

## Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>1</b>
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 Users .....	2
1.5	User Resources.....	2
1.5.1	The Help Menu .....	2
1.5.2	MHS Help Desk.....	4
1.5.3	User Aids inside a CCQAS Record .....	4
<b>2</b>	<b>Overview of the CCQAS Credentialing and Privileging Process</b> .....	<b>8</b>
2.1	The CCQAS Single Credentials Record.....	8
2.2	The CCQAS Privilege Application.....	9
2.3	The CCQAS Privilege Application Review Process .....	10
<b>3</b>	<b>Creating and Maintaining CCQAS User Accounts</b> .....	<b>12</b>
3.1	Self Service Registration.....	12
3.2	Processing Requests for New User Accounts.....	16
3.2.1	Verifying Applicants' Need for Access to CCQAS .....	16
3.2.2	Processing the Application .....	16
3.2.3	CC/MSSP/CM-Generated Applications .....	19
3.2.4	User Accounts for New Provider Applicants.....	20
3.2.5	User Accounts for Module Users.....	22
3.2.6	Granting Module Access from Existing Provider Credentials Records .....	30
3.2.7	Granting Provider Access from Existing Provider Credentials Records .....	31
3.3	Adding Roles to Existing User Accounts .....	31
3.3.1	Adding the Provider Role to an Existing "Module User" Account .....	31
3.3.2	Adding "Module User" Role to an "Existing Provider User" Account.....	33
3.4	Deactivating and Reactivating User Accounts .....	36
3.4.1	Receiving a New Username and Temporary Password.....	39
3.4.2	Accessing CCQAS for the First Time .....	39
3.5	Maintaining CCQAS User Accounts .....	44
3.5.1	Updating User Personal and Contact Information .....	44
3.5.2	Password Reset .....	47
3.5.3	Locking and Unlocking User Accounts .....	47
<b>4</b>	<b>Managing Facility Privilege Lists</b> .....	<b>49</b>
4.1	The Privilege Management Function.....	49

4.2	Maintenance of Facility Privilege Catalogs .....	53
<b>5</b>	<b>Processing the E-Application for Clinical Privileges.....</b>	<b>55</b>
5.1	User Roles in the Privilege Process .....	55
5.2	The Work List.....	56
5.3	Notifications.....	57
5.4	Types of Electronic Privilege Applications .....	57
5.5	Initial Review of a Privilege Application .....	61
5.5.1	The Provider Summary Tab.....	62
5.5.2	The Position Tab .....	63
5.5.3	The Privileges Tab .....	65
5.5.4	The Documents Tab .....	66
5.5.5	The Comments Tab.....	68
5.5.6	Taking Action on a Privilege Application .....	69
5.5.7	Reassigning Ownership of an Application to Another CC/MSSP/CM .....	70
5.5.8	Taking Ownership of an Application from another CC/MSSP/CM.....	70
5.5.9	Setting an Application as Urgent .....	71
5.6	Routing a Privilege Application for Primary Source Verification.....	72
5.7	Primary Source Verification of a Privilege Application by CC/MSSP/CM.....	73
5.8	Primary Source Verification of a Privilege Application by the CVO .....	79
5.9	Building Workflow for Application Review .....	80
5.10	Tracking an Application in Review .....	83
5.11	Pulling an Application Out of the Review Process.....	85
5.12	Level 1 Review of an Application .....	86
5.13	Levels 2, 3, and 4 Review of an Application.....	92
5.14	Levels 5 or 6 (Committee) Review of an Application.....	93
5.15	Review of an Application by the PA .....	94
5.16	Completing the Application Approval Process.....	98
5.17	The Updated Provider Credentials Record .....	102
5.18	Managing Privileging Workload: The PAC Supervisor Role.....	106
<b>6</b>	<b>Managing Provider Credentials Records .....</b>	<b>109</b>
6.1	Creation of a New Record by the Credentials Staff.....	109
6.2	Searching for a Provider’s Credentials Record.....	112
6.2.1	Searching for Records within the Facility/Unit .....	112
6.2.2	Using the Advanced Search Function.....	116
6.2.3	Locating Provider Records at Other Facilities or Units.....	121
6.3	The Provider Credentials Record.....	122

6.3.1	The Profile Section .....	124
6.3.2	The Identification Section.....	127
6.3.3	The Contact Information Section.....	128
6.3.4	The License/Certification/Registration (Lic/Cert/Reg) Section .....	129
6.3.5	The Drug Enforcement Agency/Controlled Dangerous Substances Section.....	135
6.3.6	The Education/Training Section .....	136
6.3.7	The Specialty Section .....	142
6.3.8	The Affiliation Section .....	145
6.3.9	The Continuing Education Section .....	147
6.3.10	The Contingency Training Section .....	148
6.3.11	The Custody History Section .....	152
6.3.12	The Work History Section .....	152
6.3.13	The Privileges Section .....	155
6.3.14	The Documents Section .....	159
6.3.15	The Remarks Section .....	161
6.4	Updating Credentials Records Using Batch Processing .....	163
6.5	Deactivating a Credentials Record.....	165
6.6	Generating Provider Mailing Labels.....	166
6.7	The ICTB Transaction Table Entry .....	168
<b>7</b>	<b>Modification of Provider Credentials and Clinical Privileges .....</b>	<b>171</b>
7.1	Generating an Application for Modification or Augmentation of Privileges .....	171
7.2	Processing an Application for Modification or Augmentation of Privileges .....	173
<b>8</b>	<b>ICTB Process .....</b>	<b>176</b>
8.1	Requesting an ICTB by the Gaining Location.....	176
8.2	Initiating the ICTB at the Sending Location.....	178
8.3	The ICTB Assignment Record.....	183
8.4	The Transfer (ICTB) Application for Clinical Privileges.....	184
8.5	Processing an ICTB Transfer Application for Clinical Privileges.....	186
8.6	Cancelling an ICTB .....	188
8.7	Ending an ICTB .....	188
8.8	PAR for ICTB Duty .....	189
8.9	The ICTB Process for Navy Facilities .....	189
<b>9</b>	<b>Permanent Changes of Station Process.....</b>	<b>193</b>
9.1	Requesting a PCS by the Gaining Location.....	193
9.2	Initiating the PCS at the Sending Location.....	195
9.3	The Transfer (PCS) Application for Clinical Privileges.....	198
9.4	Processing a PCS Transfer Application for Clinical Privileges.....	199

9.5	Cancelling a PCS .....	199
9.6	Changes to the CCQAS User Account after a PCS Transaction .....	200
<b>10</b>	<b>Renewal of Clinical Privileges.....</b>	<b>202</b>
10.1	Auto-Generating an Application for Renewal of Clinical Privileges .....	202
10.2	Manually Generating a Renewal Application for Clinical Privileges .....	202
10.3	The Renewal Application .....	202
10.4	Processing an Application for Renewal of Clinical Privileges.....	202
<b>11</b>	<b>The Electronic PAR .....</b>	<b>203</b>
11.1	Automated Initiation of the PAR Process.....	203
11.2	Manual Initiation of the PAR Process .....	204
11.3	Routing of the PAR.....	204
11.4	Completing the PAR – The PAR Evaluator Role.....	206
11.5	Reviewing the PAR-The PAR Reviewer Role .....	215
11.6	Reviewing the PAR-The Provider Role.....	216
11.7	Bypassing the Automated PAR Process .....	217
11.8	Cancelling the Setup PAR Task.....	218
11.9	Canceling or Reassigning a PAR In-Process .....	219
<b>12</b>	<b>Generating Credentialing and Privileging Letters .....</b>	<b>221</b>
12.1	Command Parameters and MTF Contact Information for Letter Generation.....	221
12.2	Generating Letters for Individual Providers .....	221
12.2.1	Generating a Letter from Letters Menu .....	221
12.3	Generating Batch Letters .....	228
<b>13</b>	<b>Generating Standard Credentials and Privileging Reports.....</b>	<b>231</b>
13.1	Generating a Standard Credentials Report.....	231
13.2	Generating a Standard Privileging Report .....	241
13.3	Printing a Standard Report.....	243
13.4	Cancelling a Standard Report .....	244
13.5	Exporting a Report to Microsoft® Word or Excel .....	244
<b>14</b>	<b>Generating Ad-Hoc Credentials Reports.....</b>	<b>246</b>
14.1	Generating an Ad-Hoc Credentials Report.....	246
14.2	Saving an Ad-Hoc Report Query for Future Use.....	254
14.3	Running an Ad-Hoc Report from a Saved Query .....	255
14.4	Deleting a Saved Query .....	255

14.5	Printing an Ad-Hoc Report .....	256
14.6	Exporting an Ad-hoc Report to Microsoft® Word or Excel .....	256
14.7	Sample Ad-hoc Reports .....	257
<b>15</b>	<b>System Management.....</b>	<b>262</b>
15.1	Authority Tables .....	262
15.2	Command Parameters .....	263
15.3	MTF Contacts .....	266
15.4	Applicant Processing .....	267
15.5	User Processing.....	267
15.6	Change Start Page.....	267
15.7	Tracker Status .....	268
15.8	Provider Remarks.....	270
15.9	Broadcast Messaging .....	271
15.9.1	Incoming Broadcast Messages.....	273
15.9.2	Create New Broadcast Message.....	274
15.9.3	Broadcast Message and Custody Transfers .....	275
15.10	Messaging .....	276
<b>16</b>	<b>Branch Clinic Management .....</b>	<b>278</b>
16.1	Adding a Branch Clinic .....	278
16.2	Privileging at a Branch Clinic.....	280
<b>17</b>	<b>Custody Transfer .....</b>	<b>286</b>
17.1	Custody Transfer without PCS .....	286
17.1.1	Initiate Custody Transfer (Primary UIC).....	286
17.1.2	Request Custody Transfer.....	288
17.2	Custody Transfer with PCS .....	290
	<b>Appendix A. Frequently Asked Questions (FAQs).....</b>	<b>291</b>

## List of Tables

Table 1: Types of Electronic Privilege Applications .....	58
Table 2: Mapping of Data from the Credentials File to the Advanced Search Function.....	118
Table 3: Operators for Advanced Search Function.....	119
Table 4: Descriptions of CCQAS Standard Credentialing Reports .....	240
Table 5: Descriptions of CCQAS Standard Privileging Reports .....	242
Table 6: Mapping from the Credentials Record to Ad-hoc Report Wizard.....	248
Table 7: Operators for Ad-hoc Query Criteria.....	252
Table 8: Training Scenario 1.....	258
Table 9: Training Scenario 2.....	260
Table 10: Training Scenario 3.....	261

## List of Figures

Figure 1: Help Menu .....	3
Figure 2: Calendar Icon .....	4
Figure 3: Numerical Sort Function for Field Code .....	5
Figure 4: A–Z Sort Function for Field Description .....	6
Figure 5: Record Advance Keys .....	6
Figure 6: ‘Hidden Menu’ Button .....	7
Figure 7: Hidden Menu .....	7
Figure 8: Provider Credentials Record .....	8
Figure 9: Provider Privilege Application .....	9
Figure 10: Privilege Application Review Process .....	11
Figure 11: ‘CCQAS User Registration’ Button .....	13
Figure 12: CCQAS Privacy Act Statement.....	13
Figure 13: CCQAS Registration Screen .....	14
Figure 14: CCQAS Registration Screen – Provider Applicant.....	14
Figure 15: CCQAS User Registration Screen – Module User.....	15
Figure 16: AKO Email Address Message (Army Users).....	16

Figure 17: CCQAS Registration Confirmation Screen.....	16
Figure 18: New Applicant Message.....	17
Figure 19: Applicant Processing Menu Item .....	17
Figure 20: Applicant Processing Screen .....	17
Figure 21: Module User Application Screen .....	18
Figure 22: Module User Added Message .....	18
Figure 23: Module User Processing Menu Item.....	19
Figure 24: Module User Search Screen .....	19
Figure 25: Module User Application Screen .....	20
Figure 26: ‘Demographics’ Tab for a Provider Applicant.....	21
Figure 27: ‘MTF’ Tab for a Provider Applicant.....	22
Figure 28: ‘Permissions’ Tab for a Provider Applicant.....	22
Figure 29: ‘Demographics’ Tab for an Other (Module Users).....	23
Figure 30: ‘MTF’ Tab for a Module User .....	23
Figure 31: Privileging Roles/Permissions for a Module User .....	24
Figure 32: Credentials Roles.....	25
Figure 33: Credentials Supervisor Role.....	26
Figure 34: Privileging Roles .....	27
Figure 35: System Admin Permissions.....	28
Figure 36: “Superuser Admin” Role Permissions .....	28
Figure 37: Reporting Roles Permissions.....	29
Figure 38: “Superuser” Role Permissions.....	29
Figure 39: Grant Provider Access Menu Item .....	31
Figure 40: Similar User Account(s) Screen .....	32
Figure 41: ‘MTF’ Tab for a Dual User’s Account.....	33
Figure 42: User Search Screen.....	34
Figure 43: User Listing Screen after a Search .....	34
Figure 44: ‘MTF’ Tab for a Provider User Account.....	35
Figure 45: ‘MTF’ Tab for a Dual User’s Account.....	36
Figure 46: Deactivate Menu Item .....	37

Figure 47: Deactivate User Confirmation Message.....	37
Figure 48: Activate Menu Item.....	38
Figure 49: Activate User Confirmation Message .....	38
Figure 50: New Password Issued Message.....	39
Figure 51: CCQAS Privacy Act Statement.....	41
Figure 52: DoD Authentication Screen.....	41
Figure 53: Login Screen.....	42
Figure 54: Temporary Password Alert.....	42
Figure 55: Random Password Generator Screen .....	43
Figure 56: Security Briefing .....	44
Figure 57: User Profile Menu Item for a Module User .....	45
Figure 58: Update User Screen for Other (Module Users).....	45
Figure 59: User Processing Menu Item .....	46
Figure 60: User Search Screen.....	46
Figure 61: Reset Password Menu Item .....	47
Figure 62: Account Locked Indicator .....	48
Figure 63: CCQAS Privileging Management Menu Item .....	49
Figure 64: Privilege Management Screen and Category Pick List.....	50
Figure 65: Privilege List for Family Medicine .....	50
Figure 66: Examples of Family Medicine Core Privileges.....	51
Figure 67: View Privilege Menu Item .....	52
Figure 68: View Privilege Option.....	52
Figure 69: Limitations/Restrictions Option .....	53
Figure 70: Limitations/Restrictions View.....	53
Figure 71: Comment Option for Change to Privilege Designation .....	54
Figure 72: Privilege Audit Trail.....	54
Figure 73: Flagged Credentials.....	56
Figure 74: Work List Screen for the CC/MSSP/CM .....	56
Figure 75: Status, Role, and Date Options for Work List.....	57
Figure 76: My Applications Screen .....	59

Figure 77: My Application Hidden Menu .....	59
Figure 78: ‘Pending Applications’ Tab.....	59
Figure 79: Notification Log Screen .....	60
Figure 80: Reactivate Menu Item .....	61
Figure 81: Work List Task – Application Ready for Review .....	61
Figure 82: Assign PAC Screen .....	61
Figure 83: ‘Provider Summary’ Tab.....	62
Figure 84: ‘Expanded Provider Summary’ Tab.....	63
Figure 85: Provider Privilege Application ‘Position’ Tab.....	64
Figure 86: ‘Privileges’ Tab for General Dentistry .....	65
Figure 87: ‘Documents’ Tab for PAR Snapshot.....	66
Figure 88: ‘Documents’ Tab for Provider Documents.....	66
Figure 89: Add Documents Screen for CC/MSSP/CM .....	68
Figure 90: ‘Comments’ Tab.....	68
Figure 91: Add Comments Screen.....	69
Figure 92: Action Options for E-Applications.....	70
Figure 93: Re-assign Screen .....	70
Figure 94: ‘Application Reassignment’ Button .....	70
Figure 95: Application Reassignment Screen.....	71
Figure 96: Urgent Application Menu Item .....	71
Figure 97: Urgent Application Window .....	72
Figure 98: Urgent Application Confirmation Message .....	72
Figure 99: Urgent Application Task .....	72
Figure 100: Action Options for E-Applications.....	73
Figure 101: Select PSV Screen .....	73
Figure 102: Complete PSV Task .....	74
Figure 103: Assign PSV Screen.....	74
Figure 104: Provider PSV Summary Screen .....	74
Figure 105: PSV Information Section.....	76
Figure 106: NPDB/HIPDB Section .....	78

Figure 107: NPDB/HIPDB Update Warning Message.....	78
Figure 108: PSV Complete Message .....	79
Figure 109: PSV Complete/Action Required Task.....	80
Figure 110: ‘Application Routing’ Button.....	80
Figure 111: ‘Application Routing Summary’ Tab.....	81
Figure 112: ‘Application Routing UIC’ Tab .....	81
Figure 113: ‘Application Routing Summary’ Tab after Routing is Completed .....	82
Figure 114: In Review Status Indicator .....	84
Figure 115: ‘Task Log’ Tab.....	84
Figure 116: ‘Comments’ Tab.....	85
Figure 117: Retrieving an Application in Review .....	86
Figure 118: Work List for a Level 1 Reviewer.....	86
Figure 119: ‘Privileges’ Tab for a Level 1 Reviewer .....	87
Figure 120: Reviewer Comment Screen.....	88
Figure 121: Reviewer Recommendation Screen.....	90
Figure 122: Application Returned/Action Required Task .....	90
Figure 123: ‘Comments’ Tab of a Returned Application .....	90
Figure 124: Recommendation Detail Screen .....	91
Figure 125: Return to Provider Screen .....	91
Figure 126: Yellow Diamond Icon for Review Levels 2-6 .....	92
Figure 127: Recommendation Count Menu Item .....	93
Figure 128: Recommendation Count Screen .....	93
Figure 129: ‘Privileges’ Tab for Privileging Authority Review.....	95
Figure 130: PA Review Complete Button .....	96
Figure 131: PA Decision Screen.....	97
Figure 132: ‘Notifications’ Button.....	98
Figure 133: Notification Routing Screen.....	98
Figure 134: Provider ‘Acknowledge’ Button on Summary Page .....	99
Figure 135: Privileged Provider Information Report.....	100
Figure 136: Provider “Acknowledgment” Page .....	100

Figure 137: Provider Acknowledgement Notification.....	101
Figure 138: ‘Complete’ Button.....	101
Figure 139: ‘My Applications’ Tab with Completed Applications .....	101
Figure 140: Editable Data at Primary UIC .....	102
Figure 141: Read-Only Data at Non-Primary UIC .....	103
Figure 142: Privileges Section in the Credentials Record .....	103
Figure 143: Privileged Provider Information Report.....	104
Figure 144: Selecting to View Provider Privileges.....	104
Figure 145: Provider Privileges .....	105
Figure 146: PAC Supervisor Role on the ‘Roles/Permissions’ Tab.....	106
Figure 147: Submitted Applications Screen .....	107
Figure 148: Application Reassignment Screen.....	107
Figure 149: Re-Assign CC/CM/MSSP Screen .....	108
Figure 150: Reassign Confirmation Screen .....	108
Figure 151: Provider Search Menu Item.....	109
Figure 152: Credentials Search Screen .....	110
Figure 153: Add Provider Screen with SSN.....	110
Figure 154: Add Provider Screen with FIN (Unique ID) .....	110
Figure 155: Matching Person Identifier Message.....	112
Figure 156: Credentials Provider Search Screen .....	113
Figure 157: Search Result Screen .....	116
Figure 158: Advanced Search Screen .....	117
Figure 159: Example Query Using Advanced Search Functionality.....	121
Figure 160: Provider Locator Function.....	121
Figure 161: Provider Locator Search Results screen.....	122
Figure 162: Opening a Credentials Record.....	123
Figure 163: Navigation Bar .....	123
Figure 164: Navigation Bar Expanded .....	124
Figure 165: Profile Section .....	125
Figure 166: Profile Section, Upload, Edit Photo .....	126

Figure 167: Military Section of Profile.....	127
Figure 168: Identification Section .....	127
Figure 169: Add Identification Screen.....	128
Figure 170: Contact Information Section .....	128
Figure 171: Updating a Primary Phone Number .....	129
Figure 172: Lic/Cert/Reg Section .....	129
Figure 173: State License/Certification/Registration Screen.....	130
Figure 174: Social Workers License Level Information.....	131
Figure 175: Admin Waiver Field.....	132
Figure 176: National Certification/Registration Screen .....	133
Figure 177: Unlicensed Information Screen .....	135
Figure 178: DEA/CDS Section.....	136
Figure 179: DEA/CDS Screen .....	136
Figure 180: Education/Training Section.....	137
Figure 181: Qualifying Degree Record.....	137
Figure 182: Institution Search Screen.....	138
Figure 183: ‘Post Graduate Training’ Tab.....	139
Figure 184: Post Graduate Training Record .....	140
Figure 185: ECFMG Checkbox .....	141
Figure 186: ECFMG Page .....	142
Figure 187: Specialty Section .....	143
Figure 188: Adding a Specialty .....	143
Figure 189: Board Certification Section .....	144
Figure 190: Board Search Screen .....	145
Figure 191: Affiliation Section .....	145
Figure 192: ‘Academic Affiliations’ Tab .....	146
Figure 193: ‘Organizational Memberships’ Tab.....	147
Figure 194: Continuing Education Section.....	147
Figure 195: Continuing Education Record .....	148
Figure 196: Contingency Training Section.....	148

Figure 197: Contingency Training Record .....	149
Figure 198: References Section .....	149
Figure 199: Reference Record .....	150
Figure 200: Databank Queries Section .....	151
Figure 201: Custody History Section.....	152
Figure 202: Work History Section.....	152
Figure 203: ‘Assignment’ Tab .....	153
Figure 204: MTF Assignment Record .....	153
Figure 205: ‘Work History Privileges’ Tab.....	155
Figure 206: ‘Tracker Status’ Tab.....	155
Figure 207: Privileges Section .....	155
Figure 208: Provider Privileges Screen .....	156
Figure 209: Document Section, PARs/Snapshot .....	157
Figure 210: Privileged Provider Information Report.....	158
Figure 211: Documents Section.....	159
Figure 212: PARs/Snapshots Listing .....	160
Figure 213: Remarks Section.....	161
Figure 214: Provider Remarks Section .....	161
Figure 215: Provider Remarks Window .....	162
Figure 216: Provider Remarks Type Screen.....	162
Figure 217: Provider Remarks Type Screen.....	162
Figure 218: Provider Remarks Type Screen.....	163
Figure 219: Provider Remarks Menu Options .....	163
Figure 220: Credentialing Batch Process Menu .....	164
Figure 221: Action Section of the Credentials Provider Search Screen .....	164
Figure 222: Continuing Education Batch Training Screen.....	165
Figure 223: Deactivate Provider Menu Item .....	166
Figure 224: Deactivate Provider Screen .....	166
Figure 225: ‘Provider Mailing Label’ Radio Button .....	167
Figure 226: ‘Batch Labels’ Tab .....	167

Figure 227: Batch Labels Options (i.e., Mailing Labels) .....	168
Figure 228: New Incoming Credentials Transaction Window .....	168
Figure 229: Accessing the Transaction Table.....	169
Figure 230: The Provider Transactions Screen for an Incoming ICTB .....	170
Figure 231: Request Modification Menu Item.....	172
Figure 232: Application Modification Instructions Screen .....	172
Figure 233: Provider Application (Modification).....	173
Figure 234: Provider Task – Complete Application, Modification .....	173
Figure 235: CC/MSSP/CM Task – Application Ready to Review, Modification.....	174
Figure 236: Flagged Privileges on the Modification Application .....	174
Figure 237: Assignment Menu Item on the Provider Locator, Search Results Tab .....	177
Figure 238: Request ICTB Action on Assignment Screen .....	177
Figure 239: Request ICTB Broadcast Message at Gaining Location .....	177
Figure 240: Work History Section on Navigation Menu.....	178
Figure 241: Initiate ICTB Menu Option .....	179
Figure 242: ICTB Form .....	180
Figure 243: Email Address and Phone Number Fields for User Account.....	182
Figure 244: Work History, Assignments tab for the Sending Location .....	183
Figure 245: Work History, Assignment tab for the Gaining Location .....	183
Figure 246: Provider Task – Complete Application, Transfer (ICTB).....	184
Figure 247: Transfer (ICTB) Application for Privileges .....	185
Figure 248: Gaining CC/MSSP/CM’s Pending Applications Tab .....	186
Figure 249: Gaining CC/MSSP/CM Task – Transfer (ICTB) Application .....	187
Figure 250: Cancel ICTB Menu Item .....	188
Figure 251: End ICTB Menu Item.....	189
Figure 252: Gaining CC/MSSP/CM Task – Setup PAR .....	189
Figure 253: ICTB Privilege Request Screen.....	190
Figure 254: Appendix Q Letter.....	191
Figure 255: E-Signed Appendix Q .....	191
Figure 256: Assignment Menu Item on the ‘Provider Locator’ Tab .....	194

Figure 257: Request PCS Action on Assignment tab .....	194
Figure 258: Request PCS Broadcast Message at Requesting Location .....	194
Figure 259: Open Menu Item.....	195
Figure 260: Initiate PCS Menu Option .....	196
Figure 261: Initiate PCS Prompts Screen .....	196
Figure 262: Initiate PCS Screen for additional fields for Provider User Account.....	196
Figure 263: New Incoming Message Alert.....	198
Figure 264: Provider Task – Complete Application, Transfer (PCS).....	198
Figure 265: Transfer (PCS) Application for Privileges .....	199
Figure 266: Gaining CC/MSSP/CM ‘Pending Applications’ Tab.....	199
Figure 267: Cancel PCS Menu .....	200
Figure 268: Outstanding Tasks Warning Message .....	200
Figure 269: Provider Application (Renewal).....	202
Figure 270: CC/MSSP/CM Work List Item – Setup PAR .....	203
Figure 271: Initiate PAR Menu Item .....	204
Figure 272: PAR Routing Screen .....	205
Figure 273: PAR Evaluator Work List Task – Complete PAR .....	206
Figure 274: Profile Section of the PAR .....	207
Figure 275: Privileges Evaluated Section for PAR.....	207
Figure 276: Privileges Evaluated Section for the PAR with Unacceptable.....	208
Figure 277: Privileges Evaluated Section for the PAR.....	208
Figure 278: Quality Management Measures Section of the PAR.....	209
Figure 279: Types of Quality Management Measures.....	209
Figure 280: Facility-Wide Measures Section of the PAR .....	210
Figure 281: Types of Facility-Wide Measures .....	210
Figure 282: Practice Volume Section of the PAR .....	211
Figure 283: Professional Development Section of the PAR.....	211
Figure 284: Clinical/Technical Performance Questions Section of the PAR.....	212
Figure 285: Personal Evaluation Questions Section of the PAR.....	213
Figure 286: PAR Summary Form .....	214

Figure 287: E-Signature Section of the PAR .....	214
Figure 288: E-Signature Confirmation Screen .....	215
Figure 289: PAR Reviewer Work List Task – Review PAR.....	215
Figure 290: PAR Reviewer E-Signature Screen.....	216
Figure 291: Provider Work List Task – Review PAR .....	216
Figure 292: Provider E-Signature Screen .....	217
Figure 293: ‘Offline PAR’ Radio Button.....	217
Figure 294: Evaluator Work List Task – Complete Offline PAR .....	218
Figure 295: Offline PAR Notification .....	218
Figure 296: ‘Cancel PAR’ Button.....	218
Figure 297: Complete PAR Task Menu Options .....	219
Figure 298: Cancel PAR Warning Message .....	220
Figure 299: Re-assign Task Window.....	220
Figure 300: Letters Menu Item, Provider Search.....	221
Figure 301: Pre-Populated Privileging Application Letter Transfer Message.....	222
Figure 302: Letters Menu item, Work History, Assignments Tab .....	222
Figure 303: Generate Letter Menu.....	223
Figure 304: DEA Multi–Purpose Letters .....	223
Figure 305: DEA Initial Application Form License Selection .....	224
Figure 306: Initial Application Letter .....	224
Figure 307: Notification of Change of Station .....	225
Figure 308: Notification of Change of Station Letter.....	225
Figure 309: Return of Military DEA Registration Certificate .....	226
Figure 310: Return of Military DEA Registration Certificate Letter .....	226
Figure 311: Expired Credentials Letters Selections.....	227
Figure 312: Pre-Populated Privileging Letter with Privilege Categories .....	228
Figure 313: Action Section of the Credentials Provider Search Screen .....	229
Figure 314: Batch ICTB Letter Screen .....	229
Figure 315: Additional ICTB Information Screen.....	230
Figure 316: ICTB Batch Letter .....	230

Figure 317: Accessing the CCQAS Standard Credentialing Reports .....	231
Figure 318: List of Standard Credentials Reports.....	231
Figure 319: Parameter Screen for the Contingency Training Expiration report.....	232
Figure 320: Example of Contingency Training Expiration report Parameter Screen.....	240
Figure 321: Reporting Options .....	241
Figure 322: Accessing the CCQAS Standard Privileging Reports.....	241
Figure 323: List of Standard Privileging Reports.....	241
Figure 324: Provider Privilege report Parameters Screen.....	242
Figure 325: Sample Provider Privilege report results.....	243
Figure 326: Exporting a Report to Word or Excel.....	244
Figure 327: QA Statement .....	244
Figure 328: Data Copied Message Window .....	244
Figure 329: Sample Excel Spreadsheet with CCQAS Report .....	245
Figure 330: Ad-hoc Reporting Menu for Credentialing .....	246
Figure 331: First Screen of the Ad-hoc Report Wizard.....	247
Figure 332: Provider Tab of the Ad-Hoc Report Wizard .....	249
Figure 333: The Specialty Tab of the Ad-Hoc Report Wizard.....	250
Figure 334: The Assignment/Work History Tab of the Ad-Hoc Report Wizard .....	250
Figure 335: Third Screen of the Ad-hoc Report Wizard .....	251
Figure 336: ‘AND’ and ‘OR’ Operators Selections .....	252
Figure 337: Example of Multiple Query Criteria, Ad-hoc Report Wizard.....	253
Figure 338: Action Options for a Report .....	254
Figure 339: Query Processing Screen to Save or Delete Query .....	255
Figure 340: Recall Saved Query Screen .....	255
Figure 341: Recall Saved Query Name Screen.....	255
Figure 342: Delete Query Confirmation Message .....	256
Figure 343: Copy Data to Memory for Import into Word or Excel.....	256
Figure 344: QA Statement .....	257
Figure 345: Data Copied Message Window .....	257
Figure 346: System Menu.....	262

Figure 347: Authority Tables Menu Option .....	262
Figure 348: CW and LU Mappings/Values for Display .....	263
Figure 349: Command Parameters Menu Option .....	263
Figure 350: Command Parameters Page.....	264
Figure 351: Renewal Days Parameters on the Command Parameters Screen.....	265
Figure 352: Provider Work List Item – Complete Renewal Application .....	265
Figure 353: Exp. Credentials Notice Days on the Command Parameters Screen .....	266
Figure 354: MTF Contacts Menu Option .....	266
Figure 355: Editable MTF Contacts Screen.....	267
Figure 356: Change Start Page Menu Option.....	268
Figure 357: ‘Change Start Page’ Drop-down Menu Options .....	268
Figure 358: Tracker Status Menu Option .....	269
Figure 359: Tracker Status Screen.....	269
Figure 360: Provide Remarks Menu Option.....	270
Figure 361: Provider Remarks Screen .....	270
Figure 362: Provider Remarks Type Screen (Description).....	270
Figure 363: Provider Remarks Type Screen.....	271
Figure 364: New Incoming Broadcast Message Alert.....	271
Figure 365: Broadcast Messages Menu Option .....	272
Figure 366: Broadcast Message Screen .....	272
Figure 367: New Incoming Broadcast Message Alert for Sending Location.....	273
Figure 368: Broadcast Messages Menu Item at the Sending Location.....	274
Figure 369: Broadcast Message Menu Item .....	274
Figure 370: Create Message Page.....	275
Figure 371: Messaging Menu Option .....	276
Figure 372: Email Notification Screen .....	277
Figure 373: MTF Contacts List.....	278
Figure 374: UIC Selection for Branch Clinic .....	278
Figure 375: Add Branch Clinic.....	279
Figure 376: Branch Clinic Record .....	279

Figure 377: Delete Branch Clinic .....	280
Figure 378: Branch Clinics on 'Position' Tab for Provider E-App .....	281
Figure 379: Privileges Section for Branch Clinics .....	281
Figure 380: Reviewer Routing Page .....	282
Figure 381: Reviewer Routing Page for Branch Clinic .....	282
Figure 382: Summary Page for Reviewer Routing .....	283
Figure 383: PA Review of Privileges for Parent/Branch Clinics .....	283
Figure 384: PA Decision Review Complete Screen .....	284
Figure 385: PA Decision Screen .....	285
Figure 386: Initiate Custody Transfer Option from Hidden Menu .....	286
Figure 387: Initiate Custody Transfer Screen .....	287
Figure 388: Custody Transfer Confirmations .....	287
Figure 389: Custody Transfer in Provider Transaction .....	288
Figure 390: Request Custody Transfer Option in Hidden Menu .....	289
Figure 391: Request Custody Transfer Broadcast Message Screen .....	289
Figure 392: Confirmation Message .....	290

# 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 previous version may use this guide as a reference to understand the latest version, 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, maintenance of credentials records, and online privilege applications. 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 office.

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 are due to modifications and enhancements made after this document was prepared.

## 1.3 System Overview

CCQAS is a standard Department of Defense (DoD) 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 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 as defined in DoD 6025.13 series.

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 all military and civilian health care providers, including Active Duty, Reserves, and National Guard
- Contains comprehensive Provider demographic, specialty, licensing, training, education, privileges, 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, The Joint Commission (TJC) and the Accreditation Association for Ambulatory Health Care (AAAHC) requirements
- Improves the ability of the Services to respond to medical readiness requirements

#### 1.4 Hardware and Software Requirements for CCQAS 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) Web browser (see [CCQAS logon page for version requirements](#)). CCQAS is not compatible with other Internet browsers or non PC hardware. CAC middleware software is required to access or to use CCQAS. Contact your local system administrator for questions related to CAC middleware.

**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.



**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 User Manuals Link**

This link takes users to read-only versions of this and other CCQAS user documentation. 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.

#### **1.5.1.3 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.

#### **1.5.1.4 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.

### 1.5.1.5 Submit Trouble Ticket Link

This link opens a window that enables CCQAS users to submit 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 Military Health System (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](mailto:mhssc@tma.csd.mil). Users are advised to contact their local CC/MSSP/CM ('CC' stands for Credentials Coordinator [Army]/'MSSP' stands for Medical Staff Services Professional [Navy]/'CM' stands for Credentials Manager [Air Force]), local information technology (IT), and/or their Service-level database administrator (DBA) 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 2.

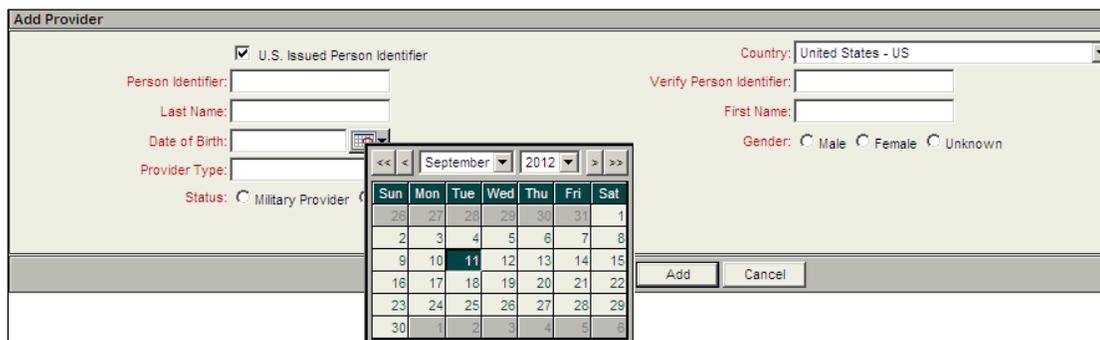


Figure 2: Calendar Icon

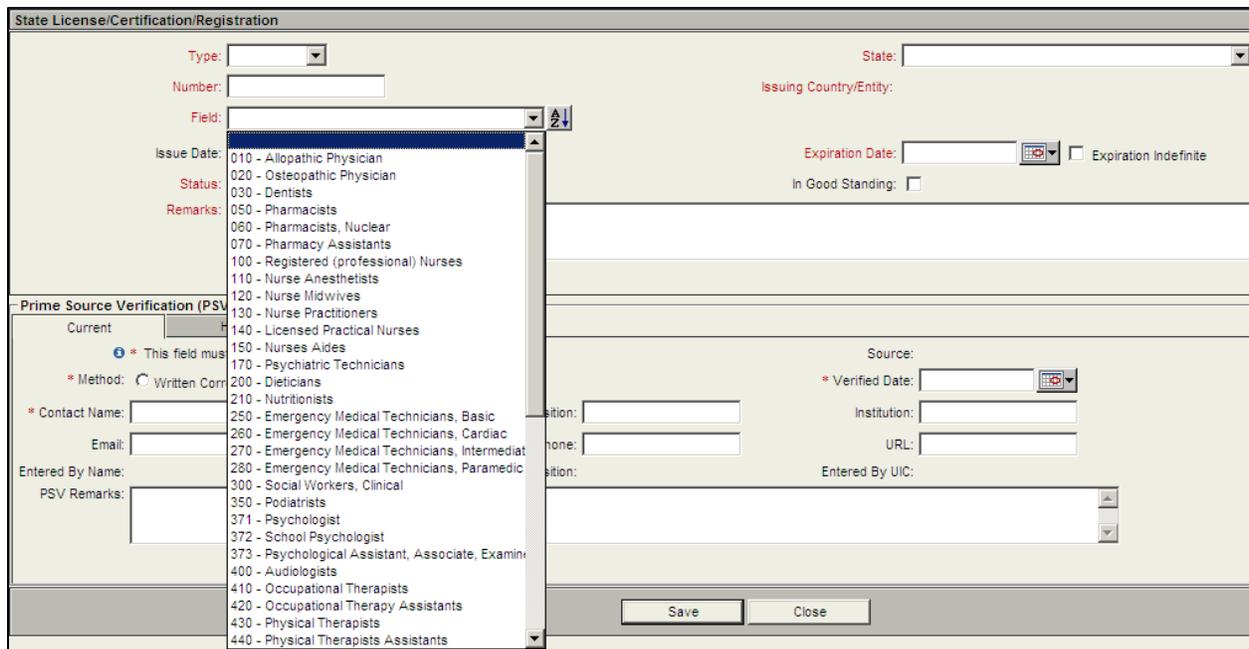
To enter the desired date, users first select the year and month from the pick lists at the top of the calendar. After users select the correct year and month, they click the desired day of the month. When users select the day, the calendar function automatically closes and the selected date populates 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.

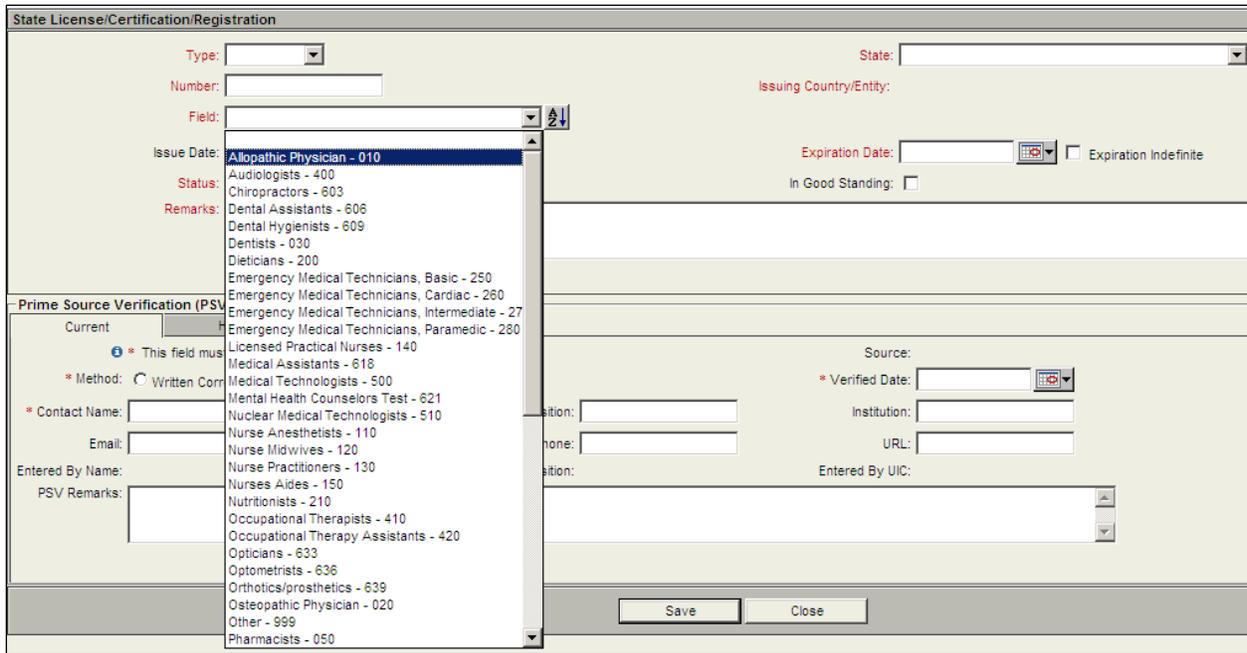
### 1.5.3.3 The A-Z Sort Function

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 3 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 3: Numerical 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 4.

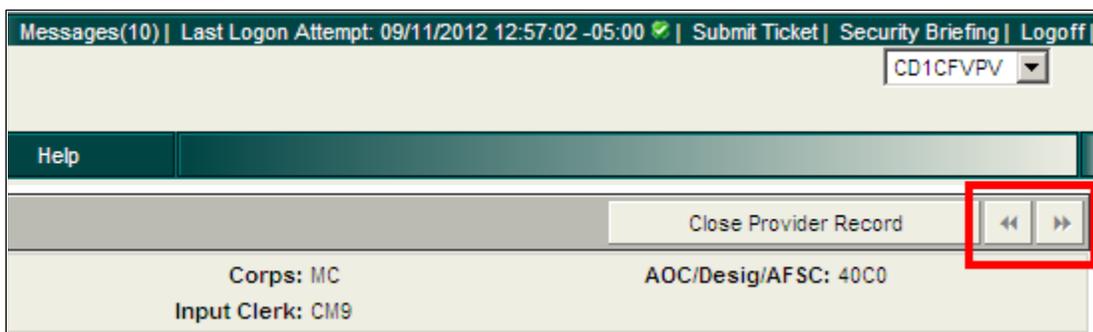


**Figure 4: A–Z Sort Function for Field Description**

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 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 5.



**Figure 5: Record Advance Keys**

### 1.5.3.5 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 6 depicts the **Hidden Menu** button next to a sample record.

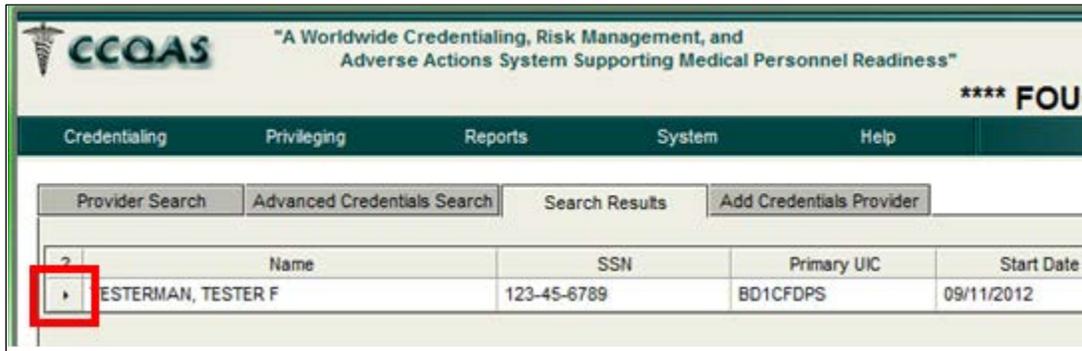


Figure 6: 'Hidden Menu' Button

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 7.

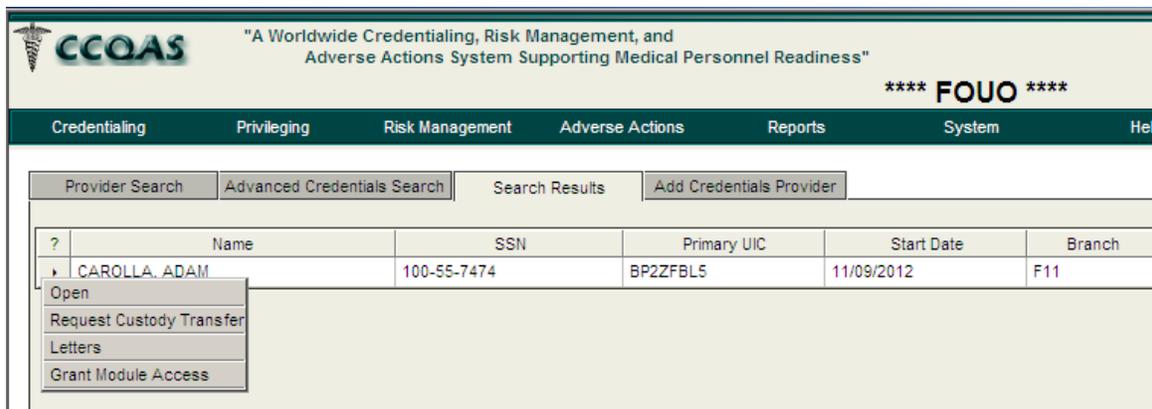


Figure 7: Hidden Menu

## 2 Overview of the CCQAS Credentialing and Privileging Process

Credentialing and privileging are processes in which health care provider's education, training, experience, and other credentials are verified and assessed prior to providing health care services in the Military Health System. 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 Single 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 single 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. A single 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 8. Each section of the credentials record is discussed in detail in Section 6, Managing Provider Credentials Records.

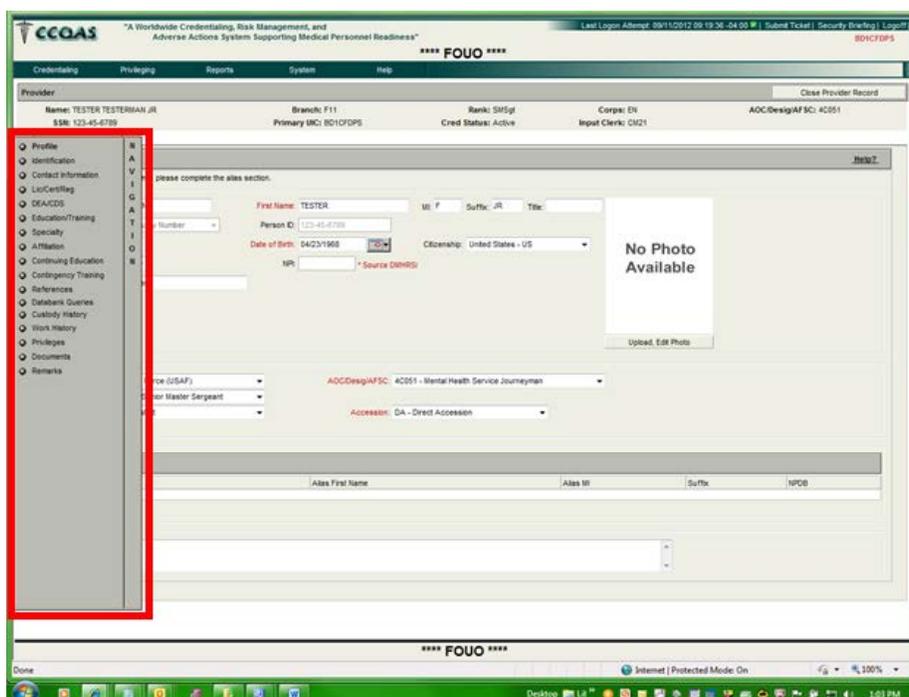
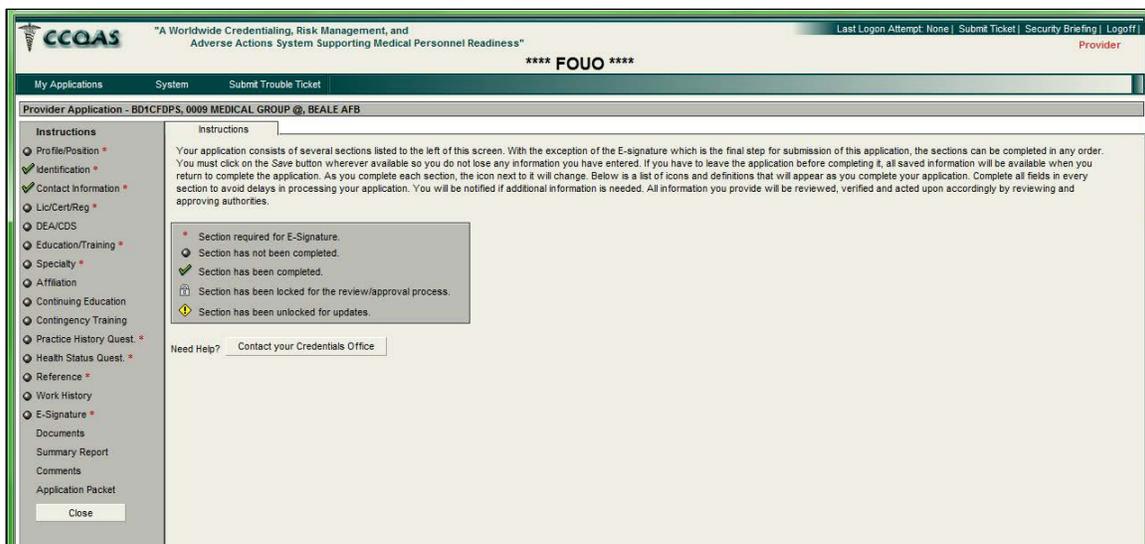


Figure 8: Provider Credentials Record

A single 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. Data may only be directly entered into a credentials record by the facility credentials staff at the primary or custodial UIC. For non-primary UICs, updates can only be made to assignment specific data or upload documents. This process is discussed in detail in [Section 6](#).

