Exempt)	10/06/2012

Submit Cancel

Figure 320: Notification of Change of Station

Before a **Return of Military DEA Registration Certificate** letter can be generated, users must select the **Return of Military DEA Registration Certificate** letter from the **Generate DEA Letter** drop-down menu (refer to Figure 317 above). Users then select the radio button for the appropriate DEA information, depicted in Figure 321 below, and then click **Submit**.

Generate DEA Letter - ADAMS, BRIAN (DW1CFDN9)

Select section of the DEA Multi-purpose form to populate:

Return of Military DEA Registration Certificate ▾

	DEA Number	DEA Type	Expiration Date
<input checked="" type="radio"/>	234	DEA (Fee Exempt)	10/06/2012

Submit Cancel

Figure 321: Return of Military DEA Registration Certificate

When users select the **Expiring Credentials** letter from the list of Provider letters menu (refer to Figure 315 above), the **Generate Expiring Credentials Letter** screen appears, as depicted in Figure 322 below. Users select the appropriate items for the letter, and then click **Submit**.

Generate Expiring Credentials Letter - MRAZ, JASON L (DW1CFDN9)

Credentials that have or will expire within next 90 days. Filter

State License/Certification/Registration

	Type	State	Number	Field	Status	Expires	ADM Waiver
<input checked="" type="checkbox"/>	License	AK	56	Allopathic Physician	Active	10/06/2012	0

National Certification/Registration

	Type	Number	Field	Status	Expires
<input checked="" type="checkbox"/>	Certification	45	Allopathic Physician	Active	10/06/2012

Contingency Training

	Type	Expires
<input checked="" type="checkbox"/>	CTTC-Combat Treatment Training Course	08/26/2012

Submit Cancel

Figure 322: Expired Credentials Letters Selections

Since the **Pre-Populated Privileging Application** letter has assignment-specific information, as mentioned above, the system prompts users about being transferred to the work history, where they can select the assignment from which the letter can be generated. Figure 323 below depicts the pre-populated privileging letter transfer message. Click **OK** to open the **Work History** screen.

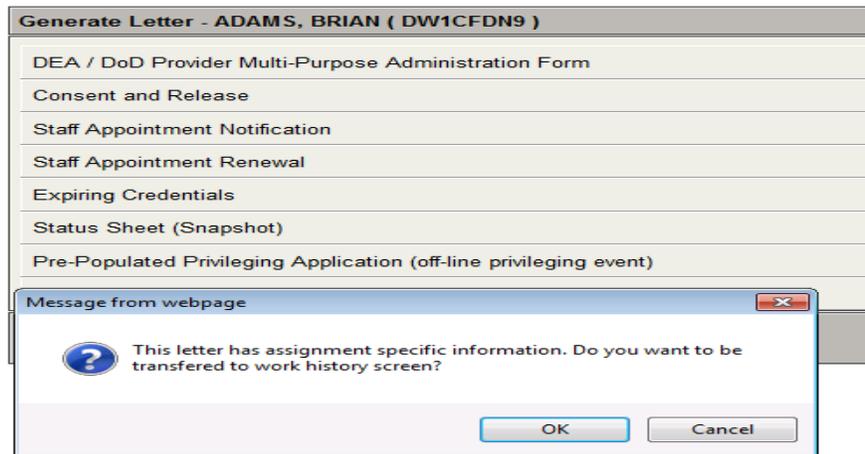


Figure 323: Pre-Populated Privileging Letter Transfer Message

When users select a specific assignment and **Pre-Populated Privileging Application** letter, a list of privileges displays, as depicted in Figure 324 below. Users select a desired privilege category, and then click **Submit** to generate the blank letter.

Figure 324: Pre-Populated Privileging Letter with listed Categories

After the selected letter has been generated, the following actions may be taken by clicking one of the buttons at the top of the screen:

- The **Print** button allows users to print the letter directly from the CCQAS application (refer to [Section 12.3](#)).
- The **Save** button allows users to save the report to their work station as a text file or PDF.
- The **Close** button closes the letter report generator and returns users to the list of letters.

ICTB letters require users to enter additional information prior to generating the letter. Users then enter the required information and select **Generate Letter**. A new browser window opens, displaying the selected letter.

12.2.2 Generating a Letter from Inside a Credentials Record or Privilege Application

Certain letters may be generated while a CC/MSSP/CM is actively working on a Provider's credentials file. These include a renewal letter, which may be run by clicking the **Renewal Letter** button in the **License/Certification/Registration** section. In addition to the letters described above to support the PSV process of an active privilege application, the **Verification References** letter is available from the hidden menu of actions for each reference record. The letter reflects the data included in a Provider's current privileging application, as depicted in Figure 325 below.

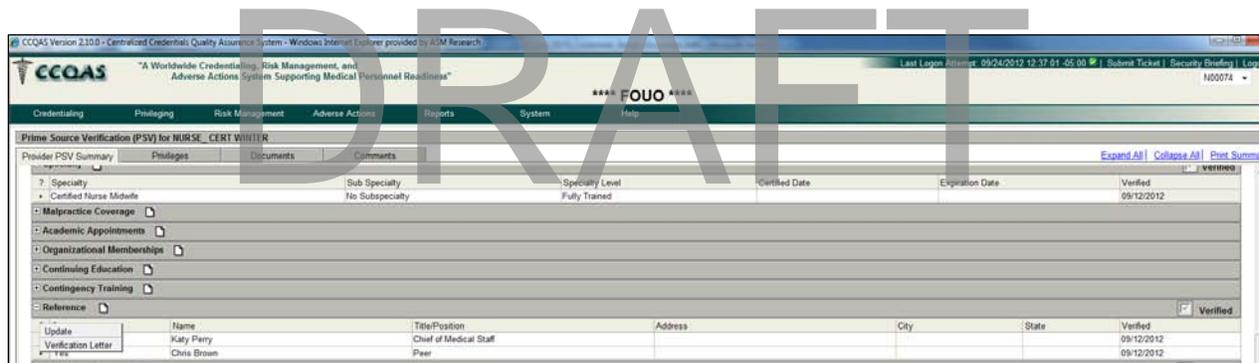


Figure 325: Verification Reference

12.3 Printing a Letter from CCQAS

Users may print a letter directly from the CCQAS application by clicking **Print** at the top of the report, as depicted in Figure 326 below. Since the letter is generated directly from the Internet, the upper or lower margins may contain the URL, date, page, and index information according to a user's browser settings. Alternatively, many users prefer to save the letter to a text file, which may then be opened in Microsoft® Word to format their letter prior to printing.

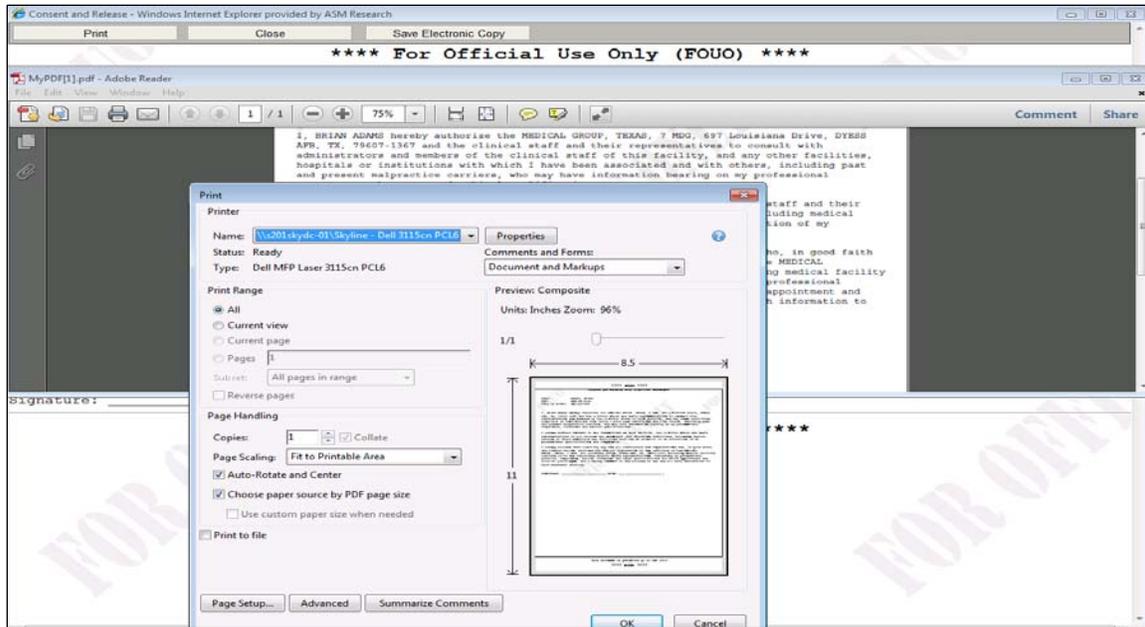


Figure 326: Letter Print

12.4 Exporting a Letter to Microsoft® Word

Users may edit a letter using Microsoft® Word and for manipulation by clicking **Save As**. After clicking this button, users must read and agree to a QA statement by clicking **OK**. The **Save HTML Document** screen then appears, as depicted in Figure 327 below.

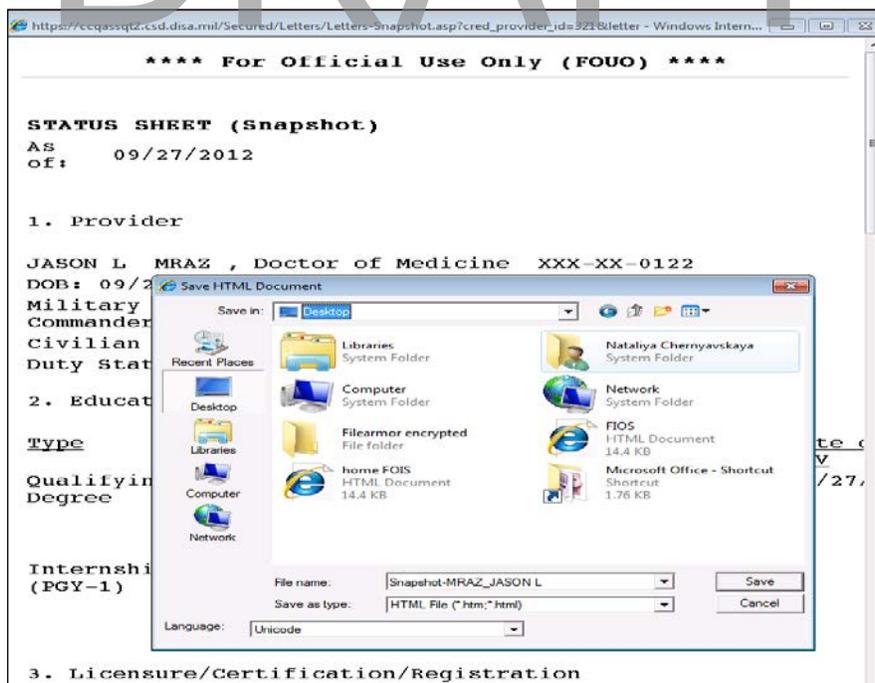


Figure 327: Exploring the Letter

The letter can be saved in PDF format when users click the **Save Electronic Copy** button at the top of the screen, as depicted in Figure 328 and Figure 329 below.