## 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 (CLP Administrator role) 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 9 depicts the structure and content of a sample Provider privilege application.



**Figure 9: 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 Processing the E-Application for Clinical Privileges.

A privilege application is only 'active' while privileging is in process. After a privilege application is approved by the Privileging Authority (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 "CC/MSSP/CM." Other roles are also defined for individuals involved in the PAR process.

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

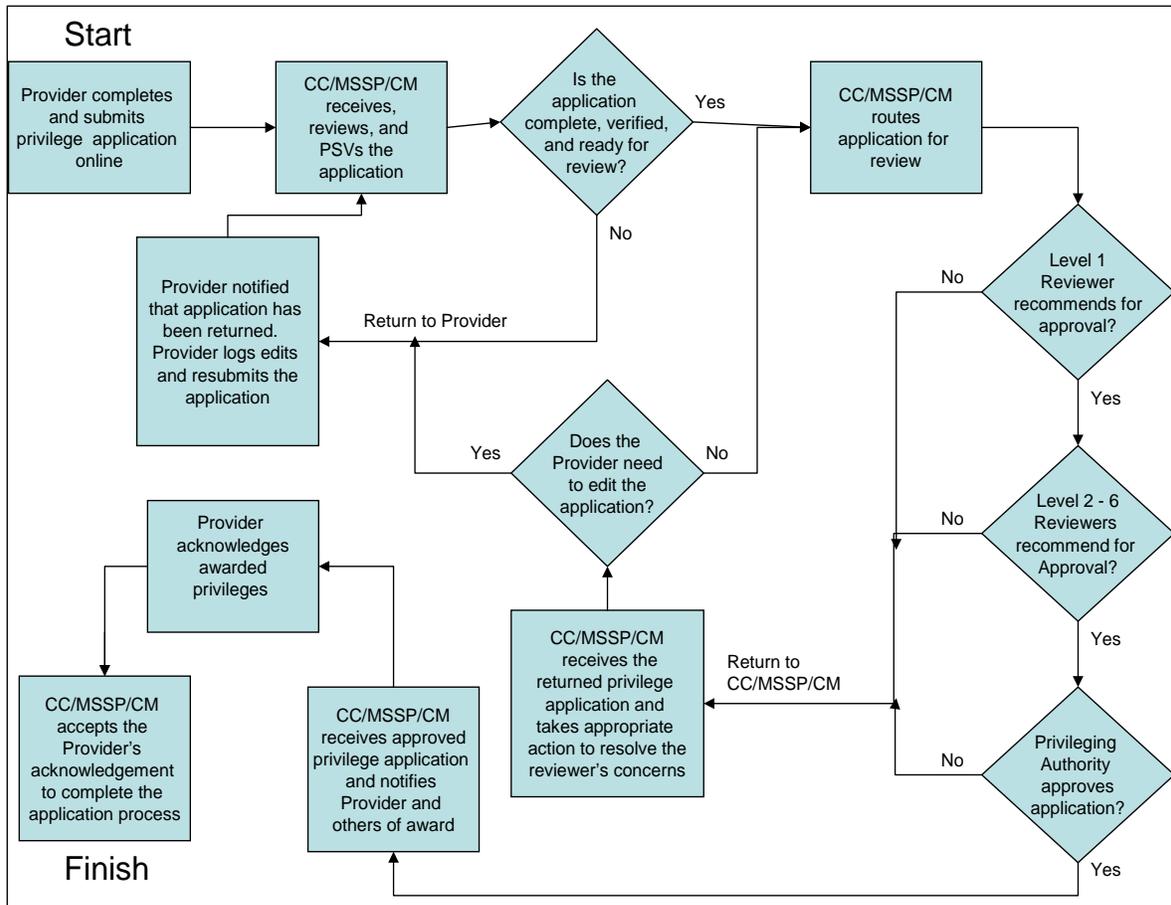
- A Provider completes and submits his or her application for clinical privileges online.
- The assigned CC/MSSP/CM receives, reviews, and performs the required PSV on the application. In Air Force facilities, the PSV may also be performed by a Centralized Verification Office (CVO). Following completion 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(ies) in which the Provider is requesting privileges.
- The Level 1 Reviewer issues his or her 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 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 10.

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 PA. 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 requested privileges. It is important to note that CCQAS is designed to facilitate the forward processing and award/denial of clinical privileges. If a decision is made to deny a Provider’s request for clinical privileges, consult your service policy to ensure the Provider’s rights to due process are preserved.



**Figure 10: Privilege Application Review Process**

### 3 Creating and Maintaining CCQAS 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/contact information, job responsibilities, or location. Guidance regarding updating user information, roles/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.” New user accounts must be created for individuals involved in the privileging process, including Providers, Reviewers, the PA, and those who are responsible for assessing performance of their clinical staff. 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 Common Access Card (CAC) or Personal Identity Verification (PIV) card to access the site.

The self-registration process begins when users click the **Registration** button on the left-hand side of the screen, as depicted in Figure 11.

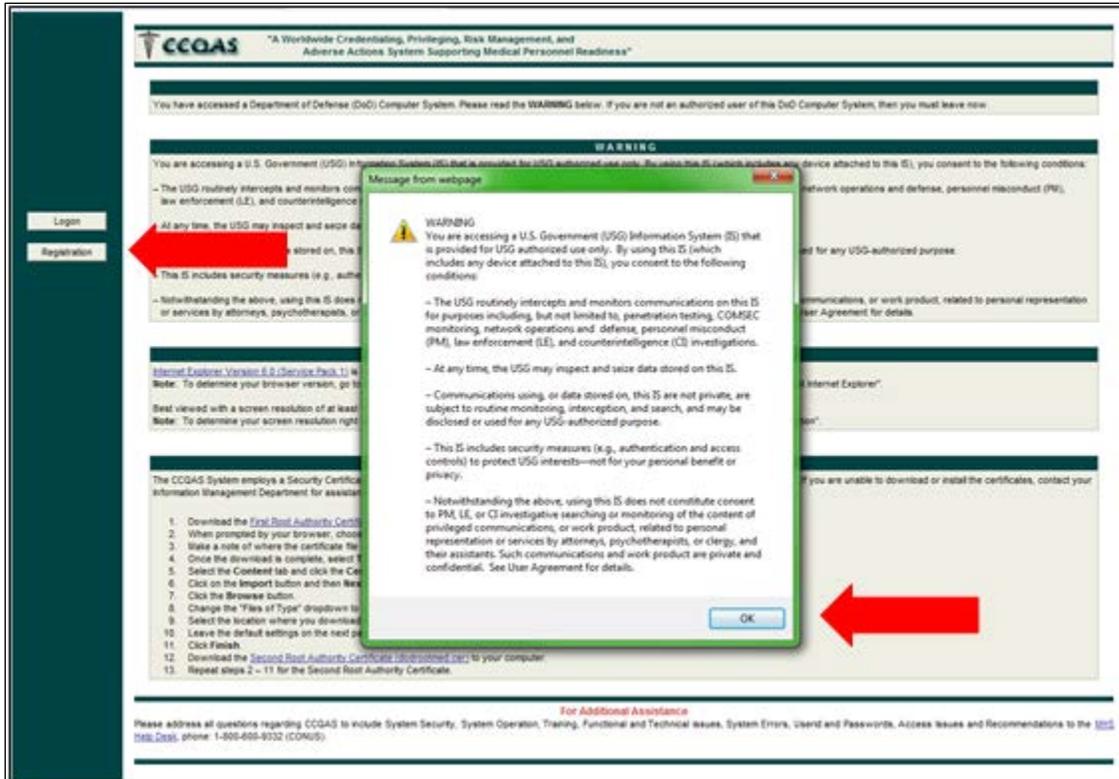


Figure 11: 'CCQAS User Registration' Button

Before completing a registration, users must read and verify the CCQAS Privacy Act Statement by selecting the **Affirmative** radio button, as depicted in Figure 12. The system does not allow prospective registrants to continue unless they select this radio button.

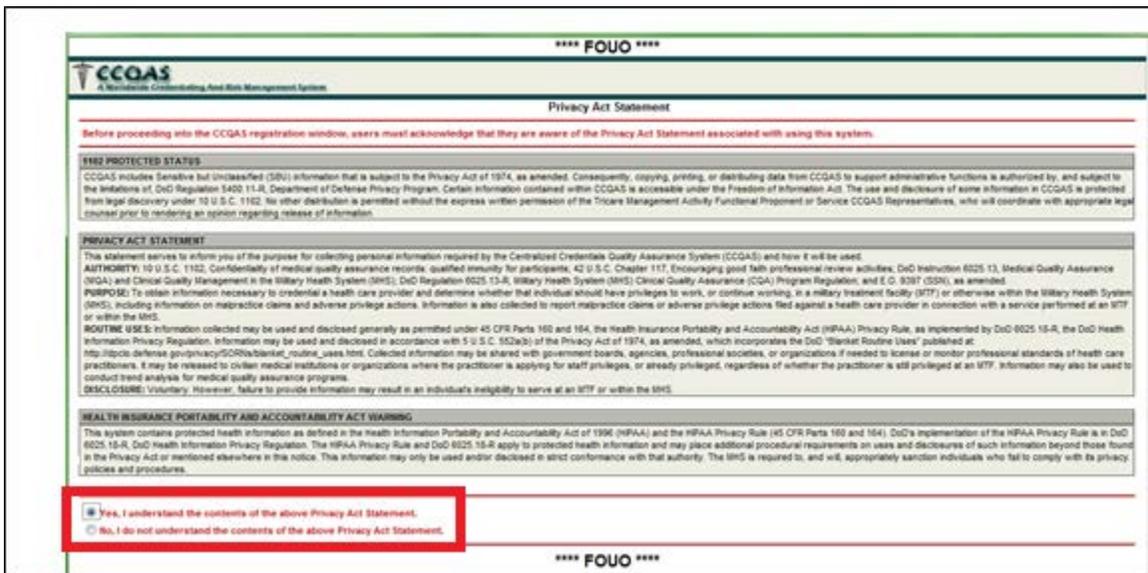


Figure 12: CCQAS Privacy Act Statement

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 13.

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**.

Figure 13: 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 14 depicts the **CCQAS Registration** screen.

Figure 14: 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, 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 15) 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 the CCQAS User Registration screen for a Module User. At the top, it says "FOUO" and "INSTRUCTIONS". Below that, there's a paragraph explaining the process. The "REGISTRATION" section is divided into three parts: "System Request", "User Information", and "Registration Validation".

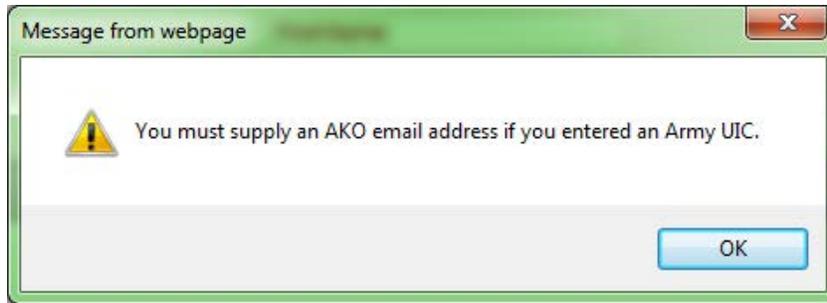
- System Request:** "User Type" is set to "Module User". "Access" checkboxes are checked for "Credentialing" and "Privileging", and unchecked for "Risk Mgt" and "Adverse Actions". "UIC" is "BD1CFDPS".
- User Information:** "Person ID Type" is "Social Security Number". "Person ID" is masked with asterisks. "Last Name" is "Tull". "Gender" is "Male". "Phone Type" is "None". "Confirm Person ID" is masked. "First Name" is "Jethro". "Middle Initial" is empty. "Birth Date" is "09/18/1966". "Phone" is "(202) 555-7090". "Email" is "email@email.com".
- Registration Validation:** "Last Name" is "Aquelung". "Comm Phone" is "(202) 555-4567". "Comm Fax" is empty. "First Name" is "Michael". "Middle Name" is empty. "DSN Phone" and "DSN Fax" are empty. "Email" and "Rank/Position" are empty.

At the bottom, there are buttons for "Submit", "Reset", "Print Form", and "Cancel". The "Submit" button is highlighted with a red box. The page ends with "FOUO".

Figure 15: 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.

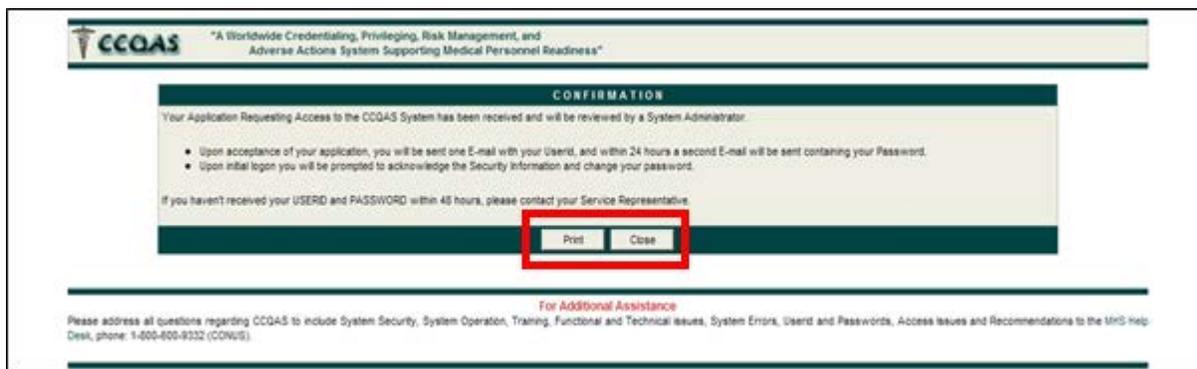
Though not all remaining fields on the form are labeled as **required**, applicants should be encouraged to populate the form as much as possible, since CC/MSSP/CMs use the information on this form to verify an applicant's identity and need for system access. **An accurate email address is critical**,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



**Figure 16: AKO Email Address Message (Army Users)**

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. 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 processing 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.

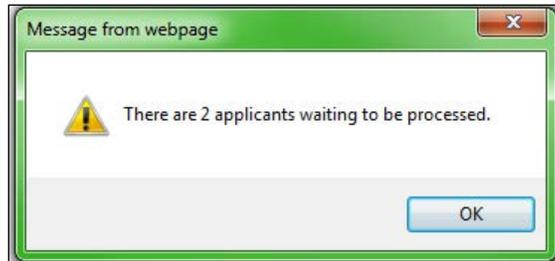
### 3.2.2 Processing the Application

There are three different user types in CCQAS:

- **Provider User** – User with a credentials record and a privileging application.
- **Module User** – User with no credentials record, but access to one or more CCQAS Modules.

- **Dual User** – User with a credentials record, privileging application, and access to one or more CCQAS modules.

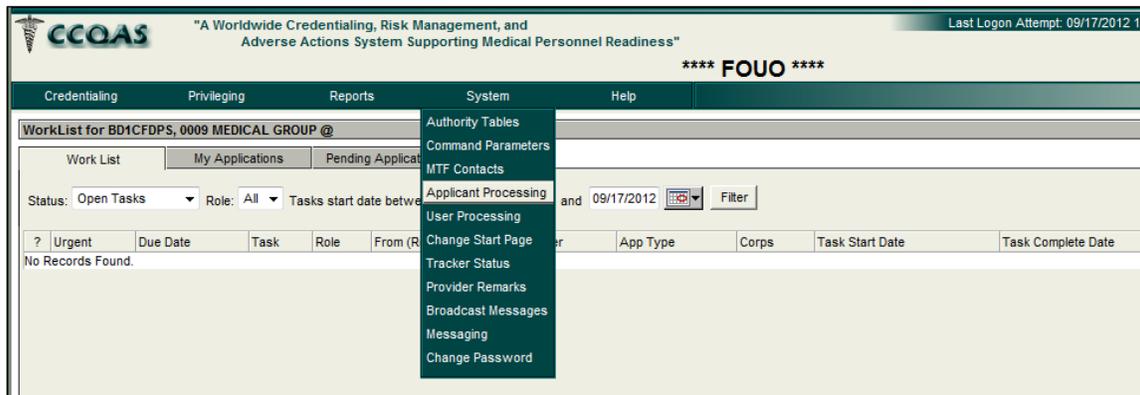
CCQAS alerts CC/MSSP/CMs to new requests for user accounts with a message, as depicted in Figure 18. This message displays when CC/MSSP/CMs log in to CCQAS.



**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.

**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.



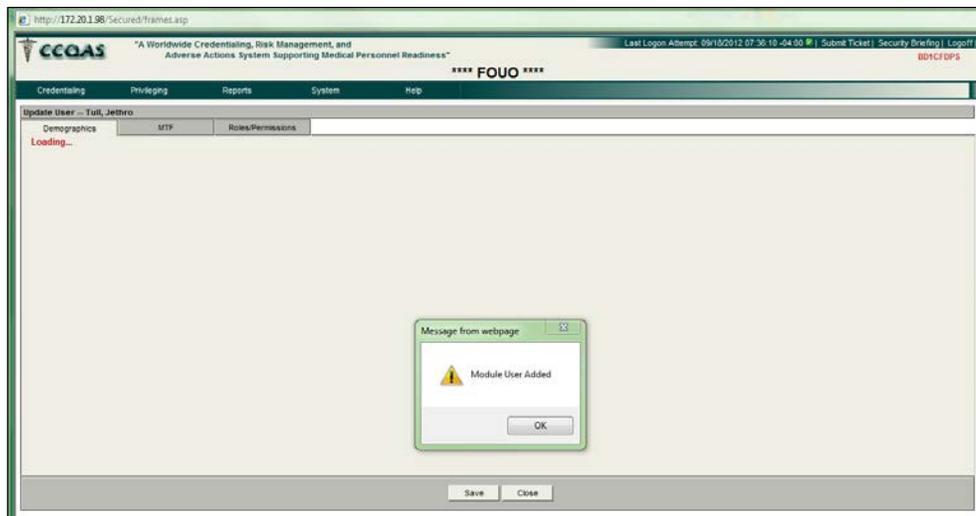
**Figure 20: Applicant Processing Screen**

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



**Figure 21: Module User Application Screen**

When CC/MSSP/CMs select **Process**, they receive a message, as depicted in Figure 22. 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 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: Module 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 40).

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 not create multiple user accounts for the same individual.

### 3.2.3 CC/MSSP/CM-Generated Applications

CC/MSSP/CMs may wish to create the CCQAS Module 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 depicts the selection of the Module **User Processing** menu item.

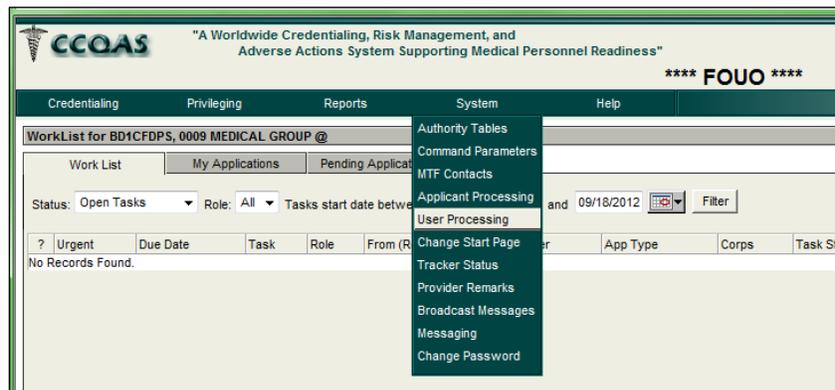


Figure 23: Module User Processing Menu Item

The Module **User Search** screen appears, as depicted in Figure 24. 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.

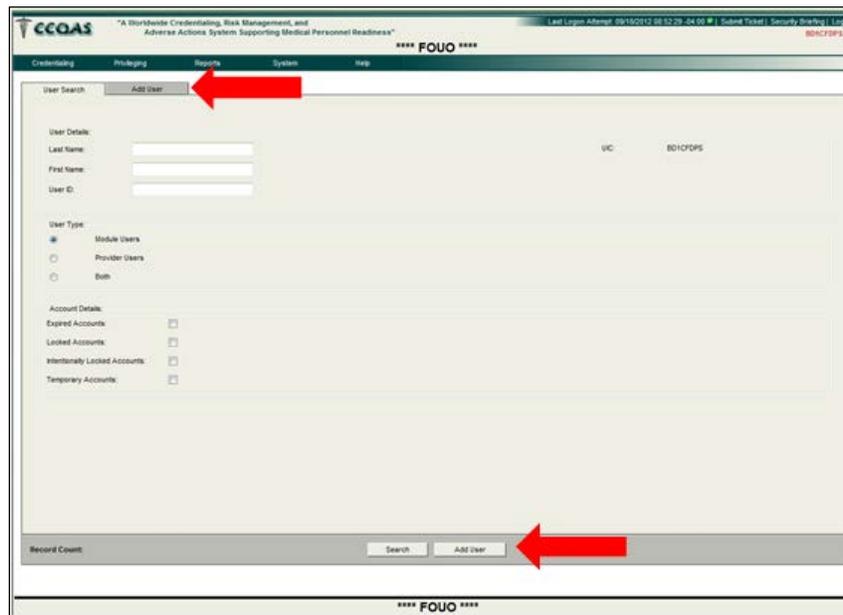


Figure 24: Module User Search Screen

The Module **User Application** screen appears, as depicted in Figure 25. 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: Module User Application Screen**

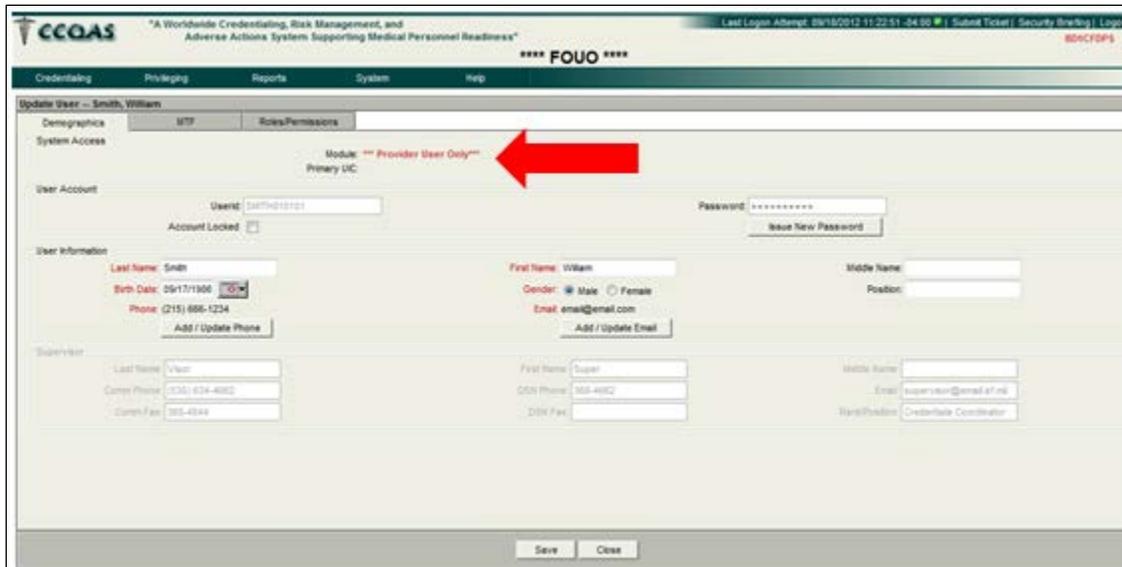
**Note:** From this point forward, the application process is the same regardless of whether the applicant applied for the user account via the **Self-Service Registration** screen, or the user account was created by a CC/MSSP/CM through the Module **User Processing** screen.

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 40. 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 not create 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.

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.

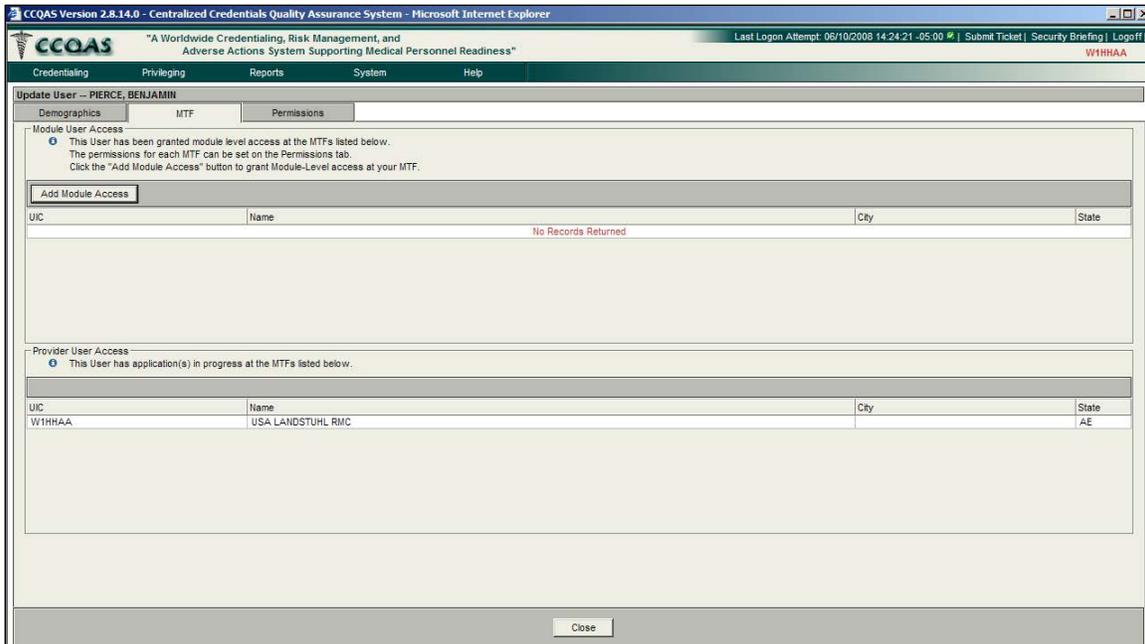


**Figure 26: ‘Demographics’ Tab for a Provider Applicant**

**Note:** If the applicant is a “Provider Applicant,” no further action is needed. The creation of the user account and first e-application 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 roles/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 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, has an application for clinical privileges currently pending or 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/permissions are assigned to a user’s account. The **Permissions** tab is depicted in Figure 28.

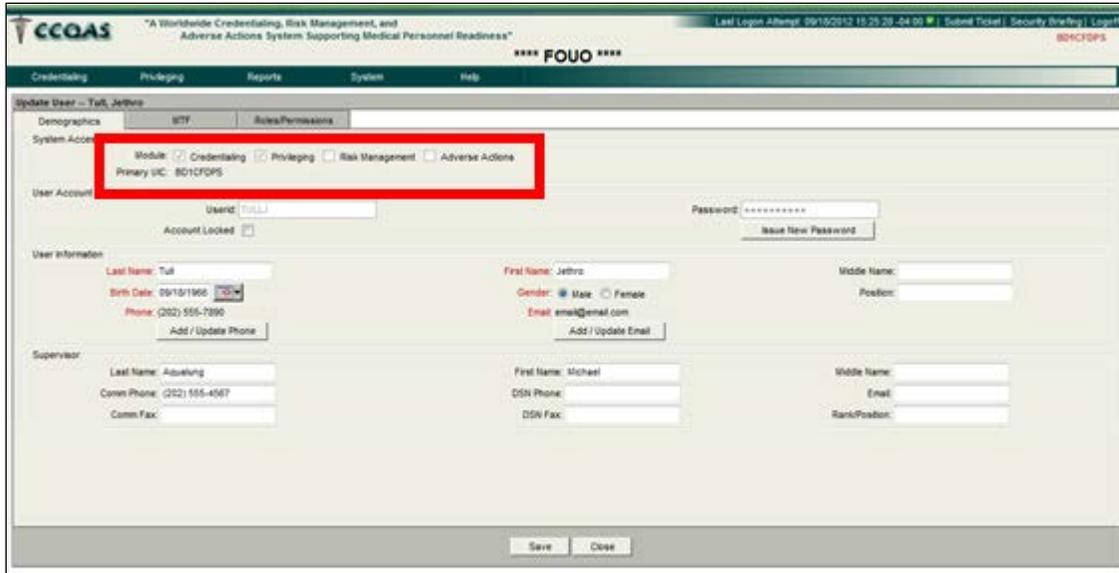


**Figure 28: ‘Permissions’ Tab for a Provider Applicant**

For “Provider Applicants,” no roles/permissions need to be configured for their user account. By processing the user registration 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 1<sup>st</sup> E-Application for clinical privileges is automatically generated (refer to Section 5). After the Provider user account is created, additional roles/permissions as a “Module User” may be added. The process of adding roles/permissions to an existing account is discussed in Section 3.3.

### 3.2.5 User Accounts for Module Users

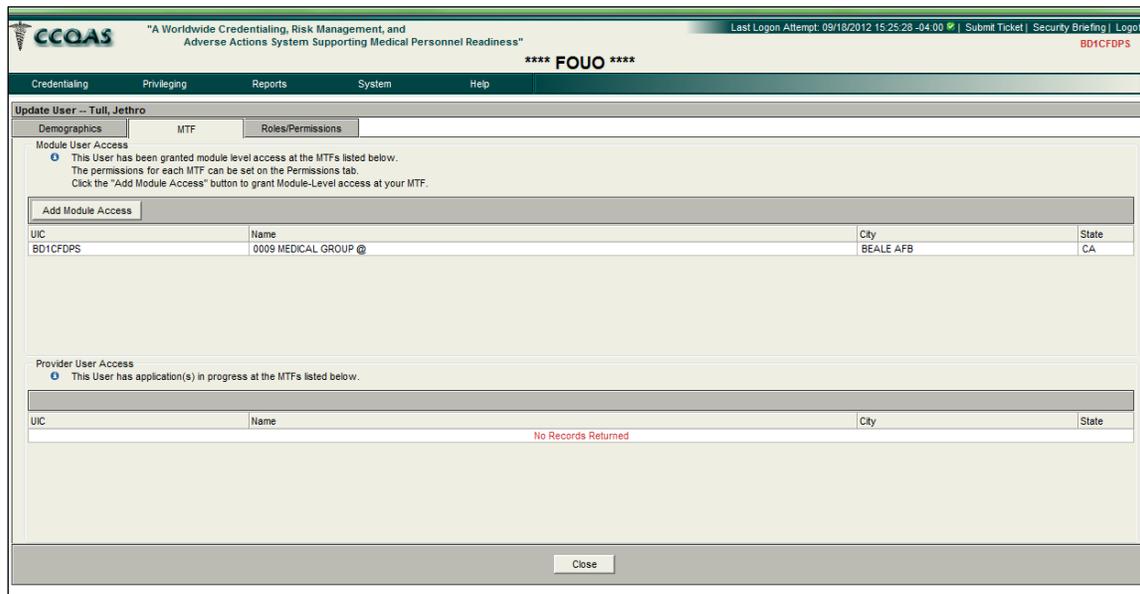
The **Demographics** tab for “Module Users” is similar to that for “Provider Applicants,” but also includes an indication of the CCQAS modules to which the user has access. The user account displayed on the **Demographics** tab in Figure 29 is an account for a user who has been granted access to the “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. 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, has an application for privileges currently pending or 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.



**Figure 30: ‘MTF’ Tab for a Module User**

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

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

**Figure 31: Privileging Roles/Permissions for a Module User**

On the privileging tab, 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 [ECOMS], Executive Committee of the Dental Staff [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 (a.k.a. Master Privilege List [MPL] 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 assigned to CC/MSSP/CMs.

- **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, the Credentials, System Administrator, and Reporting section permissions have been replaced with roles. To view the permissions for each role, select the role by clicking it, as depicted in Figure 32. A screen appears and displays the Read-Only permissions for that particular role selected (refer to Figure 33). When users select the **Close** button at the bottom of the screen, the roles/permissions screen closes and returns them to the **Role** screen. When users select “Yes” or “No” for the role, the permissions within that role are set.

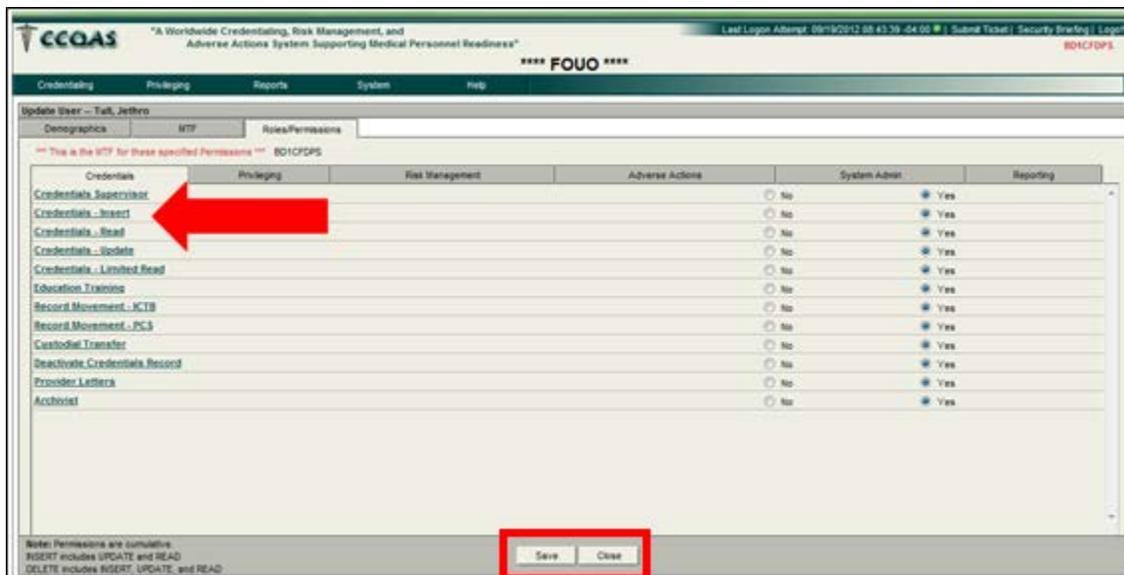


Figure 32: Credentials Roles

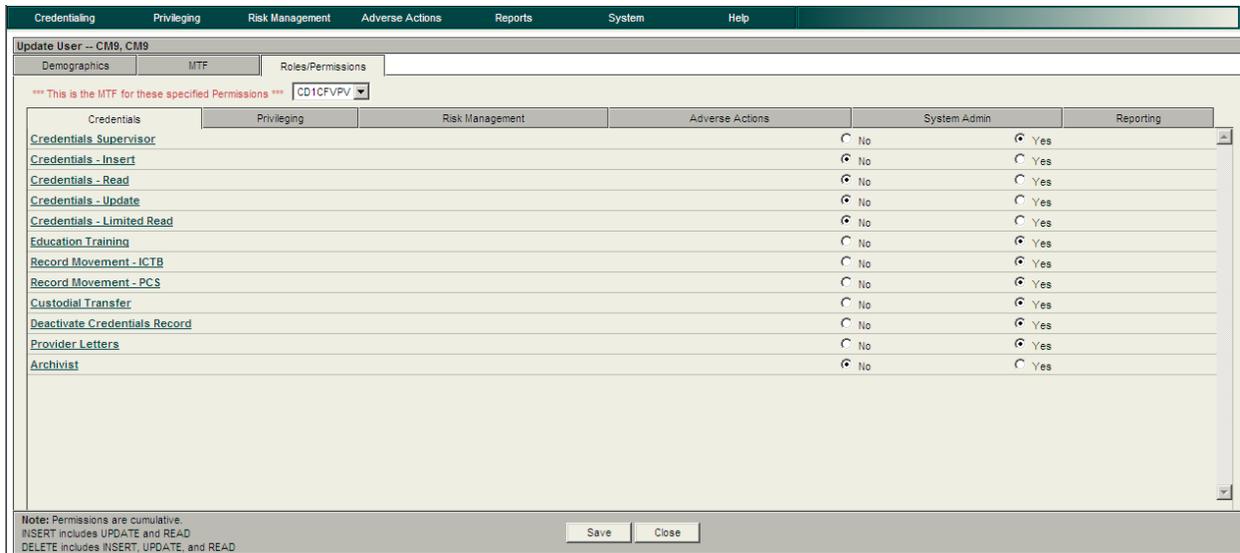
CCQAS		"A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness"		Last Logon Attempt: 05/22/2013 12:32:00 -05:00 #   Submit Ticket   Security Briefing   Lo		
		**** FOUO ****		CD1CFVPV		
Credentialing	Privileging	Risk Management	Adverse Actions	Reports	System	Help
*** Permissions for "Credentials Supervisor" Role ***						
Credentialing Module	<input type="radio"/> No	<input checked="" type="radio"/> Yes				
Demographics	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert			
Initiate PCS	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Initiate ICTB	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Add / Activate Provider Credentials Record	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Deactivate Provider Credentials Record	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Transaction Table	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Specialty	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Professional Training	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
CME / Continuing Education	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Licensure	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Affiliations	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
NPDB/HIPDB/F/SMB	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update			
Assignments	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Profile-Photo / Status	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Archive Provider	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Provider Remarks	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Privileges	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
References	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Documents	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
DEA/CDS	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Contingency Training	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Work History	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Provider Specific Letters	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
ICTB Letter Only	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Risk / Adverse Action	<input checked="" type="radio"/> None	<input checked="" type="radio"/> Read	<input checked="" type="radio"/> Update	<input checked="" type="radio"/> Insert	<input checked="" type="radio"/> Delete	
Custodial Transfer	<input checked="" type="radio"/> No	<input checked="" type="radio"/> Yes				
Close						

**Figure 33: Credentials Supervisor Role**

All roles default to “No”, 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 appropriate roles. Role selections are saved 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 sections to include Credentials, Privileging, System Admin, and Reporting tabs. Access to other sections may be granted by designating tab- and screen-level roles/permissions from the **Roles/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.

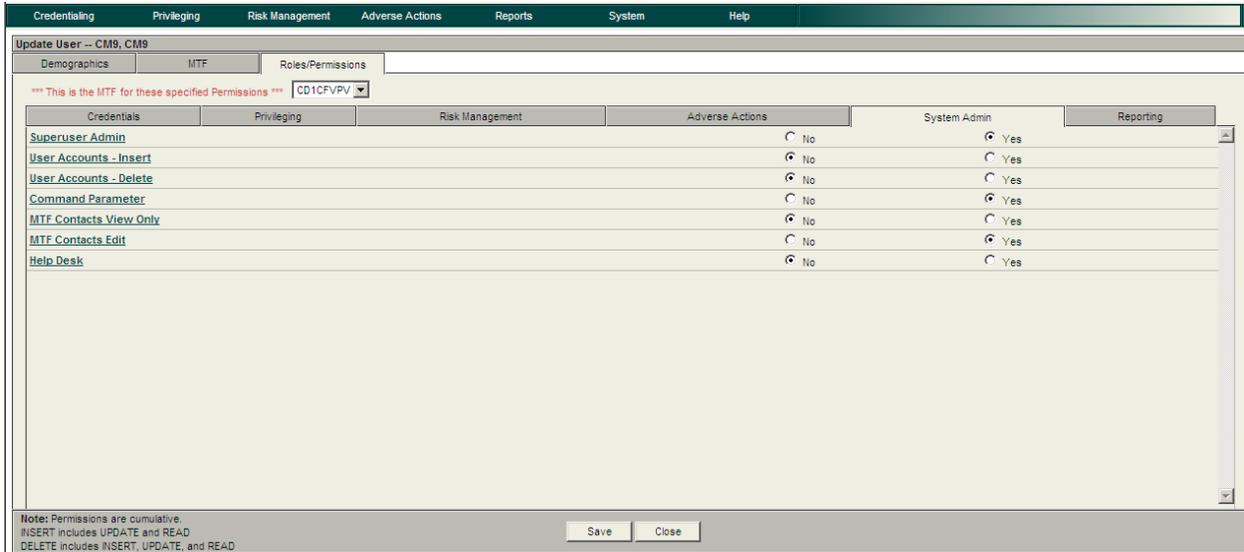


**Figure 34: Privileging Roles**

The **Privileging** tab contains roles 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, PAC Supervisor, Reviewer, or PAR Evaluator) depending on what roles/permissions are set for them. Figure 34 above depicts the privileging roles/permissions for a sample user.

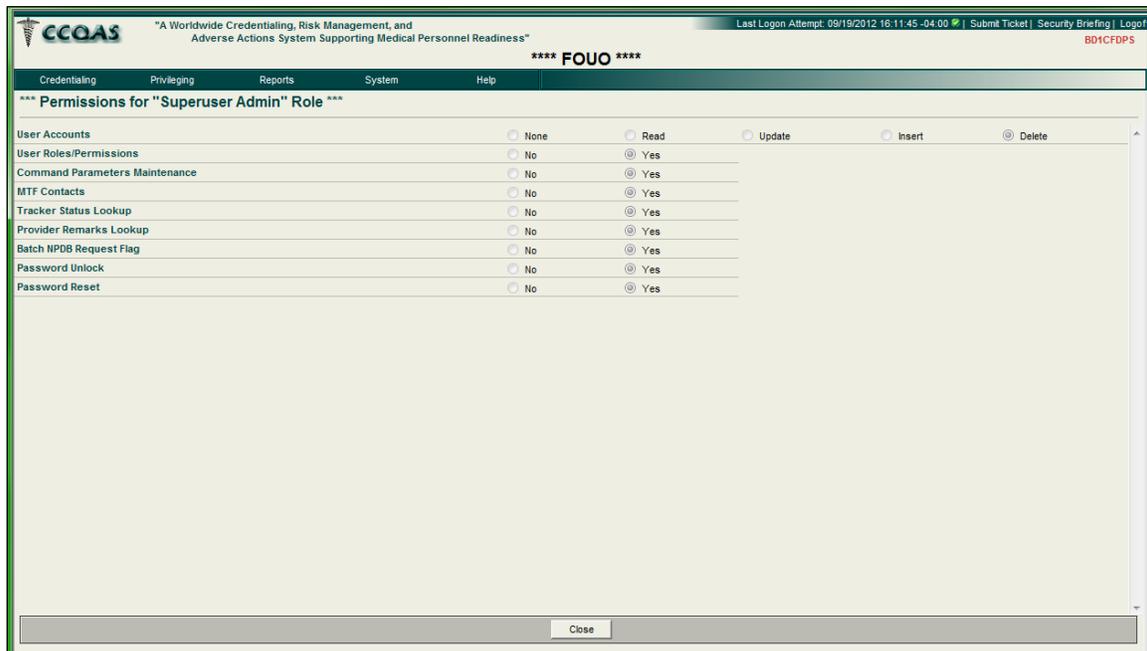
**Note:** The **Risk Management** and **Adverse Actions** tabs will be described in detail in a future version of this user guide.

The **System Admin** tab, depicted in Figure 35, contains roles/permissions that determine whether account holders may process new user accounts, access the Command Parameters and MTF Contacts, and set other roles/permissions associated with the management of the credentialing process at the facility or unit. Most roles/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 35: System Admin Permissions**

**Note:** The role “Superuser Admin” is located on the **System Admin** tab, which controls additional role-based permissions (refer to Figure 36). 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.



**Figure 36: “Superuser Admin” Role Permissions**

The **Reporting** tab, depicted in Figure 37, 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 National Practitioner Data Bank (NPDB) query function.

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

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

Figure 37: Reporting Roles Permissions

**Note:** The “Superuser role” 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 38.

Permissions	No	Yes
Credentials Reports	<input type="radio"/>	<input checked="" type="radio"/>
Risk Management Reports	<input type="radio"/>	<input checked="" type="radio"/>
Credentials Ad-hoc	<input type="radio"/>	<input checked="" type="radio"/>
NPDB Query	<input type="radio"/>	<input checked="" type="radio"/>
Adverse Actions Ad-hoc	<input type="radio"/>	<input checked="" type="radio"/>
Adverse Actions Reports	<input type="radio"/>	<input checked="" type="radio"/>
Risk Management Ad-hoc	<input type="radio"/>	<input checked="" type="radio"/>
Privileging Reports	<input type="radio"/>	<input checked="" type="radio"/>
Admin Reports	<input type="radio"/>	<input checked="" type="radio"/>
User Permissions Report	<input type="radio"/>	<input checked="" type="radio"/>
Ability to Run RM Letters	<input type="radio"/>	<input checked="" type="radio"/>

Figure 38: “Superuser” Role Permissions

The **User Processing** function within CCQAS allows anyone who has roles/permissions to grant other users roles/permission(s) up to what the “grantor” already holds. Roles/Permissions to access the Reporting section (refer to Figure 37 above), for example, cannot be granted by CC/MSSP/CMs or CVO staff who do not already have permission to access the Reporting section. 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 roles/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 the UIC user account administrator. For example, if COL Smith functions as a Reviewer at San Antonio Military Medical Center (SAMMC) and a Reviewer and PAR Evaluator at William Beaumont Army Medical Center (WBAMC), the CC at SAMMC would assign the “Reviewer” role to COL Smith for the SAMMC UIC. The CC at WBAMC would 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 Granting Module Access from Existing Provider Credentials Records**

CCQAS allows CC/MSSP/CMs to grant Module Access to a Provider user who already has an active credentials record and user account in CCQAS. This is the preferred method for creating new module user accounts for Providers.

To initiate this process, CC/MSSP/CMs perform a search for the Provider’s record in the Credentialing module. On the **Search Results** tab, click the hidden menu of actions for the Provider’s credentials record, and then select **Grant Module Access** (refer to Figure 39).

Provider Search										Advanced Credentials Search	Search Results	Add Credentials Provider	Help?
Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments				
Open	497-86-3012	N00060	05/25/2010	CIV		CIV	Active		1				
Initiate Custody Transfer	432-87-2540	N00060	04/28/2010	N11	DC	MIL	Active		1				
Deactivate Provider	999-88-9999	N00060	02/11/2009			MIL	Active		1				
Letters	444-33-4444	N00060	01/29/2010			MIL	Active		1				
Grant Module Access	100-70-2222	N00060	05/09/2012			MIL	Active		1				
BROOKES, DUINN	628-49-7361	N00060	08/22/2010	CIV		CIV	Active		1				
C, NAVY	121-23-1234	N00060	09/29/2009	CIV		CIV	Active		1				
CANNON, IVY	190-99-0000	N00060	11/06/2012			MIL	Active		1				
DATA_MIGRATE_8, DATA_MIGRATE_8 C	234-23-7893	N00060	11/16/2012	FMS	ALL	Dual	Active		2				
DATA_MIGRATE_ARNG1, DATA_MIGRATE_ARNG1 E	234-23-7892	BV1MFB57	11/16/2012	F11	MC	Dual	Active		3				
DITVSSQTTEST, MISTER	028-86-7111	N00060	07/28/2010	N11	MC	MIL	Active		1				
EXPIRING, CREDENTIALS	199-19-9199	N00060	12/10/2009	N13	MC	MIL	Active		1				
FOREIGNEDTEST, MISTER	213-50-4833	N00060	05/17/2010			MIL	Active		1				
FOUO, Test	000-00-3778	N00060	07/15/2008	N11	MC	MIL	Active		1				
FOUR, SCENARIO	544-77-8666	N00060	11/16/2012	F15	MC	Dual	Active		2				
HANSON, STEPHANIE	700-99-8888	N00060	11/29/2012	N11	MC	MIL	Active		1				
HUGHES, REPTTEST	588-21-4578	N00060	08/01/2012			MIL	Active		1				

Record Count: 85      Search      Clear Screen      Add Provider      Record Limit: 100

**Figure 39: Grant Provider Access Menu Item**

After the user account is 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.