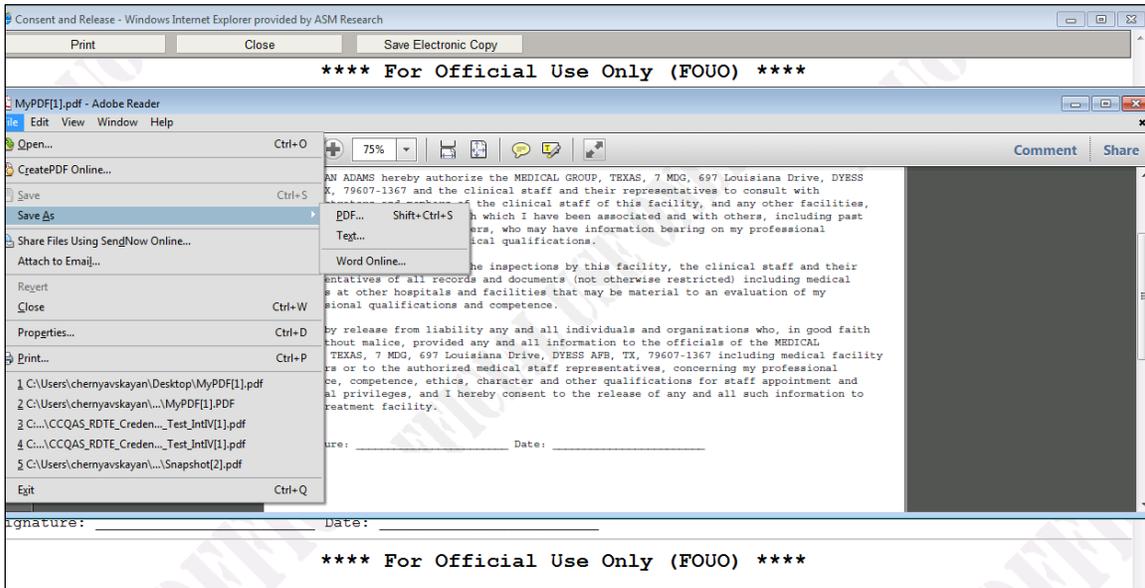


Figure 328: Save Electronic Copy

After clicking **Save**, users may now open the saved file and edit the file as appropriate.

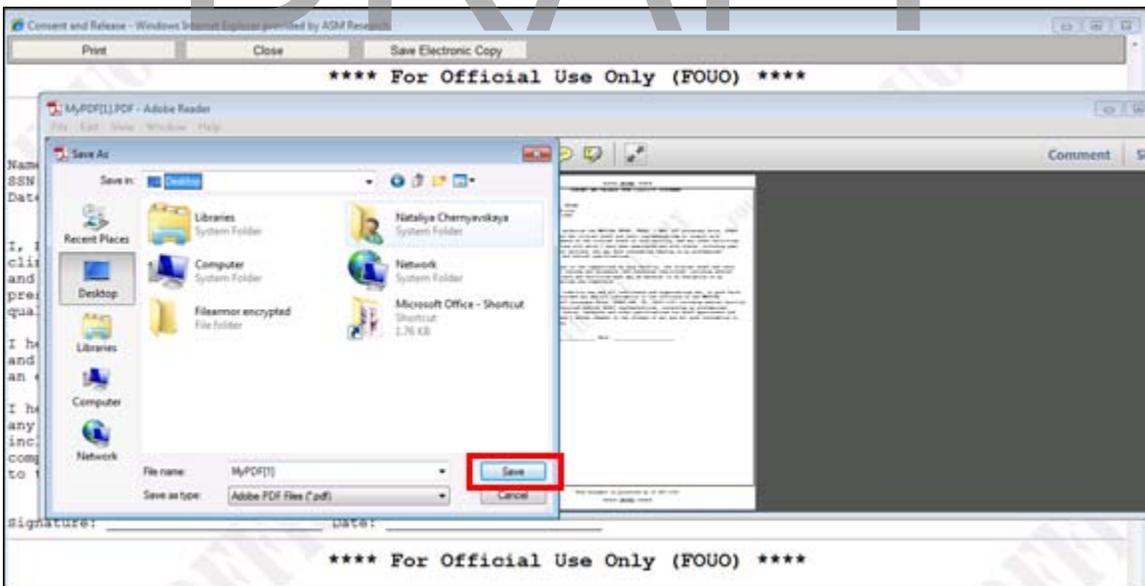


Figure 329: Save PDF Document

12.5 Generating Batch Letters

As noted in the previous section, letters may be simultaneously generated for multiple Providers in batch mode. Batch letter generation allows user to generate the same type of letter for a group of selected Providers. For example, a batch ICTB letter may be generated for all Providers that are being are ICTB'ed to the same location with the same start and end dates. If the ICTB location or ICTB dates differ for some Providers, the ICTB letters for those Providers should be generated individually.

All batch actions, including batch letters, are initiated from the **Credentials Provider Search** screen, as depicted in Figure 330 below. Provider records may be batch-processed by selecting the appropriate batch action in the **Action** section of the screen.

Additional search criteria may be entered in the upper portion of the **Credentials Provider Search** screen if users wish to limit the batch action to only certain groups of records (e.g., only Providers in a specific **Department, Work Center, Corps, or UIC**). After users enter all appropriate search criteria and select the desired batch action, they click **Search**.

The screenshot shows the 'Action' section of the 'Credentials Provider Search' screen. The interface includes a navigation menu with options like 'Credentialing', 'Privileging', 'Risk Management', 'Adverse Actions', 'Reports', 'System', and 'Help'. The 'Batch Processing' option is selected in the left-hand menu. The main area contains several search criteria fields: Branch (dropdown), Primary UIC (text), Department (text), Provider Type (dropdown), First Name (text), Corps (dropdown), Assignment UIC (text), Work Center (text), Civilian Role (dropdown), Other UIC (text), and File Manager (text). Below these fields is a 'Batch Job Type' section with two columns of radio buttons for selecting an action: Batch Training, Batch NCCPA, Batch Initiate PCS, Batch ICTB Letters, Batch Initiate ICTB, Batch Application Letters, Batch Cancel ICTB, and Provider Mailing Labels. At the bottom, there is a 'Record Count' field, 'Search', 'Clear Screen', and 'Close' buttons, and a 'Record Limit' set to 100. A large 'DRAFT' watermark is overlaid across the center of the screen.

Figure 330: Action Section of the Credentials Provider Search Screen

A list of Providers who meet the search criteria specified is displayed, as depicted in Figure 331 below. In the example below, a user is batch-generating ICTB letters. The user may check which Providers from the search list should be included in the batch, indicate whether the active duty or reserve letter ICTB is desired, then clicks **General Letters** at the bottom of the screen.

The screenshot shows the CCOAS Batch Processing Search screen. The browser title is "CCOAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research". The page header includes the CCOAS logo and the text "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". The user is logged in as "FOUO" with a session ID of "DW1CFDN9". The navigation menu includes "Credentialing", "Privileging", "Risk Management", "Adverse Actions", "Reports", "System", and "Help". The main content area is titled "Batch Processing Search" and "Batch Letters ICTB". It displays a table with the following columns: Name, SSN, UIC, Type, Brch, Crps, Start Date, and End Date. The table contains five rows of provider information, each with a checkbox in the first column. The providers are: ADAMS, BRIAN; AF, NC INC NPDB; AF, TERM, REGENERATE; Anderson, Barney; Brooks, Tom; and FORD, JOE. At the bottom of the screen, there is a "Record Count: 6" and a "Record Limit: 100". Buttons for "Generate Letters" and "Cancel" are visible at the bottom right.

	Name	SSN	UIC	Type	Brch	Crps	Start Date	End Date
<input type="checkbox"/>	ADAMS, BRIAN	091-62-0121	DW1CFDN9	CRED	F11	MC	09/18/2012	
<input type="checkbox"/>	AF, NC INC NPDB	090-72-0121	DW1CFDN9	CRED			09/07/2012	
<input type="checkbox"/>	AF, TERM, REGENERATE	083-92-0121	DW1CFDN9	CRED	C11	MO	08/29/2012	
<input checked="" type="checkbox"/>	Anderson, Barney	082-92-0123	DW1CFDN9	CRED	F11	MC	08/29/2012	
<input checked="" type="checkbox"/>	Brooks, Tom	092-02-0121	DW1CFDN9	CRED	A13	MC	09/20/2012	
<input checked="" type="checkbox"/>	FORD, JOE	291-42-0121	DW1CFDN9	CRED			09/14/2012	

Figure 331: Batch ICTB Letter Screen

On the next screen, depicted in Figure 332 below, users are prompted to enter information regarding the ICTB location and dates, and additional text for the ICTB letter. This screen may vary in content and appearance, depending on Service.

The screenshot shows the "Additional Information for ICTB Letter" screen. The browser title is "Additional Information for ICTB Letter - Windows Internet Explorer provided by ASM Research". The page is divided into several sections:

- ICTB Information:** Start Date: 09/25/2012, End Date: 09/26/2012, and an unchecked checkbox for "Evaluation (PAR/OER)".
- Provider Information:** Type of Duty: Active Duty Special Work (ADSW), Current PED: (empty), and ICTB Duty Status: Military (selected) and Civilian (unselected).
- Credential Signature Authority Information:** Credential Signature Authority / Name: Renee Marie Hutchison, Credential Signature Authority / Position: Credentials Coordinator, Credential Signature Authority / Command: MEDICAL GROUP, Credential Signature Authority / Location: TEXAS, and Credential Signature Authority / Phone: (916) 465-1232.
- Select the additional text for paragraph 13:** A list of options: "No additional information in Credentials File" (selected), "Additional license information in Credentials File", and "Additional information in Credentials File - Please Call".
- Additional comments for paragraph 14:** A radio button for "None" is selected.
- cc:** A text input field for additional recipients.

 At the bottom of the screen, there are buttons for "Generate Letter" and "Cancel".

Figure 332: Additional ICTB Information Screen

When users click **Generate Letter**, a sequential list of ICTB letters for each Provider included in the batch displays, as depicted in Figure 333 below. The letters may then be printed directly from the CCQAS application or saved. Other batch letters may be generated in a similar manner as the example below.

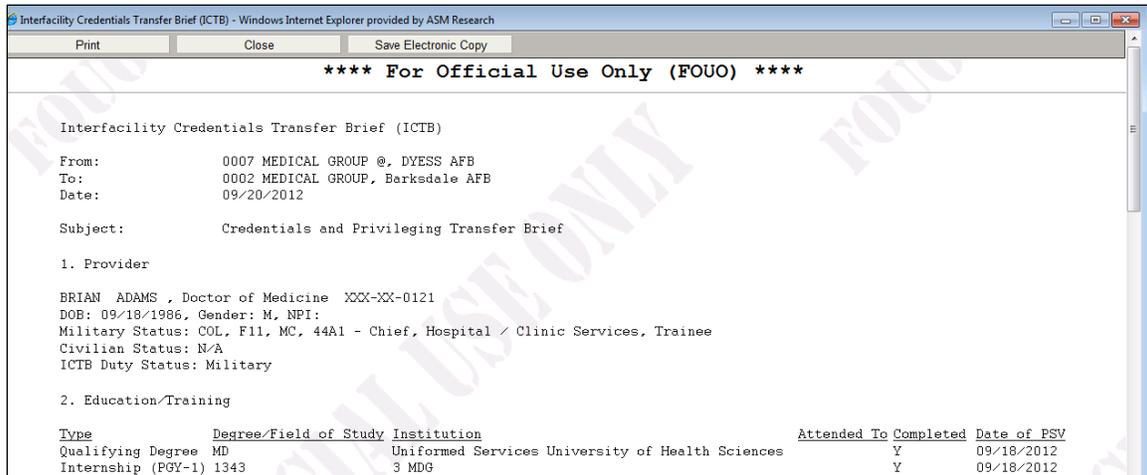


Figure 333: ICTB Batch Letter

13 Generating Standard Credentials and Privileging Reports

A number of standard credentialing and privileging reports are available from CCQAS. Although these reports enable some customization of report format and content, the query logic is hardcoded into CCQAS and cannot be changed by users. In several instances, the standard reports are built to address business questions that cannot be answered using the ad-hoc report tool, particularly in cases where Providers are missing critical credentialing information in their CCQAS record. As such, users are encouraged to use the standard reports whenever possible before trying an ad-hoc report to answer their business question.

13.1 Generating a Standard Credentials Report

Users may access a list of available standard reports by selecting **Reports** on the main menu bar, as depicted in Figure 334 below. Users then select **Standard** and **Credentialing**.



Figure 334: Accessing the CCQAS Standard Credentialing Reports

A list of standard reports is displayed, as depicted in Figure 335 below. Users may run a selected report by clicking the report name.

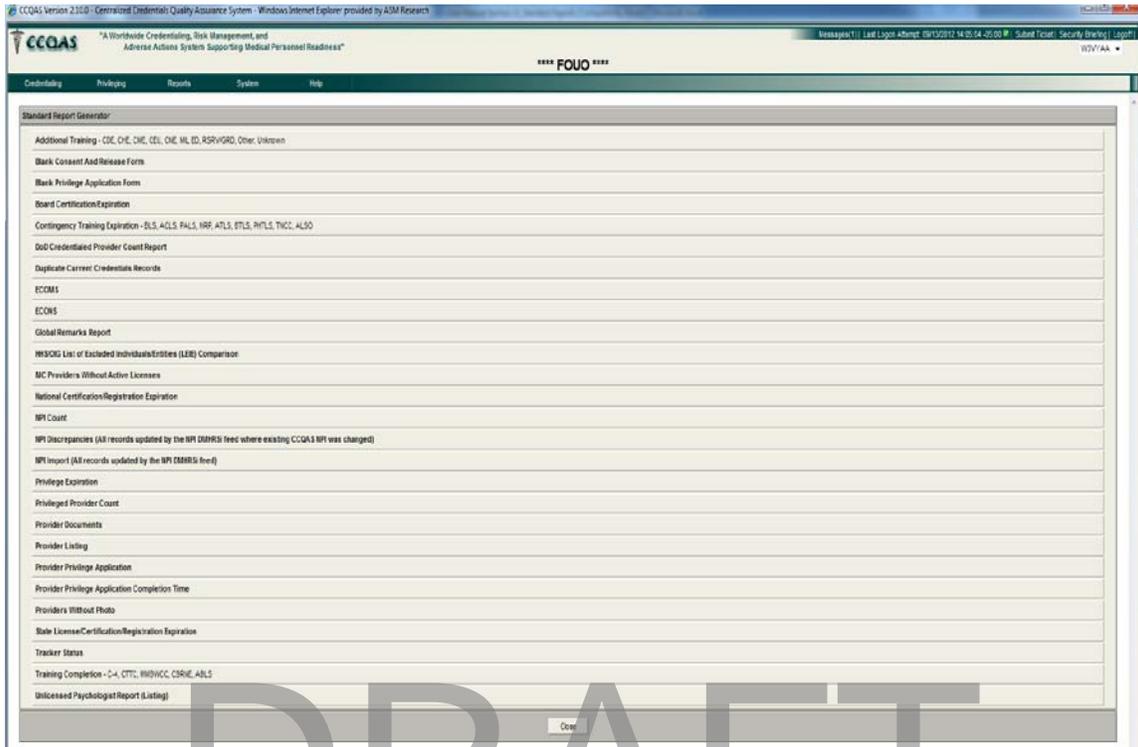


Figure 335: List of Standard Credentials Reports

The Training Expiration Report is depicted in Figure 336 below as an example.

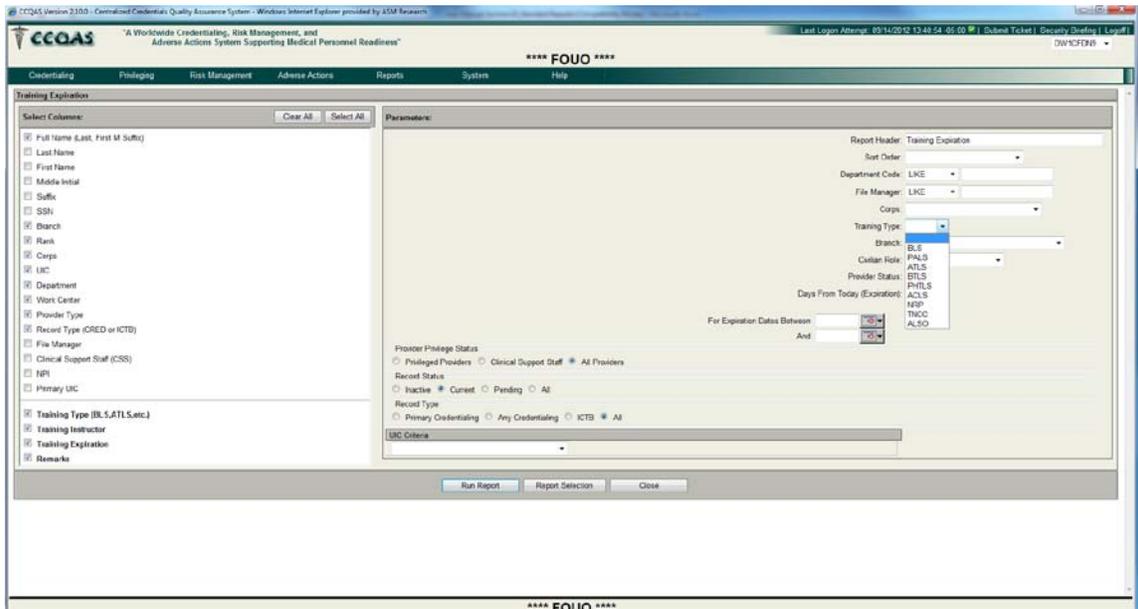


Figure 336: Parameter Screen for the Training Expiration Report

In general, the generation of standard reports is a two-step process, as follows:

Step 1. Under the **Select Columns** section, users may select/deselect the columns that will comprise the columns in their report by clicking the data fields listed. Standard demographic data fields are listed first, followed by a list of data elements that are specific to the selected report. CCQAS defaults to selected columns that users may change. Any number of columns may be checked, but at least one demographic data field must be selected to run the report. It is important to remember that the width of the report grows with each column included on the report, so users should include only those columns needed to make the report useful.

Hint: The **Clear All** button automatically deselects all the data fields and the **Select All** button automatically selects all data fields for inclusion in the report.

Step 2. Under the **Parameters** section, a series of required and optional query parameters are presented. Most standard reports offer the user the following options:

- A **Report Header** that may be edited from this screen. Users may wish to add more descriptive information to the default report name provided by CCQAS
- A **Sort Order** function that enables users to sort the rows of their report alphabetically or chronologically, using any of the data fields available for reporting. The system defaults to sorting by first letter of a Provider's last name if another sort option is not selected. (**Note:** If users select **Rank** for the sort order, the report is sorted alphabetically by the first letter of the rank, rather than by the military rank hierarchy)
- A **Department Code** filter that allows users to enter a partial department code designation that acts as a filter for the report query. For example, if users enter "**ped**" in this field, only those records with the phrase "**ped**" included in their **Department Code** field, such as "**pediatric clinic**" or "**pediatrics**" would be queried to generate the report
- A **File Manager** filter that allows users to enter a partial file CC/MSSP/CM name that acts as a filter for the report query. For example, if users enter "**Smi**" in this field, only those records with this sequence of characters in the **File Manager** field, such as "**Smith**" or "**Smiddy**" would be queried to generate the report
- A **Record Status** indicator that enables only inactive, current, pending, or all record types to be included in the report query
- A **Record Type** indicator that enable only Primary Credentials, Any Credentials, ICTB, or ALL record types to be included in the report query
- **UIC Criteria** is a pick list of UICs for which CC/MSSP/CMs may generate the report. If CC/MSSP/CMs only have permission to access credentials records for one UIC, only that UIC appears in the pick list. If CC/MSSP/CMs have permission to access credentials records for multiple UICs, results for all UICs are reported unless only one UIC is selected from the pick list
- **Expiration Dates** filter that allows users to enter applicable date ranges that should be used to generate the report

The entry of a date range is required to generate this report.

For the **Training Expiration Report**, additional fields, **Training Type** and **For Expiration Dates**, are also listed in the **Parameters** section to enable CC/MSSP/CMs to specify the type of training. If they select the **Training Type** value, all training types are included in the report.