### 3.2.7 Granting Provider Access from Existing Provider Credentials Records

If a provider already has a user account, the grant provider access option will not be available. 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 1<sup>st</sup> 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

## 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 1<sup>st</sup> 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
- CC/MSSP/CMs may use the **Initiate Application** menu item to generate the 1<sup>st</sup> 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.
- 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 40.

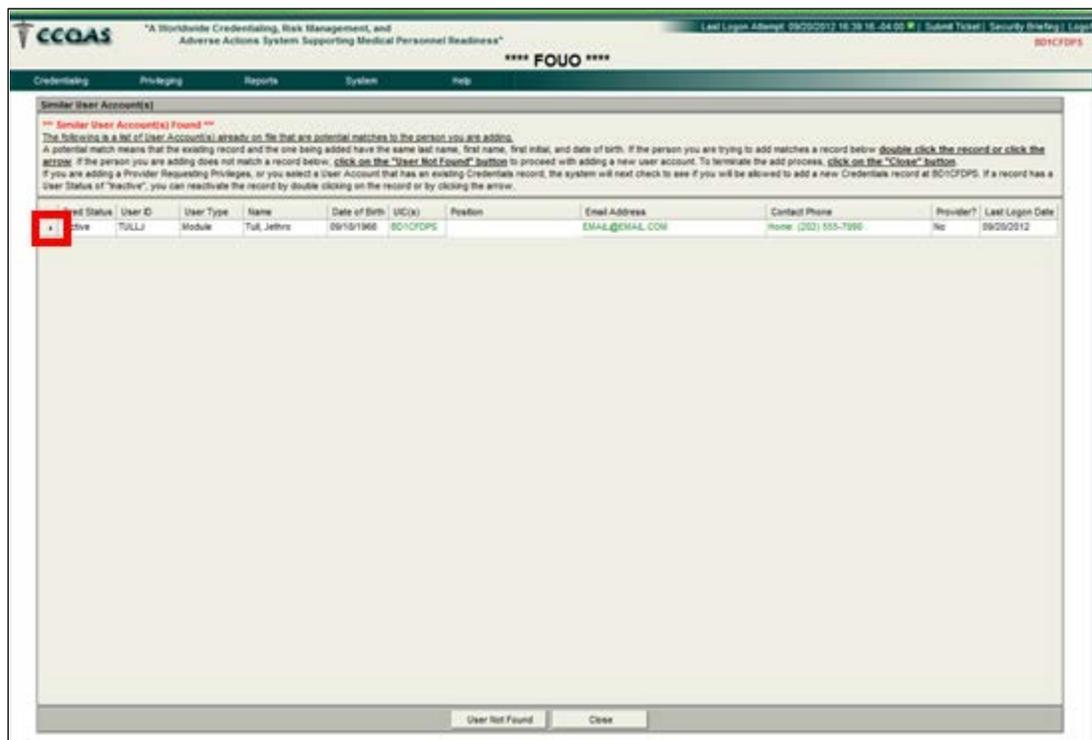
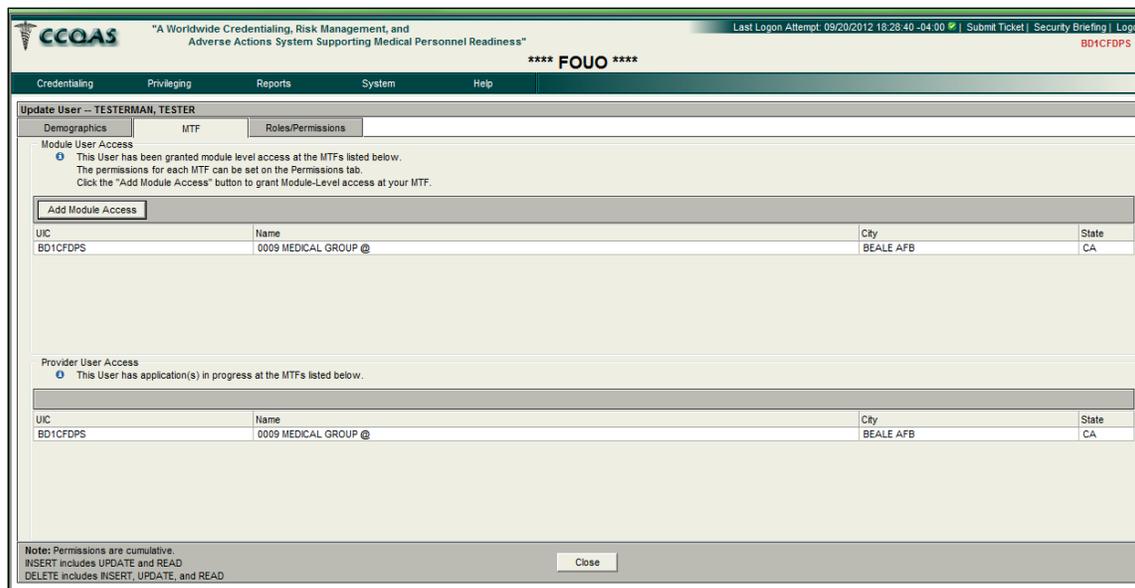


Figure 40: Similar User Account(s) Screen

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 41.



**Figure 41: ‘MTF’ Tab for a Dual User’s Account**

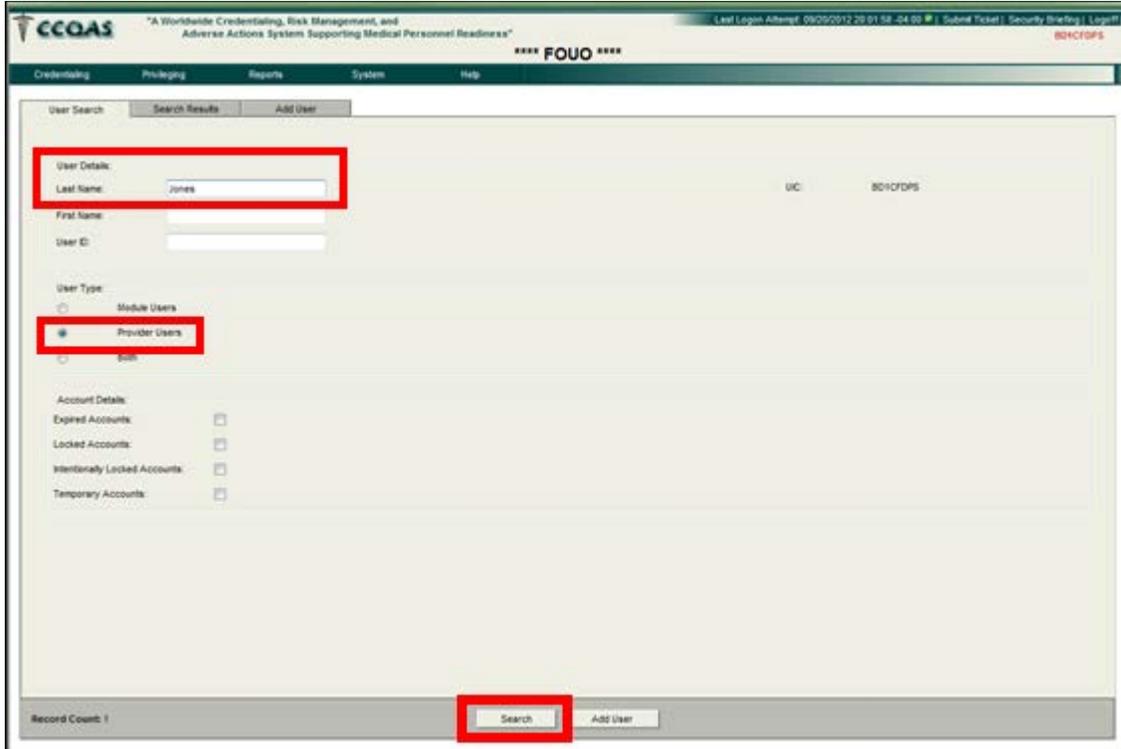
The **Permissions** tab should continue to reflect the roles and permissions that were originally assigned to the user account. The addition of the “Provider” role does not alter any of the previously-assigned roles or permissions at the UIC. When the role of “Provider” is added to the user’s account, the 1<sup>st</sup> 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 User” Account

Depending on where they are in their privileging cycle when they become CCQAS users, some CC/MSSP/CM 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 42. 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**.



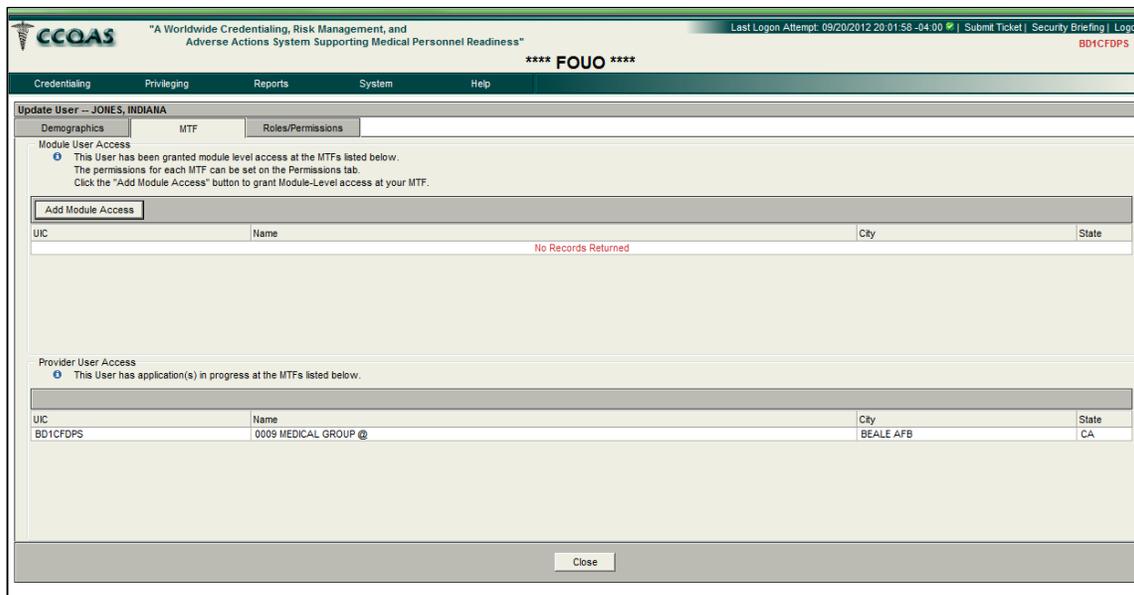
**Figure 42: User Search Screen**

The **User Listing** screen appears, as depicted in Figure 43. This screen displays all existing user accounts at the facility or unit that meet the search criteria.



**Figure 43: 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 44.



**Figure 44: ‘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 45. This record indicates that *Module User* access has been added to the Provider’s account.

The appropriate roles and permissions must 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.

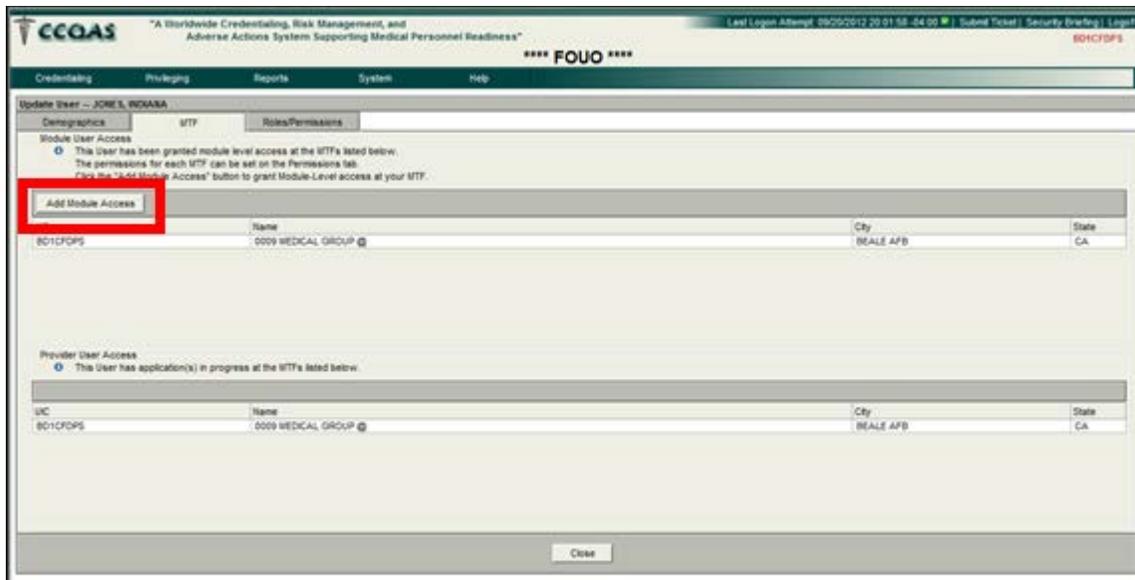


Figure 45: 'MTF' Tab for a Dual User's Account

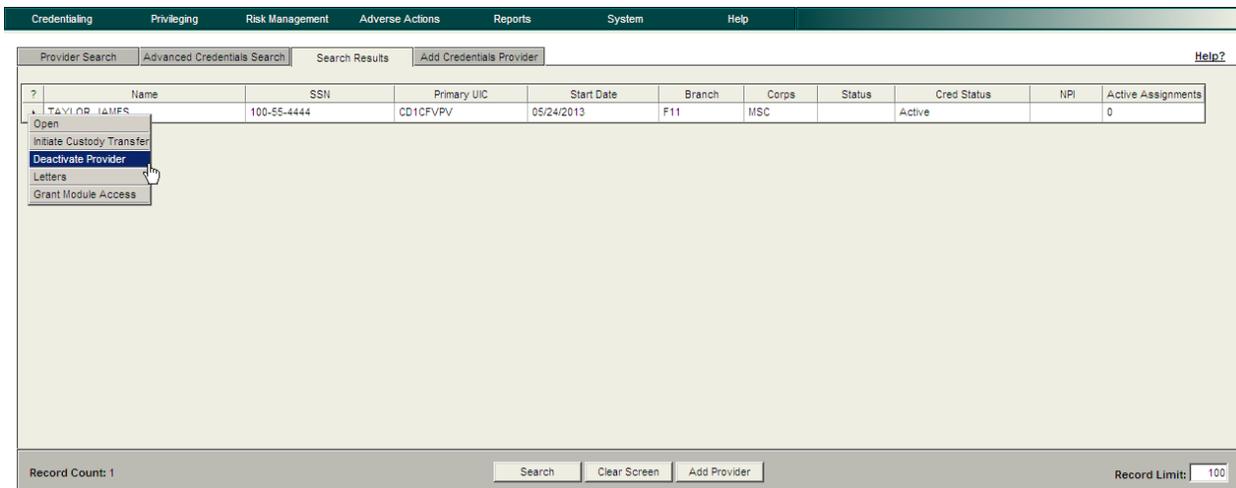
### 3.4 Deactivating and Reactivating User Accounts

Under most circumstances, CC/MSSP/CMs should not deactivate a user account while the user associated with the account is still actively working within the MHS. If a CC/MSSP/CM wishes to restrict a user's CCQAS access at a specific unit, then the user's roles at that particular unit should be adjusted to reflect the restriction for that UIC only (refer to Section 3.2.5).

Deactivating a user account prevents the user from logging in at any unit and therefore should only be done if it is the CC/MSSP/CM's desire to prevent the user from logging in to CCQAS from any unit.

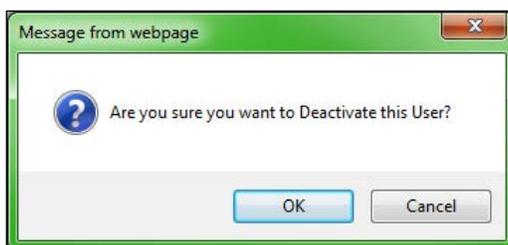
CCQAS automatically deactivates a user's account if 365 days elapse without the user logging in to the system. This will happen to provider user accounts where the associated Provider user infrequently accesses CCQAS (e.g., providers who only log in to renew their clinical privileges at their current location or apply for clinical privileges at a new duty station).

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 46.



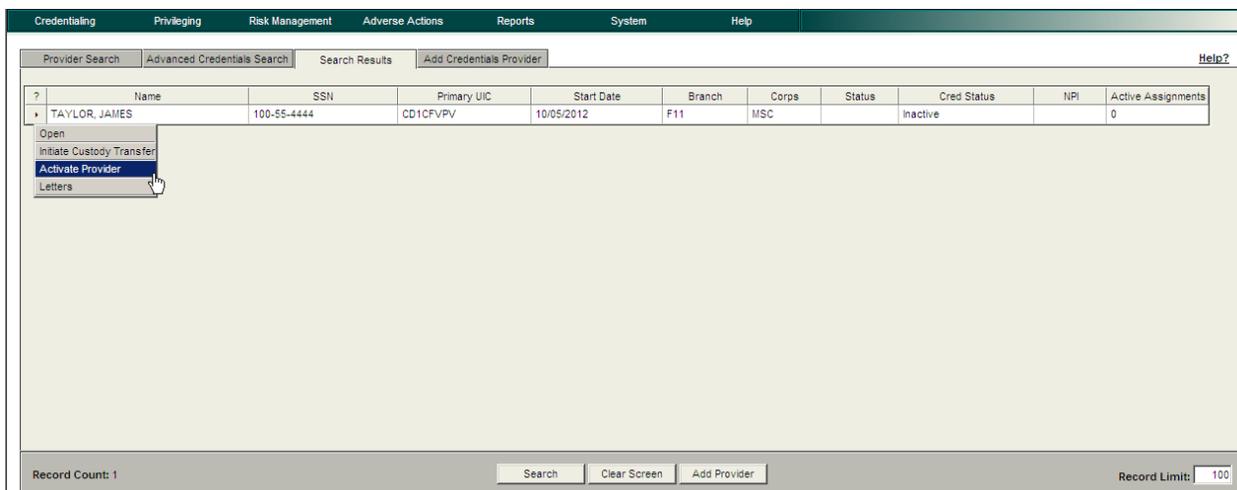
**Figure 46: Deactivate Menu Item**

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 47.



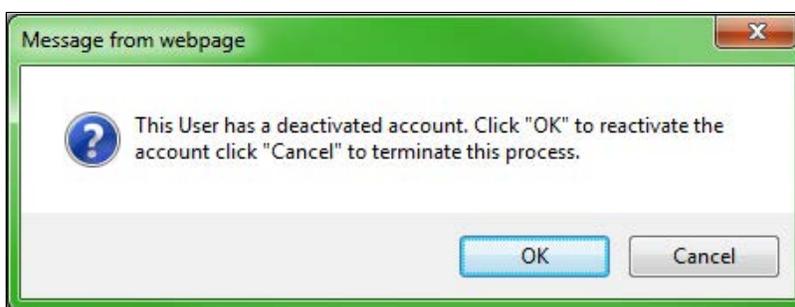
**Figure 47: Deactivate User Confirmation Message**

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 48.



**Figure 48: Activate Menu Item**

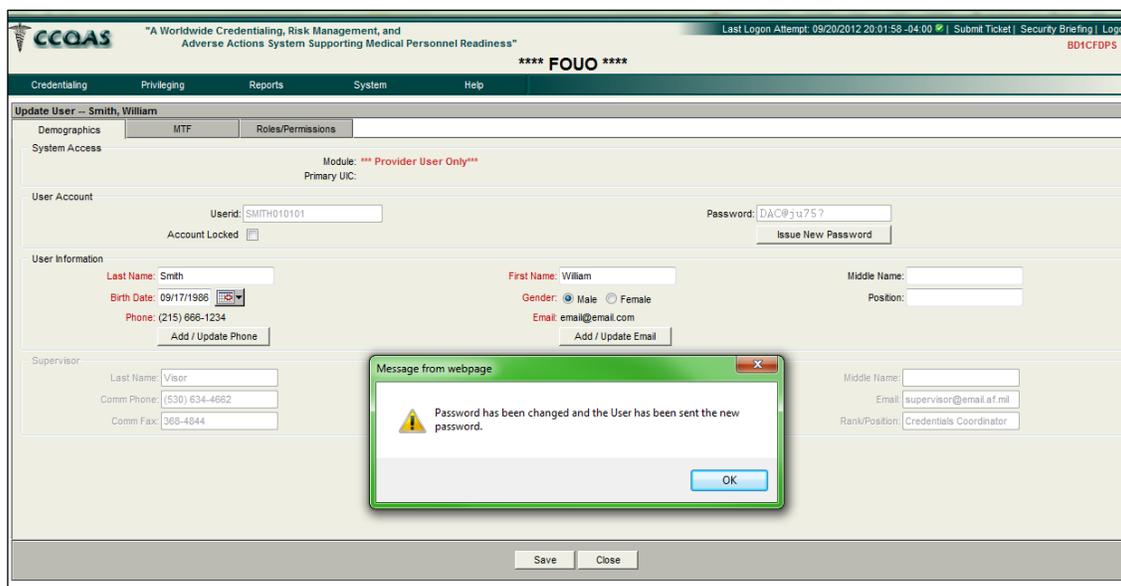
When authorized users select **Activate**, they are asked to confirm their intent to reactivate the user account, as depicted in Figure 49.



**Figure 49: 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 50. The message indicates that an email was sent to the user which contains a new temporary password.

Since the new password has already been 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 50: 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. This section describes the process of using CCQAS for the first time.

### 3.4.1 Receiving a New Username and Temporary Password

After a new user account has been processed, CCQAS notifies the new user of his or her username and a temporary password via two (2) automated email messages. Passwords for CCQAS conform to DoD Information Systems security requirements.

*The username and the password are both case-sensitive.*

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

### 3.4.2 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.

#### **3.4.2.1 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. Refer to the CCQAS main page, in the Security Certificate Add On section, there are links and instructions for downloading and installing these certificates.

#### **3.4.2.2 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 logon process begins when the users click the Logon button on the left hand side of the screen. The **CCQAS Privacy Act Statement** screen appears, as depicted in Figure 51. Users select the **Yes** radio button after they have read the statement. CCQAS does not allow access to the system without users selecting the **Yes** radio button. Users are then directed to the **DoD Network Authentication** screen, where the electronic credentials from their CAC or PIV card is authenticated as depicted in 40.

**CCOAS**  
A Worldwide Credentialing And Risk Management System

**Privacy Act Statement**

Before proceeding into the CCOAS logon window, users must acknowledge that they are aware of the Privacy Act Statement associated with using this system.

**1102 PROTECTED STATUS**  
CCOAS includes Sensitive but Unclassified (SBU) information that is subject to the Privacy Act of 1974, as amended. Consequently, copying, printing, or distributing data from CCOAS 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 CCOAS is accessible under the Freedom of Information Act. The use and disclosure of some information in CCOAS 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 CCOAS 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 (SSN), 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://oipo.defense.gov/privacy/SORris/blanket\\_routine\\_uses.html](http://oipo.defense.gov/privacy/SORris/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.

Yes, I understand the contents of the above Privacy Act Statement.  
 No, I do not understand the contents of the above Privacy Act Statement.

Figure 51: CCQAS Privacy Act Statement



U.S. Department of Defense  
**Military Health System**

**iDENTITY  
AUTHENTICATION  
SERVICES**

**This Website has been Public Key Enforced**



Please click on "CAC/PIV Access" below to access the application using your DoD Common Access Card (CAC) or Department of Veterans Affairs (VA) Personal Identification Verification (PIV) card.

Make sure that your DoD CAC or VA PIV is inserted into the CAC/PIV reader so that your identity certificate is available to the web browser.

If you need to update your Enterprise Profile click the link below:  
[Update your Enterprise Profile](#)

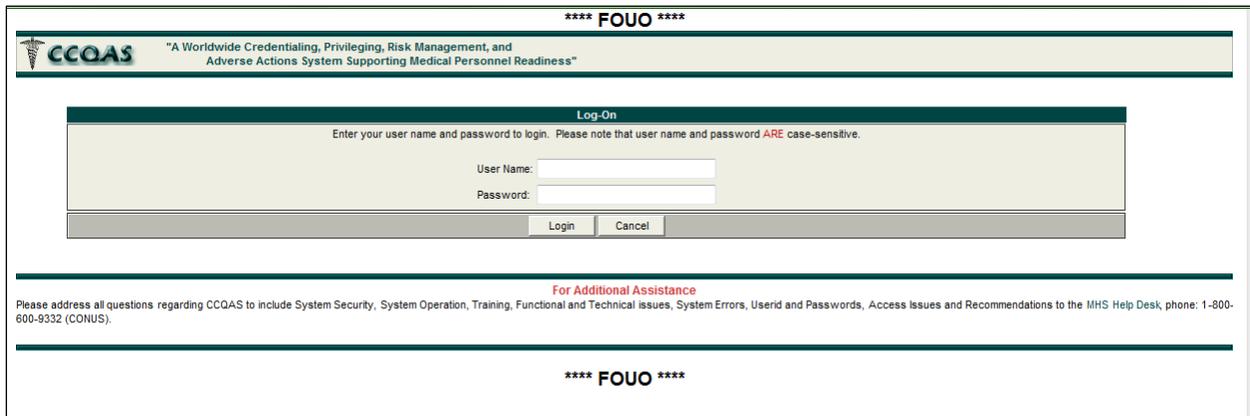
**Authenticate with your DoD CAC or VA PIV:**



This is a web site of the Military Health System - The Pentagon, Washington, D.C. 20301-1200  
For Help, please contact [MHS Helpdesk](#). For Official Use Only.

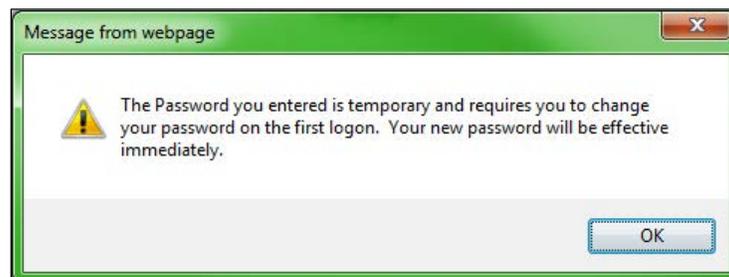
Figure 52: DoD Authentication Screen

After users CAC/PIV certificate is authenticated, they enter their username and password in the appropriate fields on the **Login** screen, as depicted in Figure 53, 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.



**Figure 53: Login Screen**

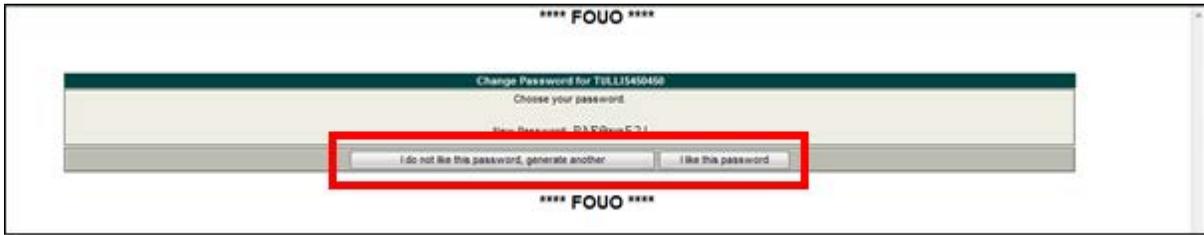
If users unsuccessfully attempt to log in more than twice, they receive a message that their account has been locked, as depicted in Figure 54. Users must contact their CC/MSSP/CM or the MHS Helpdesk to have their account unlocked before proceeding.



**Figure 54: Temporary Password Alert**

### 3.4.2.3 Changing a Temporary Password

After users log in for the first time, they are prompted to change their temporary password, as depicted in Figure 55. 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 55: 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 the CCQAS user 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.

#### **3.4.2.4 Security Briefing**

After users log in, they are presented with a security briefing, as depicted in Figure 56. 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.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Login Allowed: 09/25/2012 20:01:55 -04:00 Submit Ticket Security Briefing Logout

\*\*\*\* FOUO \*\*\*\*

CCQAS 2.6 (ASMR) is a credentialing and risk management information system that provides a single, Tri-Service, repository of information concerning active duty and reserve clinicians' licenses, training, continuing medical education, board certifications, medical malpractice insurance, and medical incidents, including potential compensatory events. The system provides standard and ad hoc reporting capability. The repository is accessible via a browser.

CCQAS CONTACT INFORMATION  
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 [Help Desk](#), phone: 1-800-460-9332 (COALS). You may wish to write this information down for further reference.

CCQAS ACCESS  
Access to CCQAS is limited to military personnel, government employees, and contractors assigned by the MTF or services to process and/or administer the quality assurance program. No other individuals may access the system without the express permission of the TriCare Management Activity Functional Proponent or applicable CCQAS Service Representatives. Access within the system is restricted to the lowest level necessary for the user to perform their job.

CCQAS USERID AND PASSWORD CONTROL  
Personnel accessing the system are required to maintain their own userid and password. The holder of the userid and password is the only authorized user of the userid. Personnel may not use another person's userid and password or allow another person to use their userid and password. The sharing of userids is expressly prohibited.  
Users may not store userids or passwords on any microcomputer or magnetic media. Users will alert the help desk or functional proponent immediately if they suspect that their userid or password may have been compromised.

CCQAS GOOD SECURITY PRACTICES  

- Users will alert help desk or their Service Functional Proponent immediately upon revocation of clearance or reassignment out of quality assurance duties.
- Users will report any known or suspected security violation to the CCQAS functional/proponent and help desk.
- Users will not leave their workstation until they have logged off CCQAS.

COPIING, PRINTING OR DISTRIBUTING CCQAS DATA (1992 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 5405.11-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 18 U.S.C. 1192. 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. Functional users must manually mark output products with the appropriate classification label and protect from unauthorized disclosure.

practitioner, it may be released to civilian medical institutions or organizations where the practitioner is applying for start privileges, or already privileges, regardless of whether the practitioner is start privileges 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.

DoD WARNING  
This is a DoD computer system. This computer system, which includes all related equipment, networks, and network devices (specifically including access to the internet), are provided only for official U.S. government business. DoD computer systems may be monitored by authorized personnel to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures. Monitoring includes "hacker" attacks to test or verify the security of this system against use by unauthorized persons. During these activities, information stored on this system may be examined, copied and used for authorized purposes and data or programs may be placed into this system. Therefore, information you place on this system is not private. Use of this DoD computer system, authorized or unauthorized, constitutes consent to official monitoring of this system. Unauthorized use of a DoD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be provided to appropriate personnel for administrative, criminal, or other action.

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 6025.15-R, DoD Health Information Privacy Regulation. The HIPAA Privacy Rule and DoD 6025.15-R apply to protected health information and may place additional procedural requirements on users 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.

Yes, I understand the contents of the above Security Briefing.  
 No, I do not understand the contents of the above Security Briefing.

Submit

\*\*\*\* FOUO \*\*\*\*

Figure 56: Security Briefing

### 3.5 Maintaining CCQAS User Accounts

This section describes the process for maintaining CCQAS user accounts.

#### 3.5.1 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 57.

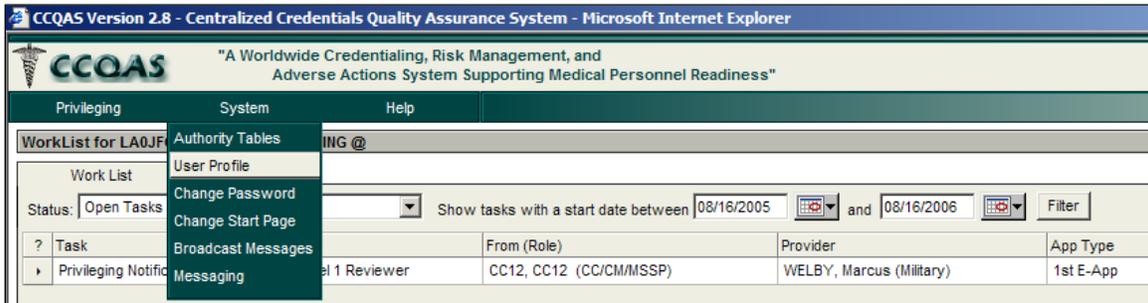


Figure 57: User Profile Menu Item for a Module User

The first tab from the user account, the **Demographics** tab, displays, as depicted in Figure 58.

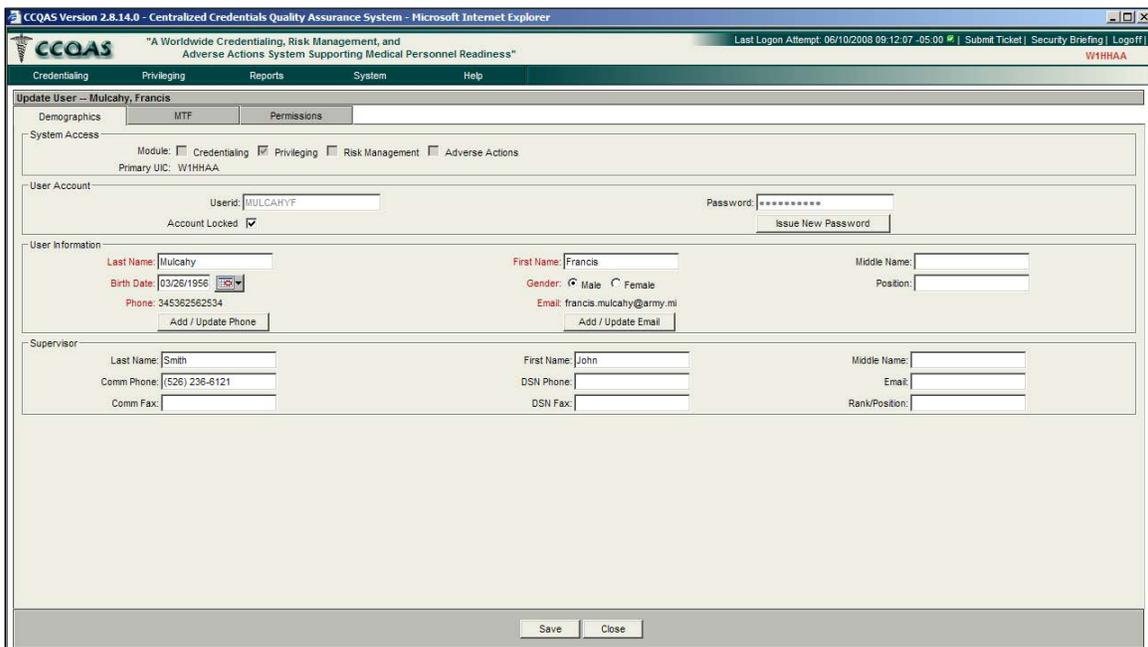
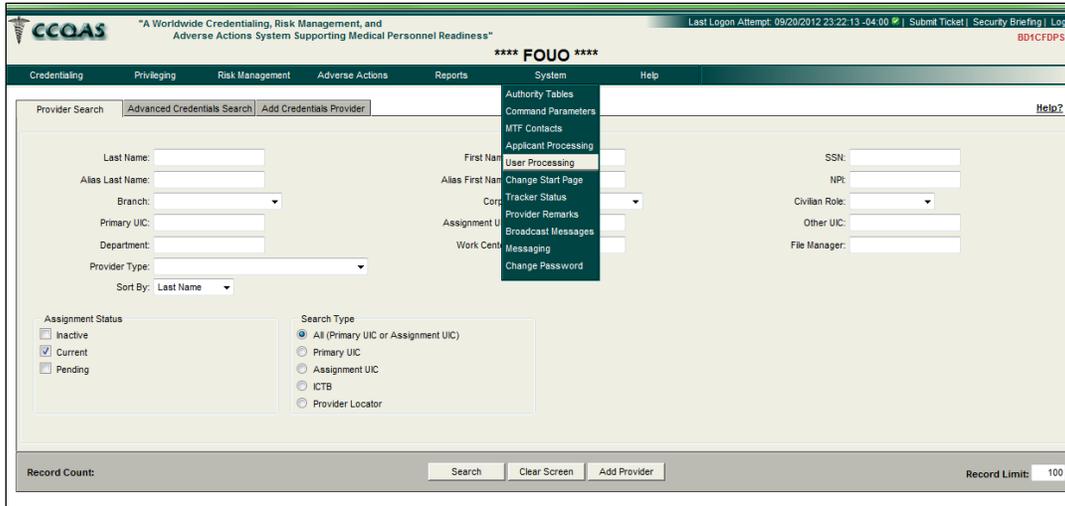


Figure 58: Update User Screen for Other (Module Users)

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.

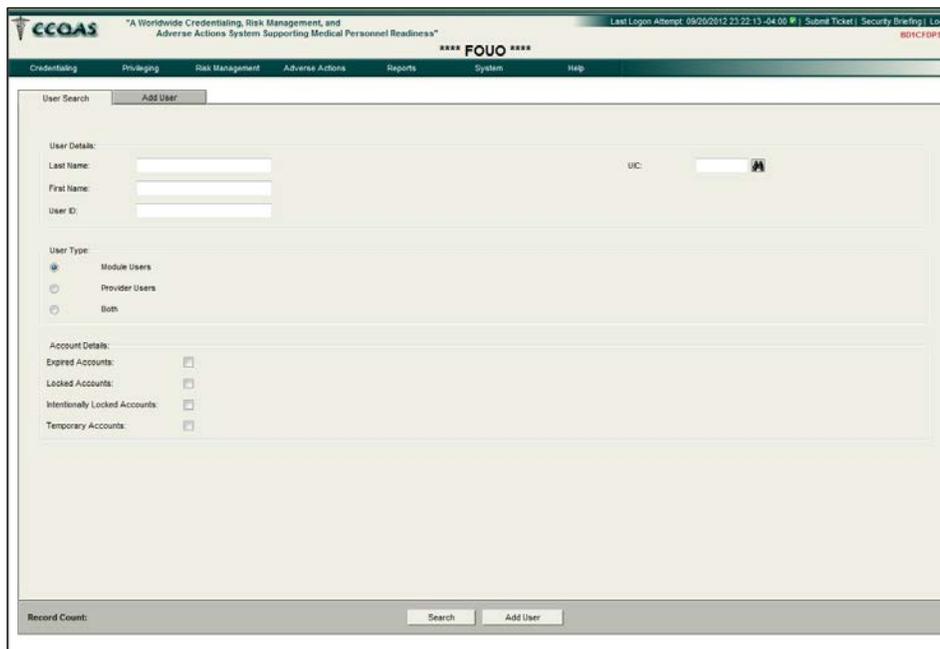
**Note:** Users with "Provider" access only in CCQAS do not have access to the **System** main menu; therefore, they cannot access the **User Profile** functionality. Providers should update their contact information when they submit their next privilege application. If their contact information changes 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 59.



**Figure 59: User Processing Menu Item**

When CC/MSSP/CMs select **User Processing**, the **User Search** screen appears, as depicted in Figure 60.



**Figure 60: 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.

### 3.5.2 Password Reset

Users may update a password using the **Reset 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, using the **User Processing** function, 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 61. An **Initiate New Password** button is also available on the **Demographics** tab of the user’s account as depicted in Figure 62.

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.

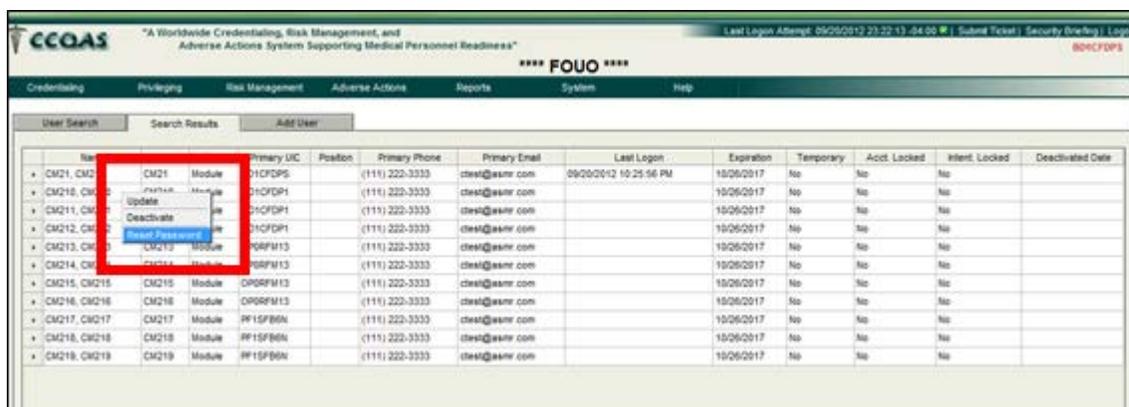


Figure 61: Reset Password Menu Item

### 3.5.3 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 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. If a new password is required, verify that the user's primary email address is correct and click the Issue New Password button. This action generates an automated email message to the account holder with a new temporary password.

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 50.

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.

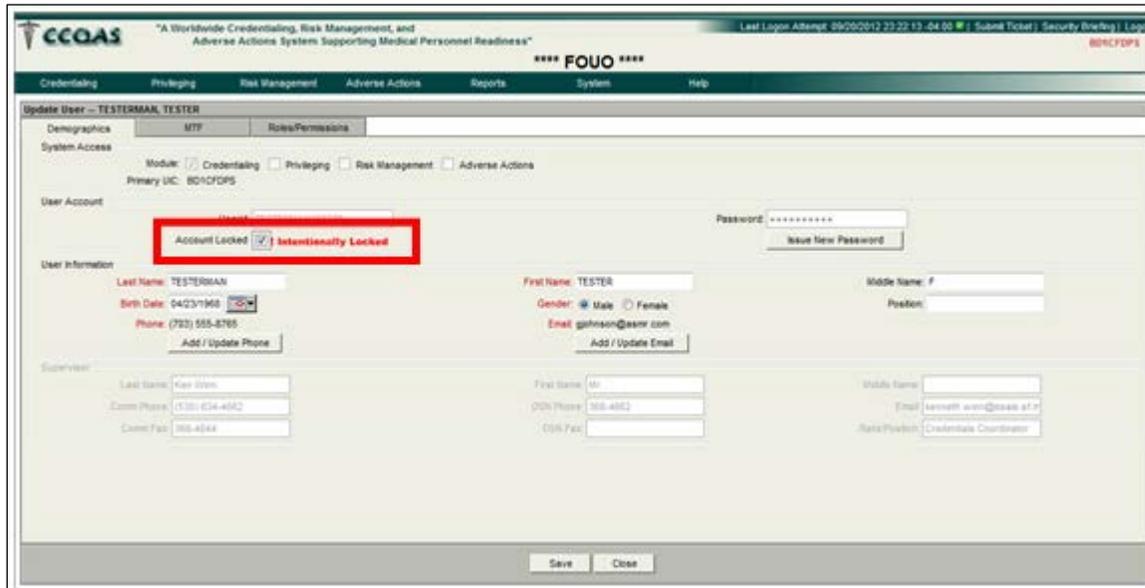


Figure 62: Account Locked Indicator

## 4 Managing Facility Privilege Lists

This section provides instructions on how to use the DoD MPLs. Changes to the MPL can only be made at the DoD level after concurrence from all Services. Each facility or unit configures its own privilege lists using the DoD MPL as a starting point.

At least one CC/MSSP/CM at each privileging facility should be designated as the MPL Administrator (with Common Language Privileging (CLP) role for Parent and Branch UICs), and is responsible for managing the privilege catalog for their 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.

### 4.1 The Privilege Management Function

The process of managing the facility privilege catalog is initiated by selecting **Privilege Management** from the Privileging main menu, as depicted in Figure 63. Only users who have the CLP role have access to the **Privilege Management** function in CCQAS.

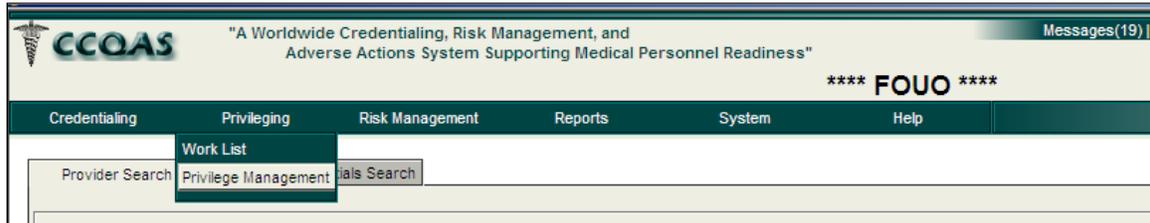


Figure 63: CCQAS Privileging Management Menu Item

When users select **Privilege Management**, the **Privilege Management** screen appears, as depicted in Figure 64. From this screen, users may select a privilege category (i.e., specialty) from the **Privilege Category** pick list.

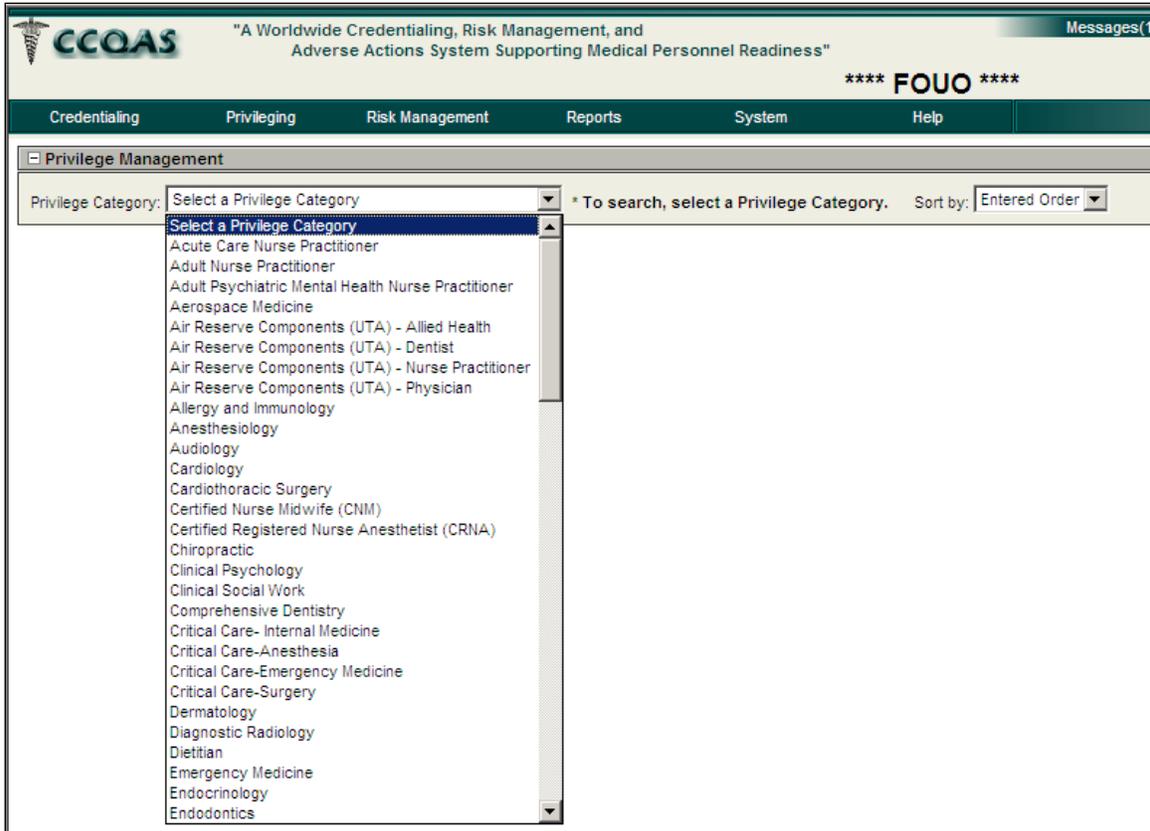


Figure 64: Privilege Management Screen and Category Pick List

Figure 65 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.