Other query parameters are available for specific reports. A description of each report and the required and optional query parameters associated with the report are listed in Table 4 below:

Table 4: Descriptions of CCQAS Standard Credentialing Reports

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Additional Training	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps, UIC Criteria	Lists Providers who have CDE, CHE, CME CEU, CNE, MIL ED, PSRV/GRD Other or Unknown - training completion dates between the date range specified. If multiple training certifications are selected as columns for the report, all Providers that meet any one of the completion date criteria are included on the report. The columns of this report are fixed; users may specify one, and only one, type of additional education (e.g., CME, CNE, etc.) for inclusion in a single Provider report. This report is not available for export to Word or Excel.
Blank Consent and Release Form		None	Consent and Release Provider liability empty statement.
Blank Privilege Application Form	Provider Category, Privilege category	Duty Section, Duty Phone, Assignment Date, Station Date	Empty report for specific privilege category with Current Assignment and Projected Station dates.
Board Certification /Expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps; UIC Criteria	Lists Providers whose ABMS, AOA, or ADA board certification expires within the specified date range. If a Provider holds multiple certifications that meet the expiration date criteria, each certification is reported as a separate row of the report. This report is generated from data entered on the Specialties tab of the electronic credentials record.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Contingency Training expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps; UIC Criteria	Lists Providers whose selected training certifications expire within the date range specified. If multiple training certifications are selected as columns for the report, all Providers who meet any one of the expiration date criteria are included on the report.
DoD Credentialed Provider Count		UIC , Provider Status	Lists all Providers count by status for the DoD Credentialed Provider as of the date specified by the report by Primary UIC, Group by Status, Group by Branch, Group by Corps/role, Filter by UIC, or Contractors only. Count Report available at Service level and DoD level only.
Duplicate Current Credentials	DRAFT	None	Lists duplicate Provider's records.
ECOMS		Provider Status	Region
ECONS	Provider Status	Region	Lists the Providers with the specified Provider Status and the person with whom their file currently resides.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Global Remarks Report	Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Most Recent File Status for specified Date range; CCS; UIC Criteria	Lists each Provider's most recent global remark, or all global remarks for each Provider entered as of a specified date.
HHS/OIG List of Excluded Individuals/Entities (LEIE) Comparison	This report is generated automatically upon selection; no query criteria are entered by users.	None	This report provides a listing of all Department of Health and Human Services (DHHS) Providers assigned to, or working at the user's facility, who have been DHHS-sanctioned.
MC Providers Without Active Licenses	Record Status; Record Type;	Branch Rank	Lists all medical corps Providers who do not have at least one active state license.
National Certification/Registration/Expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps, UIC Criteria	Lists Providers whose national certifications or registrations expire within the specified date range. If a Provider holds multiple national certifications that meet the expiration date criteria, each certification is reported as a separate row of the report. This report is generated from data entered on the National section of the Licenses/Certifications/Registration tab of the electronic credentials record.
NPI Count	This report is generated automatically upon selection; no query criteria are entered by users.	None	The report counts the number of Providers with an NPI, the number of Providers without an NPI, and the total number of Providers broken down by facility.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
NPI Discrepancies	This report is generated automatically upon selection; no query criteria are entered by users.	None	Report is a listing of Providers with Active Credential Records that have had their NPI changed by Defense Medical Human Resources System - internet (DMHRSi).
NPI Import	NPI Import Date Range;	Branch; Rank; Corp; UIC	Lists Records updated by the NPI DMHRSi feed.
Privilege Expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps; CSS, UIC Criteria	Lists privileged Providers whose privileges expire within the specified date range, or clinical support staff whose CSS review date expires within the specified date range.
Privileged Provider Count	Record status Record Type		Displays a count of Providers by UIC, command, and location for the specified Record Type and Record Status.
Provider Documents	Upload Date Range	Department Code; File Manager; Corps; UIC Criteria; Record Status; Record Type; Document Type	The report displays a list of Provider documents uploaded between the specified date range in a record at the facility the user is assigned to maintain, for the specified record status and type.
Provider Listing	Record Status; Record Type	Department Code; File Manager; Corps; Shared (between DoD and Department of Veterans Affairs [VA]); UIC Criteria	Lists all Providers who are assigned to the user's UIC. If both CRED and ICTB records are included as query criteria, individual Providers may be listed twice if they have both a CRED and an ICTB record.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Provider Privilege Expiration	PA decision Date range	Application Status; Provider status, Civilian Role; Assigned CC/CM/MSSP	Lists all Providers with E-Applications who have a record in a facility with average completion days.
Provider Privilege Application Completion Time Report	PA decision Date range	Application Status; Provider status, Civilian Role; Assigned CC/CM/MSSP	Lists all Providers with E-Applications who have a record in a facility with completion time.
Providers Without Photo	Record Status; Record Type	Department Code; File Manager; Corps; UIC Criteria	Lists Providers who do not have a photo loaded into the Photo tab. If both CRED and ICTB records are included as query criteria, individual Providers may be listed twice if they have both a CRED and an ICTB record.

DRAFT

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
State License/Certification/Registration Expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps; CSS, UIC Criteria	Lists Providers whose state license, certification, or registration expires within the specified date range. If a Provider holds multiple state licenses that meet the expiration date criteria, each certification is reported as a separate row of the report. This report is generated from data entered in the State section of the Licenses/Certifications/Registration tab of the electronic credentials record.
Tracker Status	Record Status; Record Type	Department Code; File Manager; Corps; Privilege Expiration Date Range; Provider Status for specified date range	Lists specified Providers and their relevant file status. This report queries only active, credentials (e.g., CRED) records. This report is not available for export to Word or Excel.
Tracker Status	Privileged or Clinical Support Staff	Department Code; File Manager; File Status for specified date range; Corps; Privilege Expiration Date Less Than date; File Status Date Greater Than date	Lists specified Providers and their relevant file status. This report queries only active, credentials (e.g., CRED) records. This report is not available for export to Word or Excel.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Training Completion	Completion Date range; Record Status; Record Type	Department Code; File Manager; Corps; UIC Criteria	Lists Providers who have C4, CTTC, or MMBWCC training completion dates between the date ranges specified. If multiple training certifications are selected as columns for the report, all Providers who meet any one of the completion date criteria are included in the report.

Example: Robert runs the **Training Expiration Report** to determine which members of the **Medical Corp** need to be recertified in **BLS** in the next 6 months. He also wants the results to be sorted by **Department**. For the purposes of this example, assume the current date is January 1, 2007. Robert's **Training Expiration Report Parameter** screen would look like the one depicted in Figure 337 below.

After users select the desired columns and query parameters, the standard report may be generated by clicking **Run Report** at the bottom of the screen.

The screenshot shows the 'Training Expiration' parameter screen in the CCQAS system. The interface includes a navigation menu at the top with options like 'Credentialing', 'Privileging', 'Risk Management', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area is divided into two sections: 'Select Columns' and 'Parameters'.

Select Columns: A list of checkboxes for selecting report columns. The 'Run Report' button at the bottom of this section is highlighted with a red box.

Parameters: A form for configuring the report. It includes fields for 'Report Header' (Training Expiration), 'Sort Order', 'Department Code' (LIKE), 'File Manager' (LIKE), 'Corps' (MTC - Medical Reserve Corps), 'Training Type', 'Branch' (F11 - Air Force (USAF)), 'Civilian Role' (PHY - Physician), 'Provider Status', and 'Days From Today (Expiration)'. There are also date range pickers for 'For Expiration Dates Between' and 'And'. At the bottom, there are radio buttons for 'Provider Privilege Status' (Privileged Providers, Clinical Support Staff, All Providers), 'Record Status' (Inactive, Current, Pending, All), and 'Record Type' (Primary Credentialing, Any Credentialing, ICTB, All). A 'UIC Criteria' dropdown is also present.

Figure 337: Example of Training Expiration Report Parameter Screen

The report should display on the screen after a few seconds. Larger or more complex queries may take more time. The query criteria used to generate the report is listed below the report header, and a description of the query logic is provided at the foot of the report. After a report is generated, users may either click **Print**, **Cancel**, or **Copy Data to Memory for import into Word or Excel**, as depicted in Figure 338 below.

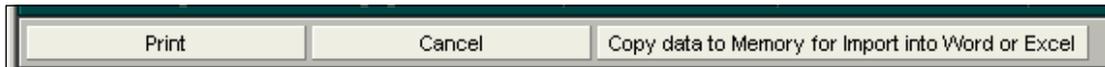


Figure 338: Reporting Options

Figure 339: Blank Privilege Application Report

These options are explained in more detail in [Sections 13.3–13.5](#).

13.2 Generating a Standard Privileging Report

Users may access a list of available standard reports by clicking **Reports** on the main menu bar, and then selecting **Standard** and **Privileging**, as depicted in Figure 340 below.



Figure 340: Accessing the CCQAS Standard Privileging Reports

A list of standard reports display, as depicted in Figure 341 below. Users may run a report by clicking the report name.

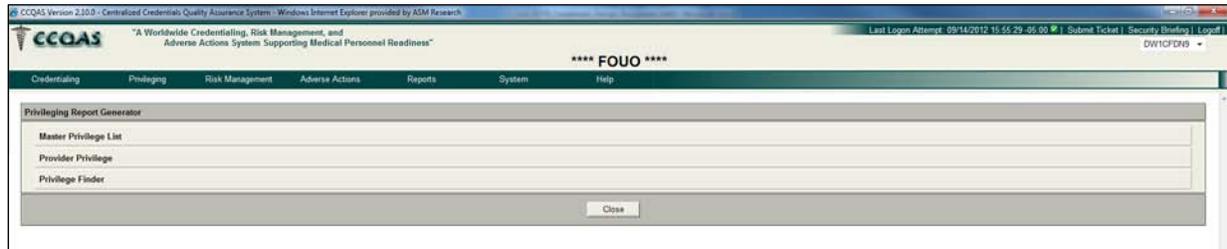


Figure 341: List of Standard Credentials Reports

The available reports are listed in Table 5 below:

Table 5: Descriptions of CCQAS Standard Privileging Reports

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Service-Level Master Privilege Report	Privilege Category	None	This report lists all privilege items included in the master Service list for the selected privilege category.
Provider Privilege	MTF, Provider, Start Date	Start Date, End Date	After the entry of initial parameters, users are directed to select the assignment for which granted privileges should be displayed. Users then select View from the hidden menu of actions for the assignment record to display the Privileged Provider Information Report . If a Provider only has one assignment record for the period of time specified, the Privileged Provider Information Report automatically generates without requiring users to select the assignment.
Privilege Finder	Code Description	Delineation	Lists Providers with selected Privilege(s).



Figure 342: Privilege Finder Report[RJ3]

After a report is generated, users may either click **Print** or **Close**. [RJ4] These options are explained in more detail in Sections 13.3–13.4.

13.3 Printing a Standard Report

Users may print a standard report directly from the CCOAS application by clicking **Print** at the top of the report. Since the report is generated directly from the Internet, the upper or lower margins may contain the URL, date, page, and index information, according to a user's browser settings. Alternatively, many users prefer to export the report to Microsoft® Word or Excel to format their report prior to printing.

13.4 Cancelling a Standard Report

Users may cancel a standard report by clicking **Cancel** or **Close** at the top of the report. These actions return users to the **Query Criteria Selection** screen, where they may either rerun the report, click **Report Selection** to return to the list of standard reports, or click **Close** to close the reporting function.