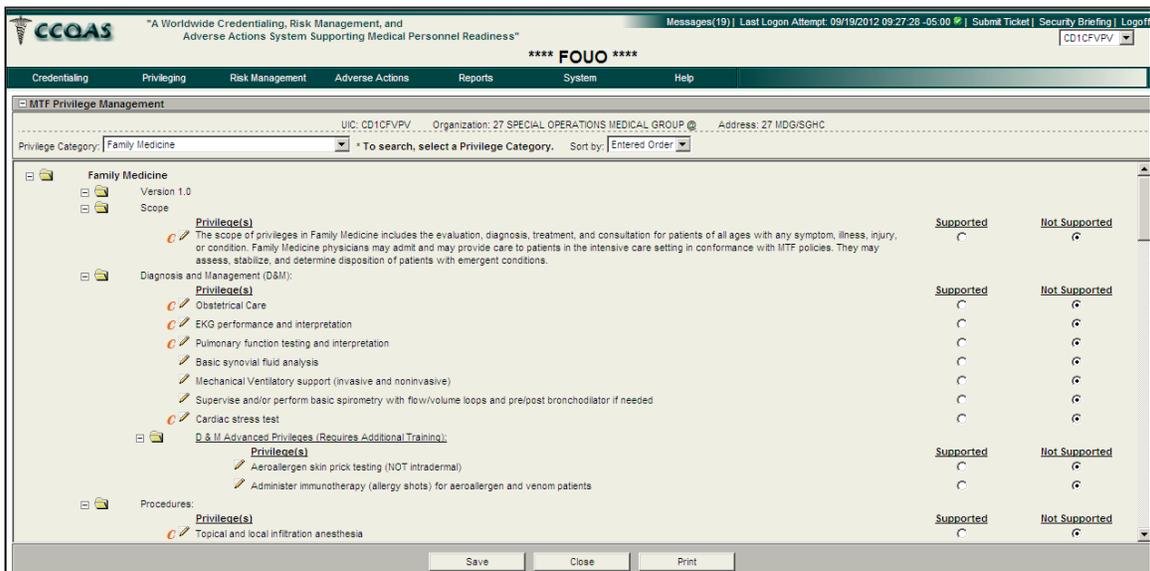


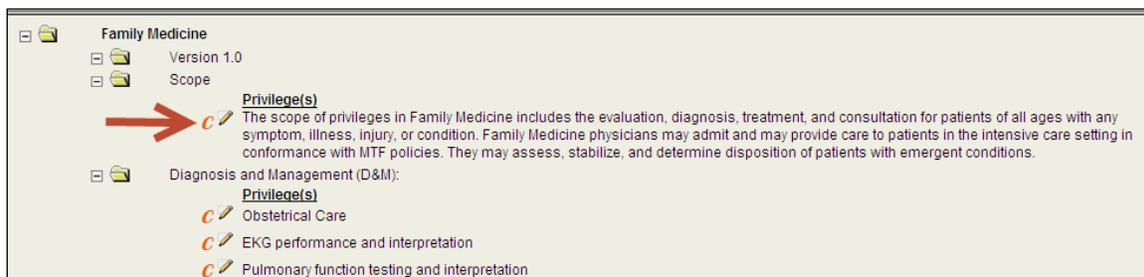
Figure 65: Privilege List for Family Medicine

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 identified with a , at the beginning of each privilege as depicted in Figure 66. **Core designation can only be changed at the direction of the Navy Service level.**

**Note:** Privilege lists may be sorted by entered order (default), description, set order, or Core order. The following is an explanation to each sort function:

- **Entered Order** = displays the privileges as they were entered when the list was created
- **Description Order** = displays the privileges in alphabetical order by sub-category
- **Set Order** = allows a privilege to be moved to a new position (To change the order of a privilege, left click a privilege description and drag it to a new position. Only privileges under the Other Privileges section may be re-positioned).
- **Core Order** = displays privileges with the core icon at the top of the list.



**Figure 66: Examples of Family Medicine Core Privileges**

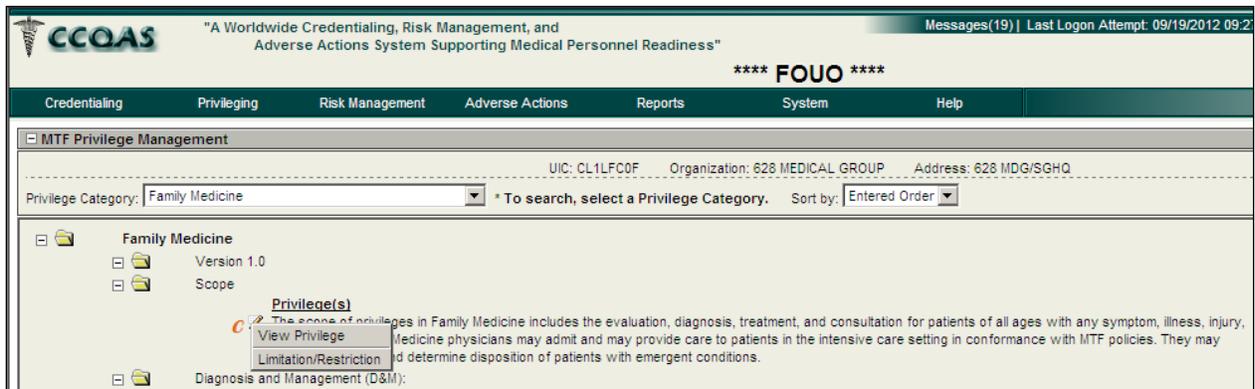
The process of building the facility privilege catalog is the same for all Services. Facility MPL Administrators must (have the CLP Role) and designate the privileges that are supported within each specialty at their facility. While MPL Administrators are the individuals who enters the information in CCQAS, department heads and other appropriate clinical staff members must 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 64 and Figure 65 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.
- All privilege items are set to a default value of **Not Supported** until such time as the MPL Administrator changes the setting.
- 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 folder 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.

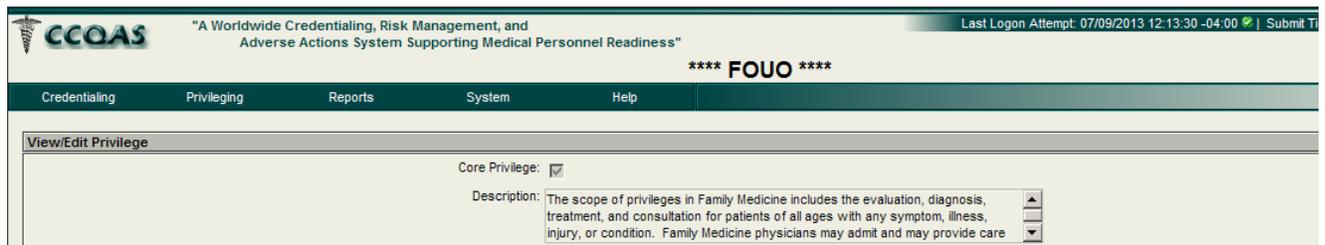
- If few or no privilege items within a given privilege folder are supported by the facility, users may click the header **Not Supported** to default all radio buttons to that value. Individual privilege items may then be changed, as appropriate.
- All changes made to the privilege items are maintained 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 67.



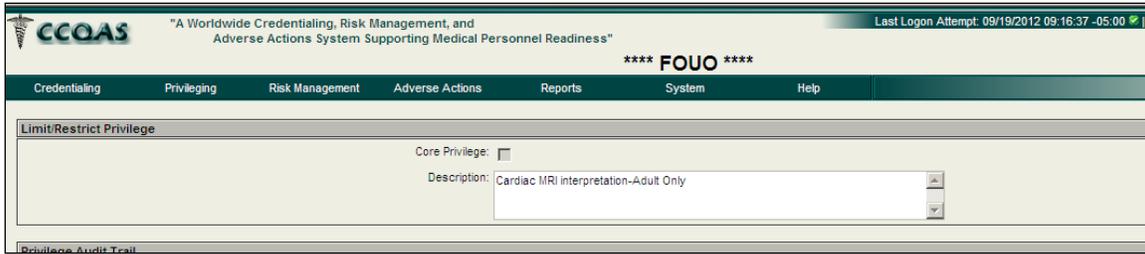
**Figure 67: View Privilege Menu Item**

The **View Privilege** option opens the **View/Edit Privilege** window, as depicted in Figure 68. 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.



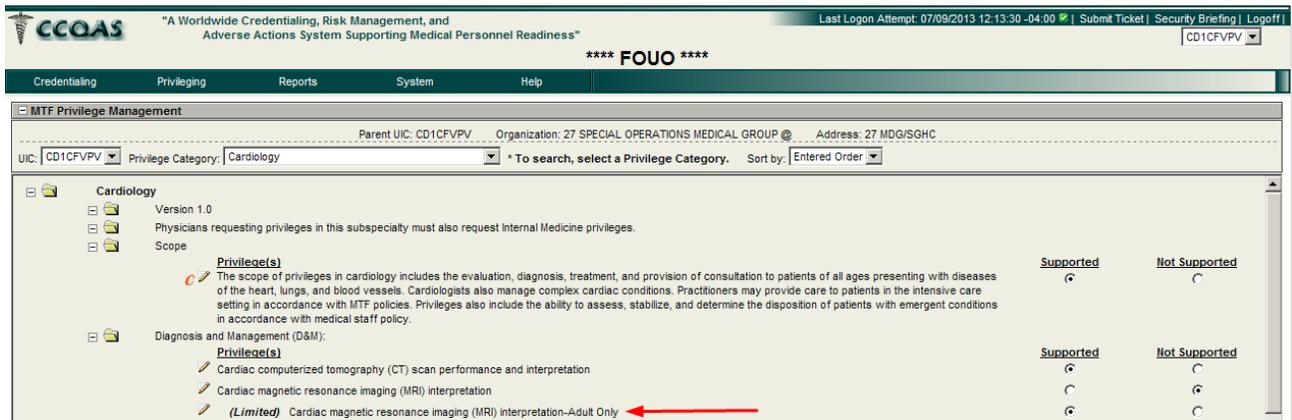
**Figure 68: View Privilege Option**

The **Limitation/Restriction** option also opens the **View Edit Privilege** window, as depicted in Figure 69 below. This option allows MPL Administrators to edit the privilege description to apply facility-specific limitations on the privilege item. Figure 69 depicts the **Description** text field, where a sample MPL Administrator has updated *Cardiac MRI Interpretation* to *Cardiac MRI Interpretation-Adult Only*.



**Figure 69: Limitations/Restrictions Option**

When MPL Administrators click **Save**, the screen refreshes to display the **MTF Privilege Management** screen, as depicted in Figure 70. The new privilege item, *Cardiac magnetic resonance imaging Interpretation-Adult Only*, has been added immediately below the original item and is automatically identified as **Supported**. Note that the original privilege item, *Cardiac MRI Interpretation*, is retained in the list of privilege items and should be changed to Not Supported. This feature allows MPL Administrators to make appropriate modifications to privilege items to narrow the scope of the privilege that may be performed at their facility.

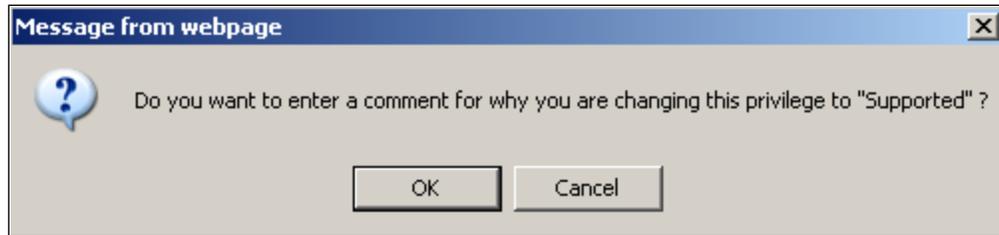


**Figure 70: Limitations/Restrictions View**

## 4.2 Maintenance of Facility Privilege Catalogs

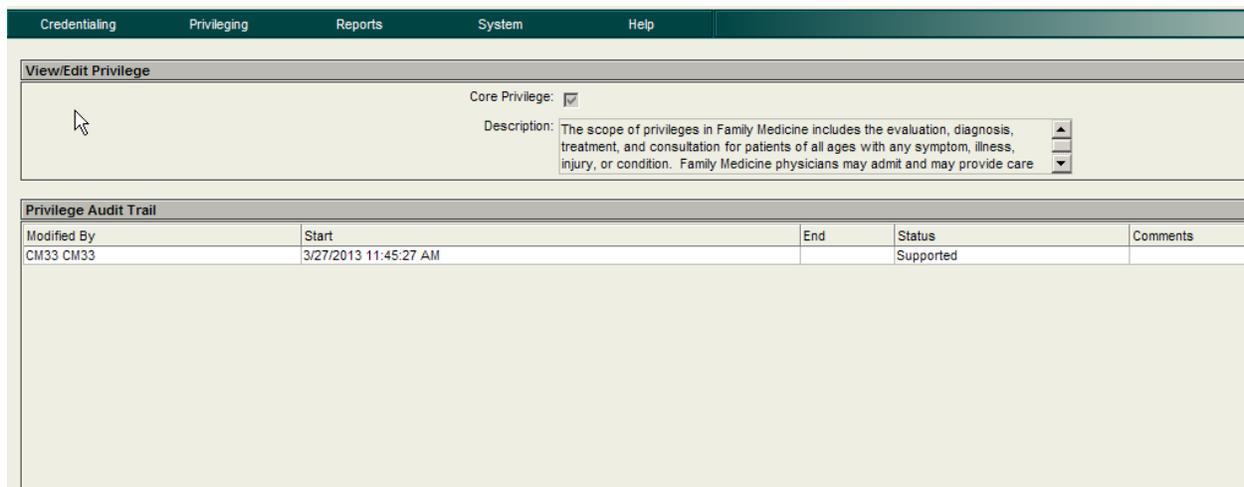
Facility Privilege Catalogs are required for the Parent UIC and any Branch Clinics. All privilege categories are initially defaulted to Not Supported. MPL Administrators are responsible for updating the facility privilege catalog to reflect changes in the facility or unit's support for an individual privilege item as a result of changes in staffing, equipment, or mission. MPL Administrators may change the designation of support for individual privilege items at any time, according to the guidance provided in [Sections 4.1](#).

After the initial configuration of a privilege item is performed, CCQAS requires MPL Administrators to enter explanatory comments for any subsequent changes made to the privilege item, as depicted in Figure 71. 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 71: Comment Option for Change to Privilege Designation**

When MPL Administrators enter and save the explanatory comments, the screen refreshes to display the updated list of supported privileges, as depicted in Figure 72. 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 72: Privilege Audit Trail**

When MPL Administrators change a privilege item from **Not Supported** to **Supported**, Providers who wish to be granted the newly supported privilege must submit a modification from approved applications on the provider’s worklist. The modification application is discussed in more detail in [Section 7](#).

When MPL 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.

MPL Changes made at the DoD/Service level are Global changes and triggers an automated email message to all CCs/MSSPs/CMs with the CLP Administrator Role, alerting them to the change(s). Any change other than CORE designation change(s) automatically defaults the new or revised privilege(s) to Not Supported. Action to update the facility privilege catalog is required if the facility supports the new/modified privilege(s).

## 5 Processing the E-Application for Clinical Privileges

CCQAS 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 Process

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

- **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 responsible for tracking and managing the review and approval of an application for clinical privileges at their UIC. If there is a question concerning credentials, the Non-Primary PAC will coordinate with the Primary PAC.
- **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 ECOMS/ECODS
- **PAs:** Usually MTF commanders or other designated personnel who are responsible for final approval of applications for clinical privileges at that UIC

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

- PACs or CC/MSSP/CMs may also be MPL Administrators (CLP Role)
- Reviewers may also be electronic 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

Each role/permission in CCQAS is differentiated from the others according to the roles/permissions assigned to the user's account. An individual can be assigned more than one privileging role. Refer to [Section 3](#) for details pertaining to the creation and maintenance of CCQAS user accounts.

Sections of the application that were modified by the Provider are flagged with new or modified icons 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. During PSV, 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 73 below depicts the flagged credentials.

Figure 73: Flagged Credentials

## 5.2 The Work List

CCQAS provides a work list to organize each Module user's work list tasks. The work list, depicted in Figure 74 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	CMS, CMS (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 74: Work List Screen for the CC/MSSP/CM

The following are important features of the **Work List** screen, which is depicted in Figure 75 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 **Completed** 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 year (360 days); 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.

The screenshot shows a web interface titled "WorkList for CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @". It features four tabs: "Work List", "My Applications", "Pending Applications", and "Submitted Applications". Below the tabs, there are three filter sections: "Status" with a dropdown menu set to "Open Tasks", "Role" with a dropdown menu set to "All", and "Tasks start date between" with two date input fields containing "10/02/2011" and "09/26/2012", each with a calendar icon. A "Filter" button is located to the right of the date fields.

**Figure 75: 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 or credentials record. 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.

### 5.4 Types of Electronic 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 electronic 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.

Type	Description
<b>1st E-App</b>	The first online application that is submitted by a Provider in CCQAS.
<b>Modification</b>	An application for a modification of clinical privileges that were previously granted or approved through the CCQAS workflow process at the assigned duty station. A modification application maintains the original expiration date
<b>Transfer (ICTB)</b>	Initiating an ICTB immediately generates an application for privileges at the temporary duty location (i.e., gaining facility), unless specifically suppressed or the UIC is not active on the privileging module.
<b>Transfer (PCS)</b>	Initiating a PCS immediately generates an application for privileges at the new duty location (i.e., gaining facility) if the UIC is active on the privileging module.
<b>Renewal</b>	An application for renewal of clinical privileges which are due to expire, including auto renewals which were previously granted through the CCQAS workflow process at the same duty station. This also refers to any EAP completed after the first EAP that is not a modification or transfer.

**Table 1: Types of Electronic Privilege Applications**

The following are important features of the electronic application:

- The application is pre-populated with a Provider’s most current credentials and assignment information from the CCQAS credentials record
- 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 new credentials to the application along with uploading supporting 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 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 application pre-populates with the Provider’s previous entries
- References are pre populated from the Credentials Record with a status of **Current = No**. Providers should edit the **References** section to indicate which references are still current or add new references
- Providers may upload scanned documents to the application, as appropriate

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

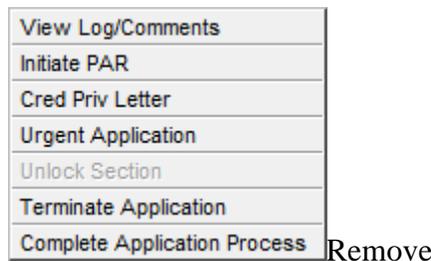
A record of all privilege applications processed through CCQAS by an individual CC/MSSP/CM is maintained on his or her **My Applications** screen, and may be accessed by clicking the **My Applications** tab, as depicted in Figure 76 below.



**Figure 76: My Applications Screen**

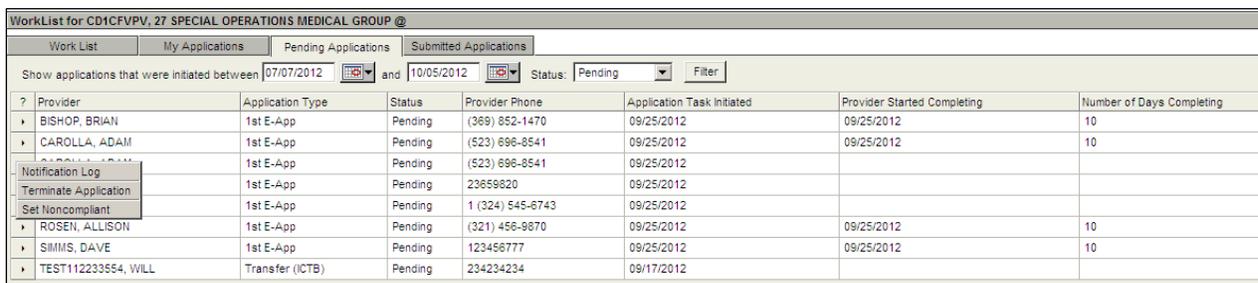
The following are important features of the **My Applications** screen:

- Users may search for a particular Provider application by entering the **Provider Last Name**, and then clicking the **Filter** button
- The **My 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



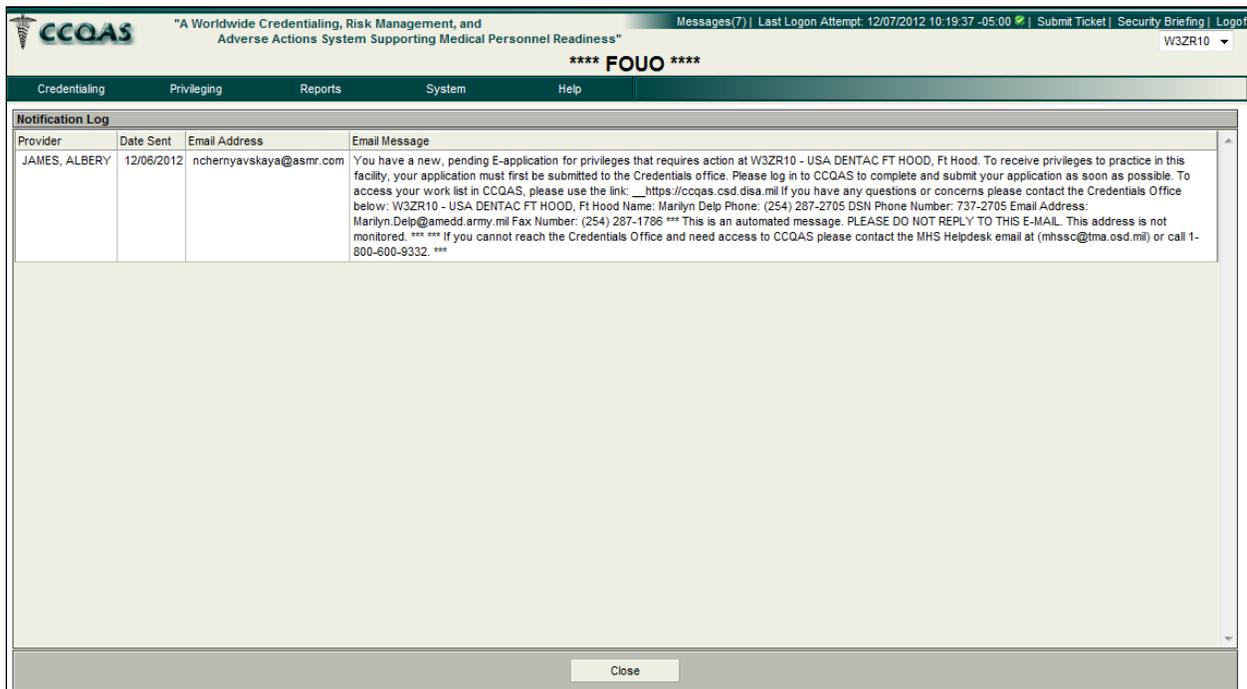
**Figure 77: My Application Hidden Menu**

The **Pending Applications** tab gives CC/MSSP/CMs visibility of all outstanding applications that have not yet been submitted at their facility or unit. It also displays the time elapsed since the application was created and the first email notification directing the provider to complete an E-application in CCQAS was sent. Figure 78 below depicts the **Pending Applications** tab.



**Figure 78: 'Pending Applications' Tab**

When CC/MSSP/CMs select the **Notification Log** option from the hidden menu, the **Notification Log** screen appears, as depicted in Figure 79 below. This screen indicates that a Provider at a facility has a new, pending E-application that requires action. The message under the **Email Message** section provides a detailed description of the action that needs to be performed, as well as contact information for questions about the action. While the E-application is in a pending status the provider is sent an email notification every 5 days up until 90 days when the E-application is deleted.



**Figure 79: Notification Log Screen**

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 necessary, CC/MSSP/CMs may select the option of **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 Provider user.

CC/MSSP/CMs may reactivate a noncompliant application at any time by selecting **Reactivate** from the hidden menu of actions, as depicted in Figure 80 below.

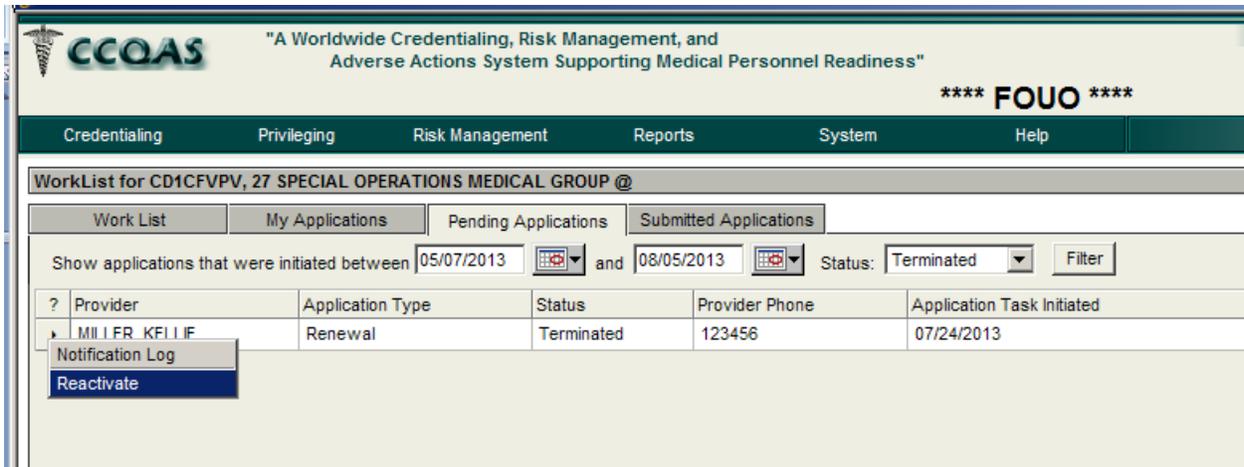


Figure 80: Reactivate Menu Item

## 5.5 Initial Review of a Privilege Application

After the Provider E-signs and submits his or her 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 81 below, or double-clicking anywhere on the record line item.



Figure 81: Work List Task – Application Ready for Review

CCQAS displays a message window asking CC/MSSP/CMs if they wish to assume responsibility for processing the application. This message window is depicted in Figure 82 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 the CC/MSSP/CM is the only staff member at his or her facility or unit who manages privilege applications, he or she must 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.

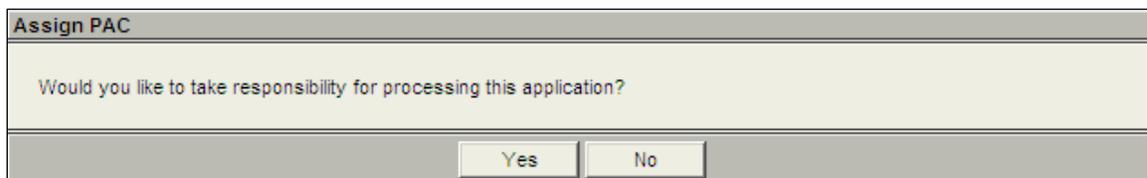


Figure 82: Assign PAC Screen

In order to move forward in the review process with this application, CC/MSSP/CMs must click **Yes**; otherwise, 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. After it is accepted, 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
- The accepting CC/MSSP/CM receives the Electronic PAR associated with these applications

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 sections.

### 5.5.1 The Provider Summary Tab

The **Provider Summary** tab is the first tab in the privilege application, as depicted in Figure 83 below. This tab displays demographic information that Providers entered into the **Profile**, **Identification**, and **Contact** sections of the electronic application.

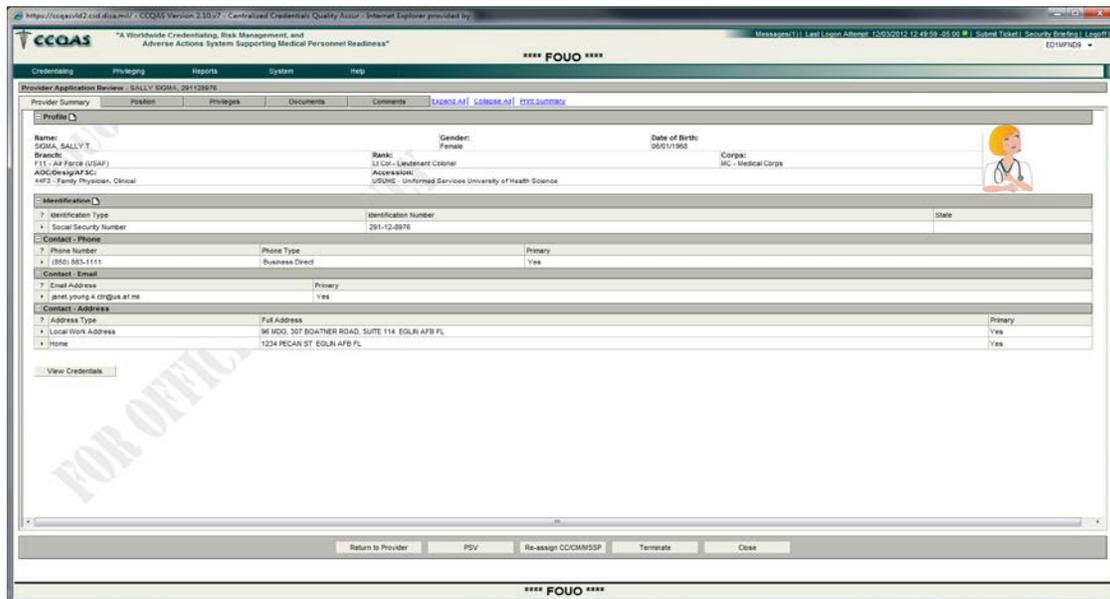
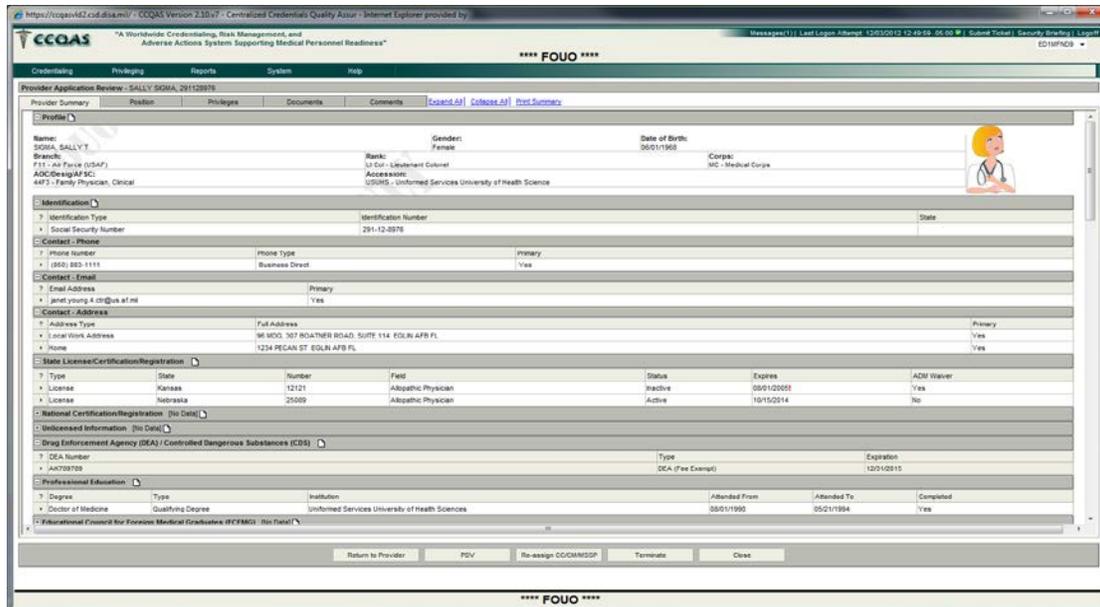


Figure 83: 'Provider Summary' Tab

The remainder of the credentials information in the application may be viewed by clicking the **View Credentials** button, as depicted in Figure 84 below.



**Figure 84: '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. After 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, depicted in Figure 85 below, is the second tab in the privilege application. This tab displays the information that Providers entered in the **Position** section of the electronic application.

Provider Application Review - PARKER SMITH, 244898989

Position

Provider Category:

Duty Section:

Duty Phone:

Date Reported to Current Assignment:

Projected Rotation/Permanent Change of Station Date:

Privileging

Are you requesting privileges at this time?  Yes  No

Type of Privileges Requested:

Type of Appointment Requested:

The E-app allows for privileges to be requested at multiple UICs.

UIC	Name	Location	Request Admitting Privileges?	Parent
<input checked="" type="checkbox"/>	CD1CFVPV	27 SPECIAL OPERATIONS MEDICAL GROUP @	<input type="checkbox"/>	Parent
<input checked="" type="checkbox"/>	FFL0LD	0161 MDG @	<input type="checkbox"/>	Branch Clinic

The E-app allows for Age Groups to be set at multiple UICs.

UIC	Neonates (Birth-28 days)	Infants (1-24 months)	Children (2-12 years)	Adolescents (13-17 years)	Young Adults (18-23 years)	Adults (24-65 years)	Geriatrics (>65 years)
CD1CFVPV	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FFL0LD	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Return to Provider PSV Re-assign CC/CM/MSSP Terminate Close

**Figure 85: Provider Privilege Application ‘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. The **Position** tab also allows CC/MSSP/CMs to view all UICs where the Provider has requested privileges via his or her e-application, as depicted at the bottom of the screen in Figure 85.

Providers who request admitting privileges must do so by checking the **Requested Admitting Privileges** check box on the **Position** tab.

**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 type of appointment and type of privileges requested 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.

CC/MSSP/CMs can edit the remainder some 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.

Based on the privilege approval date, CCQAS automatically calculates the privilege expiration date based on the type of appointments Providers select for one year for initial appointments, or two years for all other appointments.

Based on the privilege approval date, CCQAS automatically calculates the privilege expiration date based on the type of appointment one year for initial appointments, or two years for all other appointments.

### 5.5.3 The Privileges Tab

The **Privileges** tab, depicted in Figure 86, 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.

**Note:** CC/MSSP/CMs or MPL 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.

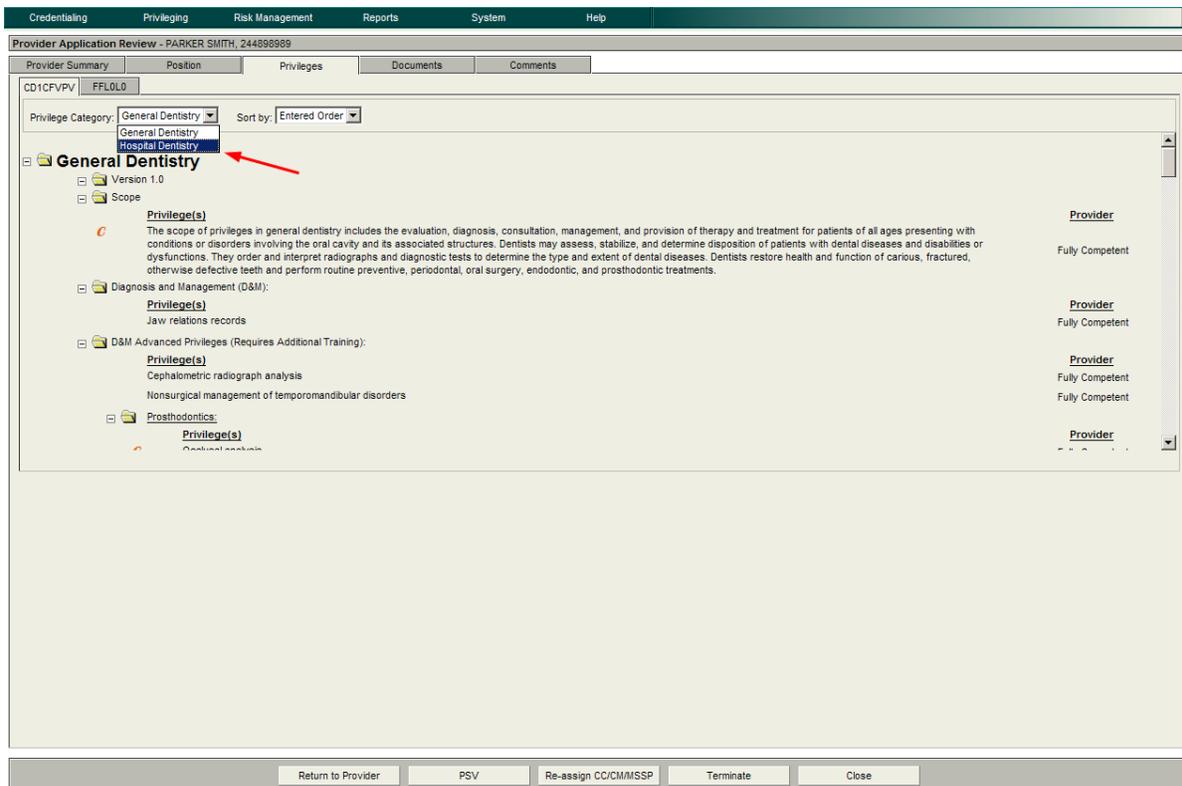


Figure 86: 'Privileges' Tab for General Dentistry

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

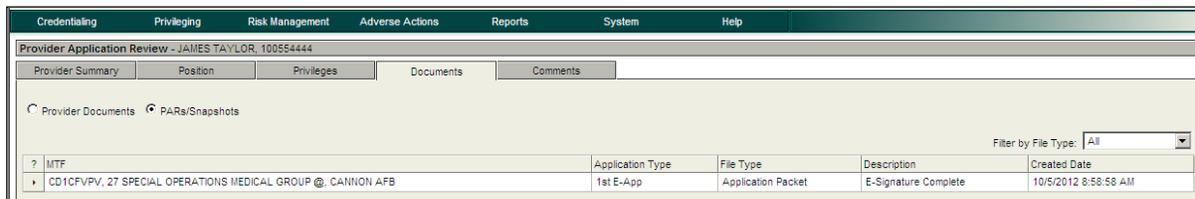


Figure 87: ‘Documents’ Tab for PAR Snapshot



Figure 88: “Documents” Tab for Provider Documents

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

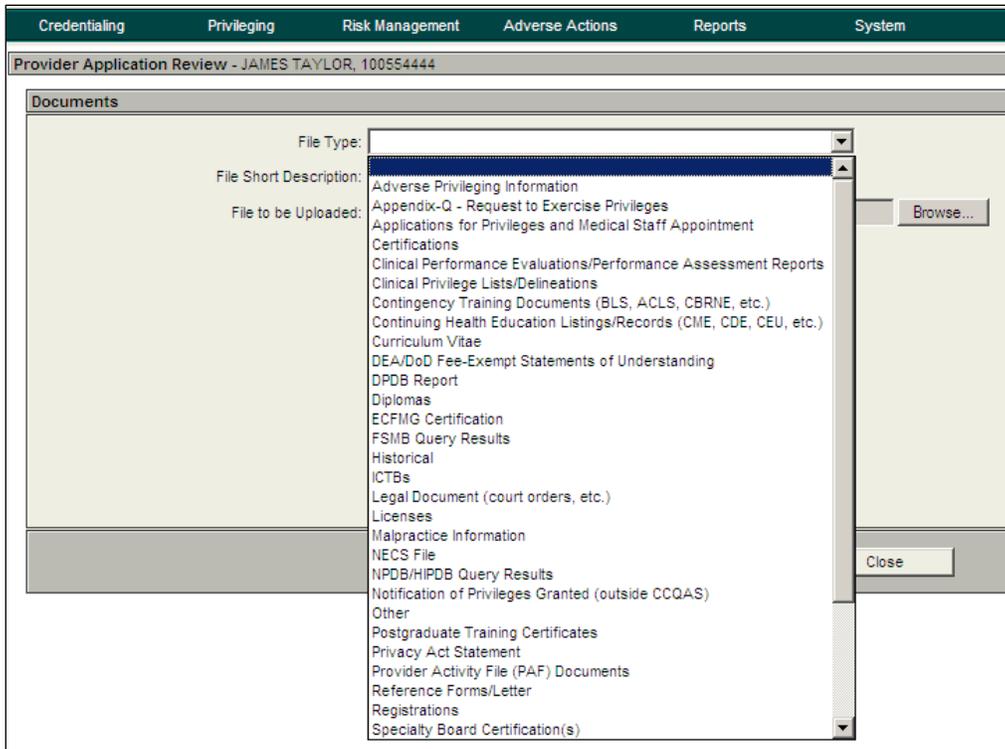
- **Provider Documents** or **PARs/Snapshots** documents may be displayed by selecting the appropriate radio button at the top of the tab, as depicted in Figure 87 and Figure 87 above.
- The list of documents associated with the application may be searched by selecting the desired document type from the **Filter by File Type** pick list
- The 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
- Provider Documents:

- 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 .gig file extension
- 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 **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
- PAR/Snapshots:
  - Snapshots are CCQAS-generated PDF files of the privilege application created each time the application is E-signed by a Provider, when the PSV is completed and when the PA's final decision is entered.
  - After PA approval, all previous snapshots will be removed for that privileging action
  - For **Clinical Support Staff**, PSV complete is the last snapshot saved

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 89 below depicts the **Add Documents** screen, where Providers and CC/MSSP/CMs can upload documents.

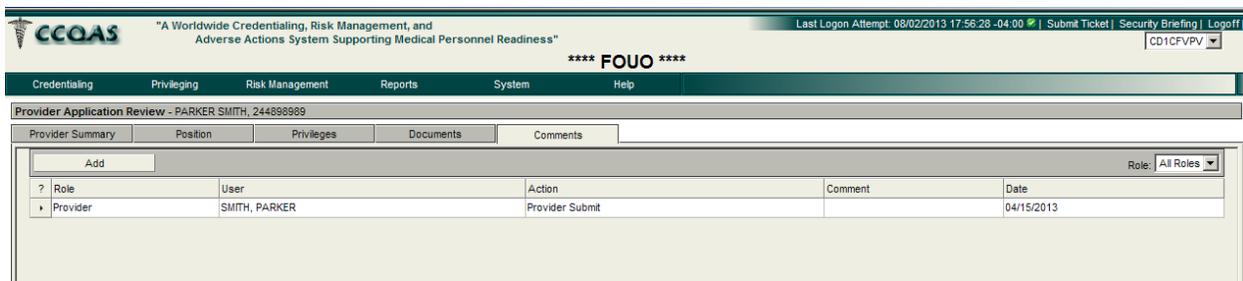


**Figure 89: Add Documents Screen for CC/MSSP/CM**

During the EAP completion process 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. After an application is submitted and PSV’ed, the attached documents may no longer be deleted. After the application is routed for review, documents uploaded by Providers can no longer be deleted.

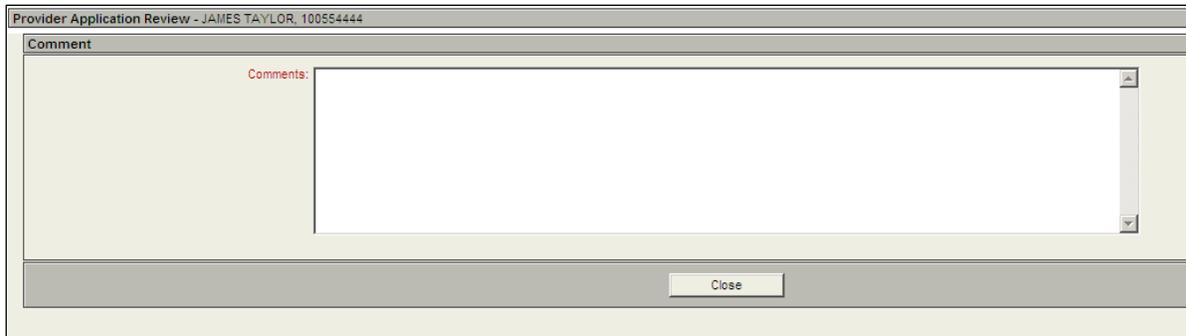
### 5.5.5 The Comments Tab

The **Comments** tab displays a summary record for all comments entered into the application as it proceeds through the review process. Figure 90 depicts the **Comments** tab.



**Figure 90: ‘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 91.



**Figure 91: 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 must select one of the buttons provided at the bottom of any tab within the application package (see Figure 92 below):

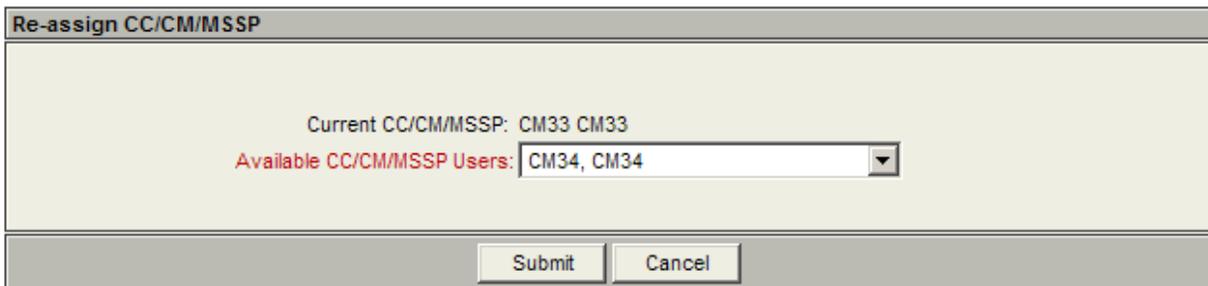
- The **Return to Provider** button routes the application back to a Provider who originally submitted it. CC/MSSP/CMs are required to unlock the section(s) and enter comments or instructions to Providers when they select this option. Providers then receive an email notification and a task, instructing 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 ownership of the application 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 92: 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 92 above. When selected, a window opens as depicted in Figure 93 below. It contains a pick list of all available CMs/MSSPs/CCs in the facility or unit to whom responsibility for the record may be transferred.



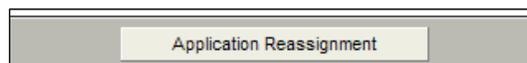
**Figure 93: Re-assign Screen**

After CC/MSSP/CMs click **Submit** (refer to Figure 93 above), full ownership 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 – Managing Privileging Workload: The PAC Supervisor Role.

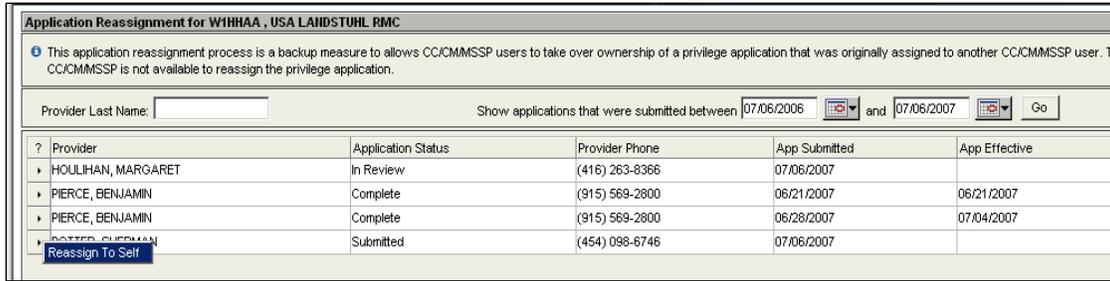
### 5.5.8 Taking Ownership of an Application from another CC/MSSP/CM

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 94 below.



**Figure 94: ‘Application Reassignment’ Button**

When CC/MSSP/CMs click the **Application Reassignment** button, the **Application Reassignment** screen appears, as depicted in Figure 95 below. This screen displays all applications submitted within the last year that are associated with a user’s facility or unit.



**Figure 95: Application Reassignment Screen**

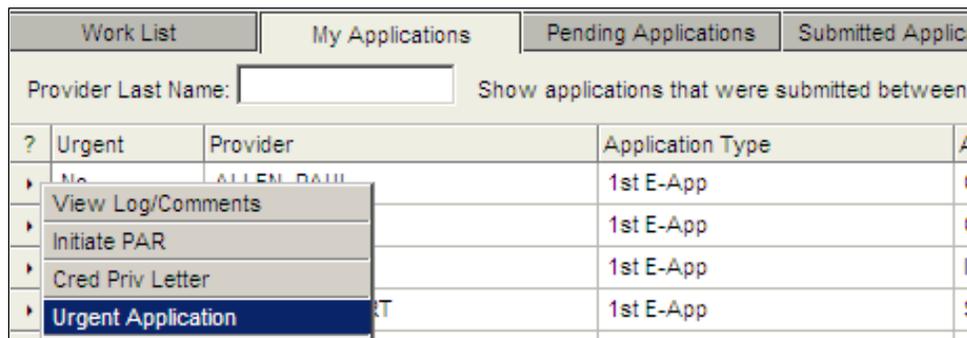
The following are important features of the **Application Reassignment** screen:

- 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 Reassignment** 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 ownership of an application by selecting **Reassign to Self** from the hidden menu of actions, as depicted in Figure 95 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 process.

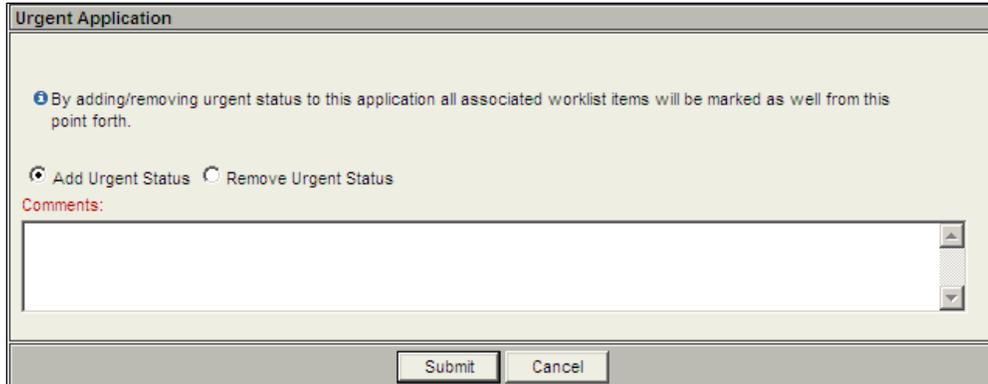
### 5.5.9 Setting an Application as Urgent

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 96 below.



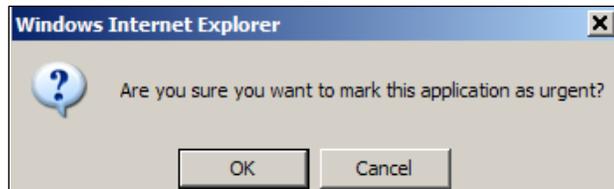
**Figure 96: Urgent Application Menu Item**

The **Urgent Application** window opens, as depicted in Figure 97 below. Users select the **Add Urgent Status** radio button, enter **Comments** explaining the details of the urgency, and click **Submit**.



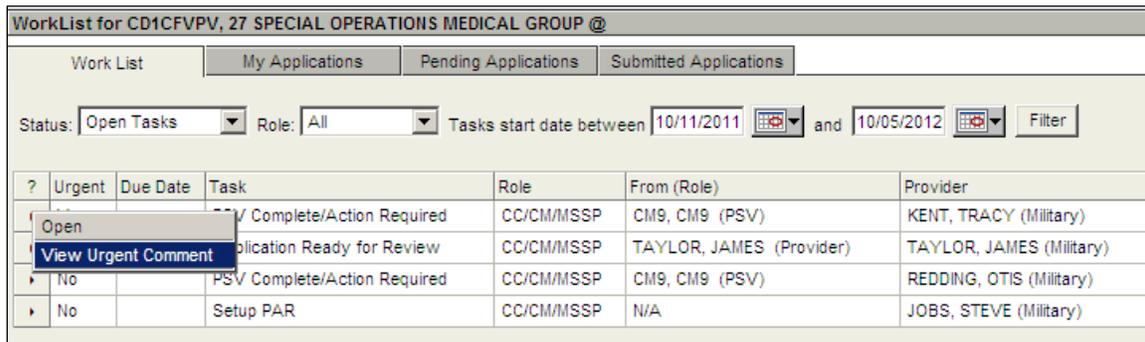
**Figure 97: Urgent Application Window**

A confirmation message is displayed, as depicted in Figure 98 below.



**Figure 98: Urgent Application Confirmation Message**

After users click **OK**, the work list is refreshed and the Urgent column for the application is now set to **Yes**. The explanatory comment that was entered may be viewed by selecting **View Urgent Comment** from the hidden menu of actions for the task on the Work List tab, as depicted in Figure 99 below.



**Figure 99: 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 97 above), the urgent status is removed.

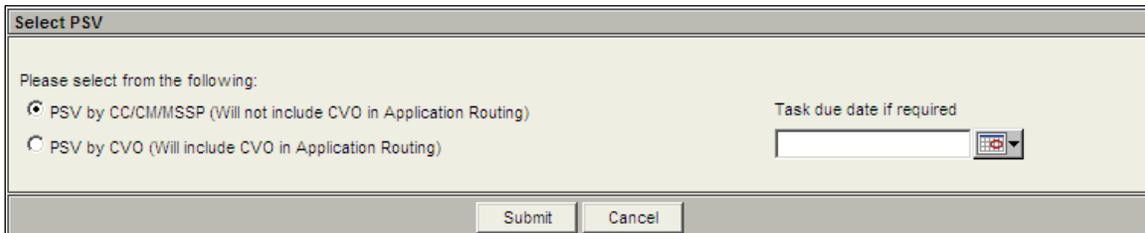
## 5.6 Routing a Privilege Application for Primary Source Verification

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 92.



**Figure 100: Action Options for E-Applications**

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 101 below depicts the **Select PSV** screen.



**Figure 101: 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 PAC Role 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 CVO Role 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.

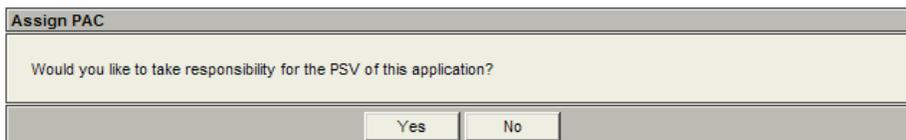
### 5.7 Primary Source Verification of a Privilege Application by CC/MSSP/CM

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 PAC Role functions for their facility or unit. Figure 102 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/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		09/17/2012

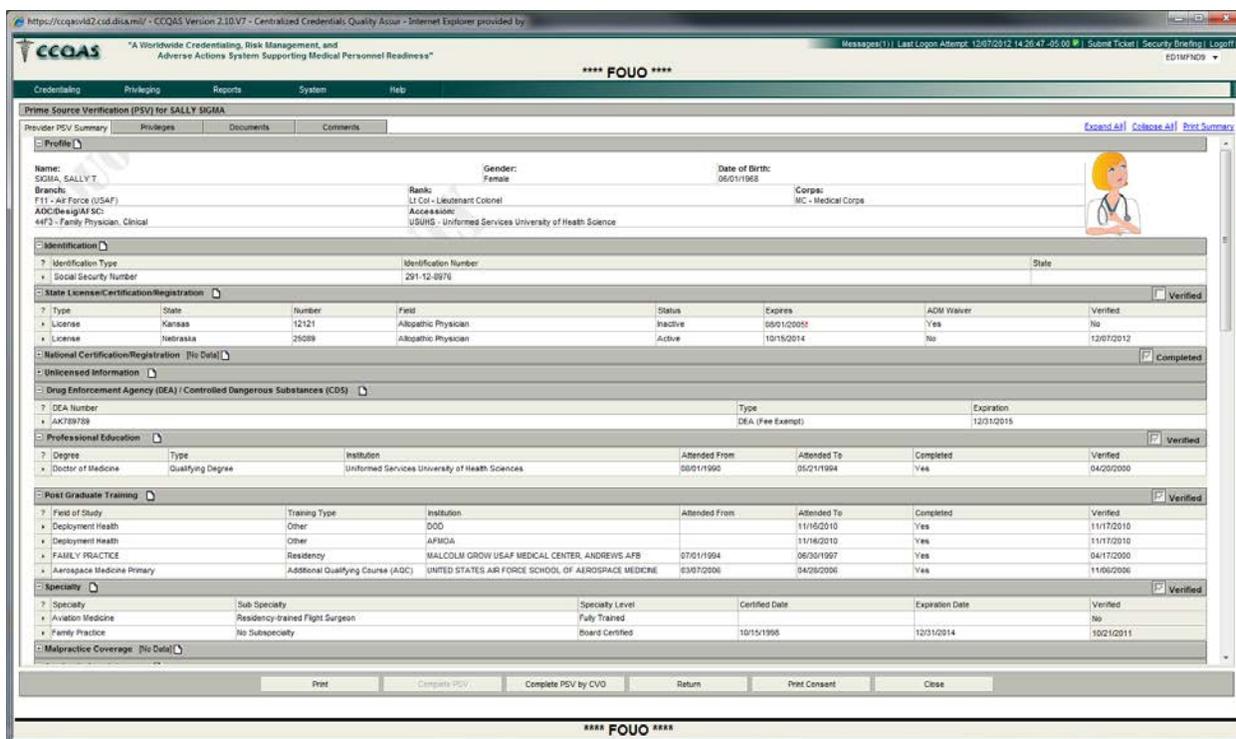
**Figure 102: Complete PSV Task**

A window opens, as depicted in Figure 103 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.



**Figure 103: 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 104 below. The **Provider PSV Summary** screen displays expanded sections of the privilege application that require PSV action.



**Figure 104: 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
- 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 1<sup>st</sup> 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 credentials record. 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
- **Complete PSV by CVO** allows the CC/MSSP/CM to reassign the Complete PSV task to the CVO
- **Return** routes the application back to the CC/MSSP/CM who has ownership of the application; the person in the role (whether it is CVO or CC/MSSP/CM) performing the PSV is required to enter comments explaining why the application is being returned. The CC/MSSP/CM then receives 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 submitted, as needed, to obtain primary source verification 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 105 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** 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 displays the 'State License/Certification/Registration' form within the CCQAS application. The form is divided into two main sections. The top section, 'State License/Certification/Registration', contains fields for License Type (License), Number (25689), Field (010 - Allopathic Physician), Issue Date (10/26/2004), Status (Active), State (NE - Nebraska), Expiration Date (10/15/2014), and an 'In Good Standing' checkbox. The bottom section, 'Prime Source Verification (PSV) Information', includes a 'Method' section with radio buttons for Written Correspondence, Telephone, Internet (selected), and Email. It also has fields for Contact Name, Position, Email, Phone, Institution, and URL (www.nebraska.gov). The form is entered by CM17 CM17 and includes a 'PSV Remarks' field. The interface includes a 'FOUO' watermark and navigation tabs at the top.

**Figure 105: 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. All current active licenses/certifications/registrations must undergo PSV each time a privilege application is processed. Inactive or Expired licenses which were not previously PSV'ed must all be PSV'ed at least one time.
- **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 (NCCPA)
- **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 may undergo PSV when a privilege application is processed. It may be appropriate to select the radio button

for **PSV Not Required** on a renewal application. The PSV section must be completed for all current references. 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 106 below) of the application becomes enabled. The performance of the required NPDB query should then be completed according to established Service and facility procedures. All NPDB queries for Navy facilities are performed centrally by the NPDB Manager.

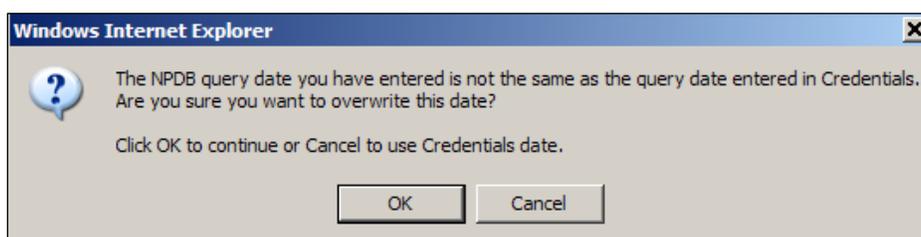
The performance of the required NPDB query should then be completed according to established Service and facility procedures. All NPDB queries for Navy facilities are performed centrally every two days by Service-level personnel only. Air Force CVOs also perform queries centrally for Air Force facilities, 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 the NPDB batch query report generated by CCQAS to perform NPDB queries. When the system has included the Provider’s name in the batch query report, it automatically un-checks **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 106: 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**, the **Result 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** and **Result 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 107 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 107: NPDB/HIPDB Update Warning Message**

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

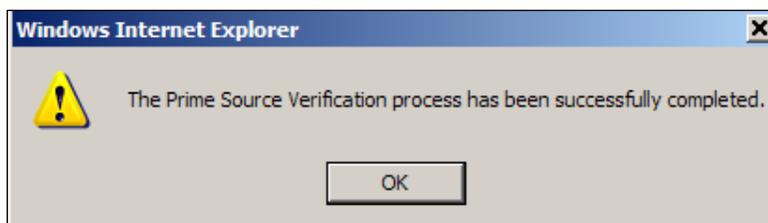
**Note:** The requirement to perform Federation of State Medical Boards (FSMB) queries is generally limited to Providers working in Air Force facilities with a practice history prior to January 1, 1995. Questions regarding FSMB query requirements should be directed to your Service Functional Representative.

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, the **Documents** tab, and **Comments** tab, are similar in form and function to the tabs described in Section 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 108 below.



**Figure 108: 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 the 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
- For **Clinical Support Staff**, PSV completes the application process

## 5.8 Primary Source Verification of a Privilege Application by the CVO

The process for PSV by CVO staff 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 ownership 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 at 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, or the PSV may be completed by clicking the **Complete PSV** 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 109 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 109: PSV Complete/Action Required Task**

**Note:** If the application was submitted by a CSS member or a Provider that is not requesting privileges, at the completion of the “Complete PSV” task the application is automatically closed by CCQAS. A read-only version of the application is permanently stored in the Provider’s **Applications** tab as part of the Provider’s historical record and the PSV Complete, PARs/Snapshot is available in the Documents section of the Provider credentials record. The **My Applications** tab only stores the Task Log for the application that a CC/MSSP/CM has ownership of.

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 110. The **Routing** button is only enabled after PSV of the application is completed.



**Figure 110: ‘Application Routing’ Button**

When selected, the **Application Routing** screen is displayed. The **Summary** tab is displayed first, as depicted in Figure 111 below, and then the **UIC** tab, as depicted in Figure 112 below.

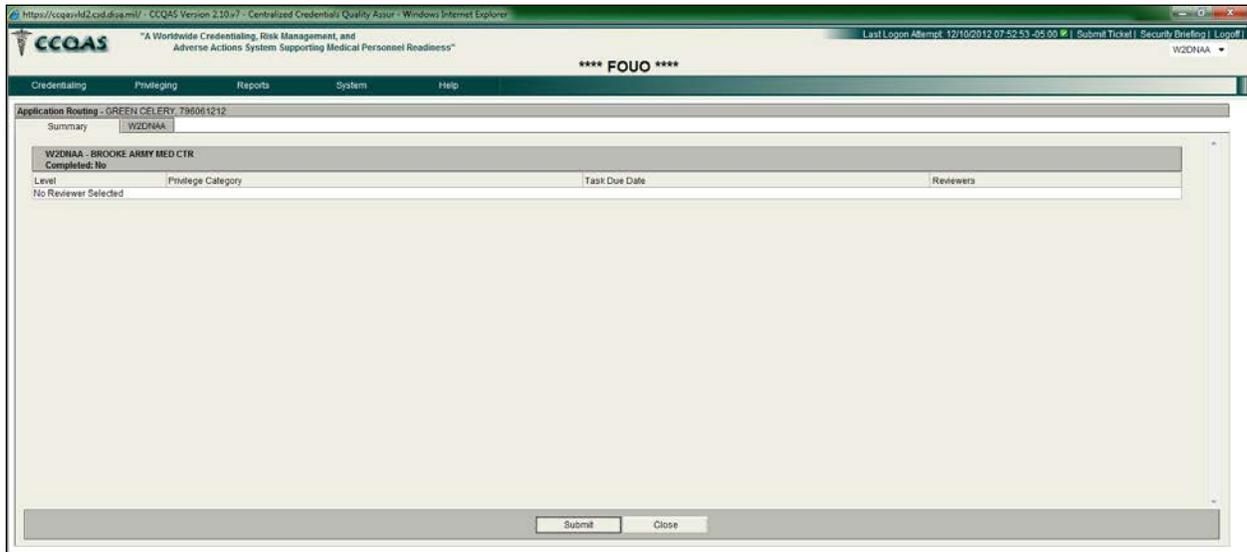


Figure 111: 'Application Routing Summary' Tab

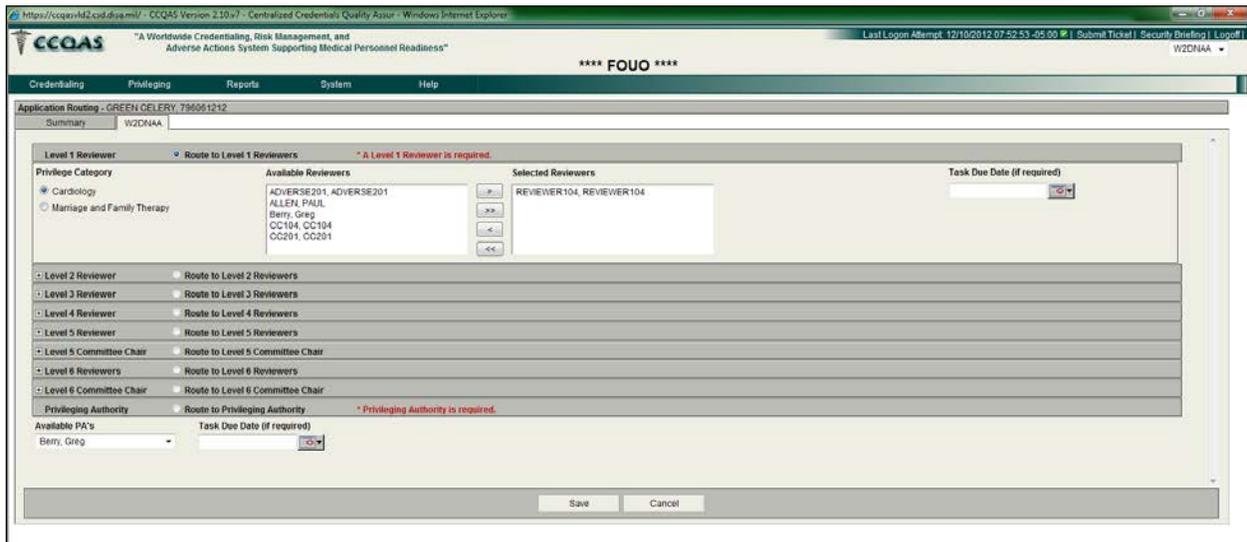
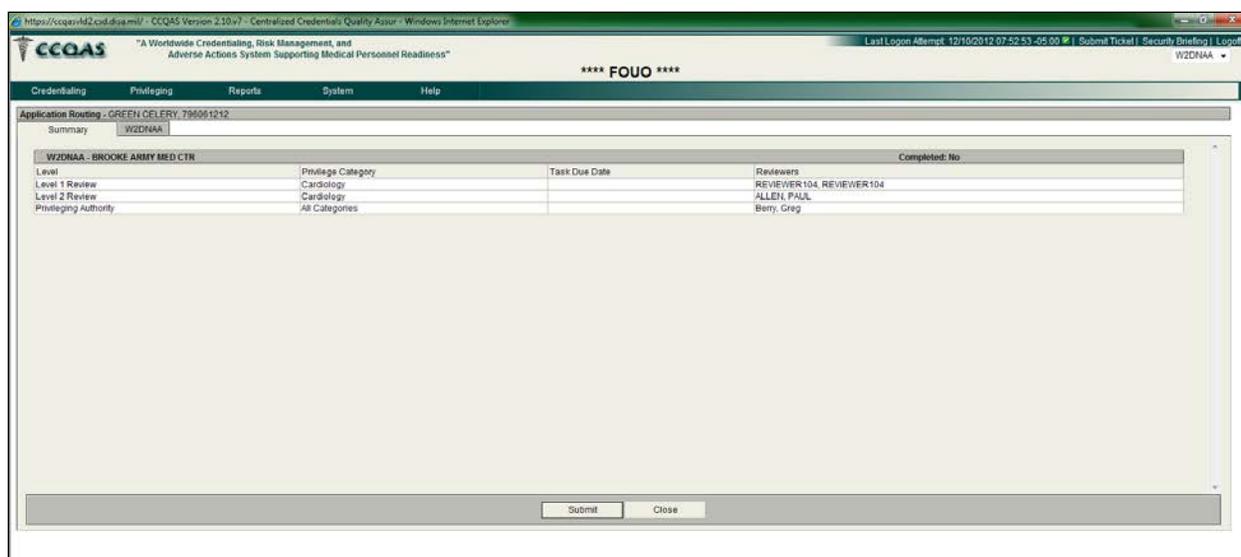


Figure 112: 'Application Routing UIC' Tab

Figure 113 below depicts the **Application Routing Summary** tab after routing is completed.



**Figure 113: ‘Application Routing Summary’ Tab after Routing is Completed**

**Note:** There are additional rules for processing branch clinic applications that differ from what is listed below. For those rules, refer to Section 16 (Branch Clinic Management):

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 and in accordance with Service policy
- 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 on the left (The names of all individuals who hold Reviewer Role are included in pick list for available reviewers.
- For each level, the list of all available Reviewers associated with the facility or unit appears in the **Available Reviewers** box on the left
- 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 on the right. 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 when the level is used, at a minimum a committee chairperson must be selected to participate in the review process
- The names of all individuals who hold PA role 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 review level order and concludes 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 Reviewer's CCQAS User account
- Level 1 review should be assigned to a Provider's clinical supervisor ; 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
- The final committee recommendation for Levels 5 and 6 reflect the recommendation submitted by the committee chair
- 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. After **Saving** the routing on the UIC tab, the CC/MSSP/CMs selects the Summary tab and clicks **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 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 CD1CFVPV, 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	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 for 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** tab, 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:			
Task Log						
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/CM/MSSP)
PSV Complete/Action Required	Closed	09/19/2012	10/05/2012	CM9 CM9	CC/CM/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/CM/MSSP	TRACY KENT (Provider)
Complete Application	Closed	09/19/2012	09/19/2012	TRACY KENT	Provider	ADMIN ADMIN
Close						

**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;"> <span>Task Log</span> <span>Comments</span> </div>				
Role	User	Action	Comment	Date
PAC	CMS, CMS	Add Urgency	dfsdf	10/05/2012 9:55:20 AM CST
Complete	CMS, CMS	Add Urgency	dfsdf	10/05/2012 9:55:20 AM CST
PSV	CMS, CMS	PSV Complete		09/19/2012 4:02:44 PM CST
Provider	KENT, TRACY	Provider Submit		09/19/2012 11:54:40 AM CST
Close				

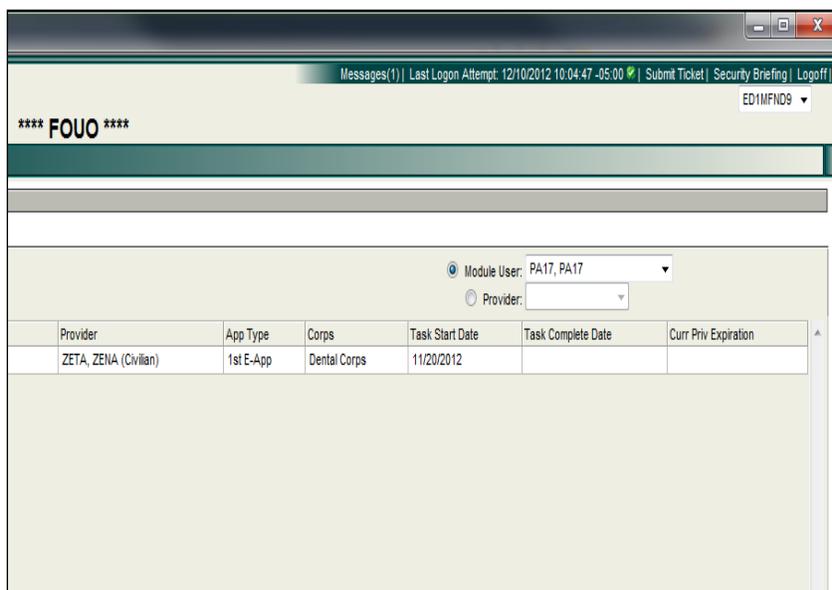
**Figure 116: ‘Comments’ Tab**

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 **Module User** pick list, located in the upper right-hand corner of the work list, as depicted in Figure 117 below.



**Figure 117: Retrieving an Application in Review**

The **Module User** pick list contains the name of all individuals who have been assigned to take some action on applications at the facility. 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

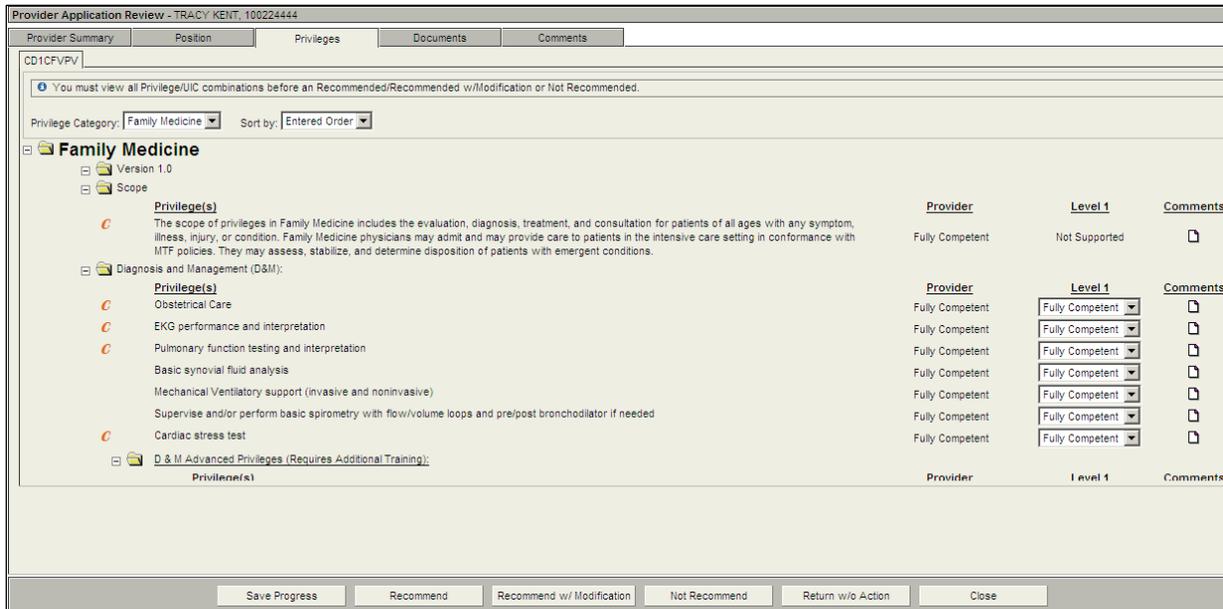
After CC/MSSP/CMs route an application for Level 1 review, each Level 1 Reviewer receives an email notification of a new task in CCQAS and a new task, **Task = Application Ready for Review** (depicted in Figure 118 below), is added to his or her work list. The application may be viewed from the work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

Privileging System Help										
WorkList for CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @										
Work List										
Status: Open Tasks Role: All Tasks start date between 10/11/2011 and 10/05/2012 Filter										
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 (🚩), on the **Provider Summary** tab, alerts Reviewers to any notes entered into the credentials portion of the application by a CC/MSSP/CM. Reviewers may view the notes by clicking on the red flag (🚩) but 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 displays privileges items requested by the Provider and defaults the Provider’s requested delineation into the Level 1 column, as depicted in Figure 119 below.



**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 can select a different delineation from the pick list and enter the required 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.

**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 are 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, entering a comment and responding to the following “Yes/No” question: “Are you recommending approval of this privilege as requested by the Provider?” Reviewers’ change of privilege designation or a “No” answer results in the **Recommend** option being disabled, and the application must be returned to the responsible CC/MSSP/CM, rather than moving forward 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. 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 (🚩), because at least one (1) Level 1 Reviewer differs from the Provider’s request, and the **Level 1** column will contain a yellow diamond (💠). When the yellow diamond is selected, it displays all Level 1 Reviewers’ delineations and comments. If the application proceeds to the PA, the PA will be the tie breaker and must select a delineation from the drop-down.

**Note:** It is recommended that all yellow diamonds are resolved prior to the application going to the PA. 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:

- **Save Progress** allows the Reviewer to review part of an application, then save his or her progress to return and complete the review at a later time/date.

- **Recommend** indicates that the Reviewer recommends approval of the Provider's request for privileges with the delineations listed in the Level 1 column
- **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 become a permanent part of the privileging application. Figure 121 below depicts the **Reviewer Recommendation** screen, where Reviewers enter their comments.

**Reviewer Recommendation**

**Recommendation:**  
Recommend w/ Modification

**Comments:**  
Review of training requirements for cardiovascular privileges is required

Submit 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	09/28/2012		
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
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 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
<b>Reviewer Recommendations/Comments</b>						
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:	
<div style="border: 1px solid black; height: 80px;"></div>	
<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.

CM/MSSP/CCs may then reroute the application to the Level 1 Reviewers. After 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 112 above.

After a Reviewer completes an application review task, the application may be viewed in read-only format from the **Work List** tab, Status=Completed Tasks. 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 yellow diamond (  ), 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.

**Note:** When the yellow diamond is selected, it displays all Level 1 Reviewers’ delineations and comments.

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

**Figure 126: Yellow Diamond Icon for Review Levels 2-6**

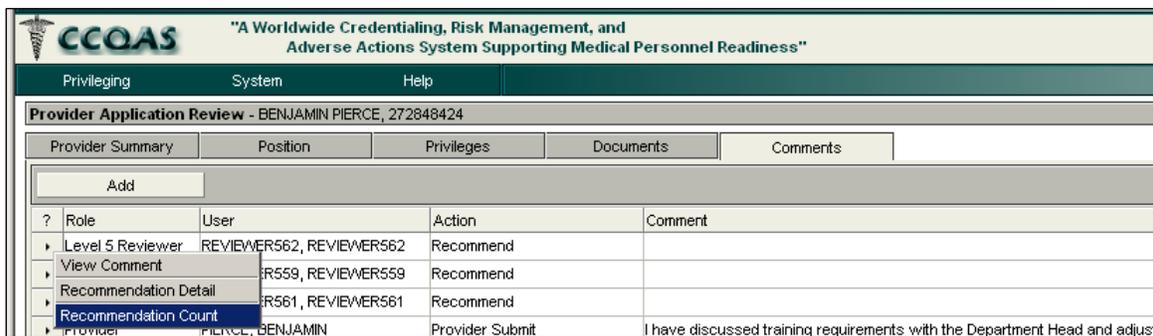
Levels 2, 3, and 4 Reviewers may also enter their own comments against any privilege item, by clicking on the empty notes icon (  ) or filled notes icon (  ) for the item. Their comments are then added to other Reviewer comments already entered for the privilege item. The entry of a comment with a “No” response to “Are you a recommending approval of this privilege as recommended by the Provider?” disables the **Recommend** option, and the application is 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.

The screenshot shows the "Recommendation Count" screen. It displays the following information:

- Provider Name: BENJAMIN PIERCE
- SSN: 272848424
- Branch: Army (USA) Active Duty
- Rank/Grade: Captain
- Application Status: Submitted
- Application Submitted: 06/13/2007
- Application Effective:
- Application Expiration:

Below this information is a table showing the tally of recommendations:

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
<b>Totals</b>	<b>4</b>	<b>1</b>	<b>0</b>

**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.

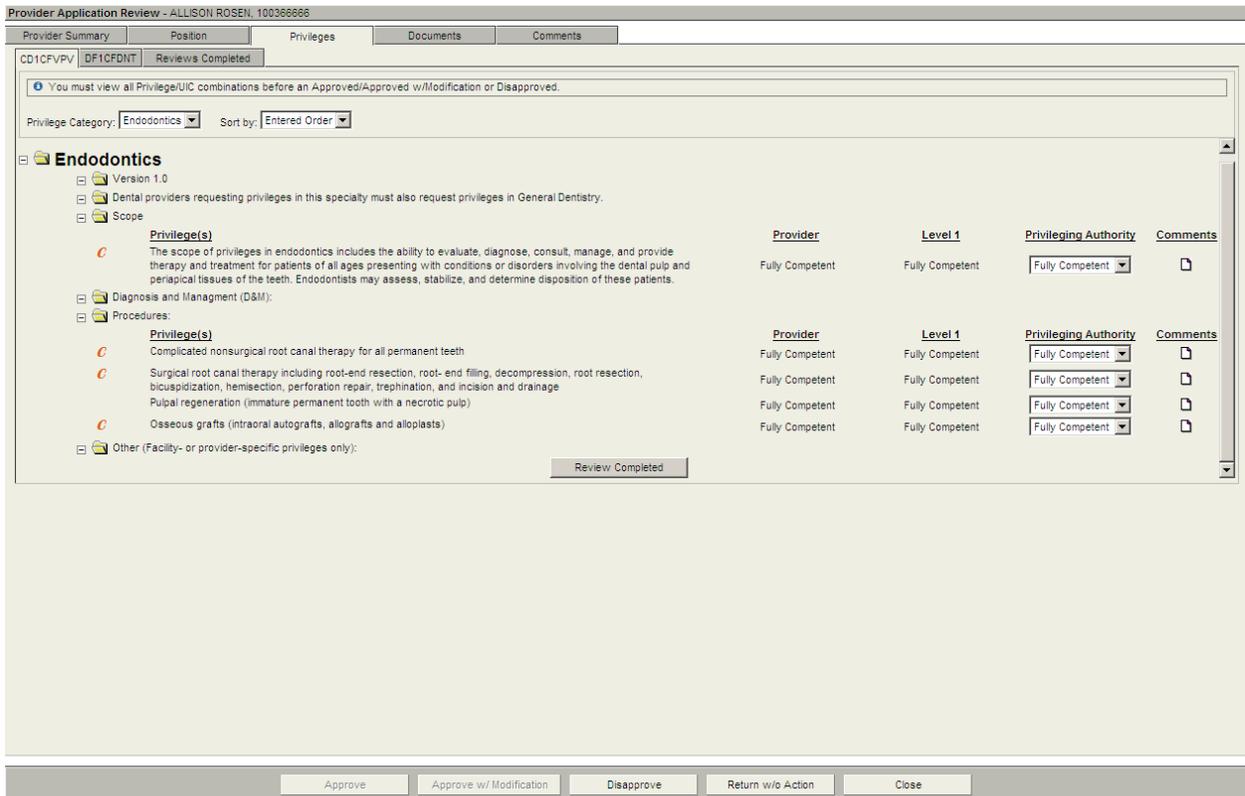
After the committee chair evaluates the individual recommendations of the committee members, he or she then submits the final committee recommendation.

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 reviews are complete after the committee chairs submit their recommendation.

**Note:** The entry of a comment with a “No” response to “Are you a recommending approval of this privilege as recommended by the Provider?” disables the **Recommend** option, and the application is returned to the CC/MSSP/CM, rather than being forwarded in the review process.

### **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 requesting privileges. 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.



**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 an additional Privileging Authority column 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 the **Privileging Authority** column is blank for a privilege item, (resulting from a difference in delineation entered by one or more Level 1 Reviewers), PAs are required to enter the delineation and comment 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 a Level 1 Reviewer’s privilege delineation are also noted with a red flag (🚩).

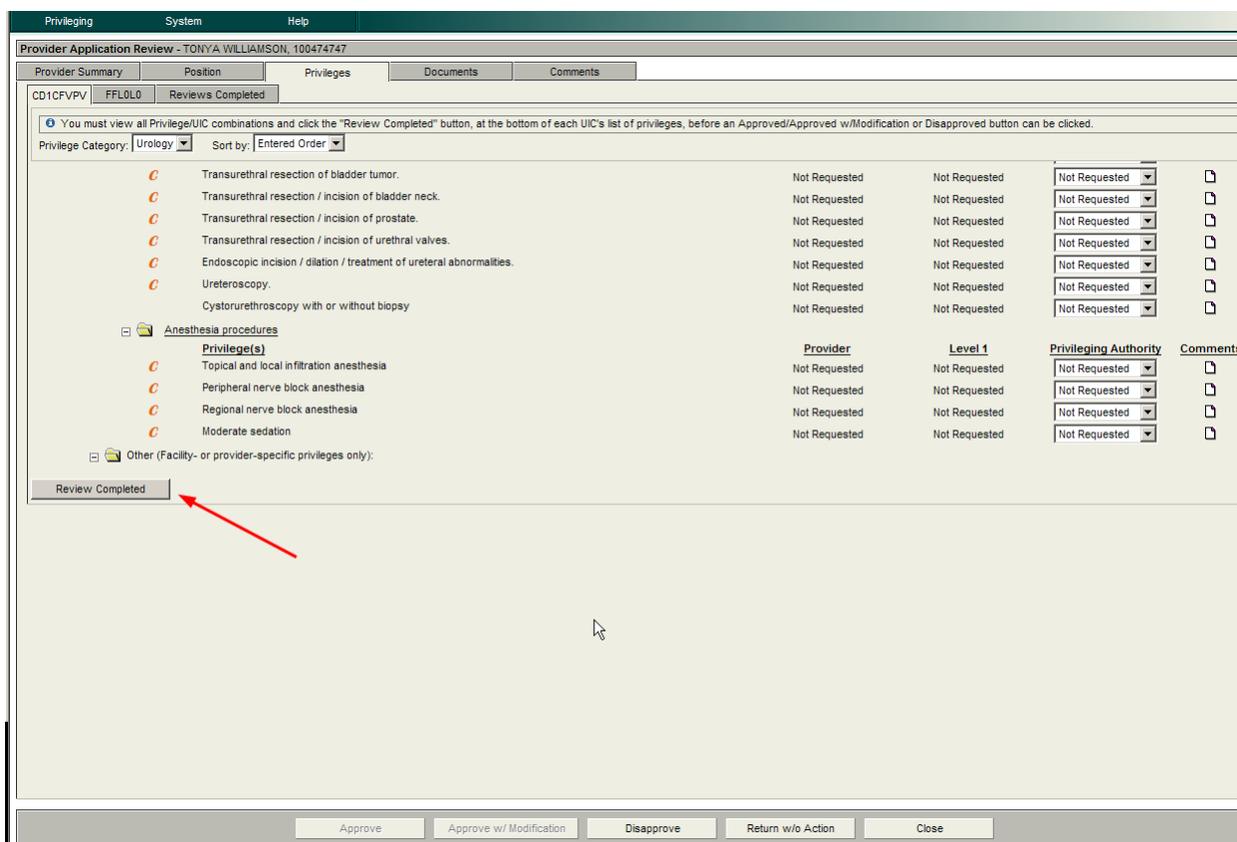
**Note:** When the yellow diamond is selected, it displays all Level 1 Reviewers’ delineations and comments.

**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 action 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 must select the **Review Completed** button (refer to Figure 130 below) at the bottom of the privilege list, and then submit his or her decision by clicking one of the following buttons at the bottom of the screen:

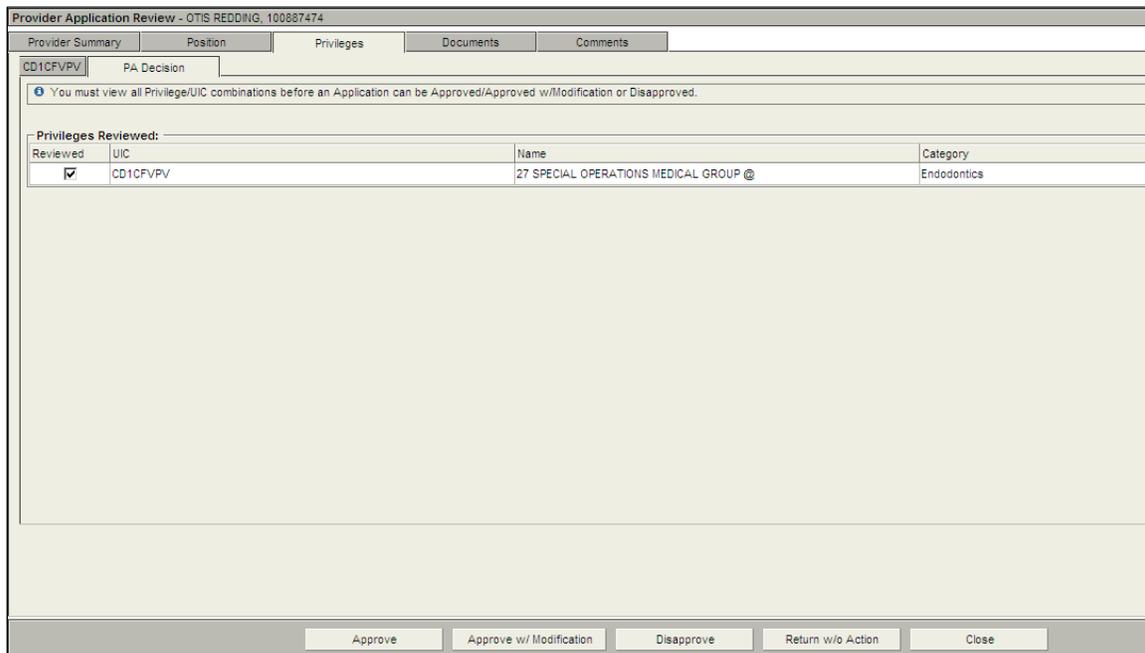


**Figure 130: PA Review Complete Button**

- **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. This is an adverse privileging action and triggers the peer review process
- **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 131 below depicts the **PA Decision** screen.



**Figure 131: 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 **Work List** tab, Status=Completed Tasks. 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

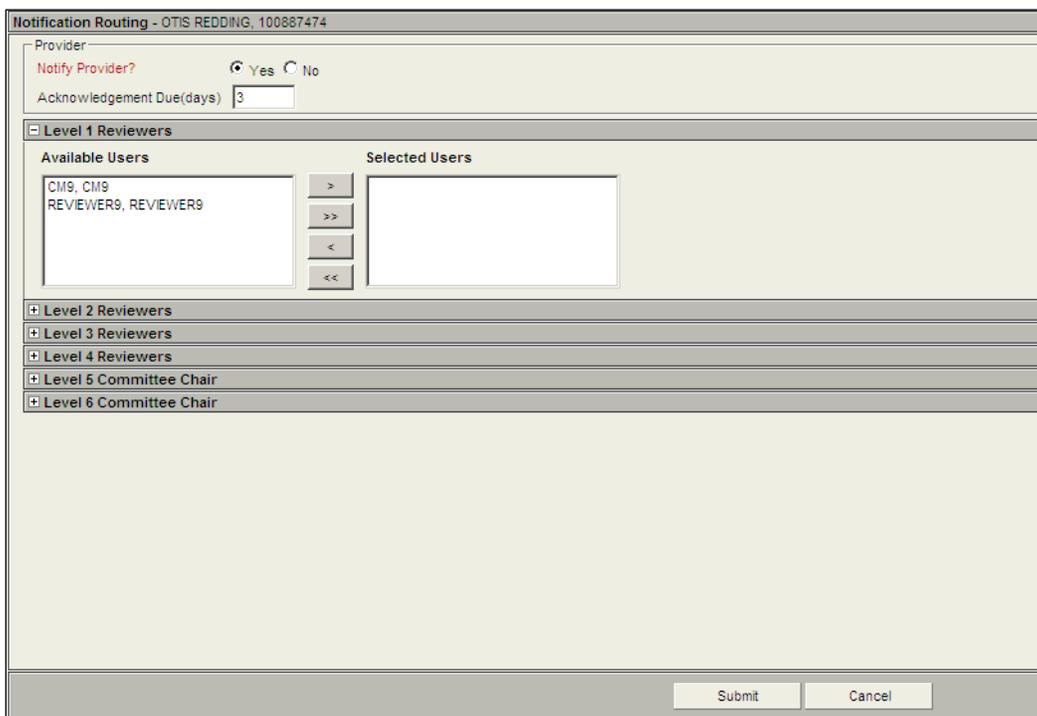
After a PA submits his or her final decision to approve the application for clinical privileges, the application is routed back to the CC/MSSP/CM. The CC/MSSP/CM receives a new work list item, **Task = PA Decision Complete/Action Required**. The CC/MSSP/CM completes the approval process by routing approval 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 132 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 132: ‘Notifications’ Button**

The **Notification Routing** screen appears, as depicted in Figure 133 below.



**Figure 133: 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. 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 134 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 134: Provider ‘Acknowledge’ Button on Summary Page

The view-only Privileged Provider Information Report is then displayed, as depicted in Figure 135 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			
<b>PRIVILEGED PROVIDER INFORMATION REPORT</b>			
SERVICE: Air Force UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @			
<b>PROVIDER</b> REDDING, OTIS	<b>SSN</b> XXX-XX-7474	<b>MILITARY/CIVILIAN</b> Military	
<b>ORGANIZATION UNIT</b> 27 SPECIAL OPERATIONS MEDICAL GROUP @	<b>MILITARY/CIVILIAN</b> Military	<b>ADMITTING</b> No	<b>TYPE OF PRIVILEGES</b>
<b>PRIVILEGE CATEGORY: Endodontics</b>			
<b>Version 1.0</b>			
<b>Dental providers requesting privileges in this specialty must also request privileges in General Dentistry.</b>			
<b>Scope</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
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	
<b>Diagnosis and Management (D&amp;M):</b>			
<b>Procedures:</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
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 135: Privileged Provider Information Report**

When Providers click the **Acknowledge** button (refer to Figure 134 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 136 below.

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

My Applications   System   Submit Trouble Ticket	
<b>Acknowledgment</b>	
<ul style="list-style-type: none"> <li>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, 12/10/2012 and expiring 12/09/2014. 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.</li> <li>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.</li> <li>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.</li> <li>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 the facility's bylaws.</li> </ul>	
<input checked="" type="radio"/> Accept <input type="radio"/> I do not concur and will submit an appeal as outlined in the facility's bylaws.	
<input type="button" value="Complete Acknowledgment"/> <input type="button" value="Cancel"/>	

**Figure 136: Provider “Acknowledgment” Page**

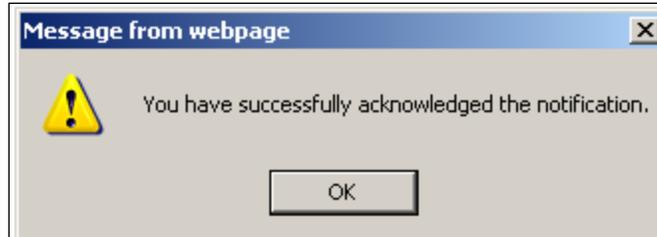


Figure 137: Provider Acknowledgement Notification

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 138 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.

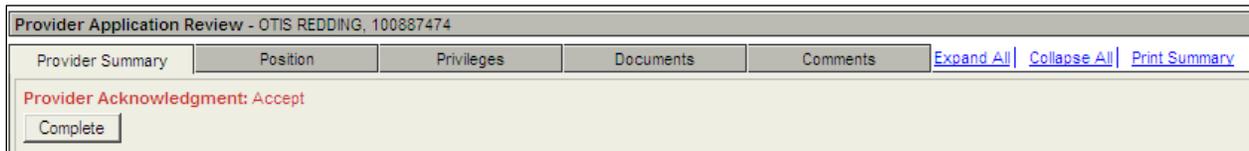


Figure 138: ‘Complete’ Button

After CC/MSSP/CMs click the **Complete** button, the application review process is closed. The assigned CC/MSSP/CM, PA, and Reviewers may access a read-only version of the approved application from the **Work List** tab, Status=Completed Tasks at any time, as depicted in Figure 139.

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv E
Yes		PSV Complete/Action Required	CC/CM/MSSP	CM33, CM33 (PSV)	PINSKY, DREW (Military)	Modification	Medical Corps	02/25/2013	04/09/2013	
Yes		Complete PSV	PSV	CM33, CM33 (PSV)	PINSKY, DREW (Military)	Modification	Medical Corps	02/25/2013	02/25/2013	
Yes		Application Ready for Review	CC/CM/MSSP	PINSKY, DREW (Provider)	PINSKY, DREW (Military)	Modification	Medical Corps	02/25/2013	02/25/2013	
Yes		Complete PSV	PSV	CM33, CM33 (PSV)	BLACK, JACOB (Military)	1st E-App	Biomedical Sciences Corps	10/09/2012	10/09/2012	
Yes		Application Ready for Review	CC/CM/MSSP	BLACK, JACOB (Provider)	BLACK, JACOB (Military)	1st E-App	Biomedical Sciences Corps	10/09/2012	10/09/2012	
No		Application Ready for Review	CC/CM/MSSP	SMITH, PARKER (Provider)	SMITH, PARKER (Military)	1st E-App	Dental Corps	04/15/2013	08/05/2013	
No		Application Ready for Review	CC/CM/MSSP	KIMMEL, JOHN (Provider)	KIMMEL, JOHN (Military)	1st E-App	Medical Corps	04/12/2013	04/12/2013	
No		PA Decision Complete/Action Required	CC/CM/MSSP	PA9, PA9 (Privileging Authority)	EVERDEEN, CATNISS (Military)	1st E-App	Medical Corps	03/27/2013	03/27/2013	
No		Application Returned/Action Required	CC/CM/MSSP	REVIEWER49, REVIEWER49 (Level 1 Reviewer)	EVERDEEN, CATNISS (Military)	1st E-App	Medical Corps	03/27/2013	03/27/2013	
No		PSV Complete/Action Required	CC/CM/MSSP	CM33, CM33 (PSV)	EVERDEEN, CATNISS (Military)	1st E-App	Medical Corps	03/27/2013	03/27/2013	
No		Complete PSV	PSV	CM33, CM33 (PSV)	EVERDEEN, CATNISS (Military)	1st E-App	Medical Corps	03/27/2013	03/27/2013	
No		Application Ready for Review	CC/CM/MSSP	EVERDEEN, CATNISS (Provider)	EVERDEEN, CATNISS (Military)	1st E-App	Medical Corps	03/27/2013	03/27/2013	
No		PA Decision Complete/Action Required	CC/CM/MSSP	PA9, PA9 (Privileging Authority)	OTS, MISTER (Military)	Modification	Medical Corps	02/28/2013	02/28/2013	02/27/2015
No		PSV Complete/Action Required	CC/CM/MSSP	CM33, CM33 (PSV)	OTS, MISTER (Military)	Modification	Medical Corps	02/28/2013	02/28/2013	02/27/2015
No		Complete PSV	PSV	CM33, CM33 (PSV)	OTS, MISTER (Military)	Modification	Medical Corps	02/28/2013	02/28/2013	02/27/2015
No		Application Ready for Review	CC/CM/MSSP	OTS, MISTER (Provider)	OTS, MISTER (Military)	Modification	Medical Corps	02/28/2013	02/28/2013	02/27/2015

Figure 139: ‘My Applications’ Tab with Completed Applications

The Provider may access a read-only version of the approved application from the **Applications** tab (for provider only users) or from the **My Applications, Applications** tab (for Dual users) at any time. The App Status will be **Closed**.