13.5 Exporting a Report to Microsoft® Word or Excel

Users may export a standard report to Microsoft® Word or Excel for editing and manipulation as a tab separated text file by clicking **Copy data to memory for import into Word or Excel**, as depicted in Figure 343 below.

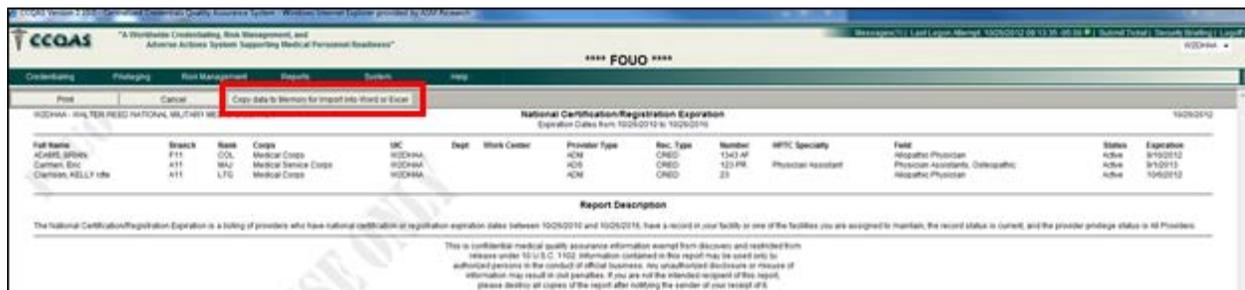


Figure 343: Exporting a Report to Word or Excel

Users must then read and agree to a QA statement in a pop-up window by clicking **OK**, as depicted in Figure 344 below.

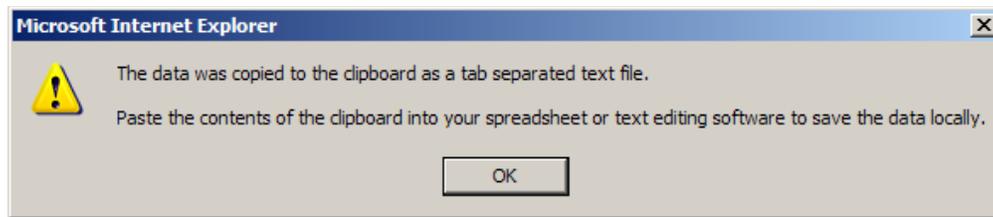


Figure 344: Data Copied Message Window

After users click **OK** to close this message, they may open the desired Microsoft® Word or Excel document into which the report will be imported. The contents of the clipboard may be pasted into a new or existing document by opening the **Edit** menu (in the Microsoft® Word or Excel application), and then selecting **Paste**. Each column and row of the CCQAS report is pasted into a column and a row, respectively, in a Microsoft® Word or table or a Microsoft® Excel spreadsheet, as depicted in Figure 345 below. The report may then be manipulated, saved, and printed as a regular Microsoft® Word or Excel file.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Full Name	Branch	Rank	Corps	UIC	Dept	Work Cen	Provider T	Rec. Type	Number	HPTC Specialty	Field	Status	Expiration
2	ADAMS, BRIAN	F11	COL	Medical Corps	W2DHAA			ADM	CRED	1343 AF		Allopathic Physician	Active	9/10/2012
3	Carmen, Eric	A11	MAJ	Medical Service Corps	W2DHAA			ADS	CRED	123 PR	Physician Assistan	Physician Assistants	Active	9/1/2013
4	Clarkson, KELLY	A11	LTG	Medical Corps	W2DHAA			ADM	CRED	23		Allopathic Physician	Active	10/6/2012
5														

Figure 345: Sample Excel Spreadsheet with CCQAS Report

Note: Only the columns and rows of the CCQAS report are pasted into the Microsoft® Word or Excel document; the report header and report description are not transferred with the data. Users must manually create a new report header and other descriptive information, as needed.

14 Generating Ad-Hoc Credentials Reports

14.1 Generating an Ad-Hoc Credentials Report

14.2 Saving an Ad-Hoc Report Query for Future Use

14.3 Running an Ad-Hoc Report from a Saved Query

14.4 Deleting a Saved Query

14.5 Printing an Ad-Hoc Report

14.6 Exporting an Ad-Hoc Report to Microsoft® Word or Excel

14.7 Sample Ad-Hoc Reports

15 System Management

16 Branch Clinic Management

Branch Clinic Management is a new function within CCQAS 2.10.0.0 that allows service level users to designate specific UICs as branch clinics to create a hierarchy. Service level users can add what are called “branch” UICs to a “parent” UIC to create the hierarchy. This is done through the Branch Clinics Management module within the **MTF Contacts** page.

16.1 Adding a Branch Clinic

To navigate to the **MTF Contacts** page, service level users select the **System** menu, and then select **MTF Contacts**. The **MTF Contacts** page opens, which displays all MTFs for all services. Service level users can then filter by service by selecting the radio button for that service, which is located at the top of the screen. After service level users filter the **MTF Contacts** page by service, they select the UIC they would like to view by clicking the **Hidden Menu** arrow, as depicted in Figure 346 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel"			
Credentialing	Privileging	Reports	System
MTF Contacts			
<input type="radio"/> All <input type="radio"/> Air Force <input checked="" type="radio"/> Army <input type="radio"/> Navy			
▶ W37PAA	Army	Yes	HQ E SECTOR US MEP COMD
▶ W37RAA	Army	Yes	HQ W SEC US MEPCOM
▶ W383AA	Army	Yes	USA MEDDAC BAVARIA
▶ W39LAA	Army	Yes	USA NG READINESS CENTER
▶ W3FBAA	Army	Yes	USA MED DEPT ACT JAPAN
▶ W3QM03	Army	Yes	USA HLTH CLN FT BUCHANAN
▶ W3QMAA	Army	Yes	DWIGHT D EISENHOWER ARMY MEDICAL CENTER
▶ W3U5AA	Army	Yes	USA DENTAL COMMAND
▶ W3VYAA	Army	Yes	USA MEDCOM
▶ W3VZ25	Army	Yes	TRAUMA TRAINING CENTER
▶ W3VZBD	Army	Yes	3VZ AMEDD STU DET
▶ W3ZR10	Army	Yes	USA DENTAC - FT HOOD
▶ W3ZR20	Army	Yes	USA DENTAC - FT SAM HOUSTON
▶ W3ZR30	Army	Yes	USA DENTAC - FT POLK
▶ W3ZR40	Army	Yes	USA DENTAC - FT SILL

Figure 346: MTF Contacts Page

When service level users select the UIC, the **MTF** page displays the following sections: **MTF**, **Credentials Coordinator**, **Branch Clinics**, **Risk Manager**, and **Remarks**. To search for a branch clinic, select the **Binoculars icon**, [R15] and then enter search criteria. After they enter the search criteria and click **Search**, service level users can select the UIC they want to add as a branch clinic, as depicted in Figure 347 below.

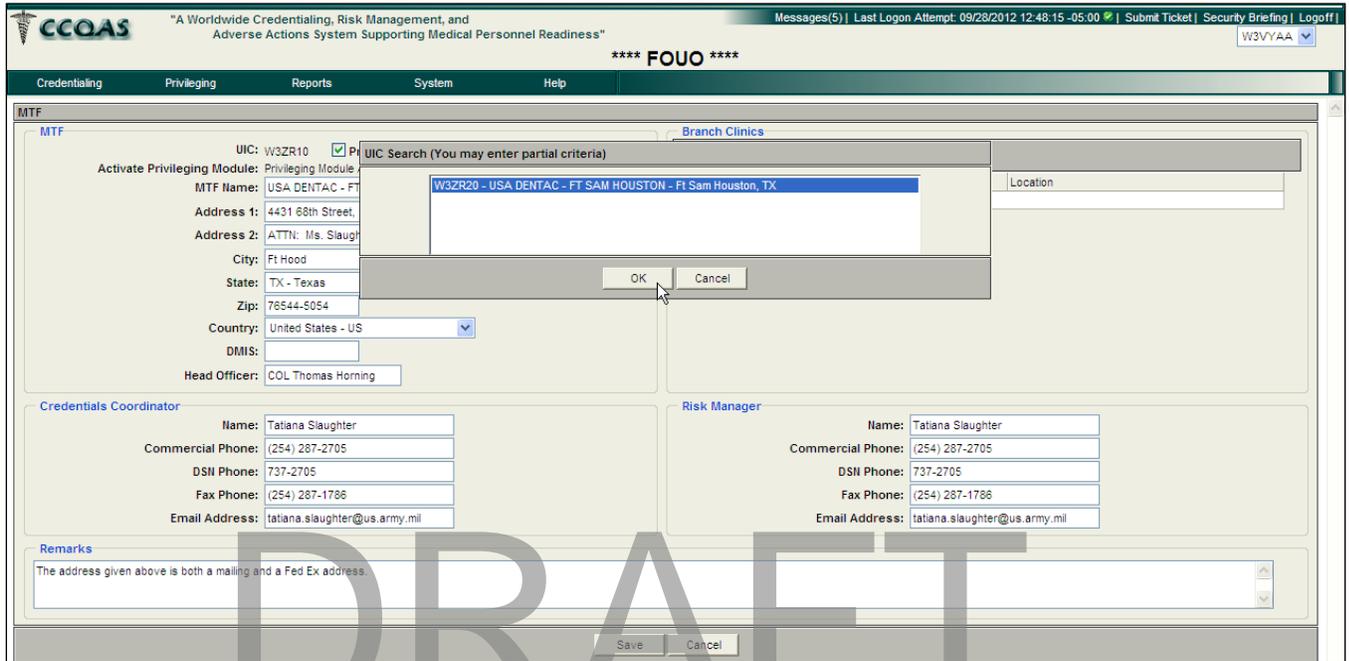


Figure 347: UIC Selection for Branch Clinic

When service level users select the appropriate UIC, it displays in the **UIC** field, as depicted in Figure 348 below. To add the UIC as a branch clinic, click the **Add Branch Clinic** button.