### 5.17 The Updated Provider Credentials Record

Following the completion of the PSV process, the credentials information entered into the electronic application updates the Provider’s credentials record in CCQAS. The Provider’s CCQAS credentials record is explained in detail in [Section 6](#).

The updated credentials record at the primary UIC will be editable (refer to Figure 140 below), and the updated record at the non-primary UIC will be primarily read-only (refer to Figure 141 below).

The screenshot shows the 'Provider' profile page for Robert Peters. The top header includes a 'Close Provider Record' button and navigation arrows. Below the header, key information is displayed: Name: ROBERT PETERS, SSN: 123-99-0000, Branch: F11, Primary UIC: CD1CFVPV, Rank: Maj Gen, Cred Status: Active, Corps: MC, Input Clerk: CM9, AOC/Desig/AFSC: 40C0, and Provider Status: Dual.

The main form area is titled 'Profile' and contains a 'Save' button and a 'Help?' link. A note states: 'If known under another name, please complete the alias section.' The 'Provider' section includes fields for Last Name (PETERS), First Name (ROBERT), MI, Suffix, Title, Person ID Type (Social Security Number), Person ID (123-99-0000), Gender (Male), Date of Birth (08/01/1973), Citizenship, Marital Status (Married), NPI, and File Mgr (Married/Single). A 'No Photo Available' placeholder is present with an 'Upload, Edit Photo' button.

The 'Military Information' section is checked and includes dropdowns for Branch (F11 - Air Force (USAF)), Rank (Maj Gen - Major General), Corps (MC - Medical Corps), AOC/Desig/AFSC (40C0 - Medical Commander), and Accession (DA - Direct Accession).

The 'Alias Information' section has an 'Add' button and a table with columns: Alias Last Name, Alias First Name, Alias MI, Suffix, and NPDB. The table currently shows 'No records returned.'

**Figure 140: Editable Data at Primary UIC**

**Provider** Name: ROBERT PETERS SSN: 123-99-0000 Branch: F11 Primary UIC: CD1CFVPV Rank: Maj Gen Cred Status: Active Corps: MC Input Clerk: CM9 AOC/Desig/AFSC: 40C0 Provider Status: Dual

**Profile**

Last Name: PETERS First Name: ROBERT MI: Suffix: Title:

Person ID Type: Social Security Number Person ID: 123-99-0000

Gender: Male Date of Birth: 08/01/1973 Citizenship:

Marital Status: Married NPI: Source DMHRS

File Mgr:

No Photo Available

Upload, Edit Photo

**Military Information**

Branch: F11 - Air Force (USAF) AOC/Desig/AFSC: 40C0 - Medical Commander

Rank: Maj Gen - Major General

Corps: MC - Medical Corps Accession: DA - Direct Accession

**Alias Information**

Add

Alias Last Name	Alias First Name	Alias MI	Suffix	NPDB
No records returned.				

**Figure 141: Read-Only Data at Non-Primary UIC**

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 142 below. Following this update, the appointment 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 has been approved at all facilities.

**Provider** Name: OTIS REDDING SSN: 100-88-7474 Branch: F11 Primary UIC: CD1CFVPV Rank: Brig Gen Cred Status: Active Corps: DC Input Clerk: CM9 AOC/Desig/AFSC: 47E4

**Privileges**

All UICs Current UIC

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

Open View Privileges

**Figure 142: Privileges Section in the Credentials Record**

The same privileging information is also updated and available in the **Work History**, **Assignments** tab of the credentials record. Open the assignment and then select the **Privileges** tab. All approved privilege applications for the specific assignment are listed and can be edited as described above in the **Privileges** section.

To view the approved electronic 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 143 below.

\*\*\*\* 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**

<b>SERVICE: Air Force</b>		
<b>UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @</b>		
<b>PROVIDER</b>	<b>SSN</b>	<b>MILITARY/CIVILIAN</b>
REDDING, OTIS	XX-XX-7474	Military
<b>ORGANIZATION UNIT</b>	<b>MILITARY/CIVILIAN ADMITTING</b>	<b>TYPE OF PRIVILEGES</b>
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- and 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
Ossaeous grafts (intraoral autografts, allografts and alloplasts)	Fully Competent	Fully Competent

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

**Figure 143: 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 all other appointments.

CC/MSSP/CMs may view and edit these expiration dates in the **Privileges** section of a Provider’s credentials record by selecting from the hidden menu of actions for the application. The **Provider Privileges** page opens, as depicted in Figure 144 below.

Credentiaing	Priviling	Risk Management	Reports	System	Help																						
<div style="text-align: right; border-bottom: 1px solid black;">Close Provider Record    &lt;&lt;    &gt;&gt;</div>																											
<b>Provider</b> Name: ADAM COROLLA                      SSN: 100-99-5656                      Primary UIC: CD1CFVPV                      Cred Status: Active                      Input Clerk: CM33                      Provider Status: ML																											
<div style="border-bottom: 1px solid black;">Privileges</div> <div style="display: flex; justify-content: space-between;"> <span>All UICs    Current UIC</span> <span><a href="#">Help?</a></span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>UIC</th> <th>Status</th> <th>App Type</th> <th>Provider Category</th> <th>Corps</th> <th>Military/Civilian</th> <th>Type of Appointment</th> <th>Type of Privileges</th> <th>App Date</th> <th>Effective Date</th> <th>Expiration Date</th> </tr> </thead> <tbody> <tr> <td>CD1CFVPV</td> <td>Inactive</td> <td>1st E-App</td> <td>Physician</td> <td>MC</td> <td>ML</td> <td>Active</td> <td>Regular</td> <td>02/21/2013</td> <td>02/21/2013</td> <td>02/22/2013</td> </tr> </tbody> </table> <div style="margin-top: 5px;"> <span>Open</span>    <span style="border: 1px solid black; padding: 2px;">View Privileges</span> </div>						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	Physician	MC	ML	Active	Regular	02/21/2013	02/21/2013	02/22/2013
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	Physician	MC	ML	Active	Regular	02/21/2013	02/21/2013	02/22/2013																	

**Figure 144: Selecting to View Provider Privileges**

\*\*\*\* FOUO \*\*\*\*

Name: COROLLA, ADAM, Appointment: Active Priv. Granted Date: 21 Feb 13  
 Mil/Civ: Military Corps: MC Privileges: Regular Priv. Expiration Date: 22 Feb 13

PRIVILEGED PROVIDER INFORMATION REPORT

<b>SERVICE: Air Force</b>			
<b>UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @</b>			
<b>PROVIDER</b>	<b>SSN</b>	<b>MILITARY/CIVILIAN</b>	
COROLLA, ADAM	XXX-XX-5656	Military	
<b>ORGANIZATION UNIT</b>	<b>MILITARY/CIVILIAN ADMITTING</b>	<b>TYPE OF PRIVILEGES</b>	
27 SPECIAL OPERATIONS MEDICAL GROUP @	Military	No	Regular
<b>PRIVILEGE CATEGORY: Aerospace Medicine</b>			
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.			
<b>Scope</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
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. Additionally, Aerospace Medicine physicians apply preventive medicine and occupational medicine principles as they apply to the aerospace/flight communities which they serve.	Fully Competent	Fully Competent	
<b>Diagnosis and Management (D&amp;M):</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
Manage radiation health conditions	Fully Competent	Fully Competent	
Interpret pulmonary function studies	Fully Competent	Fully Competent	
Interpret biological monitoring studies	Fully Competent	Fully Competent	
Interpret audiograms	Fully Competent	Fully Competent	
Perform occupational-specific medical examinations and certify respirator use	Fully Competent	Fully Competent	
<b>Hyperbaric Medicine:</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
Management of decompression sickness	Not Requested	Not Requested	

This document is protected by 10 USC 1102

\*\*\*\* FOUO \*\*\*\*

Page 1

Figure 145: Provider Privileges

The expiration dates entered on the **Privileges** 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.

### 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.

**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 146 below. In most cases, Service-level CCQAS Administrators assign the “PAC Supervisor” role to the appropriate facility personnel.



**Figure 146: PAC Supervisor Role on the ‘Roles/Permissions’ Tab**

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. CCQAS only allows for either CVO Supervisor or PAC Supervisor roles.

Users who have “PAC Supervisor” permissions can see an additional tab labeled **Submitted Applications** when they access the Privileging module, as depicted in Figure 147 below.

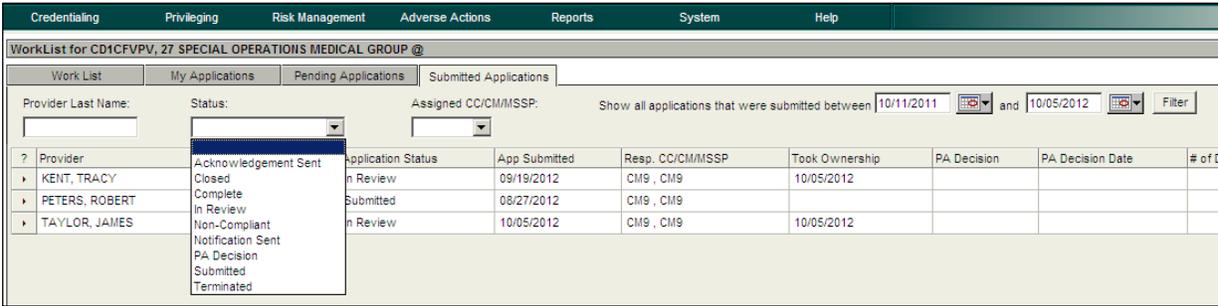


Figure 147: Submitted Applications Screen

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

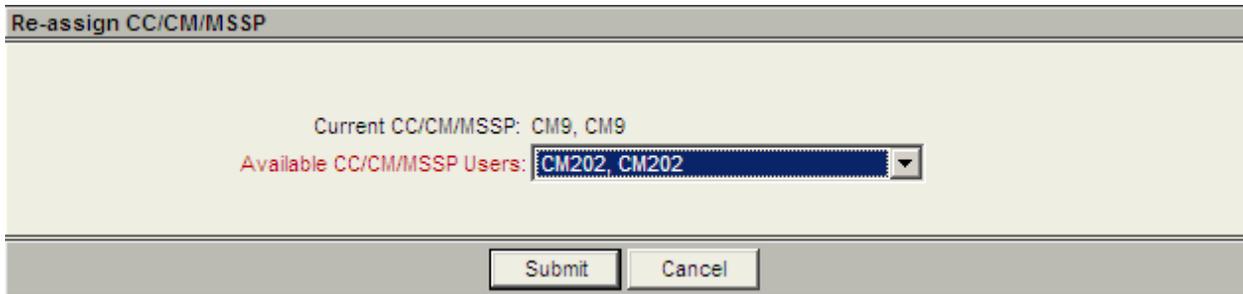
- Users may search for a particular application by entering **Provider Last Name** in free text, and then selecting a value from the **Status** or **Assigned CC/CM/MSSP** pick lists
- If no **Provider Last Name** is specified, CCQAS displays all Providers whose applications are in the selected **Status**
- If no **Provider Last Name** or **Status** is specified, CCQAS displays all Providers whose applications are assigned to the selected **Assigned**
- 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 360 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.

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 148 below. Users are given a list of Provider Application tasks available for re-assignment, and they can select **Reassign to Self** or **Reassign to Other**. (Refer to 5.57 reassigning ownership of and application.)



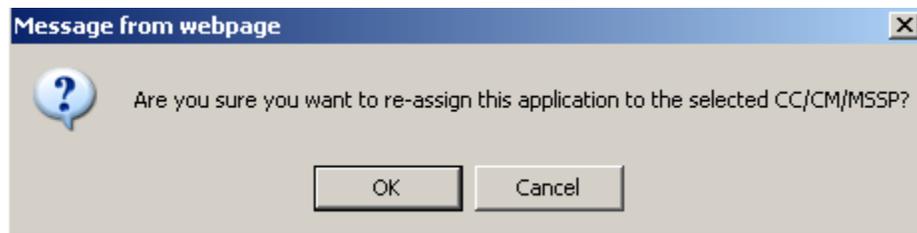
Figure 148: Application Reassignment Screen

If “**The Reassign To Other**” button is selected users are then given a choice of **Available CC/CM/MSSP Users**, as depicted in Figure 149 below. Click **Submit**.



**Figure 149: Re-Assign CC/CM/MSSP Screen**

A message displays in a pop-up window, as depicted in Figure 150 below. Users must confirm or deny their intent to re-assign 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 150: 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 updated through the processing of his or her E-application for clinical privileges. This section addresses the creation and management of a Provider's credentials record by the primary facility's credentials staff using the CCQAS Credentials module.

- **Primary UIC:** UIC that has current custody or ownership of the provider's credentials record and is responsible for its maintenance.
- **Non-Primary UIC:** Assignment UIC that does not have custody of the provider's credentials record. They have Read-Only access to the credentials record. They can update their own assignment information, and add documents to the record.

### 6.1 Creation of a New Record by the Credentials Staff

The process of adding a new provider credentials 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 151 below.



Figure 151: Provider Search Menu Item

The resulting screen contains three tabs, the first two of which enables users to search for existing credentials records (See Figure 152 below).

**Figure 152: Credentials Search Screen**

The third tab, **Add Credentials Provider**, allows users to create a new credentials record.

**Note:** 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 153 below. CC/MSSP/CMs are required to populate all data fields on this screen (except **Middle Initial** and **Suffix**) to create a new credential record.

**Figure 153: Add Provider Screen with SSN**

**Figure 154: Add Provider Screen with FIN (Unique ID)**

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

- **U.S. Issued SSN** is automatically checked (Figure 153); if this box is unchecked (Figure 154), the user is required to enter a country code and CCQAS automatically generates a Foreign Identification Number (FIN).  
**Note:** System defaults to SSN; be careful that FIN is not selected for American providers.
- 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 systematically checks its database to ensure that no record exists for this Provider. If a record does not exist, CCQAS creates a new record for the Provider, populated only with 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 Person Identifier" message displays (refer to Figure 155 below) with information regarding the UIC to which the Provider with the matching SSN is currently assigned. If this message displays, the system will not allow users to proceed with creating a new credentials record. The user should verify they are entering the correct SSN, and then contact the credentials personnel where the Provider is assigned to determine if the entered SSN is correct, and discuss the appropriate course of action.



**Figure 155: Matching Person Identifier Message**

For detailed information on the custody transfer process, refer to [Section 17](#).

## 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

Roles in CCQAS are structured to limit users' access to only those credentials records that they are responsible for tracking. 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 156 below.

**Figure 156: 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 **Assignment Status, Provider Credentials Status** and **Search Type**
- Users may specify the number of records returned when querying the database by adjusting the **Record Limit**
- Only Providers whose Primary UIC is, or who have a current, prior or pending assignment at 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 Assignment Status
- Selecting the Provider Credentials Status
- Selecting the Search 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 156 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 = (Specify Provider Type)**, CCQAS only retrieves those records that match both criteria (e.g., civilian physicians with selected Provider type). 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 Assignment Status**

Assignment Status options allow users to search for Provider records based on the Provider's assignment status at their facility/unit. The default value is **Assignment 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 **Assignment Status = Inactive** indicates records associated with Providers who performed duty at the facility/unit in the past, and the assignment at that facility/unit has ended. **Assignment Status = Pending** indicates assignments for Providers who are projected to begin performing duty at the facility/unit at some future date (e.g., a scheduled incoming ICTB or PCS that has not yet commenced). To view records for all assignments, regardless of assignment status, select all status checkboxes.

### Step 3: Selecting Provider Credentials Status

The Provider Credentials Status radio button options allow users to search for provider's credentials records based on the records being active or inactive. The default value is **Provider Credentials Status = Active**. Active credentials records include all records that have not been deactivated. Inactive credentials records include all records that are no longer active.

### Step 4: Selecting the Search Type

**Search Type** options allow users to search for records based on the nature of the Provider's assignment at their facility/unit.

- **All:** Includes all Provider records with the facility/unit as the Primary UIC or the Assignment UIC in the query.
- **Primary UIC:** Limits the search to only records for which the facility/unit has primary custody.
- **Assignment UIC:** Includes all assignments regardless of whether the Provider is permanently or temporarily (ICTB) assigned to the facility/unit.
- **ICTB:** Includes all incoming ICTBs (i.e., sent from another facility) are included in the query.

### Step 5: 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 157 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 6: The Search Results

After users enter all search criteria on the **Credentials Provider Search** screen, they then click **Search** at the bottom of the screen to execute the query, as depicted in Figure 157 below. The results of the query are returned on a newly-created **Search Results** tab.

?	Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
▾	PROVIDER3526, PROVIDER3526	D00-00-3526	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3527, PROVIDER3527	D00-00-3527	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3528, PROVIDER3528	D00-00-3528	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3529, PROVIDER3529	D00-00-3529	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3530, PROVIDER3530	D00-00-3530	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3531, PROVIDER3531	D00-00-3531	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3532, PROVIDER3532	D00-00-3532	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3533, PROVIDER3533	D00-00-3533	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3534, PROVIDER3534	D00-00-3534	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3535, PROVIDER3535	D00-00-3535	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3536, PROVIDER3536	D00-00-3536	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3537, PROVIDER3537	D00-00-3537	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3538, PROVIDER3538	D00-00-3538	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3539, PROVIDER3539	D00-00-3539	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3540, PROVIDER3540	D00-00-3540	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3541, PROVIDER3541	D00-00-3541	W3ZT30	07/15/2008			MIL	Active		1
▾	PROVIDER3542, PROVIDER3542	D00-00-3542	W3ZT30	07/15/2008			MIL	Active		1

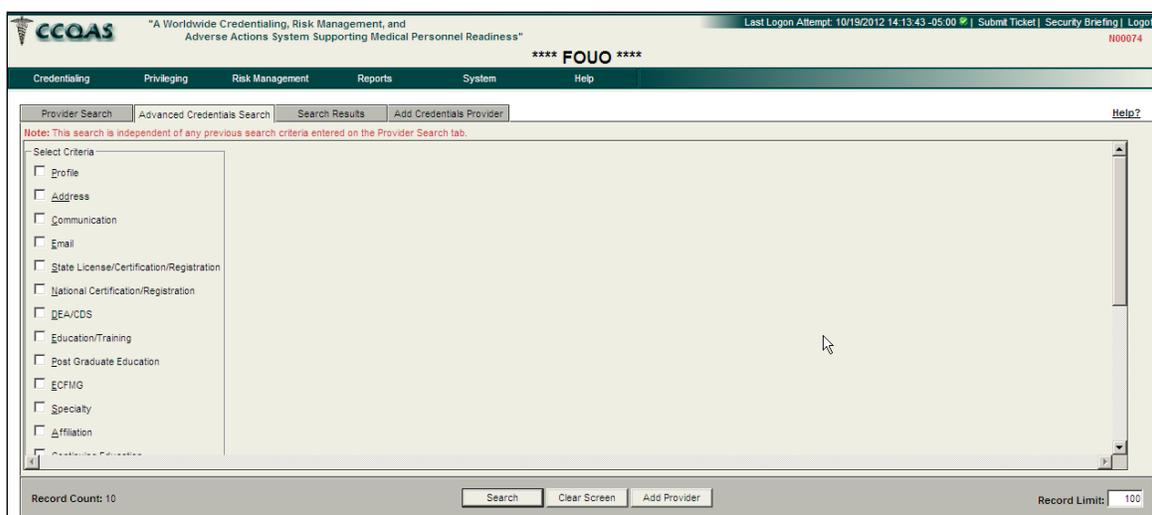
**Figure 157: Search Result Screen**

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 158 below.



**Figure 158: 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, plus:

- Select the Advanced Credentials Search tab
- Set the Record Limit
- Select the criteria for the search
- Click Search to produce search results

### 6.2.2.1 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 (see Figure 158 above.)

Credentials File Section	Credentials File Tab or Subsection	Example Data Fields	Advanced Search Category
Profile	all	Person Last Name	Profile
Identification	all	Identification Type	Profile
Contact Information	Address	Address Type	Address
Contact Information	Email	Primary Email	Email
Contact Information	Phone	Phone Type	Communication
Lic/Cert/Reg	State	Number, State, Field	State License/Certification/Registration
Lic/Cert/Reg	National	Type, Field, Agency	National Certification/Registration
Lic/Cert/Reg	Unlicensed Information	Reason	
DEA/CDS	all	DEA Number, DEA Expiration Date	DEA/CDS
Education/Training	Professional Education	Degree, Institution Name	Education/Training
Education/Training	ECFMG	Certificate Number	ECFMG
Education/Training	Post Graduate Training	Type, Field of Study	Post Graduate Education
Specialty	all	HPTC Specialty, Level	Specialty
Affiliation	Academic Affiliations	Institution Name, Position	Affiliation
Affiliation	Organizational Memberships	Institution Name, Position	Affiliation
Continuing Education	all	Type, Course Title, Training Location	Continuing Education
References	all	Current Reference, Reference Name	References
Databank Queries	NPDB/HIPDB	Last Query Date, Result Date	NPDB, HIPDB
Databank Queries	FSMB/Other	Last Query Date, Result Date	FSMB, Other
Work History	Assignments	Assigned UIC, Provider Type	Assignment
Work History	Work History	Facility Type, Facility Name	Work History
Work History	Malpractice Insurance	Name, Policy Number	Malpractice
Remarks	all	Type, Remarks Text	Remarks
Documents	all	File Name, Document Type	Documents

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

When users select a category of data, a window opens (as depicted in Figure 7a below), 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.

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

**Table 3: Operators for Advanced Search Function**

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.

## Steps 1 & 2. Selecting the Assignment Status, Provider Credentials Status and Search Type

Users select the desired **Assignment Status**, **Provider Credentials Status** and **Search Type** options 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 3. 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 4: 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.

The following example illustrates the advanced search functionality:

**Example:** Robert, an experienced CCQAS user, wishes to query CCQAS for all Active Duty Providers at his facility, who have a specialty of Internal Medicine or Family Practice. Robert needs to use multiple query criteria to generate this query. He needs to identify Active Duty Providers by selecting Branch = A11, N11 or F11, etc. via the Basic Search, and then use the Advanced criteria to identify a specific Specialty. He then selects **Specialty** from the Advanced Search tab, and selects operator ‘equal to’. He uses the binoculars to look up the Specialty of “Internal Medicine”, then adds and OR operator, and uses the binoculars to look the Specialty of “Family Practice.”

The screenshot shows the 'Advanced Search' tab in the 'Credentials Provider Search' section. The 'Specialty Criteria' table is populated with two rows: 'HPTC Specialty' with the operator 'Equal to' and value 'Internal Medicine', and 'HPTC Specialty' with the operator 'Equal to' and value 'Family Practice'. The 'OR' operator is selected in the dropdown between the two rows. The 'Specialty' checkbox is checked in the 'Select Criteria' list on the left. The 'Record Count' is 14 and the 'Record Limit' is 200.

Specialty Criteria	Column	Operator	Value
	HPTC Specialty	Equal to	Internal Medicine
OR	HPTC Specialty	Equal to	Family Practice
[Add Criteria]			

**Figure 159: Example Query Using Advanced Search Functionality**

Written as a parenthetical expression, Robert's query would display as follows:  
Branch is Active Duty AND (Specialty is equal to Internal Medicine OR Family Practice.)

### 6.2.3 Locating Provider Records at Other Facilities or Units

CCQAS only permits CC/MSSP/CMs to access a Provider's credentials files for Providers with current or previous assignments at that UIC. 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 under **Search Type**, and then click Search. Figure 160 below depicts the **Provider Locator** function.

The screenshot shows the CCQAS web 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 is a navigation bar with tabs for "Credentialing", "Privileging", "Reports", "System", and "Help". The main content area is titled "Provider Search" and contains several search criteria fields: "Last Name", "First Name", "SSN", "Alias Last Name", "Alias First Name", "NP#", "Branch", "Corps", "Civilian Role", "Primary UIC", "Assignment UIC", "Other UIC", "Department", "Work Center", "File Manager", "Provider Type", and "Sort By". There are three sections of radio buttons: "Assignment Status" (Inactive, Current, Pending), "Provider Credentials Status" (Inactive, Active), and "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 in the "Search Type" section. At the bottom, there are buttons for "Search", "Clear Screen", and "Add Provider", along with a "Record Count" field and a "Record Limit" of 100.

**Figure 160: Provider Locator Function**

The **Provider Locator** screen appears, listing all Provider records in CCQAS that meet the search criteria.

Credentiaing Privileging Risk Management Reports System Help												
Provider Search		Advanced Credentials Search		Search Results				Add Credentials Provider		Help?		
?	Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	Facility Name	Credentials Coordinator	DSN Phone	Commercial Phone
▶	SMITH, PAUL	100-89-8888	CD1CFVPV	07/09/2012			MIL	Active	27 SPECIAL OPERATIONS MEDICAL GROUP @	Mrs. Karen Bair (SGHC)	681.6608	575.784.6608
▶	SMITH, PARKER	244-89-8889	CD1CFVPV	04/15/2013	F11	DC	MIL	Active	27 SPECIAL OPERATIONS MEDICAL GROUP @	Mrs. Karen Bair (SGHC)	681.6608	575.784.6608
▶	SMITH, HOLLY	200-33-6666	BP2ZFBL5	07/16/2013	F11	BSC	MIL	Active	AF MEDICAL OPS AGENCY FO	Ms. Janet Young / Ms. Kathy Smith	969-9066 / 969-9064	(210) 395-9066 / (210) 395-9064

**Figure 161: Provider Locator Search Results screen**

**Note:** Users may also 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. See [Section 15](#) for additional details on MTF Contacts.

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

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.

### 6.3 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 162 below. CC/MSSP/CMs may also open the record by double-clicking anywhere on the summary record line.

**Note:** The CC/MSSP/CMs can only update records for which they have custody. Non-Primary UICs can request credentials updates via the documents section of the credentials record.

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 03/25/2013 11:07:42 -05:00 Submit Ticket! Security Briefing! Logout! W3ZT30											
**** FOUO ****											
Credentialing Privileging Reports System Help											
Provider Search Advanced Credentials Search Search Results Add Credentials Provider Help?											
Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments		
PROVIDER3526	D00-00-3526	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3527	D00-00-3527	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3528	D00-00-3528	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3529	D00-00-3529	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3530	D00-00-3530	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3531	D00-00-3531	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3532	D00-00-3532	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3533	D00-00-3533	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3534	D00-00-3534	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3535	D00-00-3535	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3536	D00-00-3536	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3537	D00-00-3537	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3538	D00-00-3538	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3539	D00-00-3539	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3540	D00-00-3540	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3541	D00-00-3541	W3ZT30	07/15/2008			ML	Active		1		
PROVIDER3542	D00-00-3542	W3ZT30	07/15/2008			ML	Active		1		

Record Count: 25 Search Clear Screen Add Provider Record Limit: 100

**Figure 162: 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 163 and Figure 164 below.

**Note:** Moving the cursor over the navigation bar will expand or collapse it.

Credentialing Privileging Risk Management Reports System Help												
Provider											Close Provider Record	
Name: JACOB BLACK		SSN: 100-76-6666		Primary UIC: CD1CFVPV		Cred Status: Active		Input Clerk: CM33		Provider Status: ML		
N A V I G A T I O N	Profile											
	Save											
	If known under another name, please complete the alias section.											
	Provider											
	Last Name: BLACK			First Name: JACOB			MI: [ ] Suffix: [ ] Title: [ ]					
	Person ID Type: Social Security Number		Person ID: 100-76-6666									
	Gender: Male		Date of Birth: 10/02/1980		Citizenship: [ ]							
	Marital Status: [ ]		NPI: [ ] * Source DMHRSI									
	File Mgr: [ ]											
	Upload, Edit Photo											
Military Information												
Branch: F11 - Air Force (USAF)			AOC/Desig/AFSC: 4291C - Clincl Psychology - Child/Adol Psychology - Entry									
Rank: Maj - Major			Accession: DA - Direct Accession									
Corps: BSC - Biomedical Sciences Corps												
Alias Information												
Add												
Alias Last Name		Alias First Name			Alias MI		Suffix		NPDB			
No records returned.												
Remarks												
[ ]												

**Figure 163: Navigation Bar**

The screenshot displays the 'Provider' record for JACOB BLACK. The header bar contains the following information: Name: JACOB BLACK, SSN: 100-76-6666, Primary UIC: CD1CFVPV, Cred Status: Active, Input Clerk: CM33, and Provider Status: MIL. The navigation bar on the left is expanded, showing a list of sections: 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, Adverse Actions, and Risk Management. The main content area is the 'Profile' section, which includes a 'Name' field with sub-fields for First Name (JACOB), MI, Suffix, and Title. Other fields include Person ID (100-76-6666), Date of Birth (10/02/1980), Citizenship, and NPI. A photo upload area is present with a cartoon doctor icon and an 'Upload, Edit Photo' button. Below these are dropdown menus for Force (USAF), AOC/Desig/AFSC (4291C - Clincl Psychology - Child/Adol Psychology - Entry), and Accession (DA - Direct Accession). At the bottom, there is a table for aliases with columns for Alias First Name, Alias MI, Suffix, and NPDB.

**Figure 164: Navigation Bar Expanded**

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 demographics, Photo, Military and Alias information, as depicted in Figure 165 below.

The screenshot shows a web-based form for a provider's profile. At the top, there are navigation tabs: Credentialing, Privileging, Risk Management, Reports, System, and Help. Below these, a header bar displays provider details: Name: JACOB BLACK, SSN: 100-76-6666, Primary UIC: CD1CFVPV, Cred Status: Active, Input Clerk: CM33, and Provider Status: ML. A 'Close Provider Record' button is on the right. The main form area is titled 'Profile' and has a 'Save' button. It contains several sections:
 

- Provider Information:** Includes fields for Last Name (BLACK), First Name (JACOB), MI, Suffix, Title, Person ID Type (Social Security Number), Person ID (100-76-6666), Gender (Male), Date of Birth (10/02/1980), Citizenship, Marital Status, NPI (with a note '\* Source DMHRSi'), and File Mgr.
- Military Information:** A checked section with dropdowns for Branch (F11 - Air Force (USAF)), Rank (Maj - Major), Corps (BSC - Biomedical Sciences Corps), AOC/Desig/AFSC (4291C - Clncl Psychology - Child/Adol Psychology - Entry), and Accession (DA - Direct Accession).
- Alias Information:** An 'Add' button and a table with columns: Alias Last Name, Alias First Name, Alias MI, Suffix, NPDB. The table currently shows 'No records returned.'
- Remarks:** A text area for additional notes.

 A cartoon illustration of a doctor is on the right side of the form.

**Figure 165: 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.

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 to assist 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). If entry or changes are needed to the NPI, they must be performed in DMHRSi.

The **Upload, Edit Photo** feature allows CC/MSSP/CMs to upload and store a photograph of a Provider in his or her credentials record, as depicted in Figure 166 below. The addition of a photo to the credentials record is important to support visual confirmation of a Provider's identity. The Photo is present in a Provider's E-Application for the CC/MSSP/CM, the Reviewers and the PA. It is the responsibility of CC/MSSP/CMs to upload an authenticated photo of a Provider into the Provider's credentials record in accordance with Service guidance.



**Figure 166: Profile Section, Upload, Edit Photo**

The photograph must be 1 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**.

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.

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 167 below. **Civilian** information is captured on the **Work History, Assignment** screen, as part of the civilian assignment information. Military Providers encompass all active duty and guard/reserve personnel.

The screenshot shows the 'Military Section of Profile' for a provider named ADAM CAROLLA. The form is divided into several sections. At the top, there are navigation tabs: Credentiaing, Privileging, Risk Management, Adverse Actions, Reports, System, and Help. Below these, the provider's basic information is displayed: Name: ADAM CAROLLA, Branch: Primary UIC: CD1CFVPV, Rank: Cred Status: Active, Corps: Input Clerk: CM9, and AOC/Desig/AFSC. The 'Profile' section includes a 'Save' button and a note: 'If known under another name, please complete the alias section.' The 'Provider' section contains fields for Last Name (CAROLLA), First Name (ADAM), MI, Suffix, Title, Person ID Type (Social Security Number), Person ID (100-55-7474), Gender (Male), Date of Birth (09/02/1980), Citizenship, Marital Status, File Mgr, and NPI. A 'No Photo Available' message is shown on the right with an 'Upload, Edit Photo' button. The 'Military Information' section is currently inactive, indicated by a checkbox. It includes fields for Branch, Rank, Corps, AOC/Desig/AFSC, ASI (N/A), and Accession.

**Figure 167: Military Section of Profile**

When users enter a checkmark for **Military Information**, 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. The **Accession** captures 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.

### 6.3.2 The Identification Section

Users may create a record of a Provider's SSN or FIN in the **Identification** section at the time the credentials record is first created, as depicted in Figure 168 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 'Identification Section' for the same provider, ADAM CAROLLA. The top navigation tabs are Credentiaing, Privileging, Adverse Actions, Reports, System, and Help. The provider's basic information is repeated. The 'Identification' section is active, showing an 'Add' button and a table with the following data:

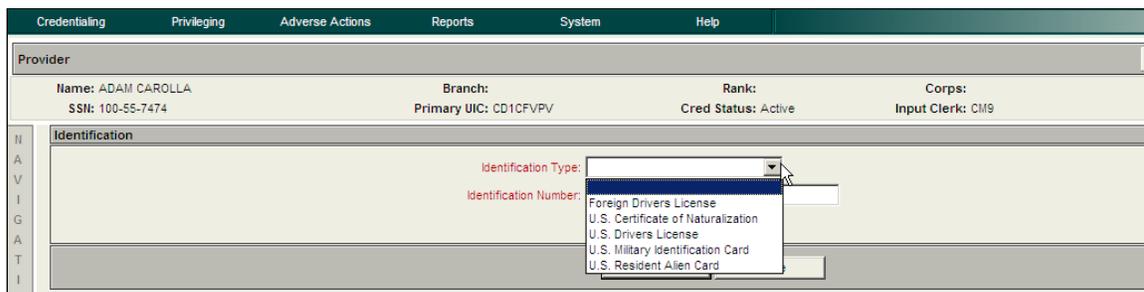
Identification Type	Identification Number	State
Social Security Number	100-55-7474	

**Figure 168: 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 169 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.

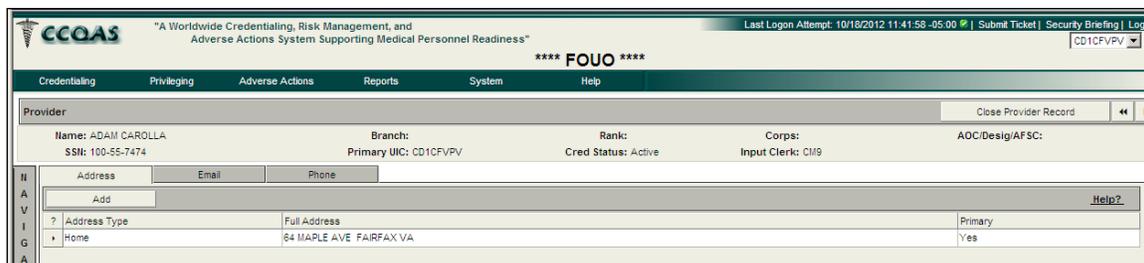
If it is discovered that a SSN or FIN for an existing credentials record is incorrect, consult your Service CCQAS Administrator for further guidance.



**Figure 169: Add Identification Screen**

### 6.3.3 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 170 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.



**Figure 170: Contact Information Section**

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 171 below depicts the screen to update a Provider’s primary phone number.

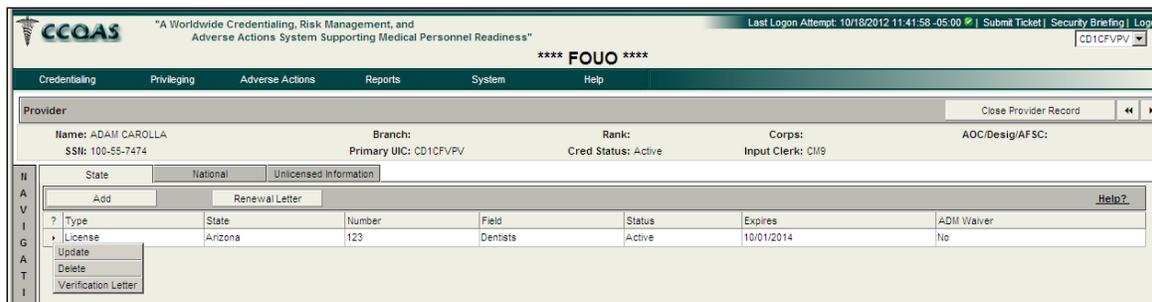


**Figure 171: Updating a Primary Phone Number**

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.

### 6.3.4 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, and/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 172 below depicts the **Licensure/Certification/Registration** section.



**Figure 172: 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.

#### 6.3.4.1 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, military, civilian and contract Providers, with the exception of Non-Personal Service Contractors (NPSCs), may

render care in any DoD facility worldwide as long as they hold one current and valid license from any U.S. state or territory (in accordance with current DoD and Service policy). 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 in the next section.

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 173 below.

The screenshot shows the 'State License/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 menu with tabs for 'Credentialing', 'Privileging', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area is divided into two sections. The top section is for the 'Provider' record, showing details for ADAM CAROLLA, including his name, SSN, branch (F11), rank (Lt Gen), corps (DC), and primary UIC (CD1CFVPV). The bottom section is for the 'State License/Certification/Registration' form. This form has several fields: 'Type' (License), 'Number' (123), 'Field' (030 - Dentists), 'State' (AZ - Arizona), 'Issue Date', 'Status' (Active), 'Expiration Date' (10/01/2014), and 'In Good Standing' (checked). Below the license form is the 'Prime Source Verification (PSV) Information' section, which includes fields for 'Method' (Written Correspondence), 'Contact Name' (JESSICA), 'Position', 'Phone', 'URL', and 'Entered By Name' (MSSP152 MSSP152). The screen also has a 'Save' and 'Close' button at the bottom.

Figure 173: 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 description.

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 or requires a new PSV, 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 original PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated, and a PSV entry is added to the PSV History tab.

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. 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 [6.3.4.2](#) and [6.3.4.4](#), 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](#).

### 6.3.4.2 Documentation of Social Worker License Level

When Social Workers field (300) is chosen, the user must designate the level of the license. The drop down menu has selections for the following (mouse over seen in Figure 174):

- Entry Level- First license, post-master social worker. Requires 2 years of supervision. This selection is valid for Army and Air Force provider.
- Independent-Licensed Clinical Social Worker (LCSW)



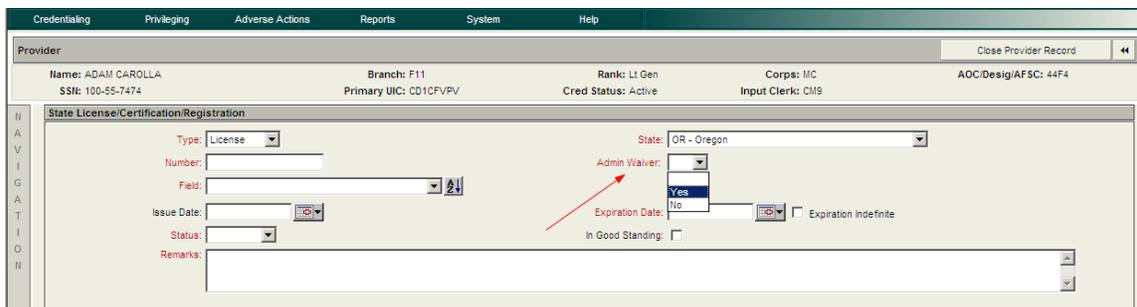
Figure 174: Social Workers License Level Information

### 6.3.4.3 Administrative Waivers for 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 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. See DoD guidance and Service regulations/instructions for additional guidance.

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 the DoD approved waiver states. Figure 175 below depicts the **Admin Waiver** field.



**Figure 175: 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.

#### **6.3.4.4 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 in DoD facilities. This includes PAs, nurse practitioners, and allied health professionals.

**Note:** Specialty board certification information 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 176 below.

**Figure 176: 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 description.

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 or requires a new PSV, 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 original PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated and a PSV entry is added to the PSV History tab.

After an active certification 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.

#### 6.3.4.5 Waivers of Licensure Requirements for Qualified PAs

PA's are certified by the National Commission on Certification of PA's (NCCPA) and may also be licensed by state medical boards as competent to practice medicine. 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 NCCPA certification, and has been granted privileges via an E-app or offline privileges entered into the system, CCQAS automatically creates an administrative waiver on the **State Licensure/Certification/Registration** tab. 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 Work History, Assignment screen
- 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 Privilege Expiration Date must not be expired

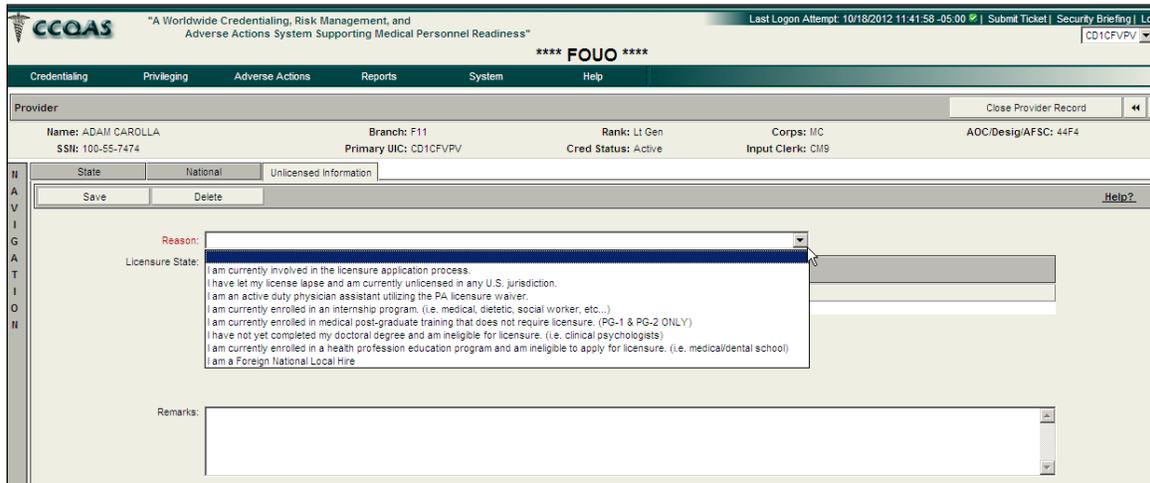
If these conditions are met, CCQAS automatically generates a PA Waiver entry on the **State Licensure/Certification** screen, which has the following characteristics:

- Number = PA Waiver
- Field = The value enter for Field on the PA's national certification record
- Status = Active
- Expiration Date = The lesser of NCCPA Expiration Date or the Privilege 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. PA's who are contracted under non-personal services contracts are not eligible for a PA waiver, and must hold a valid state license in the state where the MTF is located.

#### 6.3.4.6 Unlicensed Information Screen

The **Unlicensed Information** screen, depicted in Figure 177 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.



**Figure 177: 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 screen.

### **6.3.5 The Drug Enforcement Agency/Controlled Dangerous Substances Section**

The **Drug Enforcement Administration/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 178 below.

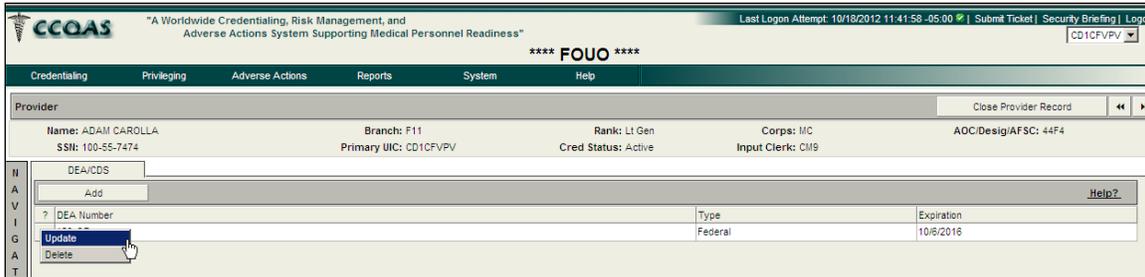


Figure 178: DEA/CDS Section

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 qualifying Provider, use **Type = DEA (fee exempt)**. A fee-exempt DEA certification may only be used when the individual is performing official duties. 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 179 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.

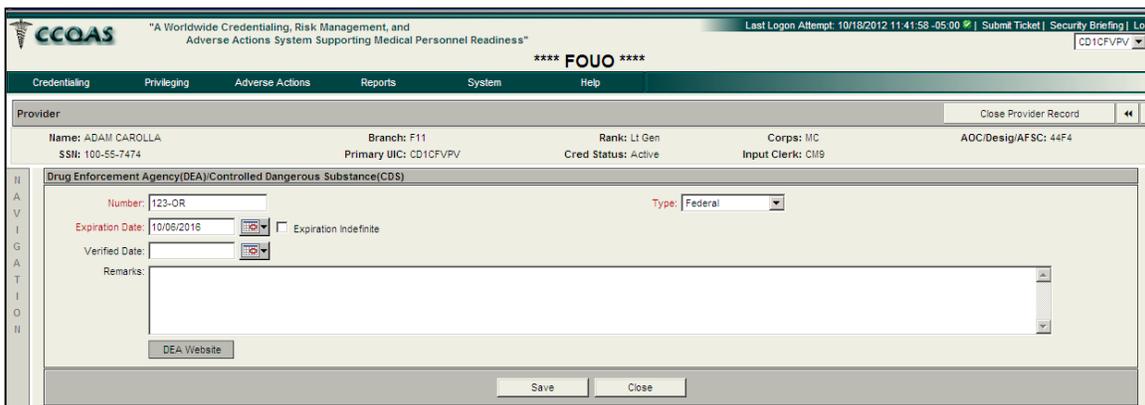


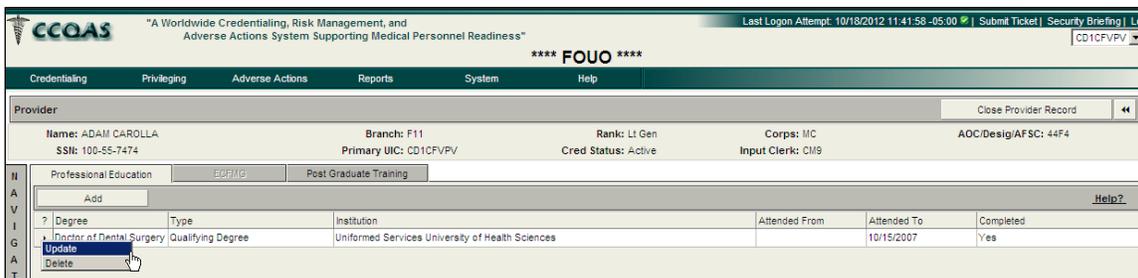
Figure 179: DEA/CDS Screen

### 6.3.6 The Education/Training Section

The **Education/Training** section supports the documentation of the academic and practical educational credentials for Providers that is required for their professional specialty. 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

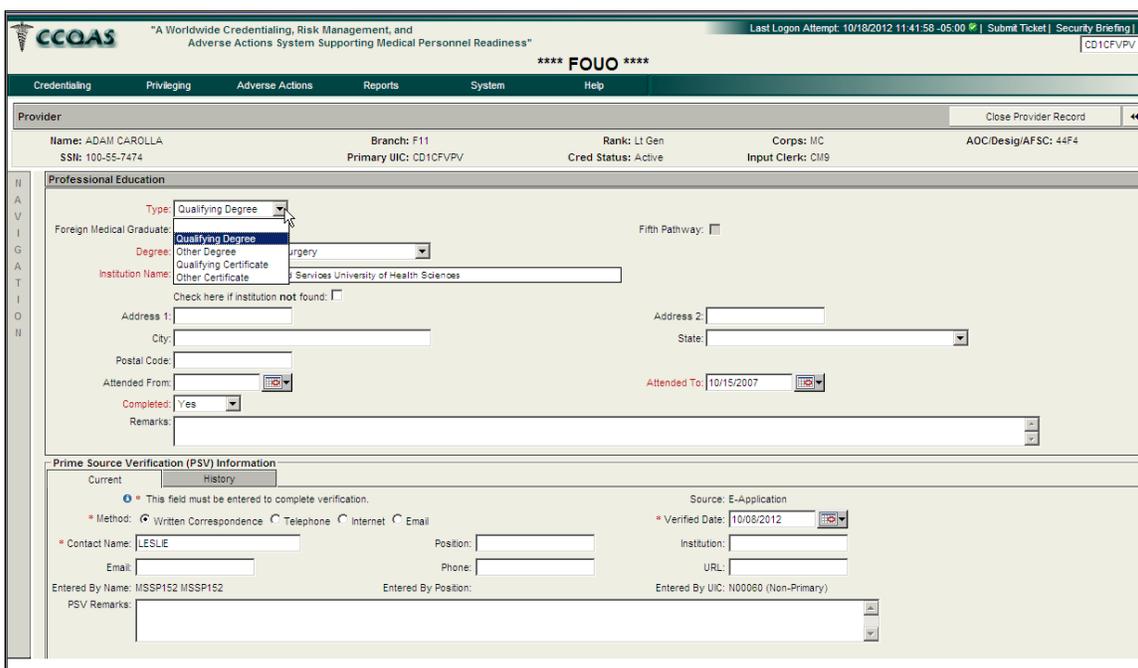
credentials to a Provider's record between privileging cycles. CC/MSSP/CMs may add a new record to the appropriate screen by clicking the **Add** button in the upper left-hand corner of the screen, as depicted in Figure 180 below.