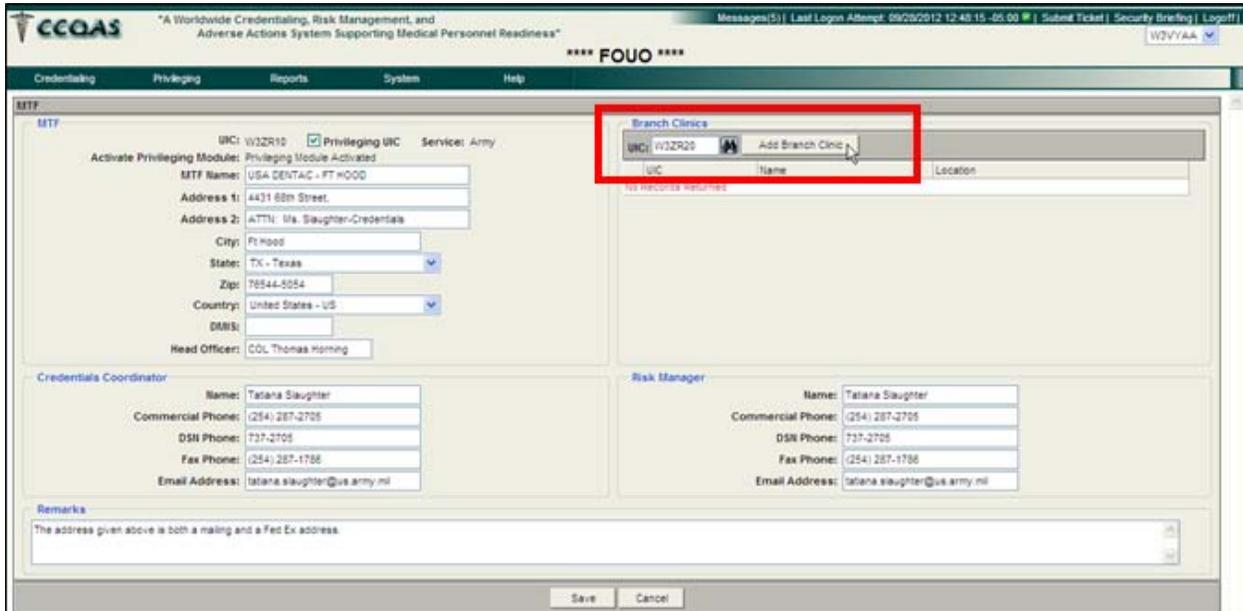


Figure 348: Add Branch Clinic

When service level users click the **Add Branch Clinic** button, the new branch clinic displays in the **Branch Clinics** section, as depicted in Figure 117 below. Service level users have successfully added a branch clinic to the parent UIC’s hierarchy.

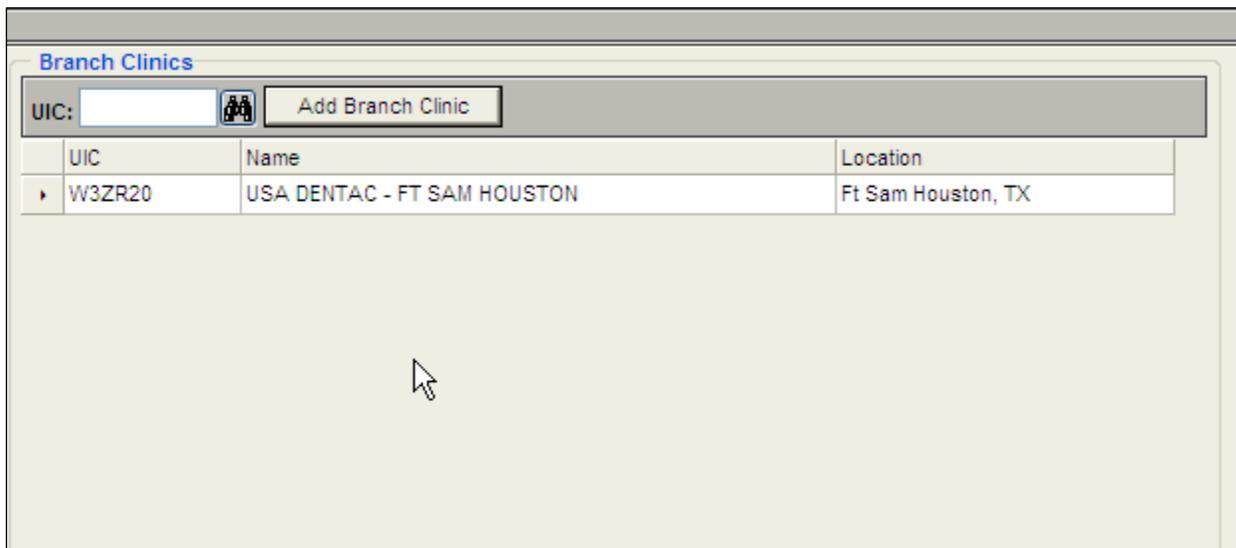


Figure 349: Branch Clinic Record

Service level users can remove this branch clinic by clicking the **Hidden Menu** button, and then selecting **Delete** from the down-down list, as depicted in Figure 350 below.

Note: A UIC that has previously been established as a branch UIC cannot be a parent UIC in any other parent/branch UIC privileging relationship. Also, a UIC that has been added to a parent/branch UIC privileging relationship cannot be a branch UIC in any other parent/branch UIC privileging relationships.

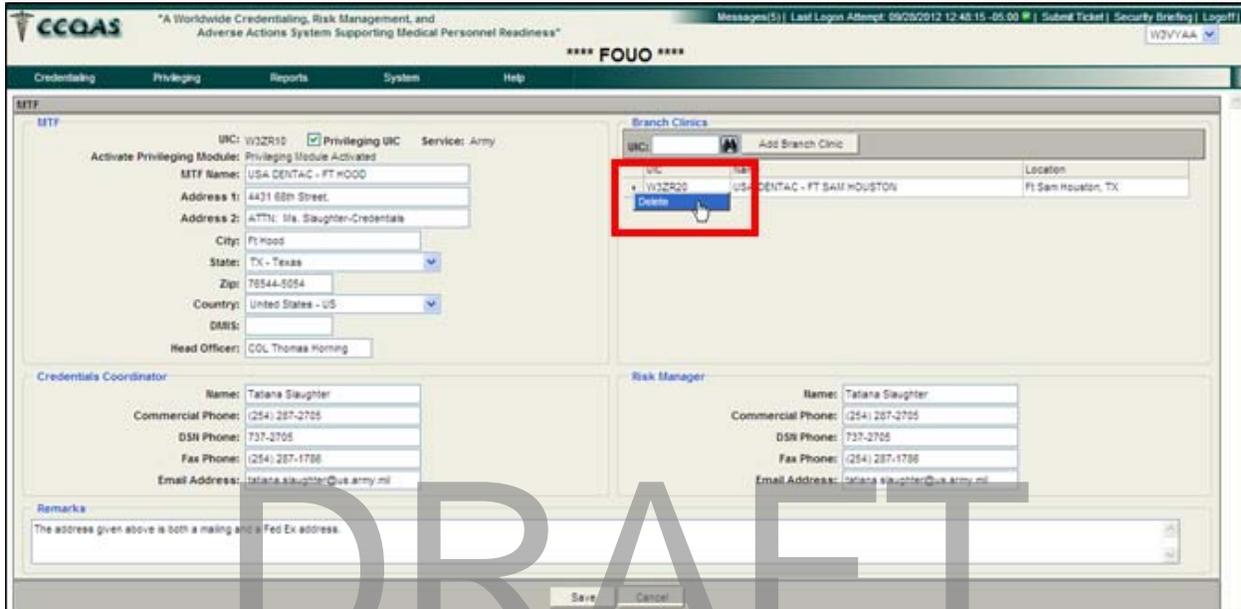


Figure 350: Delete Branch Clinic

16.2 Privileging at a Branch Clinic

Providers who have the ability to add a branch clinic to a parent clinic can also request privileges not only at the parent UIC, but the corresponding branch UICs. On the **Position** tab of their electronic application, Providers have the option to request privileges at the parent UIC and any associated branch UICs. Figure 351 below depicts a sample Provider's application, which displays parent and branch clinics.

UIC	Name	Location	Requester Assigning Privileges?	Parent	Branch Clinic
<input checked="" type="checkbox"/>	112DHT8	FORT BELVOIR COMMUNITY HOSPITAL	8306 DEWITT LOOP, VA	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	112DHA4	WALTER REED NATIONAL MILITARY MEDICAL CENTER	Walter Reed National Military Medical Center, MD	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	112DHB1	USA MEDDAC FT MEADE	2402 LLEVELLYN AVENUE, MD	<input type="checkbox"/>	<input type="checkbox"/>

Figure 351: Branch Clinics on 'Position' Tab for Provider E-App

When Providers select the parent UIC and corresponding branch UICs, the **Privileges** section for each UIC displays on the **Navigation** menu on the left (refer to Figure 352 below). Each UIC displays as a different privileges section on the electronic application. Providers must go through each **Privileges** section and request privileges specific to that UIC.

Privilege Category: Physician

Select all privilege categories that apply, and then click Save. Individual privilege items may be selected on the Privileges tab.

Privilege Category	Type
<input type="checkbox"/> Aerospace Medicine	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Air Reserve Components (ART) - Physician	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input checked="" type="checkbox"/> Allergy and Immunology	<input type="radio"/> Core Supplemental <input checked="" type="radio"/> Specialty
<input type="checkbox"/> Anesthesiology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Cardiology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Cardiothoracic Surgery	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Critical Care- Internal Medicine	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Critical Care-Anesthesia	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Critical Care-Emergency Medicine	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Critical Care-Surgery	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Dermatology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Diagnostic Radiology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Emergency Medicine	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Endocrinology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Family Medicine	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Flight Surgeon	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Gastroenterology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> General Medical Officer	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> General Surgery	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Genetics	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Hematology - Oncology	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Infectious Disease	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty
<input type="checkbox"/> Internal Medicine	<input type="radio"/> Core Supplemental <input type="radio"/> Specialty

Figure 352: Privileges Section for Branch Clinics

After Providers complete their electronic application with requested privileges, they must submit it for PSV through the PAC at their MTF. Primary PACs at parent UICs receive a notification to PSV. After PACs complete the PSV for the electronic application, they route it to at least one level of review for each UIC and PA. A PA is selected from the Primary/Parent UIC. Figure 353 and Figure 354 below depict the **Routing** page.

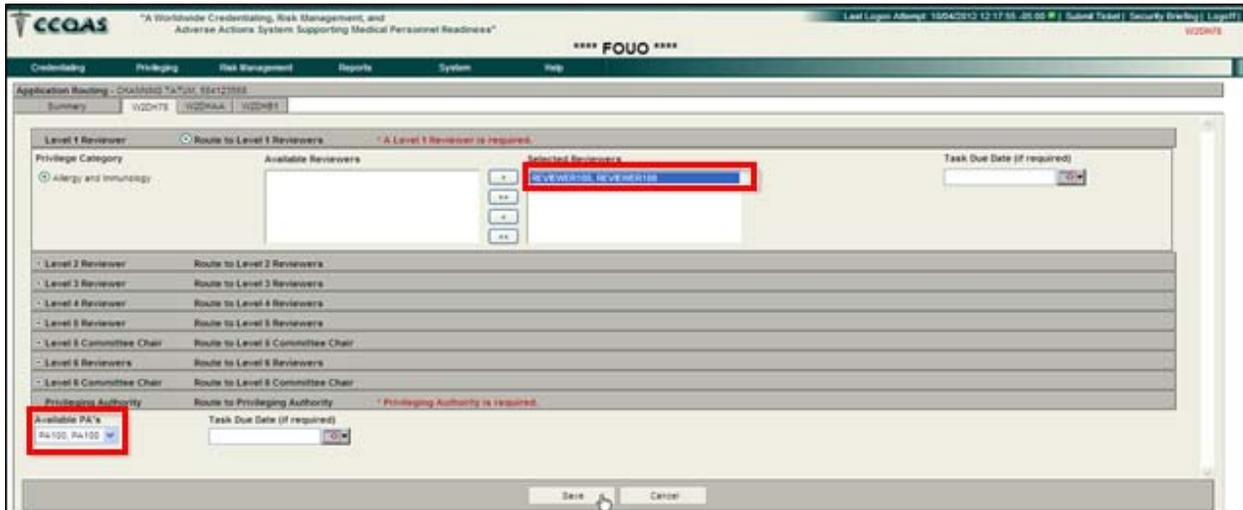


Figure 353: Reviewer Routing Page

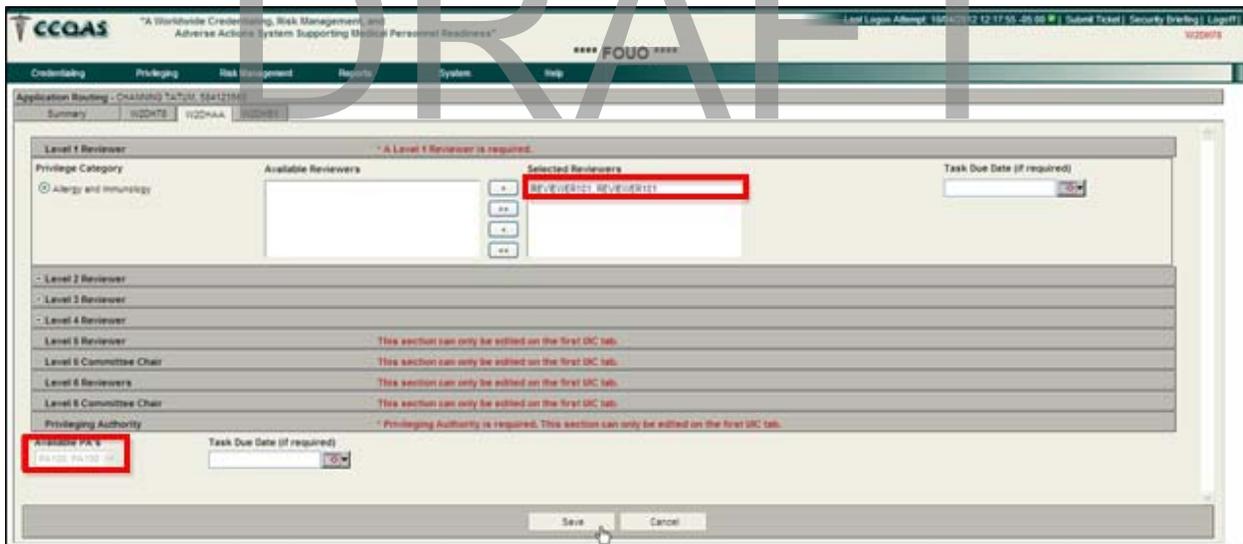


Figure 354: Reviewer Routing Page for Branch Clinic

After the Reviewers and the PA are selected, PACs can view the summary of the application routing before submitting it. Figure 355 below depicts the **Summary** page.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 10/04/2012 12:17:55 -05:00 | Submit Ticket | Security Briefing | Logout | W2DH78

**** FOUO ****

Credentialing Privileging Risk Management Reports System Help

Application Routing - CHANNING TATUM, 584123568

Summary W2DH78 W2DHAA W2DH81

W2DH78 - FORT BELVOIR COMMUNITY HOSPITAL			Completed: Yes
Level	Privilege Category	Task Due Date	Reviewers
Level 1 Review	Allergy and Immunology		REVIEWER100, REVIEWER100
Privileging Authority	All Categories		PA100, PA100
W2DHAA - WALTER REED NATIONAL MILITARY MEDICAL CENTER			Completed: Yes
Level	Privilege Category	Task Due Date	Reviewers
Level 1 Review	Allergy and Immunology		REVIEWER101, REVIEWER101
Privileging Authority	All Categories		PA100, PA100
W2DH81 - USA MEDDAC FT MEADE			Completed: Yes
Level	Privilege Category	Task Due Date	Reviewers
Level 1 Review	Allergy and Immunology		REVIEWER102, REVIEWER102
Privileging Authority	All Categories		PA100, PA100

Submit Close

Figure 355: Summary Page for Reviewer Routing

After PACs submit the application for routing, the Reviewers can view new tasks in their Work List after they log in to review the application. The Reviewers can only see the privileges that the Provider requested at his or her UIC. After all Reviewers approve the electronic application, a task is added in the PA's Work List to approve the requested privileges. When PAs open the **Application Ready for Review** task, they can review privileges requested at the parent and branch UICs, as depicted in Figure 356 below.

Provider Application Review - CHANNING TATUM, 584123568

Provider Summary Privileges Documents Comments

W2DH78 W2DHAA W2DH81 Pa Decided

You must view all Privileging applications before an Approve/Approved or Disapprove/Disapproved.

Privilege Category: Allergy and Immunology Sort by: Entered Order

Allergy and Immunology

- Version 1.0
- Physicians requesting privileges in this subspecialty must also request privileges in their primary discipline
- Scope

Privilege(s)	Provider	Level 1	Privileging Authority	Comments
The scope of privileges in Allergy and Immunology includes the evaluation, diagnosis, consultation, management, and provision of therapy and treatment for patients presenting with hypersensitivity and immunologic conditions or disorders. The scope also includes the consultation, management, education, and provision of therapy and treatment for patients presenting for immunization healthcare including routine prevention, travel, education, military readiness and adverse events. Physicians may admit and may provide care to patients in the intensive care setting in accordance with WTP policies.	Fully Competent	Fully Competent	Fully Competent	
Knee Pain	Fully Competent	Fully Competent	Fully Competent	
Diagnosis and Management	Provider	Level 1	Privileging Authority	Comments
Performance and interpretation of diagnostic testing for immediate hypersensitivity disease (skin testing, challenges)	Fully Competent	Fully Competent	Fully Competent	
Performance and interpretation of diagnostic testing for delayed hypersensitivity	Fully Competent	Fully Competent	Fully Competent	
Performance and interpretation of diagnostic testing for reactive airway disease and asthma (e.g., spirometry with flow-volume loops,	Fully Competent	Fully Competent	Fully Competent	

Approve Approve with Notification Disapprove Return with Action Close

Figure 356: PA Review of Privileges for Parent/Branch Clinics

After PAs review all privileges for all UICs, they click the **PA Decision** tab. On this tab, PAs must check each box under the **Reviewed** column before approving the application. After all boxes are checked, the Provider clicks either the **Approve** or **Approve with Modification** button at the bottom of the page, as depicted in Figure 357 below.

This completes the task for reviewing the Provider’s application. The Provider is now privileged at the parent UIC and branch UICs for the privileges that he or she requested and were approved.

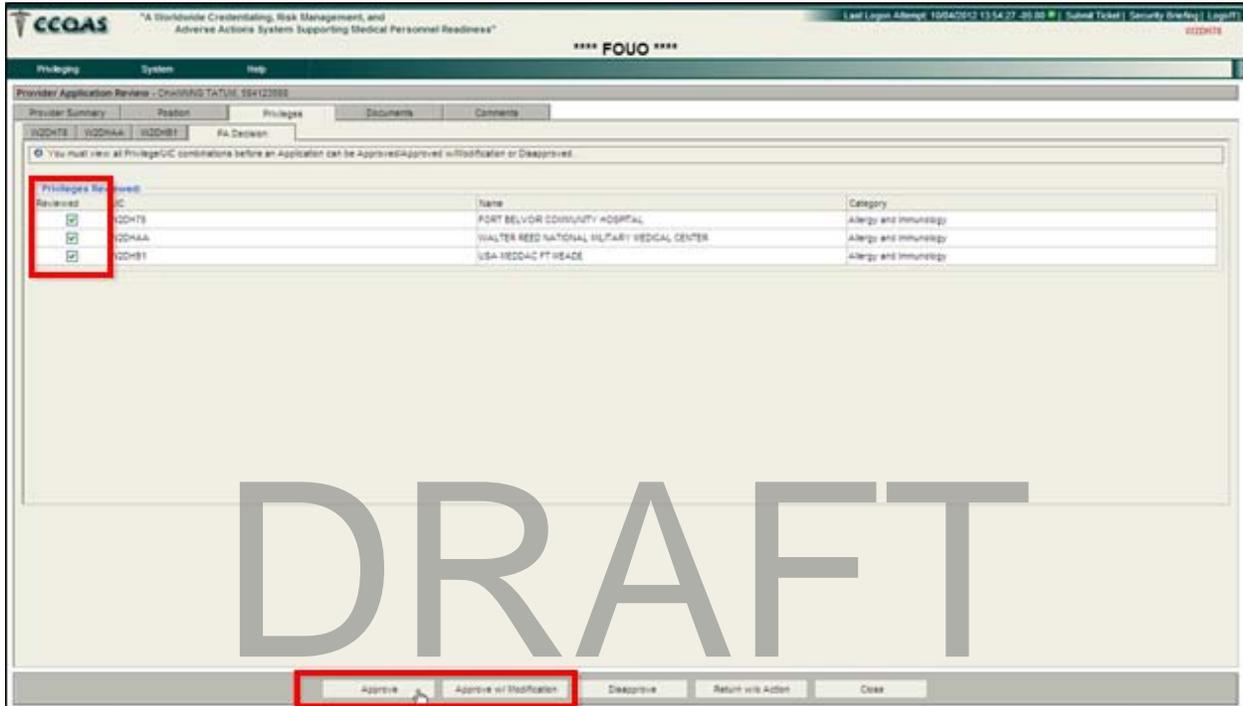


Figure 357: PA Decision Screen

17 Custody Transfer

Appendix A - Credentialing and Privileging Data Dictionary

This data dictionary provides the following information for every data field in the Credentials and Privileging application:

Field location: Module(s), tab(s), and/or screens on which the field is located

Field name: Field name as it appears in the module

Field type: Radio button, date, drop down menu, free text, etc.