**Figure 180: Education/Training Section**

### 6.3.6.1 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 181 below.



**Figure 181: Qualifying Degree Record**

The *Qualifying Degree* or *Qualifying Certificate* requires full PSV documentation. 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 original PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated and a PSV entry is added to the PSV History tab. 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.

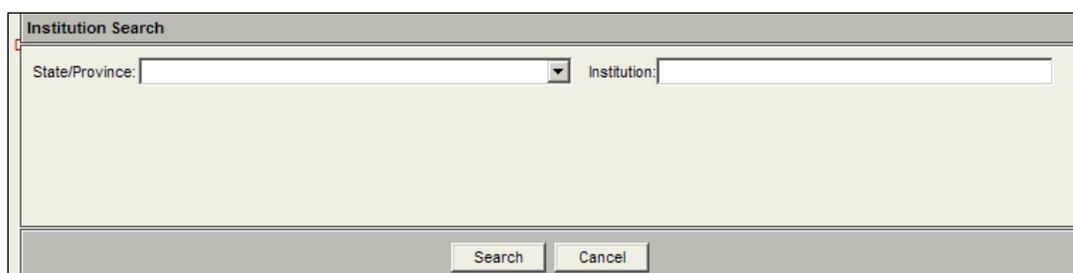
Additional academic degrees obtained by Providers should also be entered into CCQAS as **Type = Other Degree or Other Certificate**. Each unique degree or certificate held by Providers should be documented in a separate record on the **Professional Education** tab.

**Example:** The primary, qualifying 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 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 *In-Training* or *No* respectively. Explanatory **Remarks** are required when *No* is selected.

If the academic credentials were obtained at the Uniform Services University of Health Sciences (USUHS), users should click **USUHS** to auto-populate the **Institution**. If obtained elsewhere, users should enter the institution where the degree or certificate was obtained into CCQAS using the **Search** function  as depicted in Figure 182 below.



**Figure 182: 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:** The recommended method for locating an Institution is to leave the State/Province blank and search by Institution name. When searching for institutions by name enter a key word or phrase to locate the correct institution. The less specific the search criteria, the broader the

results. 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.

**If the institution is not found contact CC/MSSP/CM to contact the Service Representative.** Send an email to the CC/MSSP/CM to add the valid institution to pick list. The Email should contain the following:

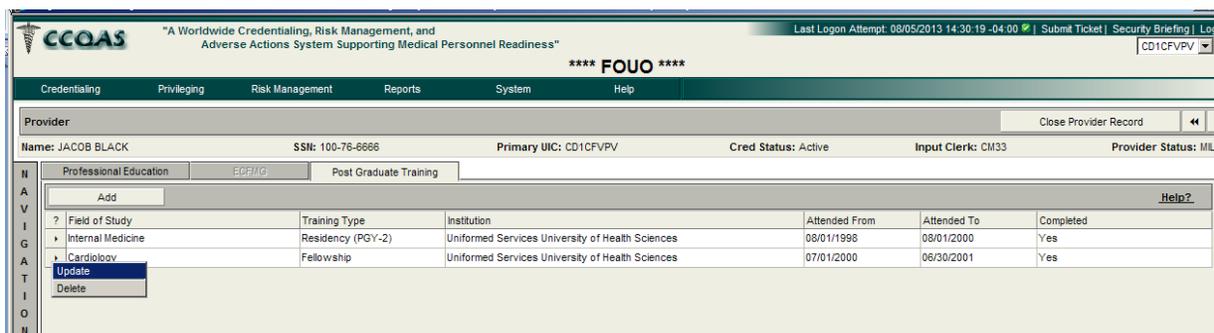
- Name of institution
- Address of institution
- State or Country of institution

**Note:** If several search attempts have failed to find the correct institution name and the user is unable to contact the CC/MSSP/CM, the user 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.

### 6.3.6.2 Documenting Post Graduate Training

The **Post Graduate Training** tab is designed to capture the practical education and training for Providers, as depicted in Figure 183 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).



**Figure 183: ‘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 184 below.

**Figure 184: Post Graduate Training Record**

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**.

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 original PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated and a PSV entry is added to the PSV History tab. After the PSV of the completed training is documented in CCQAS, the PSV does not have to be repeated during future privileging actions.

If Providers are currently in Post Graduate Training, or have never completed it, they should mark **Completed** as **In-Training** or **No** respectively. Explanatory **Remarks** are required when **No** is selected.

### 6.3.6.3 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 are not 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 has 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 185 below.

The screenshot shows the 'Professional Education' form for provider JACOB BLACK. The 'Foreign Medical Graduate' checkbox is checked, and a red arrow points to it. The 'Degree' is 'Bachelor of Medicine' and the 'Institution Name' is 'USUHS UNIVERSIDAD DE BARCELONA'. The 'Attended To' date is '05/22/1998'. The 'Prime Source Verification (PSV) Information' section is also visible, with a note that a field must be entered to complete verification.

**Figure 185: ECFMG Checkbox**

The screenshot displays the ECFMG page for provider JACOB BLACK. At the top, there are navigation tabs: Credentialing, Privileging, Risk Management, Reports, System, and Help. Below these, the provider's details are shown: Name: JACOB BLACK, SSN: 100-78-6666, Primary UIC: CD1CFVPV, Cred Status: Active, Input Clerk: CM33, and Provider Status. The ECFMG section includes a 'Save' button and a 'Delete' button. The Certificate # is 2385214. The Date Taken is 07/01/1998, and the Certified Date is 07/10/1998. The Expiration Date field is empty. The Remarks field contains 'ECFMG Information'. Below this is the Prime Source Verification (PSV) Information section, which has 'Current' and 'History' tabs. A note indicates that the 'Source' field must be entered to complete verification. The Method is set to 'Written Correspondence'. The Source field is empty. The Verified Date, Institution, and URL fields are also empty. The Contact Name, Position, and Phone fields are empty. The Entered By Name, Entered By Position, and Entered By UIC fields are empty. The PSV Remarks field is empty.

**Figure 186: ECFMG Page**

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 original PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated and a PSV entry is added to the PSV History tab. After the PSV of the ECFMG certification is documented in CCQAS, the PSV does not have to be repeated during future privileging actions.

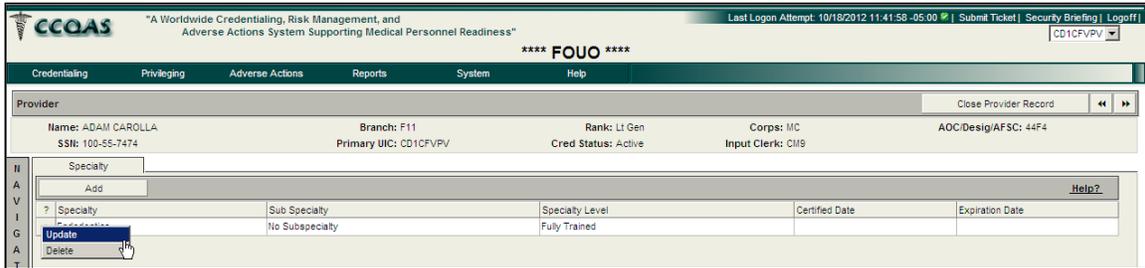
The Fifth Pathway and ECFMG certifications apply only to physicians and should be left blank for all other types of Providers who are trained outside the U.S.

### 6.3.7 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.

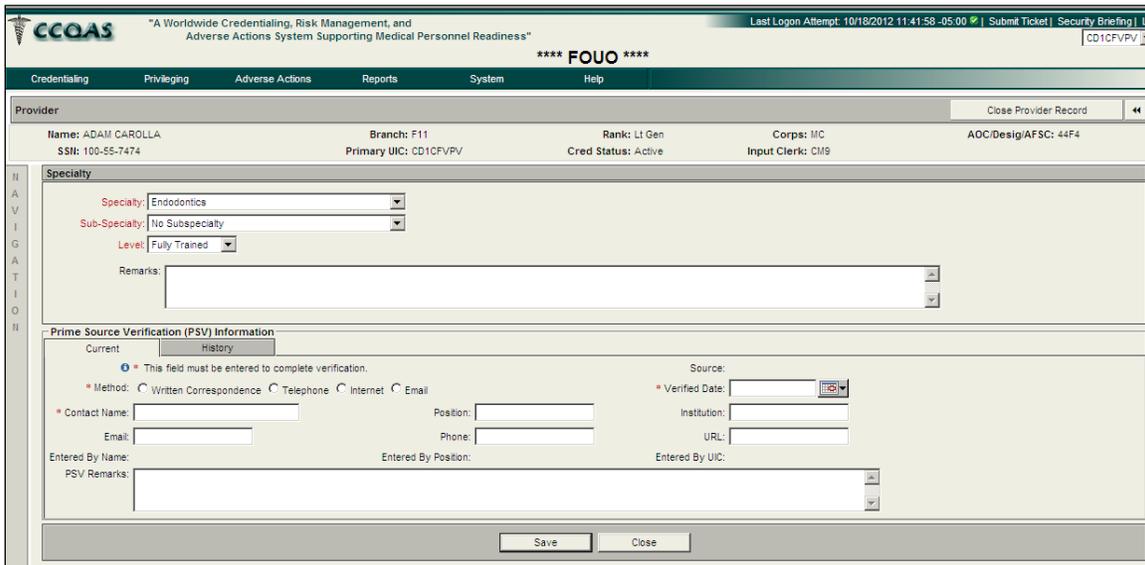
**Note:** Entries from the Specialty Section automatically populate the Specialty field on the Assignment Tab, and are necessary to indicate what the provider is privileged in for each assignment.

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 187 below.



**Figure 187: Specialty Section**

The **Specialty** screen appears, as depicted in Figure 188 below. Users are required to enter the **Specialty**, **Sub-Specialty**, and **Level** of training to create a new specialty record.



**Figure 188: Adding a Specialty**

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.

Specialty board certification information is documented on the **Specialties** tab and **not** on the **Licensure/Certification/Registration** tab.

**Note:** The agencies **ABMS**, **AOA**, and **ADA** are currently the only agencies that are selectable from the lookup screen, and are specific to Physicians and Dentists.

If a Provider has completed all required professional training and licensure, but is not board certified, then **Level** = **Fully Trained**.

Providers who have not completed their required professional training should be designated as *In Training*.

**Note:** Users must document qualifying National certifications and registrations on the **Licensure/Certification/Registration** tab (refer to [Section 6.3.5](#)).

### 6.3.7.1 Documenting Board Certification

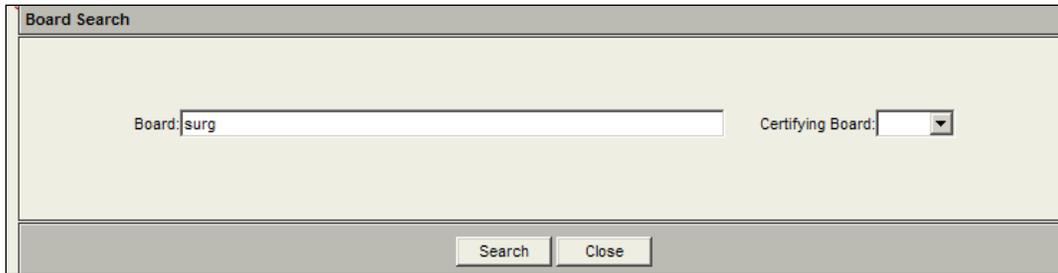
When Providers have been designated as board-certified, additional data fields are presented that capture the information contained on the Provider's certificate of board certification, as depicted in Figure 189 below.

The screenshot displays the CCQAS web application interface. At the top, the logo and tagline are visible. The main navigation bar includes tabs for Credentiaing, Privileging, Adverse Actions, Reports, System, and Help. The current view is the Board Certification section for provider ADAM CAROLLA. The Specialty section contains several dropdown menus and text input fields for specifying the board certification details. The PSV Information section at the bottom provides options for verification methods and contact information.

**Figure 189: Board Certification Section**

To ensure data consistency, users should activate the search function **AA** to enter the name of the certifying board. The search function allows users to search for an agency/board by entering a partial board name (e.g., enter “*surg*” to search for *American Board of Surgery*) or a certifying board affiliation (i.e., *ABMS*, *AOA*, or *ADA*), as depicted in Figure 190 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 only when the certifying board is *ABMS*, *AOA*, or *ADS*.



**Figure 190: Board Search Screen**

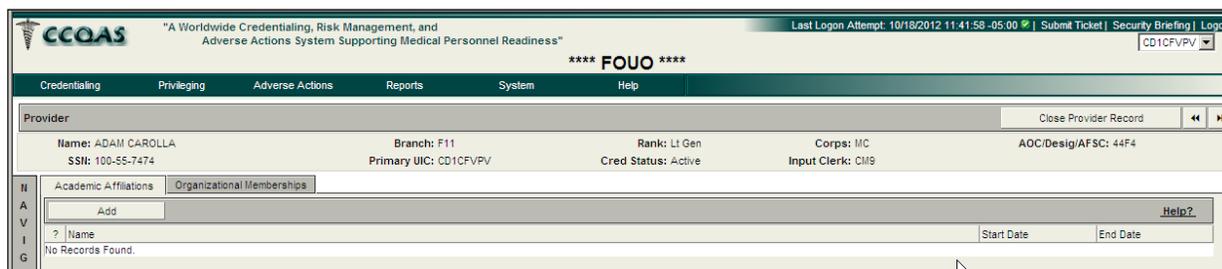
**Note:** If several search attempts have failed to find the correct board name, users should consult their Service CCQAS representative for further assistance.

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 current PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated and a PSV entry is added to the PSV History tab. PSV is required each time the board certification is renewed.

### 6.3.8 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 191 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 191: Affiliation Section**

### 6.3.8.1 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 192 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.

The screenshot displays the 'Academic Affiliations' tab within the CCQAS system. At the top, the header includes the CCQAS logo, the system name 'A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness', and a 'FOUO' (For Official Use Only) warning. Below the header, a navigation bar contains tabs for 'Credentialing', 'Privileging', 'Adverse Actions', 'Reports', 'System', and 'Help'. The main content area shows a provider record for 'ADAM CAROLLA' with details such as 'Branch: F11', 'Rank: Lt Gen', 'Corps: MC', and 'AOC/Design/AFSC: 44F4'. The 'Academic Affiliations' section is active, featuring a search function for 'Institution Name' (populated with 'USPHS') and a 'Position' field. Other fields include 'Address 1', 'Address 2', 'City/Town', 'State', 'Postal Code', 'Phone', 'Start Date', 'End Date', 'POC Name', and 'POC E-mail'. The form is completed with 'Save' and 'Close' buttons at the bottom.

Figure 192: 'Academic Affiliations' Tab

### 6.3.8.2 The Organizational Memberships Tab

An **Organization Membership** refers to a Provider's membership in professional societies, associations, or other organizations, as depicted in Figure 193 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.

**Figure 193: ‘Organizational Memberships’ Tab**

### 6.3.9 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.

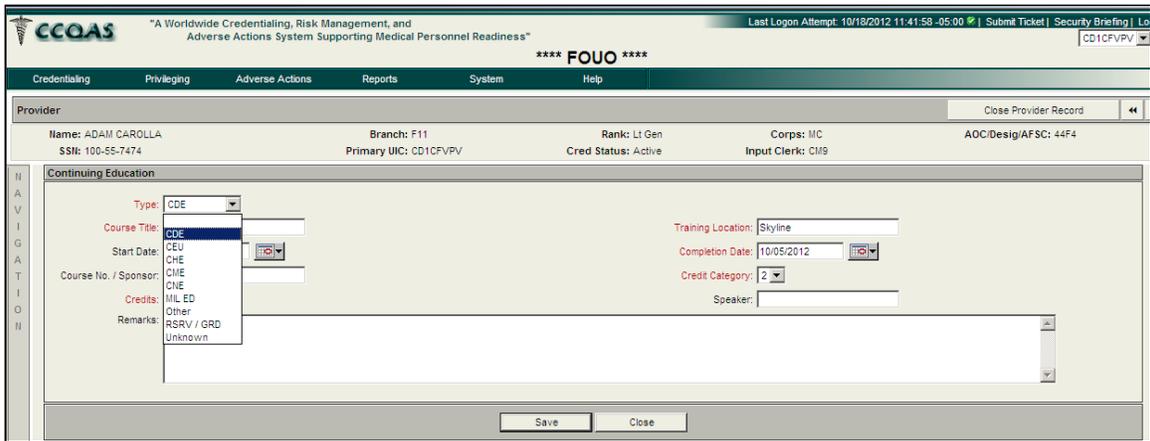
Users may edit an existing education record by selecting **Update** from the hidden menu of options. Users may create a new education record by clicking **Add** in the upper left-hand corner of the screen, as depicted in Figure 194 below.

Course Type	Credit Hours	Course Number / Sponsor	Training Description	Started	Completed
Dental Safety	3		Dental Safety	10/01/2012	10/05/2012

**Figure 194: Continuing Education Section**

The **Continuing Education** screen displays, as depicted in Figure 195 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.



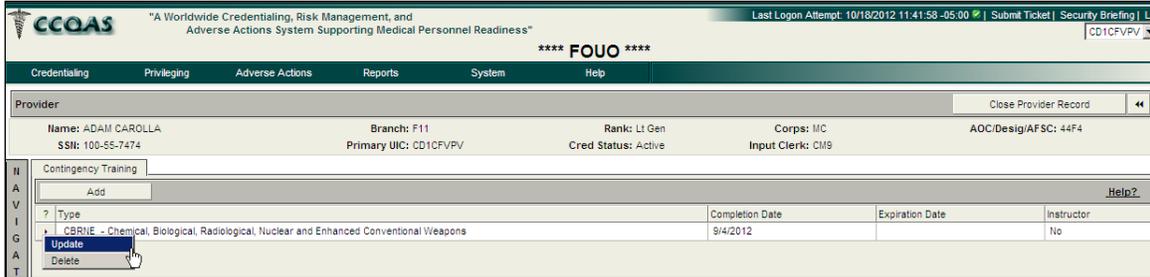
**Figure 195: Continuing Education Record**

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.

**6.3.10 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 196 below. Users may add a new training record by clicking **Add** in the upper left-hand corner of the screen.



**Figure 196: Contingency Training Section**

The Contingency Training screen appears, as depicted in Figure 197 below. Each contingency training record includes the **Training Type** and either an **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 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.

The screenshot shows the CCOAS web interface. At the top, it displays the CCOAS logo and the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". The user is logged in as "\*\*\*\* 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 (SSN: 100-55-7474, Branch: F11, Rank: Lt Gen, Corps: MC, Cred Status: Active, Input Clerk: CM9). Below this is the "Contingency Training" section, which includes a dropdown for "Training Type" (set to "CBRNE - Chemical, Biological, Radiological, Nuclear and Enhanced Conventional Weapons"), a "Completion Date" field, a checkbox for "Check here if you are an instructor", and a "Remarks" text area. "Save" and "Close" buttons are at the bottom.

**Figure 197: Contingency Training Record**

If the Provider is an instructor for any of the on-going courses being documented, check the **Check here if you are an instructor** checkbox, 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. Users may run the “Training Expiration” standard report to identify all Providers who have expired training certifications.

### 6.3.10.1 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 198 below.

The screenshot shows the "References" section of the CCOAS interface for ADAM CAROLLA. It features a table with columns for Name, Title/Position, Address, City, and State. There are "Add", "Update", and "Delete" buttons. The "Update" button is highlighted with a mouse cursor. A "Help?" link is also visible.

	Name	Title/Position	Address	City	State
Update	DAVE	Clinical Supervisor			
Delete	JESSICA	Clinical Supervisor			

**Figure 198: References Section**

The **Reference Name** and **Title/Position** are required on every reference record, as depicted in Figure 199 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.

**Figure 199: 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 original PSV document. When the screen is saved, the name, UIC, and position of the individual who entered the current PSV is auto-populated and a PSV entry is added to the PSV History tab. PSV of current references is required with each E-Application submitted.

### 6.3.10.2 The Databank Queries Section

The **Databank Queries** tab, depicted in Figure 200 below, supports the documentation of the results of NPDB, (HIPDB historical data only), 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 **Result Date** in the NPDB section of the screen should reflect the date when a Provider's last E-application was PSV'ed. The **Last Query Date** and **Result Date** are 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 outside the normal privileging cycle by checking the **Request Query** checkbox and clicking **Save**.

**Figure 200: Databank Queries Section**

### 6.3.10.3 NPDB 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.

DoD Directive 6025.13 states that NPDB 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. Users should consult Service policy if questions arise concerning the requirements and procedures associated with queries in the NPDB database.

There is a charge associated with performing NPDB 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 query results.

**Note:** As of, 6 May 2013 the HIPDB merged with the NPDB so there is now only one query process and document. Historical HIPDB data is retained in the credentials record and is read-only.

### 6.3.10.4 FSMB Query Requirements

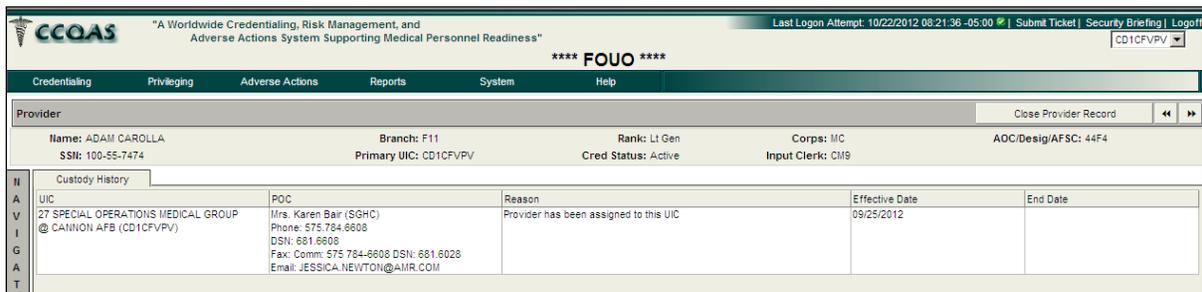
The FSMB maintains the Federation Physician Data Center, a central repository for formal actions taken against physicians by state licensing and disciplinary boards, Canadian licensing authorities, the U.S. Armed Forces, the U.S. Department of Health and Human Services, and other regulatory bodies. After an action is reported to the Federation, it becomes part of a physician's permanent record.

**Note:** Within DoD, FSMB requirements may vary according to Service regulations.

### 6.3.11 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 201 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.

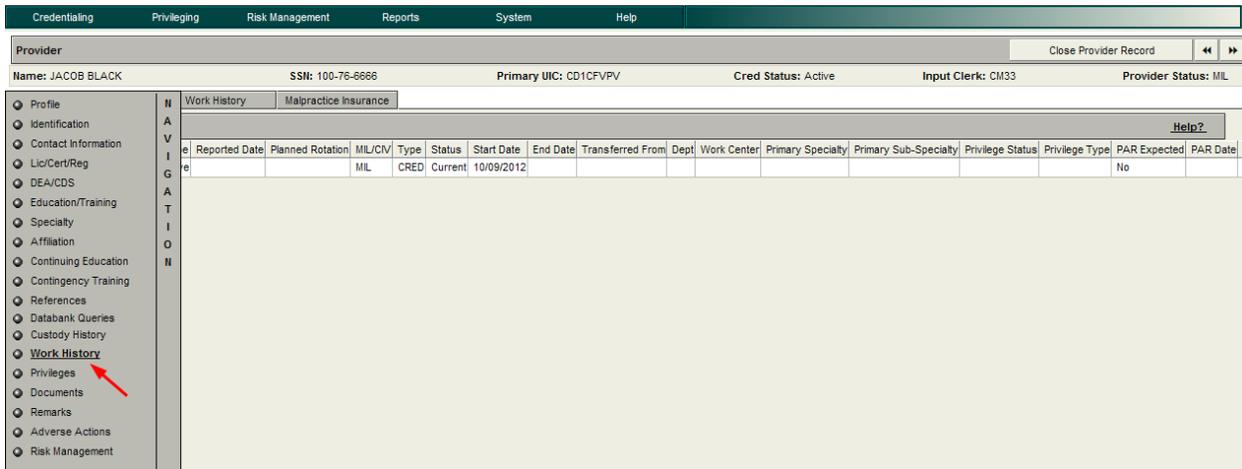
**Note:** Custody History was not recorded prior to deployment of CCQAS 2.10, and reflects ownership from migration forward.



**Figure 201: Custody History Section**

### 6.3.12 The Work History Section

The **Work History** section in the credentials record is designed to manage all current and past Assignments (MIL/CIV) for Providers, their Work History, and their Malpractice Insurance, as depicted in Figure 202 below.



**Figure 202: Work History Section**

#### 6.3.12.1 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 203 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.



Figure 203: 'Assignment' Tab

The UIC for the assignment record that pertains to a CC/MSSP/CM's own location is displayed in bold text on the **Assignments** screen. 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.

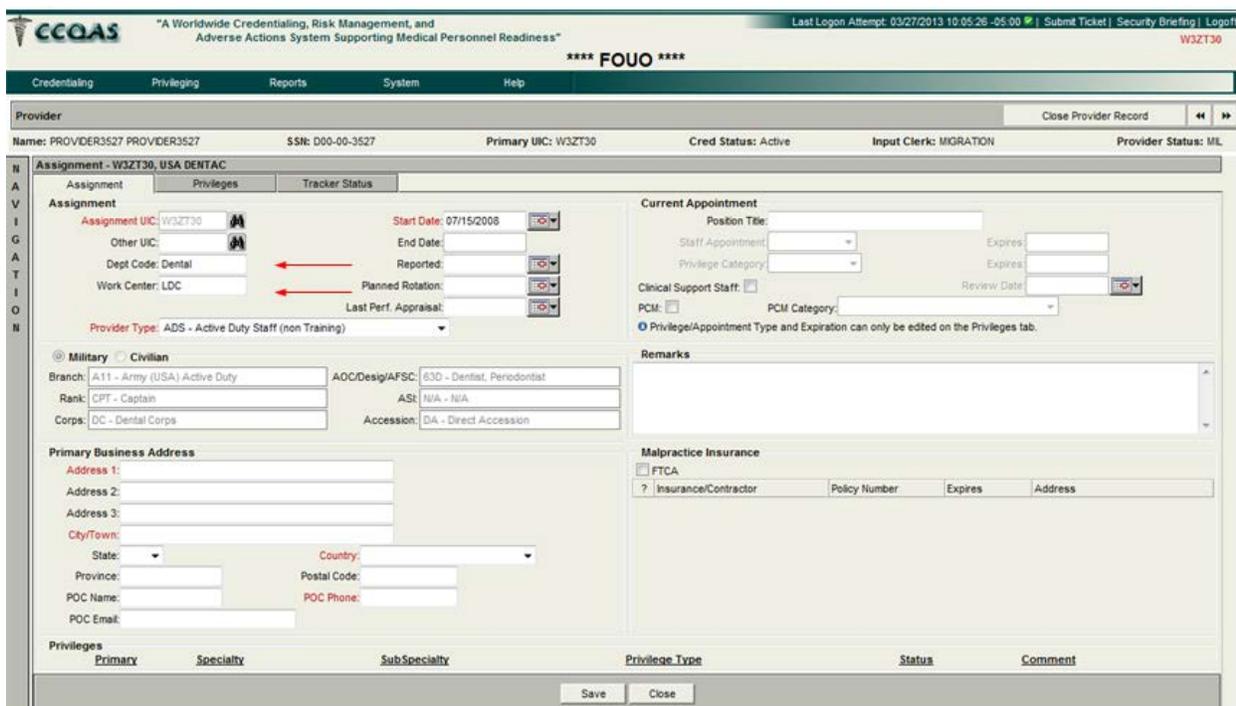


Figure 204: MTF Assignment Record

The **Assignment** section of an "Assignment" record is designed to capture the location and dates associated with the assignment, as depicted in Figure 204 above. The value for **Assigned UIC** is pre-populated with the UIC listed in the upper right-hand corner of the screen. The **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**, to ensure the code is entered correctly.

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 (see arrows in Figure 48).

The **Reported** and **Planned Rotation** date fields 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 **Provider Type** describes the specific situation under which a Provider is performing duty at the assignment location.

**Military** information is auto-populated from the **Profile** section of the credentials record at the Primary UIC. Any changes or updates to Military information must be made in the **Profile** section. **Civilian** fields can also be entered/updated in this section.

The CC/MSSP/CMs should enter the facility/unit's primary work address in the **Primary Business Address** section of an assignment. Complete the **POC** fields with the CC/MSSP/CMs contact information.

In the **Privileges** section of the Assignment screen, appropriate checkboxes and radio buttons should be selected to indicate specialties in which the Provider is privileged at the current assignment. The **Specialty** and **Sub Specialty** fields are pre-populated with values entered in the Specialty section of the credentials record.

In the **Current Appointment** section, the **Staff Appointment**, **Privilege Category** and their respective **Expiration** dates are view-only and auto-populated from information entered in the assignment Privileges tab or in the Privileges section (refer to [Section 6.3.13](#)) of the credentials record. CC/MSSP/CMs should enter the **Position Title**, select the **Clinical Support Staff** checkbox if appropriate and/or update any appropriate **PCM** information. Pertinent explanatory remarks may be entered in the **Remarks** section of the record.

In the **Malpractice Insurance** section, select the FTCA (Federal Torts Claim Act) checkbox if appropriate. Any Malpractice Insurance documented in the assignment, Malpractice Insurance tab is listed as view-only.

The **Privileges** tab of the assignment record, depicted in Figure 205 below, summarizes the Provider's privileging status at that assignment. The CC/MSSP/CMs can update the Type of Appointment, Type of Privileges and Expiration Dates, similar to processing described in Figure 52 below.



Figure 205: 'Work History Privileges' Tab.

The **Tracker Status** tab of the **Work History** section, depicted in Figure 206 below, is designed to display and add **Assignment Status**, **Assignment Status Date**, and **Assignment Status Remarks** data.



Figure 206: 'Tracker Status' Tab

### 6.3.13 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. Figure 207 below depicts the **Privileges** section.

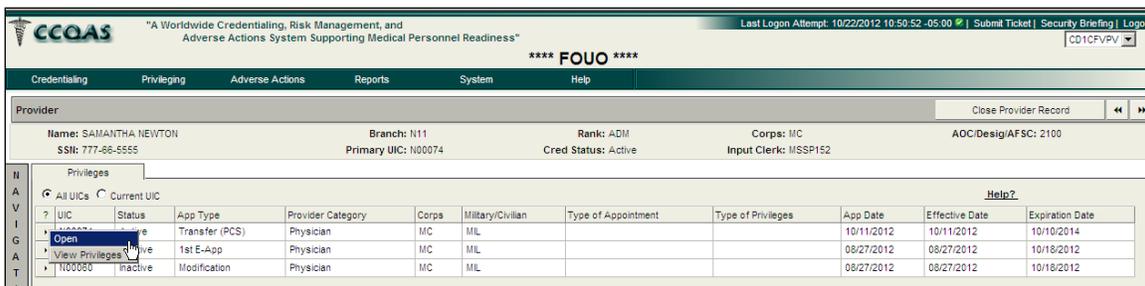


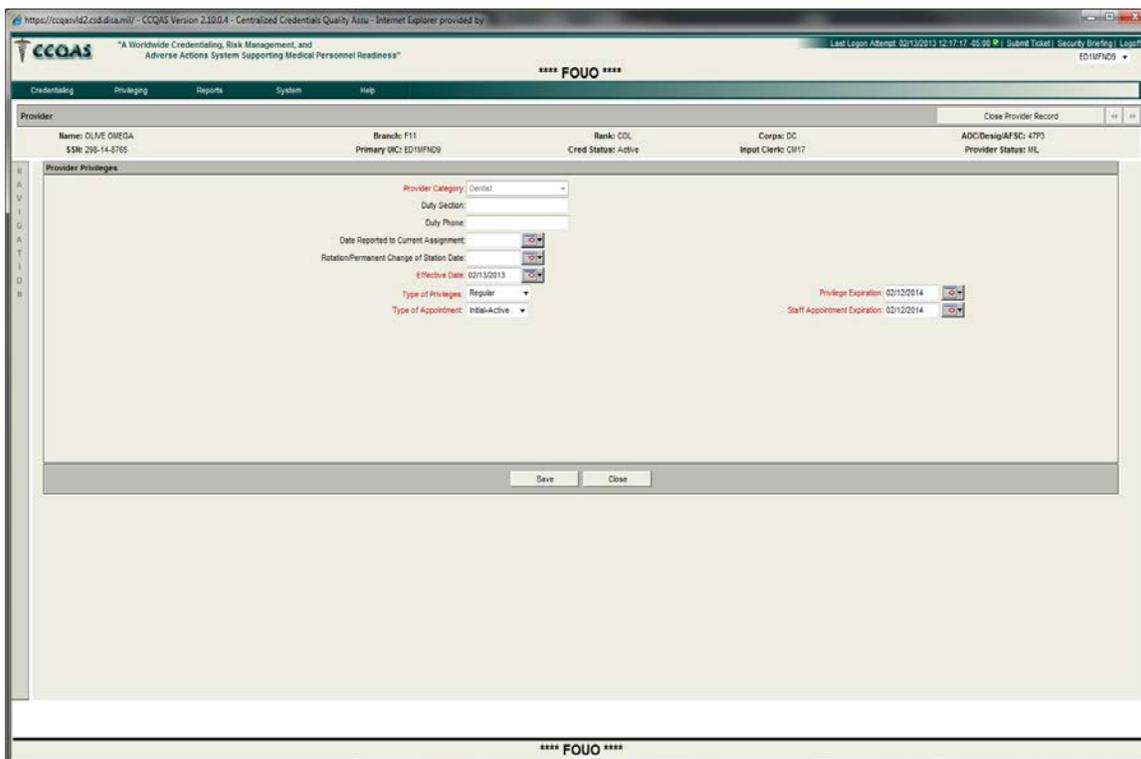
Figure 207: Privileges Section

Each privileging record provides a hidden menu of options. The **Open** option opens the **Provider Privileges** screen, as depicted in Figure 208 below.

This screen is auto-populated from the information contained in the **Position** tab of the approved privilege application. For current privileging records, with the exception of the provider category, CC/MSSP/CMs may edit the information on this screen, as needed, to reflect the Provider's assignment information. CCQAS automatically calculates the staff appointment and

privilege expiration dates using the date that the PA approved the privilege application. CC/MSSP/CMs may edit the type of appointment and privileges requested, as well as their respective expiration dates. After all edits are made, click **Save** to save the information.

**Note:** For specific guidance regarding types of privileges and appointments, refer to Service-specific directives.



**Figure 208: 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.

If the Type of Privileges, the Privilege Expiration date, the Type of Appointment and/or the Staff Appointment Expiration date are updated, CC/MSSP/CMs will be required to enter a reason for the update, and a new “appended” snapshot is generated (refer to Figure 209 below). Refer to Section 6.3.15 for information on how to access stored documents.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 02/05/2013 14:30:19 -04:00 Submit Ticket Security Briefing Logout DW1CFD9S

\*\*\*\* FOUO \*\*\*\*

Credentialing Privileging Reports System Help

Provider Name: JACOB BLACK SSN: 100-76-6666 Primary UIC: CD1CFVPV Cred Status: Active Input Clerk: CM33 Provider Status: Dual

Documents

Provider Documents PARs/Snapshots

Application Type	File Type	Description	Created Date
1st E-App	Application Packet	PSV Complete	2/19/2013 10:35:39 AM
1st E-App	Application Packet	E-Signature Complete	2/19/2013 10:31:31 AM
1st E-App	Application Packet	PSV Complete	10/9/2012 2:24:36 PM
1st E-App	Application Packet	E-Signature Complete	10/9/2012 1:51:47 PM

**Figure 209: Document Section, PARs/Snapshot**

A view-only listing of any approved electronic 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 210 below.

\*\*\*\* FOUO \*\*\*\*

Name: OMEGA, OLIVE, P      Appointment: Initial-Active      Priv. Granted Date: 13 Feb 13  
 Mil/Civ: Military      Corps: DC      Privileges: Regular      Priv. Expiration Date: 12 Feb 14

PRIVILEGED PROVIDER INFORMATION REPORT

SERVICE: Air Force			
UIC: ED1MFND9 MTF: 0096 MEDICAL GROUP @			
PROVIDER	SSN	MILITARY/CIVILIAN	
OMEGA, OLIVE P	XXX-XX-8765	Military	
ORGANIZATION UNIT	MILITARY/CIVILIAN ADMITTING	TYPE OF PRIVILEGES	
0096 MEDICAL GROUP @	Military	Yes	Regular
PRIVILEGE CATEGORY: General Dentistry			
Version 1.0			
Scope			
PRIVILEGE ITEM (S)	REQUESTED	APPROVED	
The scope of privileges in general dentistry includes the evaluation, diagnosis, consultation, management, and provision of therapy and treatment for patients of all ages presenting with conditions or disorders involving the oral cavity and its associated structures. Dentists may assess, stabilize, and determine disposition of patients with dental diseases and disabilities or dysfunctions. They order and interpret radiographs and diagnostic tests to determine the type and extent of dental diseases. Dentists restore health and function of carious, fractured, otherwise defective teeth and perform routine preventive, periodontal, oral surgery, endodontic, and prosthodontic treatments.	Fully Competent	Fully Competent	
Diagnosis and Management (D&M):			
PRIVILEGE ITEM (S)	REQUESTED	APPROVED	
Jaw relations records	Fully Competent	Fully Competent	
D&M Advanced Privileges (Requires Additional Training):			
PRIVILEGE ITEM (S)	REQUESTED	APPROVED	
Cephalometric radiograph analysis	Fully Competent	Fully Competent	
Nonsurgical management of temporomandibular disorders	Fully Competent	Fully Competent	
Prosthodontics:			
PRIVILEGE ITEM (S)	REQUESTED	APPROVED	
Occlusal analysis	Fully Competent	Fully Competent	
Orthodontics:			
PRIVILEGE ITEM (S)	REQUESTED	APPROVED	
Minor tooth movement	Fully Competent	Fully Competent	
Pediatric Dentistry:			
PRIVILEGE ITEM (S)	REQUESTED	APPROVED	

This document is protected by 10 USC 1102

\*\*\*\* FOUO \*\*\*\*

Page 1

Figure 210: 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.

### 6.3.14 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 immediately listed in the **Documents** section of the credentials record. 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 211 below.

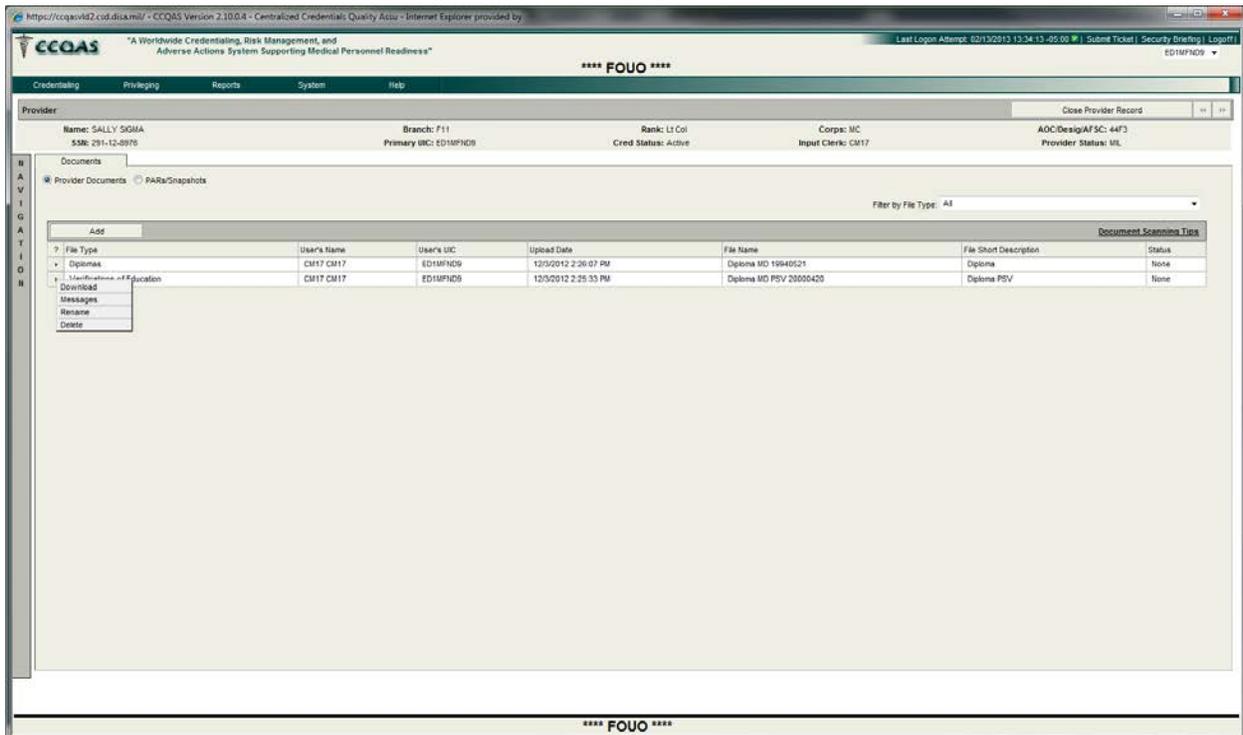


Figure 211: Documents Section

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. The **File Name** should only contain one period before the file extension.

Other important features of the **Provider Documents** screen include the following:

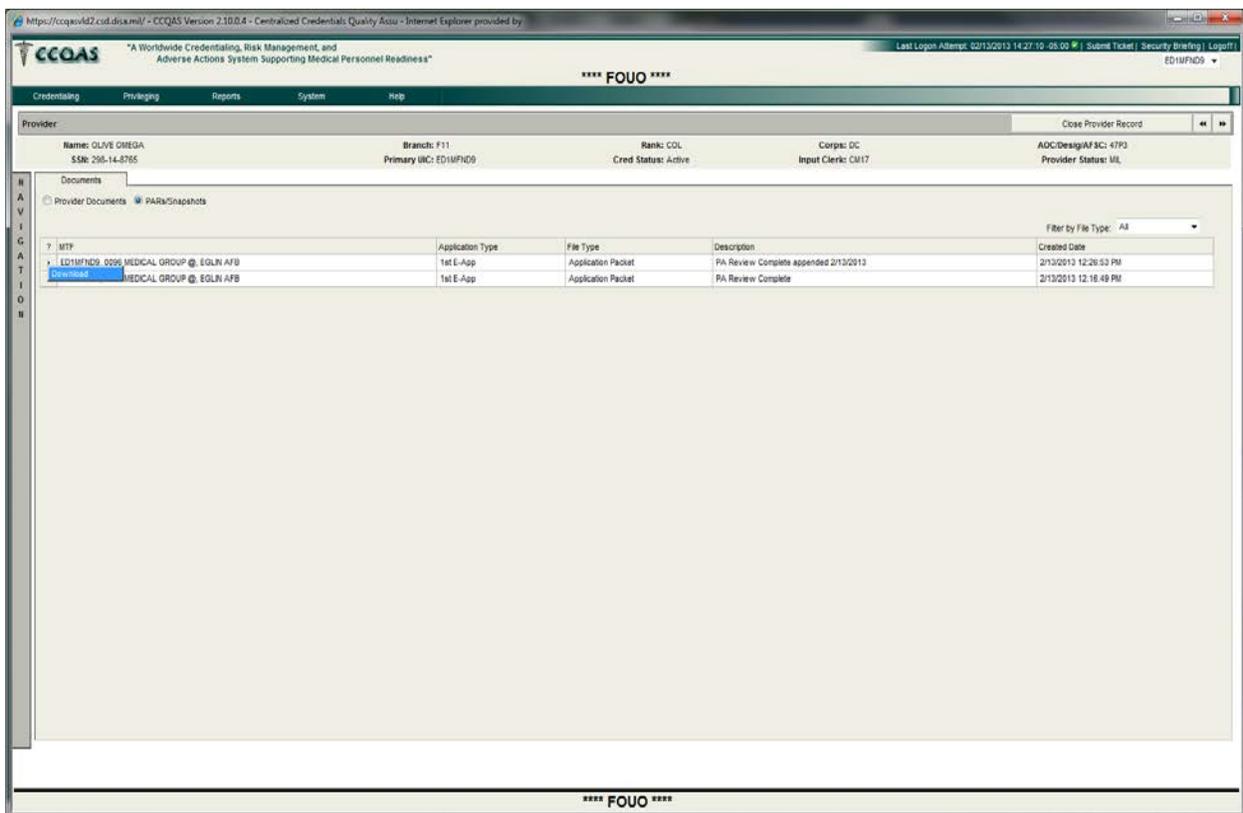
- Users may search the list of documents associated with the application by selecting the desired document type from the **Filter by File Type** pick list

**Note:** The Filter by File Type pick list defaults to Adverse Privileging Information, so be sure to select the correct file type.

- 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 **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
- The **Status** field identifies documents associated with a request for a Credentials Update.

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 212 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 E-signs the E-application or Appendix Q, and when PSV of the E-application has been completed. When the PA renders a final decision, a final PA Review Complete snapshot is generated and prior PDF versions for the application are deleted. There may be cases with multiple snapshots prior to approval for applications that were terminated.

**Note: PSV Complete** is the final PDF Snapshot generated for Clinical Support Staff.



**Figure 212: 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 approved E-Applications, Appendix Q documents, and PAR forms, regardless of privileging location, are displayed on this screen.

### 6.3.15 The Remarks Section

The **Remarks** section is the final listed section of the of a Provider’s credentials record, as depicted in Figure 213 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.

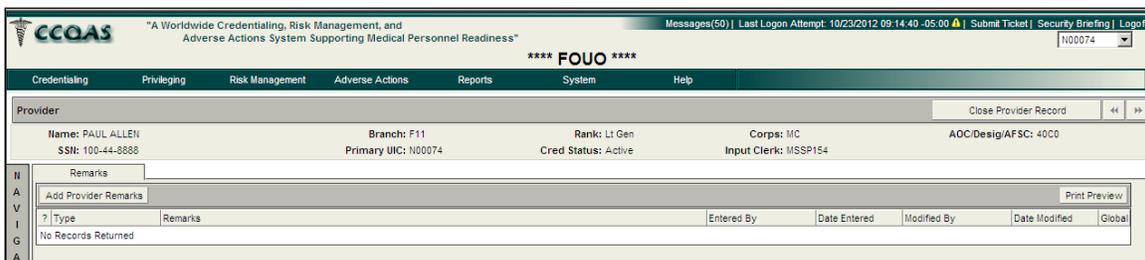


Figure 213: Remarks Section

The **Remarks** section remains empty until the **Provider Remarks Type** pick list is configured (See [Section 15](#) for details.) 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 214 below depicts the **Provider Remarks** section.