Valid values: List of valid values that may be used to populate the data field

Field requirement: Indicator of whether the field is required or optional

Field definition: Description of meaning of the data field

System business rules: Automated system edits associated with the data field

Service business rules: Service-specific business rules associated with the data field

DRAFT

Appendix B - Directives, Regulations, Instructions, HA Policy Memoranda, and References

The following documents govern access to and administration of data contained within the CCQAS application:

- American Medical Association. *State Medical Licensure Requirements and Statistics, 2013*
- DoD Directive 5400.11, DoD Privacy Program, November 16, 2004
<http://www.dtic.mil/whs/directives/>
- DoD Directive 6025.13, Medical Quality Assurance (MQA) in the Military Health System (MHS), February 17, 2011
- DoD Directive 6025.14, Department of Defense Participation in the National Practitioner Data Bank (NPDB), November 1, 1990
- DoD Directive 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs, December 2, 2009
- DoD Instruction 6025.15, Implementation of Department of Defense Participation in the National Practitioner Data Bank (NPDB), October 12, 2000
- DoD Regulation 5400.11-R, Department of Defense Privacy Program, May 2007
- DoD Regulation 6025.13-R, Military Health System (MHS) Clinical Quality Assurance (CQA) Program Regulation, June 11, 2004
- DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation, January 2003
- Hoppa M., & Cooper, J. (2010). *The Greeley Company Guide to Medical Staff Bylaws, Third Edition*. Marblehead, MA: HCPro.
https://catalog.ama-assn.org/Catalog/product/product_detail.jsp?productId=prod2040049)
- Matzka, K. (Ed.). (2010). *2010 Credentials Verification Desk Reference*. Marblehead, MA: HCPro.
- Memorandum for Assistant Secretary of the Army (M&RA), Assistant Secretary of the Navy (M&RA), Assistant Secretary of the Air Force (M&RA). Subject: Waivers of Licensure Requirement for Quality Military Physician Assistants, January 15, 2004 [HA Policy: 04-002]
- Memorandum for Executive Director, TRICARE Management Activity. Subject: Drug Enforcement Administration (DEA) Numbers for DoD Providers, April 7, 2000
- Memorandum for Secretary of the Army, Secretary of the Navy, Secretary of the Air Force. Subject: DoD Policy on Physician Licensure, January 29, 1999 [HA Policy 99-007] - http://www.health.mil/libraries/HA_Policies_and_Guidelines/99-007.pdf
- Memorandum for Secretary of the Army; Secretary of the Navy; Secretary of the Air Force; Director, Defense Logistics Agency; Director, TRICARE Management Activity.

Subject: DoD Participation in the Health Integrity and Protection Data Bank, October 31, 2000 [HA Policy 00-009]

- Memorandum for Surgeon General of the Army, Surgeon General of the Navy, Surgeon General of the Air Force. Subject: Permissible Waivers of State Physician Licensure Inharmonious with Federal Policy, May 14, 1999
- Memorandum for Surgeon General of the Army, Surgeon General of the Navy, Surgeon General of the Air Force. Subject: Additional Guidance Regarding DoD Policy on Physician Licensure, September 28, 1999
- Memorandum for Surgeon General of the Army, Surgeon General of the Navy, Surgeon General of the Air Force. Subject: An Additional Permissible Waiver of State Physician Licensure due to Administrative or Financial Requirements Inharmonious with Federal Policy, April 19, 2000
- Memorandum for Surgeon General of the Army, Surgeon General of the Navy, Surgeon General of the Air Force. Subject: Codification of Business Rules for Mandatory Inclusion of Certain Providers/Practitioners in the Centralized Credentials Quality Assurance System, April 22, 2003 [HA Policy: 03-027]
- Memorandum for Surgeon General of the Army, Surgeon General of the Navy, Surgeon General of the Air Force. Subject: Policy on Reporting Joint Commission on Accreditation of Healthcare Organizations-Reviewable Sentinel Events in the Military Health System, July 13, 2004 [HA Policy: 04-018]
- Memorandum for Surgeon General of the Army, Surgeon General of the Navy, Surgeon General of the Air Force. Subject: Department of Defense Centralized Credentials Quality Assurance System, September 1, 2006 [HA Policy]
- U.S. Code, Title 10, Section 1102, Confidentiality of medical quality assurance records: qualified immunity for participants, January 3, 2012

Appendix C - FAQs - Creating and Maintaining CCQAS 2.10.0.0 User Accounts

FAQ: A user received his username and temporary password via email a few weeks ago, but CCQAS will not accept the password that was given to the user. What should I do?

Answer: If more than 60 days have lapsed since the user received the email message containing his new username and temporary password, then the user's password has expired and a new temporary password will need to be issued. This can be done through the **User Processing** function. Open the System menu and select **User Processing**. Then open the user's account and click **Issue New Password** on the **Demographics** tab. The user will then receive a new temporary password via an email message. The user will then have 60 days to log in to CCQAS using the temporary password and select a new password.

FAQ: A user's CCQAS password has expired. What should I do?

Answer: If a user's password has expired, a new temporary password will need to be issued. Follow the guidance provided in the previous FAQ to issue the new password.

FAQ: A user forgot his password. What should I do?

Answer: If a user has forgotten his or her password, a new temporary password will need to be issued. Follow the guidance provided in the first FAQ to issue the new password.

FAQ: CCQAS will not allow one of my users to log in, but I know he is using a valid password. What should I do?

Answer: If a username and password are both current and valid, it is likely that the user's account has been locked. An account is locked after three consecutive login attempts fail using the same username. Most often, lock outs occur as a result of user error when entering the case-sensitive password.

FAQ: CCQAS 2.10.0.0 is currently being implemented at my MTF, and my facility commander needs immediate access to CCQAS to enable him to approve privilege applications online. His privileges are also expiring and need to be renewed. Thus, he needs access to CCQAS both as a "Provider" and a "Privileging Authority." How do I create his user account to assign him both roles?

Answer: Your commander needs access to CCQAS both as a "Provider" and a "Module User." The easiest way to create his user account would be as follows: use the **Grant Provider Access** function (refer to [Section 3.2.6](#) to create the new user account for his role as a Provider. Then add **Module User** permissions to the account to grant him access to the Privileging Module as the PA (refer to [Section 3.3.2](#)).

FAQ: A new civilian nurse practitioner was just hired at my facility and she needs to be privileged. How do I generate her electronic privilege application?

Answer: The 1st E-application may be generated for a new accession or a new employee in one of two ways. You may either direct her to self-register for a new user account or initiate the creation of her new user account yourself. The user account may then be processed according to the process described in [Section 5](#). The creation of her new user account as a Provider will automatically generate her 1st E-application.

FAQ: A Provider has just PCS'ed into my facility, but says he has never completed an online CCQAS privilege application or had a CCQAS user account. How do I generate his online privilege application now?

Answer: If this Provider has not received and completed his 1st E-application, he has not yet been integrated into the CCQAS privileging process. The best way to integrate a Provider who already has an active credentials record in your facility, is by using the "Grant Provider Access" function. Using this function generates the 1st E-application for the Provider. If the "Grant Provider Access" menu item is not available from the hidden menu of actions for the Provider's credentials record, the user account has already been associated with their credentials record at some time in the past. The "Initiate Application" menu item may then be used to generate an E-application for the Provider.

FAQ: A Provider has just PCS'ed into my facility. He says he has never completed an online CCQAS privilege application, but he did use CCQAS at his former duty station to review privilege applications. How do I generate his online privilege application now? Should I create a new user account for him?

Answer: Do not create a new user account for this Provider since he already has a CCQAS user account. This would result in multiple user accounts, username, and passwords for the same person, which is not appropriate. Use the "Grant Provider Access" function within the Credentials module to add Provider access to his current user account. If CCQAS does not recognize that the Provider already has a user account, contact your Service CCQAS representative for assistance.

FAQ: I am the CM at a small facility and sometimes need to request clinic staff at other locations to review privilege applications for my location. These Reviewers have CCQAS user accounts to review applications at their own location. How do I give these individuals access to CCQAS to review privilege applications for my facility? I cannot access their user account via my User Processing function. Should I create a new user account for them?

Answer: Do not create a new user account for any individual that already has a CCQAS user account. This would result in multiple user accounts, username, and passwords for the same person, which is not appropriate. To have these individuals function as Reviewers for your UIC, your UIC must be added to the MTF tab in their existing user account. You should first contact the CM at the facility where the Reviewer is currently assigned, to determine if the CM has permission to add UICs to the Reviewer's account. If the other facility CM does not have this

permission, contact your Service-level CCQAS administrator to have your UIC added to the Reviewer's account. After your UIC has been added to a user account, the Reviewer's user account should be accessible through your User Processing function, and you can assign the appropriate roles to the his or her account.

DRAFT

Appendix D - FAQs - Managing Facility Privilege Lists

DRAFT

Appendix E - FAQs - Processing the 1st E-Application for Clinical Privileges

DRAFT

Appendix F - FAQs - Modification of Provider Credentials and Clinical Privileges

FAQ: One of my Providers created a Modification Application and then decided that he did not want to request modified privileges. The task to complete the modification application is still active in his work list. What should he do?

Answer: After a period of 90 days, if not acted upon during that time, the application will become a “non-compliant” application and will be closed, thus disappearing from his open work list. After 90 days, he may initiate another application for modification of privileges, or the CC/MSSP/CM may reinstate the application to the status of “Pending” and notify the Provider of the status change. The Provider may then complete the application.

DRAFT

Appendix G - FAQs - ICTB Process

FAQ: One of my Providers is deploying to a classified location that is not supported by CCQAS. When I initiated the ICTB, he received a work list task to complete his ICTB application. What should I instruct him to do with this task?

Answer: Instruct the Provider to ignore the task on his CCQAS work list. He does not have to open the task and complete that application. After 90 days, the task will be closed and disappear from his “open” work list. The paperwork for the ICTB should be handled outside CCQAS and should follow current Service policy.

DRAFT

Appendix H - FAQs - Renewal of Clinical Privileges

FAQ: One of my Providers holds privileges that will expire in 60 days. The Provider, however, expects to PCS close to the time his privileges expire and does not wish to renew them at this facility. He already has the Renewal Application as an active task in his work list. What should he do?

Answer: He does not have to open the task and complete the renewal application. After 90 days, the task will be closed and disappear from his 'Open' work list. Once you generate an "Initiate PCS" task, the system will automatically send the Provider an email tasking him to complete a PCS application, and a new task will be added to his work list, thus: "**Task = Complete Application (PCS)**".

DRAFT

Appendix I - FAQs - The PAR

FAQ: One of my Provider's PCS'ed and a PAR was completed by the evaluator. However, the evaluator wants to do another because he feels that the PAR he completed was not accurate. Can he do this even if the Provider already completed his PCS application?

Answer: Yes. You can manually initiate a **PAR** task by selecting the **Work List** menu item from the Privileging module, and then clicking the **My Applications** tab. From the summary listing, select the appropriate Provider and his last approved or completed application. Click the hidden menu and select **Initiate PAR**. You may have to select a reason for the PAR from the pick list and change the dates for the "Period of Evaluation." You can then set up the PAR routing to include the evaluator who wishes to accomplish this PAR. After he completes the PAR, it will become part of the Provider's record and will be available to Reviewers and the PA at the Provider's gaining facility.

DRAFT

Appendix J - FAQs - Generating Ad-Hoc Credentials Reports

DRAFT