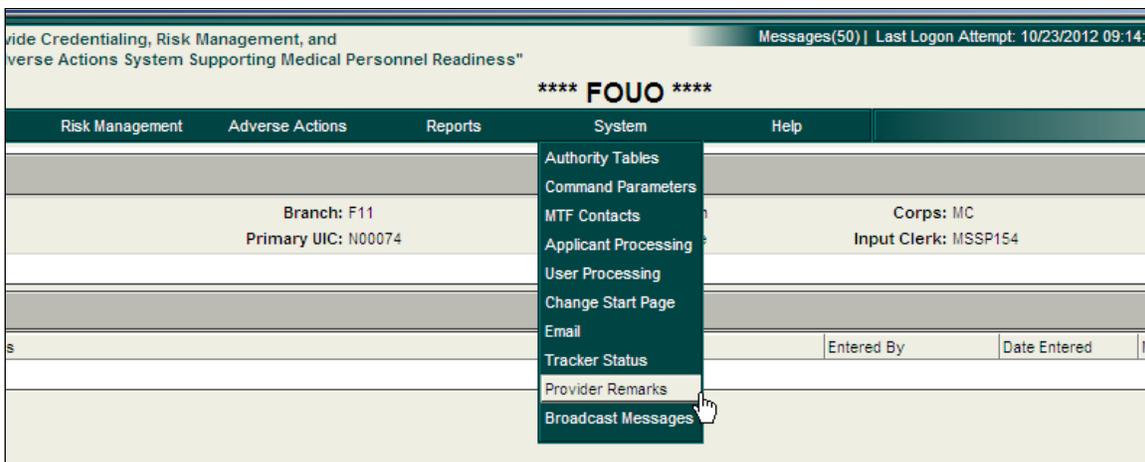
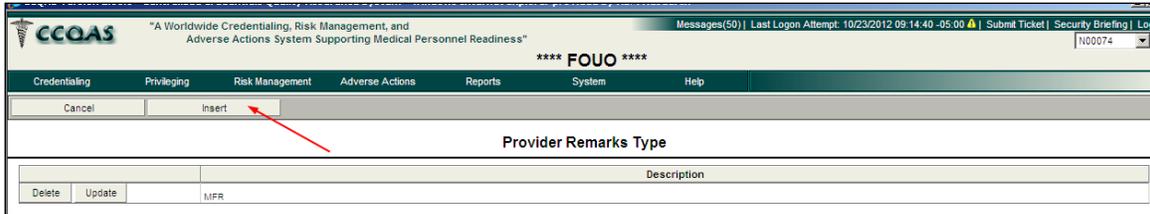


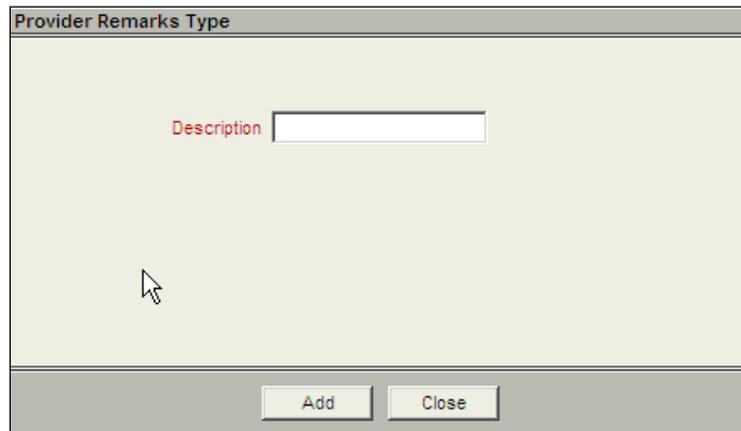
Figure 214: Provider Remarks Section

The **Provider Remarks Type** window opens, as depicted in Figure 215 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.



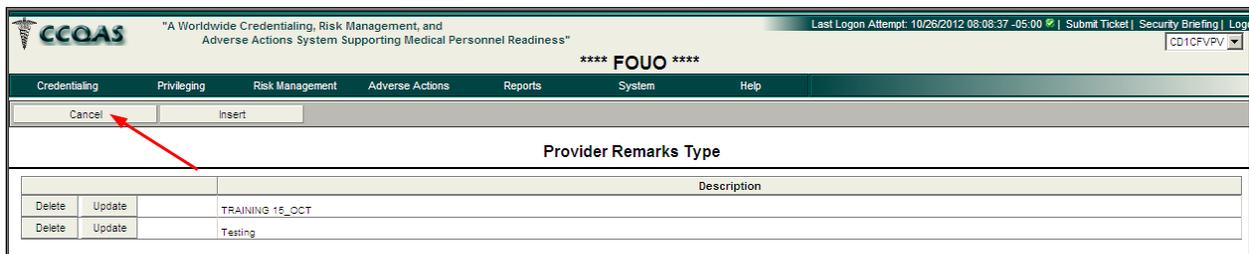
**Figure 215: Provider Remarks Window**

After CC/MSSP/CMs enter a free-text **Description** and click **Add**, the **Provider Remarks Type** displays one new entry. Figure 216 below depicts the **Provider Remarks Type** screen.



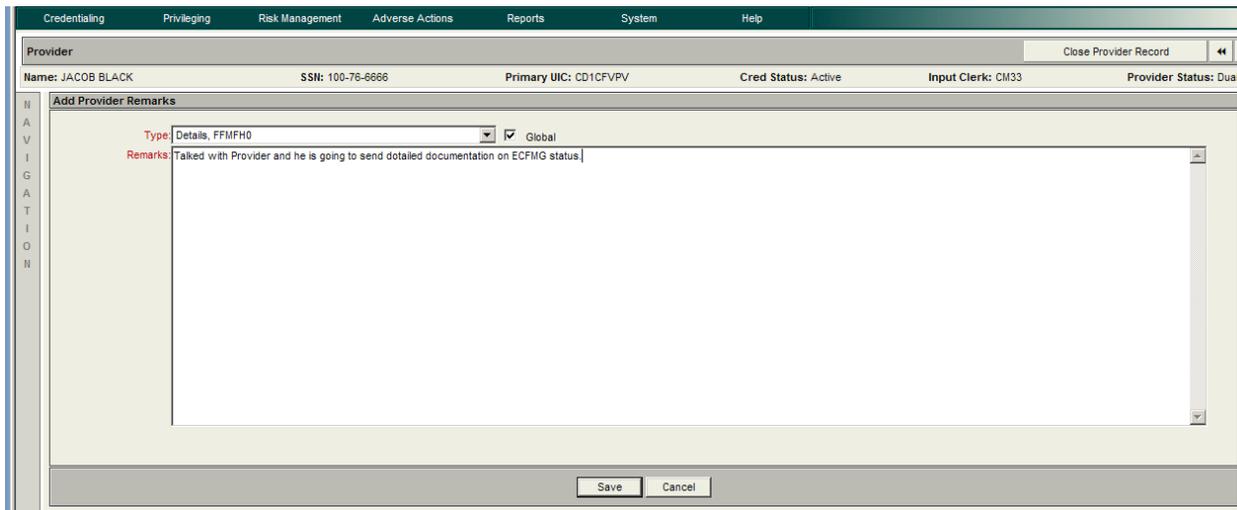
**Figure 216: Provider Remarks Type Screen**

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 217 below. After all desired values have been created CC/MSSP/CMs click **Cancel** to complete the configuration process.



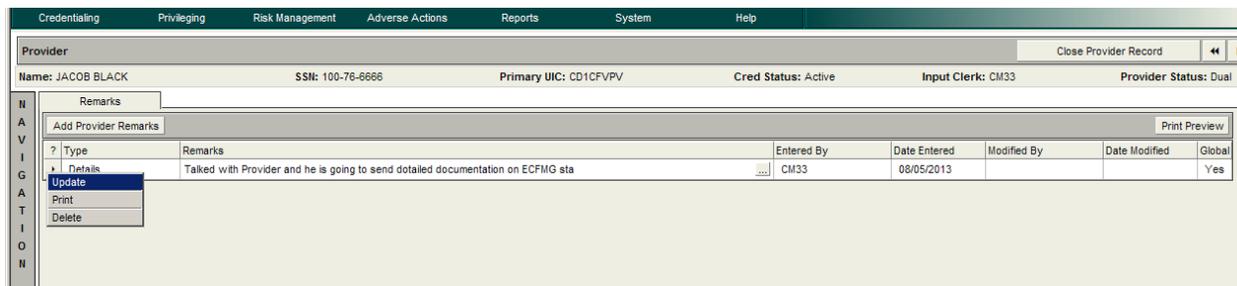
**Figure 217: Provider Remarks Type Screen**

After the **Provider Remarks** pick list has been configured, CC/MSSP/CMs may enter remarks into the credentials record, as depicted in Figure 218 below.



**Figure 218: 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 219 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.



**Figure 219: 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 are 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/MSSP/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), and a variety of letters.

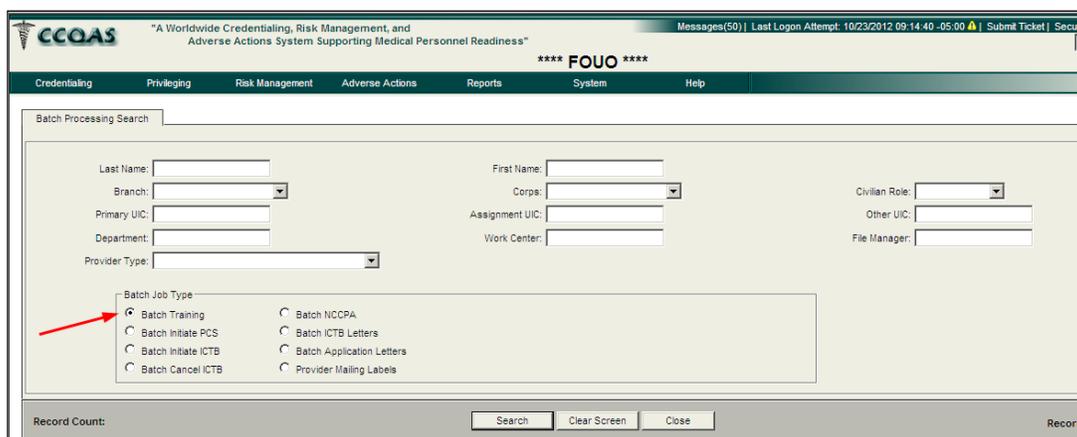
All batch actions are initiated from the **Credentialing > Batch Processing** menu, as depicted in Figure 220 below.



**Figure 220: 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 221 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.

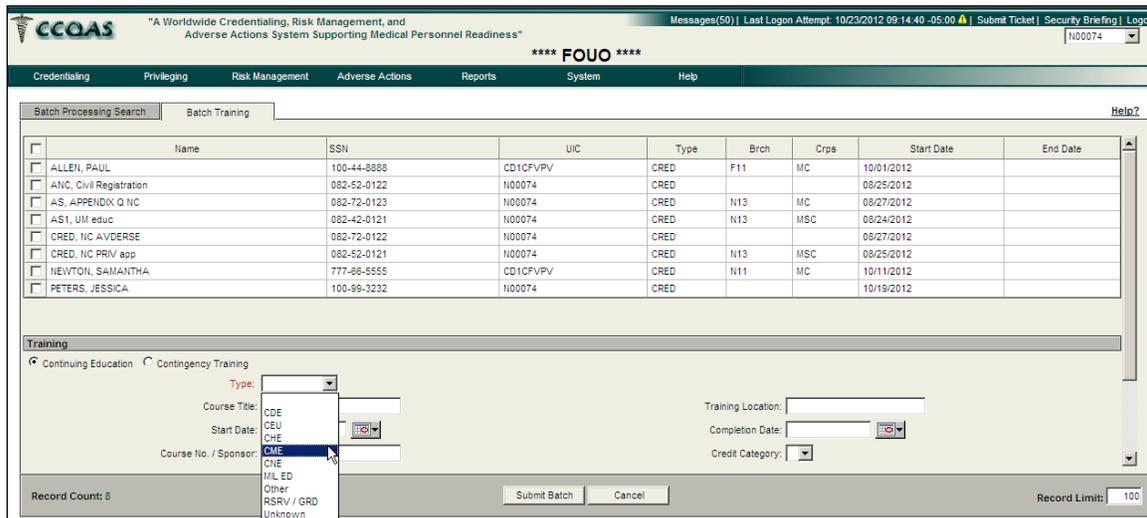
Users may enter additional search criteria in the upper portion of the **Credentials Provider Search** screen if they wish to limit the batch action to only certain groups of records (e.g., only Providers in a specific department, work center, corps, or unit). After all appropriate search criteria are entered and the desired batch action is selected, users click **Search**.



**Figure 221: 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 222 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.



**Figure 222: 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.

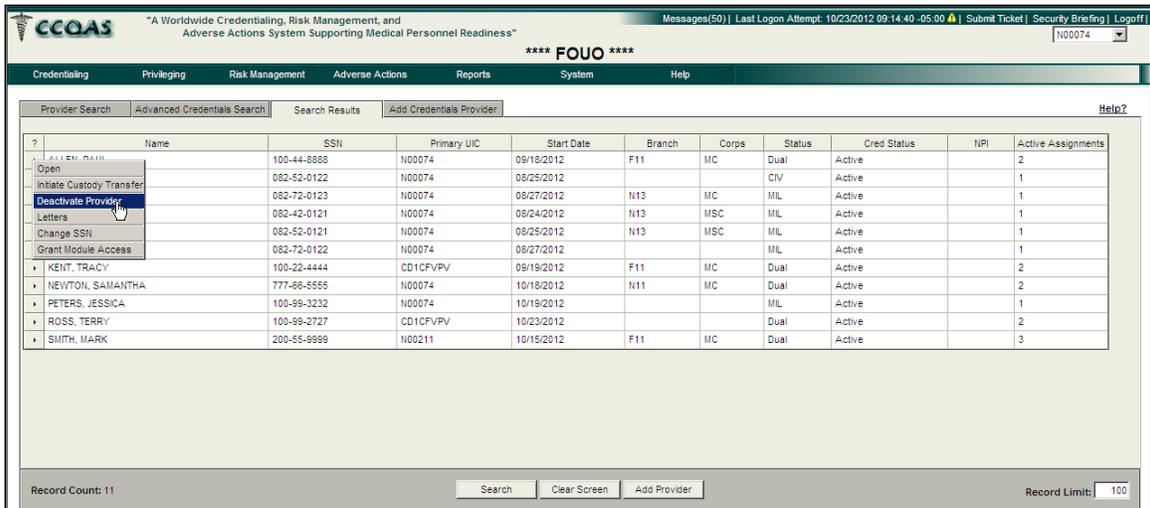
Records that are updated or transacted through batch processing remain independent of each other after the batch action has been completed. For example, if a **Batch ICTB** transaction is performed, and then one or more Providers in the batch do not perform the ICTB as planned, individual ICTB transactions may be cancelled or ended without impacting the ICTB transactions for the remainder of the batch.

**Note:** Use Batch Processes with caution, as only the ICTB can be undone (i.e., cancelled) in the batch.

## 6.5 Deactivating a Credentials Record

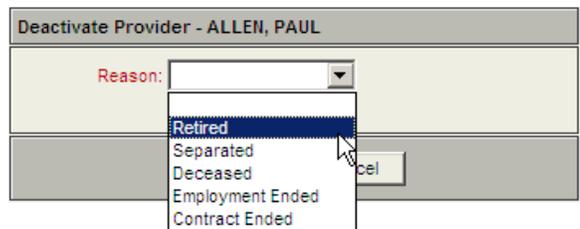
When a Provider's record is deactivated, the record status in CCQAS changes from *Current* to *Inactive*. This action may be appropriate when military Providers retire from active duty service or for civilian or contract employees whose employment arrangement has ended. Not all users have the necessary permissions to deactivate a Provider's record. Users should consult Service policies prior to deactivating any Provider credentials records.

In order to deactivate an individual Provider's credentials record that is currently in active status, the Primary UIC user must perform a [search](#) for the record, using record **Provider Credentials Status = Active** (the default setting). An individual Provider may be deactivated by selecting **Deactivate Provider** from the menu of Provider hidden menu actions, as depicted in Figure 223 below.



**Figure 223: Deactivate Provider Menu Item**

The user then selects a disposition **Reason**, indicating why the record is being deactivated, as depicted in Figure 224 below.



**Figure 224: Deactivate Provider Screen**

The Provider’s credentials record and any current assignments in the Primary UIC are immediately inactivated with the current date. If the Assignment needs to be ended for a prior date, use the End Assignment action off the **Work History Assignment** tab first and then use Deactivate Provider to inactivate the credentials record. 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.

**Note:** A credentials record cannot be deactivated by the Primary UIC if there is a current assignment at another UIC. In this case, use End Assignment to end the current assignment at the Primary UIC and then use the Initiate Custody Transfer action to transfer the credentials record according to current business rules. Typically, this will be the UIC that has the current assignment.

## 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.

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 225 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 225: 'Provider Mailing Label' Radio Button**

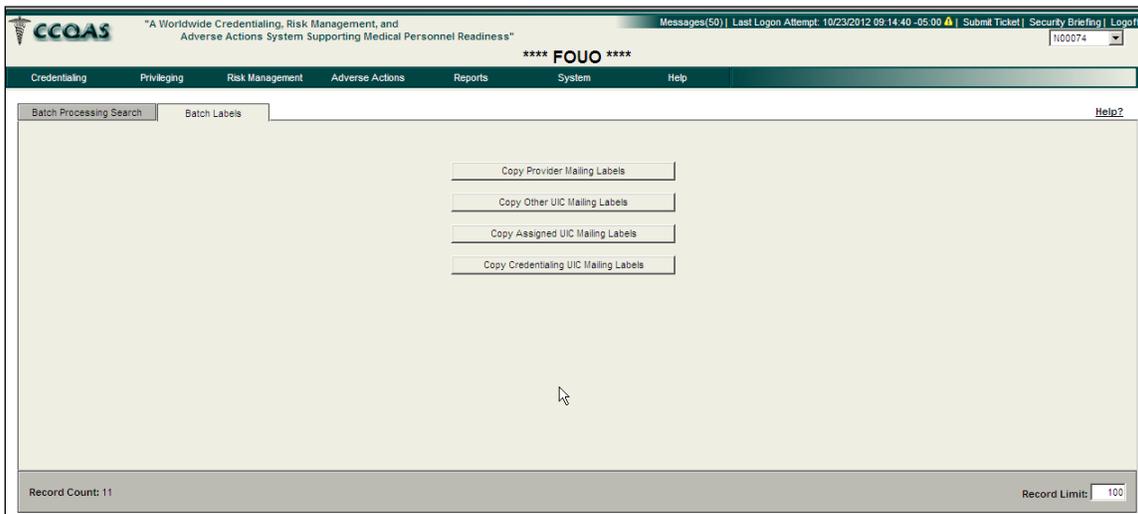
A list of Providers that meet the search criteria specified displays on the **Batch Labels** tab, as depicted in Figure 226 below. CC/MSSP/CMs may check which Providers for whom mailing labels should be generated, and then click **Submit Batch**.

<input type="checkbox"/>	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 checked="" type="checkbox"/>	ANC, Civil Registration	082-52-0122	N00074	CRED			Current	08/25/2012			N00074	Non-Personal Service Contractor			No
<input type="checkbox"/>	AS, APPENDIX Q NC	082-72-0123	N00074	CRED	N13	MC	Current	08/27/2012			N00074	Administrative			No
<input type="checkbox"/>	AS1, UH educ	082-42-0121	N00074	CRED	N13	MSC	Current	08/24/2012			N00074	Active Duty Staff (non Training)			No
<input type="checkbox"/>	CRED, NC AVDERSE	082-72-0122	N00074	CRED			Current	08/27/2012			N00074	Administrative			No
<input type="checkbox"/>	CRED, NC PRIV app	082-52-0121	N00074	CRED	N13	MSC	Current	08/25/2012			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	777-66-5555	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

**Figure 226: '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 227 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.

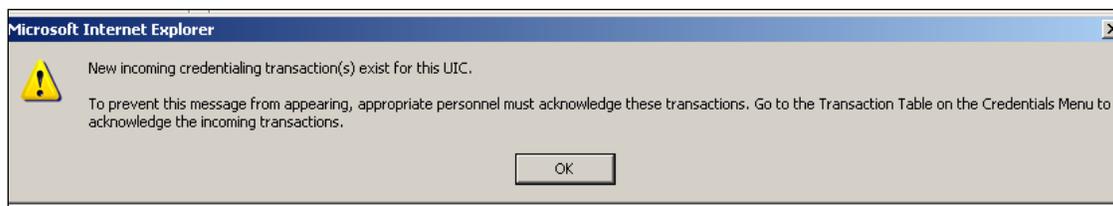


**Figure 227: Batch Labels Options (i.e., Mailing Labels)**

### 6.7 The ICTB Transaction Table Entry

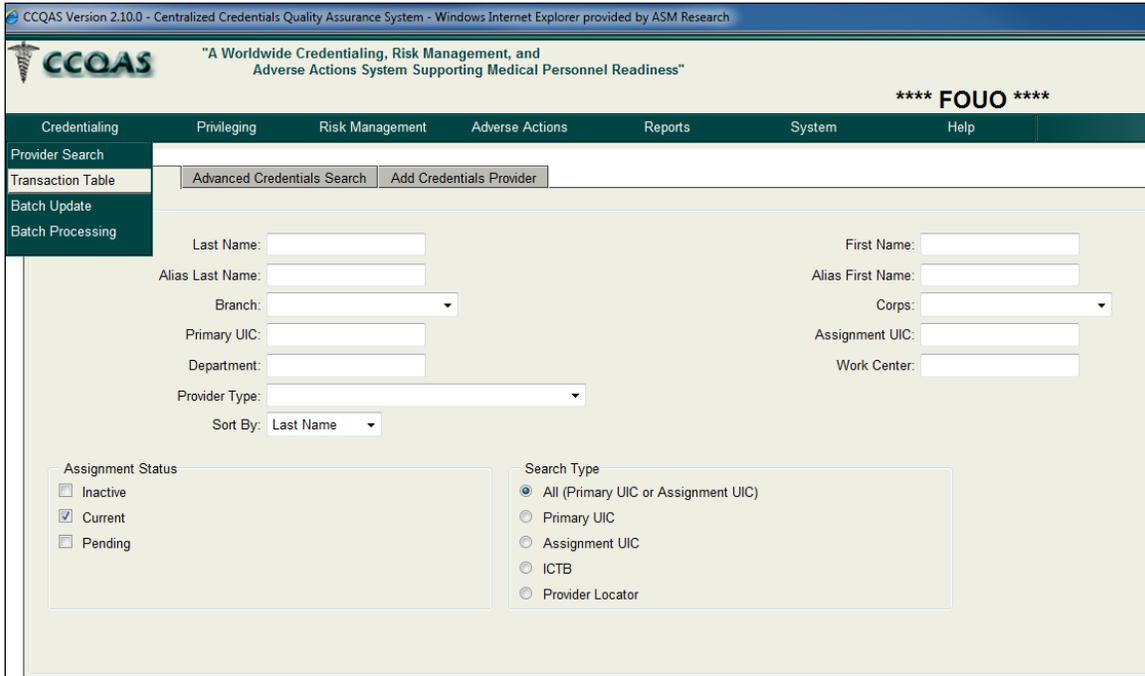
Although CCQAS does not require it, gaining CM/MSSP/CCs should acknowledge receipt of the ICTB transaction in the Transaction Table. This acknowledgment allows the sending facility to know that the transaction was received and accepted. CC/MSSP/CMs are alerted to a new entry in the Transaction Table by a message window that appears each time they access the Credentials module, as depicted in Figure 228 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 228: New Incoming Credentials Transaction Window**

The Transaction Table may be viewed by clicking the **Credentiaing** main menu bar across the top of the screen, and then selecting **Transaction Table**, as depicted in Figure 229 below.



**Figure 229: Accessing the Transaction Table**

The **Provider Transactions** screen displays, as depicted in Figure 230 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 230below.

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" Last Logon Attempt: 10/26/2012 08:08:37 -05:00 Submit Ticket | Security Briefing | Log

\*\*\*\* FOUO \*\*\*\*

Credentialing Privileging Risk Management Adverse Actions Reports System Help

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 230: 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.

## 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, at the Primary UIC, 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. Non-Primary UIC must request a credentials update via the Document section of the credentials record or by contacting the Primary UIC. 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](#))

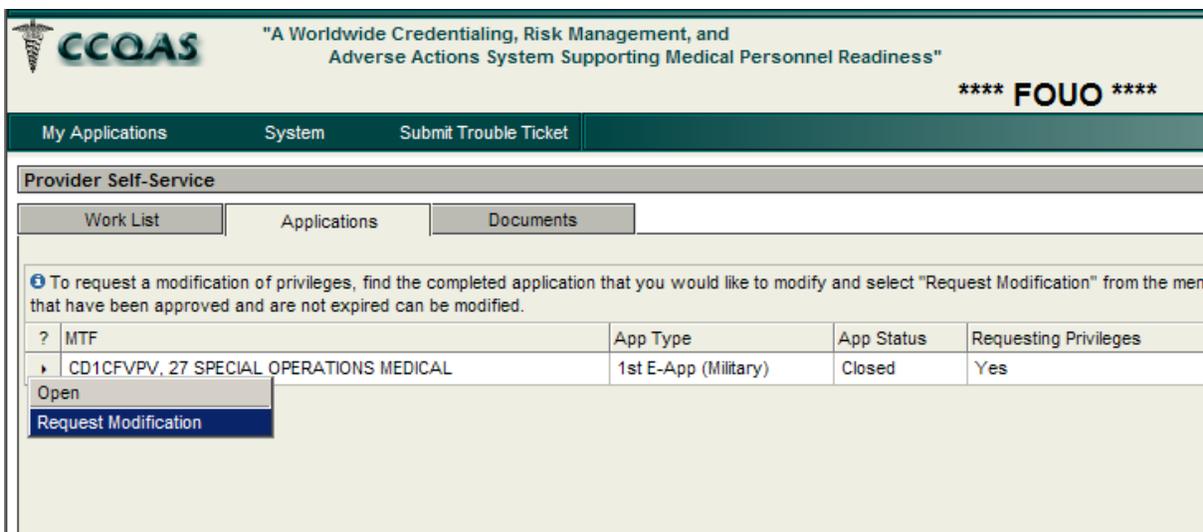
If the change in credentials supports a change to the Provider's current clinical privileges, then the Provider may wish to request modification of privileges before the next privilege renewal cycle. In this case, the Provider may submit an application for modification or augmentation of privileges and 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 CC/MSSP/CM.

To generate a modification application the CC/MSSP/CM will use **Initiate Application** from the provider's current Credentials (CRED) Assignment.

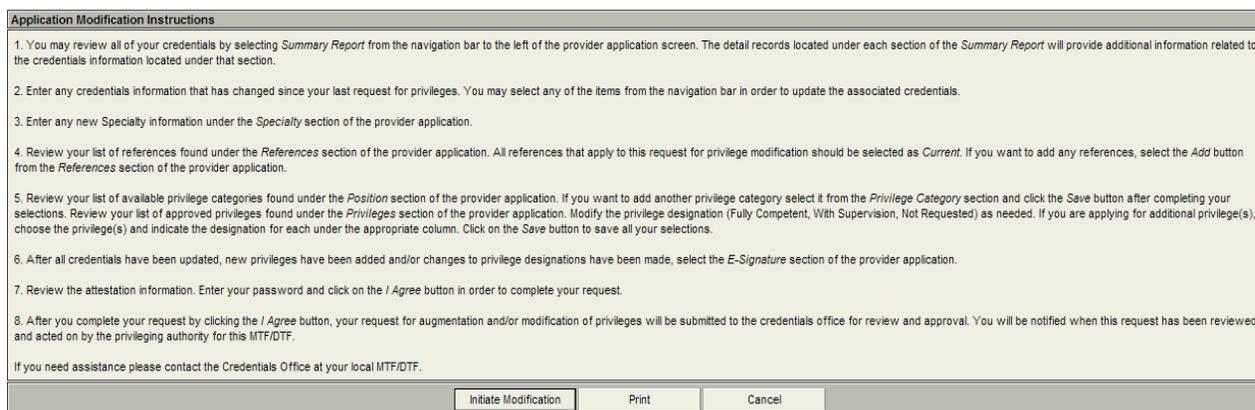
The Provider may also generate a modification application for the most recent approved application at that facility. Provider will click the **Applications** tab, and select "**Request Modification**" as depicted in Figure 231.



**Figure 231: 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 232. Providers may print these instructions by clicking **Print**, or they may cancel the request and return to the **Applications** tab by clicking **Cancel**.



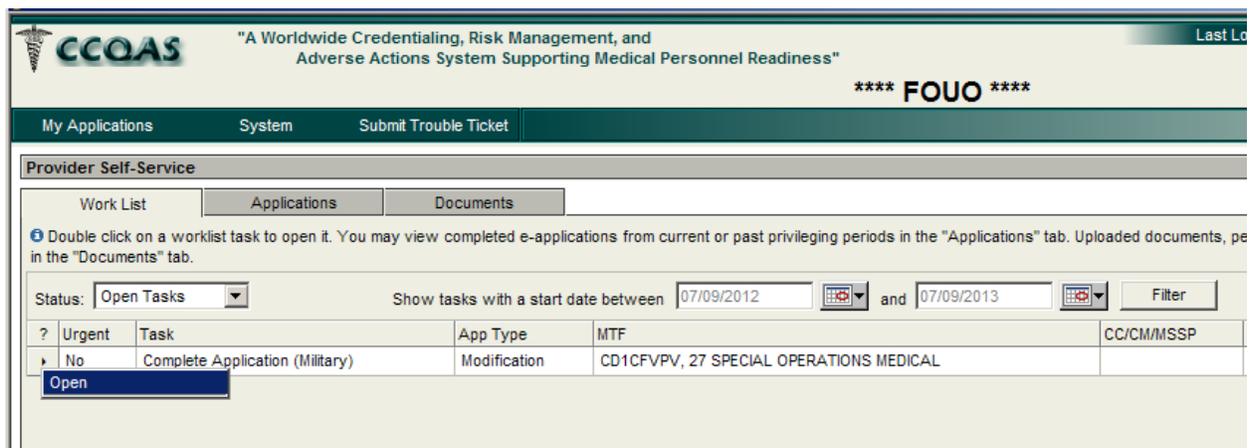
**Figure 232: Application Modification Instructions Screen**

When Providers click **Initiate Modification**, a new application for modification of privileges appears, as depicted in Figure 233. Providers must proceed with the application process, according to the instructions provided.



**Figure 233: Provider Application (Modification)**

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 234 depicts a sample modified application.

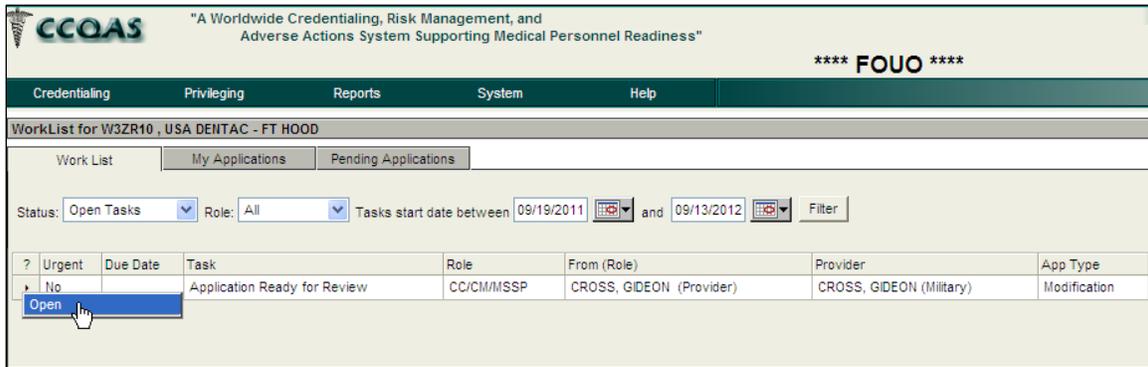


**Figure 234: Provider Task – Complete Application, Modification**

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

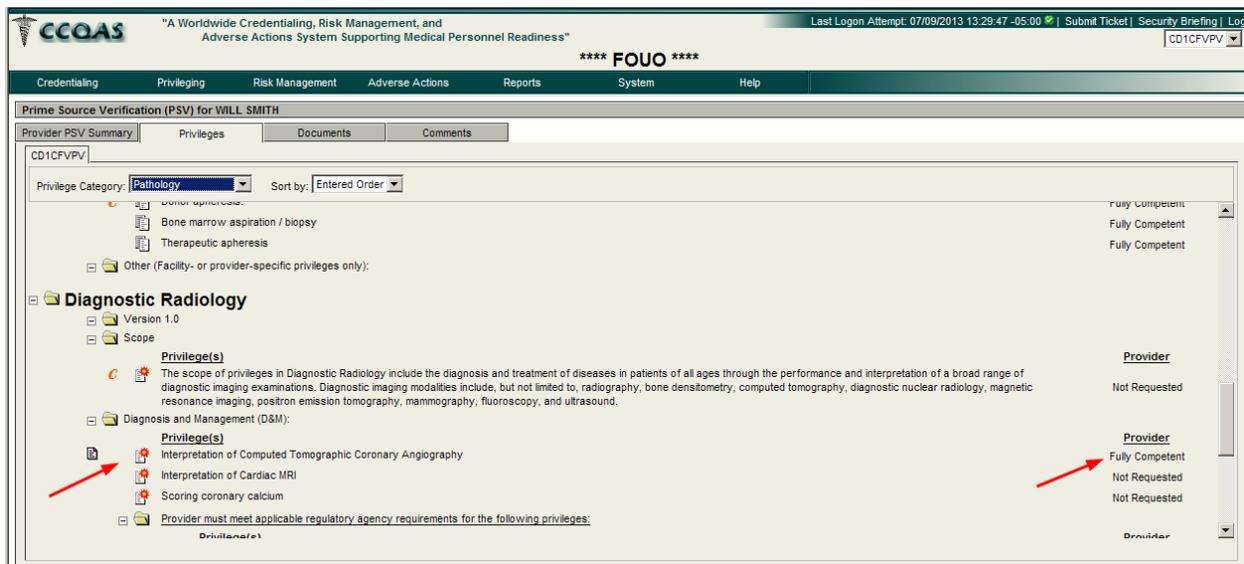
After the Provider signs and submits the Modification Application, the system forwards it to the CC/MSSP/CM. The CC/MSSP/CM receives a new work list item with **App Type = Modification**, as depicted in Figure 235.



**Figure 235: CC/MSSP/CM Task – Application Ready to Review, Modification**

Processing a Modification Application is the same as processing any other Electronic Application (e-App), see [Section 5](#) for details.

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 236.



**Figure 236: 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.

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. Interfacility Credentials Transfer Briefs (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 a Provider has a current assignment)
- When the sending location initiates an ICTB, CCQAS creates an ICTB assignment at the gaining location with view-only access to the Provider’s credentials record.
- When the sending location initiates an ICTB, CCQAS also generates a new electronic privilege application, provided it is not suppressed by the sending facility or the gaining facility has not activated the Privileging Module, for the Provider to request privileges at the ICTB location. This application is referred to as an ICTB application. An option exists for Navy providers who are requesting to exercise only currently approved core privileges at the gaining Navy UIC to complete an Appendix Q form vice a complete application.
- Following the completion of ICTB duty that is longer than 3 days in duration, CCQAS automatically initiates the online PAR process at the gaining location

### 8.1 Requesting an ICTB by the Gaining Location

Through its Credentialing module, CCQAS 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, first name or SSN 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 237 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 **All (Primary UIC or Assignment UIC)** radio button, CCQAS only searches for the Provider among those who are already performing duty at the user’s location.

?	Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	Facility Name	Credentials Coordinator	DSN Phone	Commercial Ph
?	10802_CRS	100-22-4444	CD1CFVPV	08/15/2012	F11	MC	MIL	Active	27 SPECIAL OPERATIONS MEDICAL GROUP @	Mrs. Karen Bair (SGHC)	681.8608	575.784.6608
?	Assignment	384-51-1124	DW1CFD9S	07/12/2012			CIV	Active	0007 MEDICAL GROUP	Ms. Renee Marie Hutchison (SGQ)	461-4262	(325) 696-4262
?	Request Custody Transfer Letters	071-22-0123	DW1CFD9S	07/12/2012			MIL	Active	0007 MEDICAL GROUP	Ms. Renee Marie Hutchison (SGQ)	461-4262	(325) 696-4262
?	100-66-5555	100-66-5555	CD1CFVPV	08/17/2012			MIL	Active	27 SPECIAL OPERATIONS MEDICAL GROUP @	Mrs. Karen Bair (SGHC)	681.8608	575.784.6608
?	A18_GROHPT	201-30-1014	N68470	01/09/2013			MIL	Active	US NAVAL HOSPITAL	Philip Bennett	(315) 643-0228	011-81-611-743-0228
?	A18_Military	072-32-0121	N00074	07/23/2012			MIL	Active	NAVAL SPECIAL WARFARE COMMAND	Ms. Jocelyn Fonseca	(456) 111-1333	(619) 537-7771
?	A18C_CIVIL CRED	072-32-0123	N00074	07/23/2012			CIV	Active	NAVAL SPECIAL WARFARE COMMAND	Ms. Jocelyn Fonseca	(456) 111-1333	(619) 537-7771
?	A1NC ICTB	082-42-0125	N00074	08/24/2012	N13	MSC	Dual	Active	NAVAL SPECIAL WARFARE COMMAND	Ms. Jocelyn Fonseca	(456) 111-1333	(619) 537-7771

Figure 237: Assignment Menu Item on the Provider Locator, 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, as depicted in Figure 2 below, which generates an ICTB Broadcast Message.

?	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	PAR Date
?	Administrative	Administrative			MIL	CRED	Current	12/10/2012									No	

Figure 238: Request ICTB Action on Assignment Screen

CC/MSSP/CMs must enter the **ICTB Begin Date**, **ICTB End Date** and **Type of Duty** and then click **Send**, as depicted in Figure 239 below. A message displays, which indicates that the request was sent.

Subject: ICTB Transfer Requested

ICTB Begin Date: 02/19/2013

ICTB End Date: 02/19/2014

Type of Duty: TDY

Message Preview: CC104 CC104 is requesting that the credentialing record for Anders, DR (219-99-4000), be ICTB'd to WZ01AA, BROOK ARMY MED CTR, with a beginning date of 02/19/2013 and ending date of 02/19/2014.

Contact information as follows:  
 Username: CC104  
 Email: rick.martin@usa.army.mil  
 Phone: (111) 222-3333 (Home)

Buttons: Send, Close

Figure 239: Request ICTB Broadcast Message at Gaining Location

The responsible CC/MSSP/CM at the ICTB sending location receives the request through the **Broadcast Messages** function within CCQAS. The next time the CC/MSSP/CM at the ICTB sending location logs in to CCQAS, he or she is alerted to a new incoming broadcast message. See [Section 15.9](#) for more on Broadcast Messages.

In all instances, it is the responsibility of the ICTB sending facility or unit to initiate the ICTB transaction. The gaining unit can only request the ICTB transaction, but cannot initiate it.

## 8.2 Initiating the ICTB at the Sending Location

CC/MSSP/CMs at sending locations initiate an ICTB for temporary duty, regardless of whether or not the gaining location submits a Broadcast Message requesting the ICTB. Any location that has a current CRED assignment can initiate an ICTB. The sending facility, however, may initiate multiple ICTBs from the same CRED assignment as the situation, facility, and Service protocol dictates.

Sending facility CC/MSSP/CMs initiate an ICTB through the Credentialing module. To initiate an ICTB, select **Provider Search** from the **Credentialing** drop-down menu. Enter the last name and first name or SSN 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 240 below.

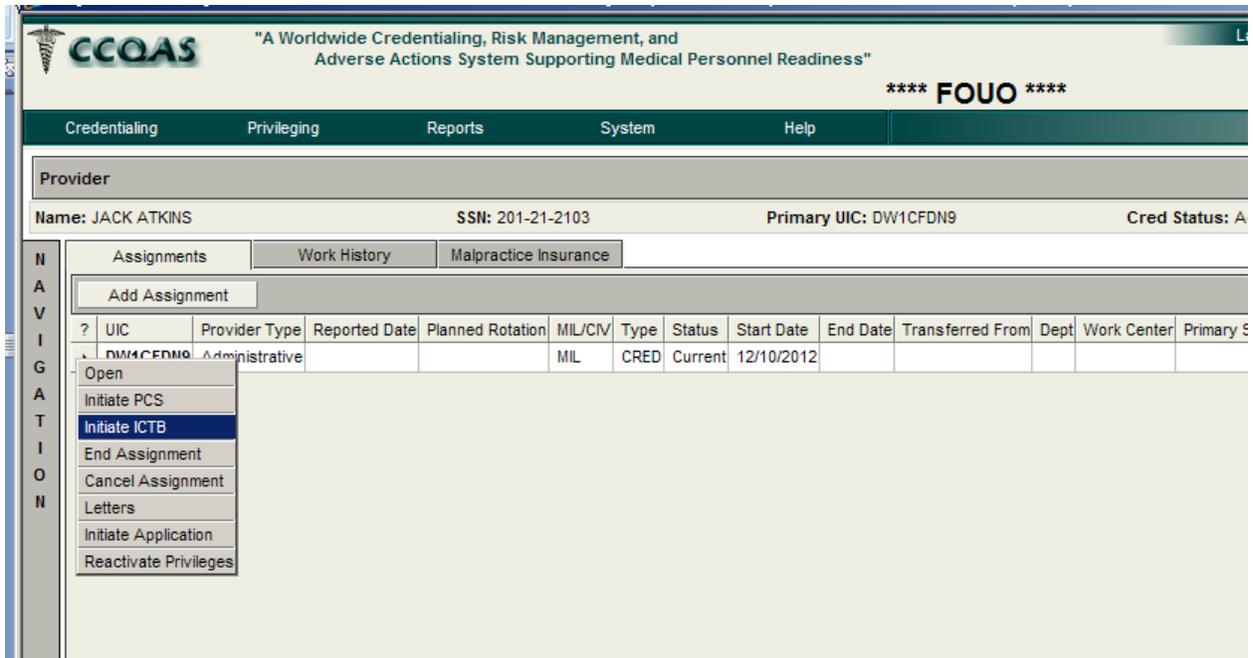
The screenshot shows the CCQAS interface with the following details:

- Header:** CCQAS logo, "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness", and "Last Logon Attempt: 02/24/2013 19:04".
- Navigation Tabs:** Credentialing, Privileging, Reports, System, Help.
- Provider Information:** Name: BILL ANDERS, SSN: 219-99-0000, Branch: A11, Primary UIC: W0Q1AA, Rank: CPT, Cred Status: Active, Corps: MC, Input Clerk: CC93.
- Navigation Menu (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** (highlighted), Privileges, Documents, Remarks.
- Work History Table:**

	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date	Transferred From	Dept	Work Cer
(non Training)			MIL	CRED	Current	09/24/2012				
(non Training)			MIL	ICTB	Current	02/19/2013	02/18/2014	W0Q1AA (ICTB)		

Figure 240: Work History Section on Navigation Menu

From the hidden menu of actions, next to the current assignment record, click **Initiate ICTB** in the menu as depicted in see Figure 241 below.



**Figure 241: 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 click **Submit** to initiate the ICTB transaction. Figure 242 below depicts the ICTB form.

**Initiate ICTB - JACK, ATKINS**

To Command: CD1CFVPV

**ICTB Information**

Start Date: 08/06/2013

End Date: 09/06/2013

Evaluation (PAR/OER)

**Provider Information**

Type of Duty: Mobilization (non-humanitarian)

Current PED:

ICTB Duty Status:  Military  Civilian

**Credential Signature Authority Information**

Credential Signature Authority / Name: American Hero

Credential Signature Authority / Position: Commander

Credential Signature Authority / Command: Hospital

Credential Signature Authority / Location: USAFA

Credential Signature Authority / Phone: 5102623333

Select the additional text for paragraph 13:

No additional information in Credentials File

Additional license information in Credentials File

Additional information in Credentials File - Please Call

Additional comments for paragraph 14:

None

cc:

Suppress ICTB E-Application:  Yes  No

Generate ICTB Letter:  Yes  No

**Figure 242: ICTB Form**

**Note:** 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. See [Section 15](#) for Command Parameters.

**Note:** The End Date on an ICTB cannot extend beyond the Privilege Expiration Date (PED).

**Note:** There is an option to **Suppress ICTB E-Application** for the temporary ICTB gaining location, which suppresses an electronic privileging application from being generated as part of the Initiate ICTB function. CCQAS cannot issue an electronic privileging application at a site where the electronic privileging module is not turned on (check MTF Contacts to determine

whether the privileging module has not been activated, see Section 15 for MTF Contacts). There is another option **Generate ICTB Letter**, in which users can designate **Yes** or **No** to include the generation of a letter as part of the transaction.

The **Initiate ICTB** screen appears differently for Providers who do not have a user account. 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 243 below. When the ICTB transaction is initiated for a new Provider user, the system will automatically generate a new user account.

**Initiate ICTB - HEATH, BANKS**

A user account for the provider will be created as part of the ICTB process. This will allow the provider to be able to use CCQAS to complete his application online.

To Command:  

**ICTB Information**

Start Date:  

End Date:  

Evaluation (PAR/OEP)

**Provider Information**

Type of Duty:  

Current PED:

Provider's Primary Email:

Provider's Phone Type:   Provider's Phone Number:

ICTB Duty Status:  Military  Civilian

**Credential Signature Authority Information**

Credential Signature Authority / Name:

Credential Signature Authority / Position:

Credential Signature Authority / Command:

Credential Signature Authority / Location:

Credential Signature Authority / Phone:

Select the additional text for paragraph 13:

No additional information in Credentials File

Additional license information in Credentials File

Additional information in Credentials File - Please Call

Additional comments for paragraph 14:

None

cc:

Suppress ICTB E-Application:  Yes  No

Generate ICTB Letter:  Yes  No

**Figure 243: 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.

After a sending facility initiates an ICTB transaction, the following actions automatically occur:

- CCQAS generates a new ICTB assignment that the gaining facility may use to document the assignment and other details of the duty performed by the Provider at the ICTB location
- CCQAS generates an ICTB privilege application for the Provider to request privileges at the gaining location (unless users selected Yes for the Suppress ICTB E-Application selection or the gaining location has not activated the privileging module)

### 8.3 The ICTB Assignment Record

Sending CM/MSSP/CCs at the Primary UIC retain full access to, and responsibility for, maintaining a Provider’s primary credentials record, while gaining facility personnel have view-only access to the Provider’s credentials data but maintain the ability to update ICTB assignment information and upload documents.

Based on the ICTB start date, a new assignment record with **Status = Current or Pending** and **Type = ICTB** is created at the sending facility, as depicted in Figure 244 below. In a Provider’s **Work History** section, **Assignments** tab new ICTB assignment information is read-only at the sending facility.



Figure 244: Work History, Assignments tab for the Sending Location

At the same time the ICTB assignment is created at the sending facility, the same ICTB assignment with **Status = Current or Pending** and **Type = ICTB** becomes available to the gaining location, as depicted in Figure 245 below. The sections in this record are read-only, with the exception of the newly-created assignment record for the ICTB location on the **Assignment** tab. 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.



Figure 245: Work History, Assignment tab for the Gaining Location

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 is initiated. If the ICTB was initiated using a future date as the effective date, the Provider’s ICTB assignment remains in pending status at the sending and gaining facilities until midnight (Central Time) on the day before the effective date. The ICTB is classified as pending until the effective date is reached. ICTB assignments may be included in system queries or reports.

**Note:** A transaction is written to the Transaction Table at both the sending facility and gaining facilities each time an ICTB is initiated. Refer to Transaction Table (section xxx) for additional guidance.

#### 8.4 The Transfer (ICTB) Application for Clinical Privileges

After an ICTB transaction has been initiated, the system automatically sends an email notification to the Provider, and an active task is placed in their work list, with **Task = Complete Application** and **App Type = Transfer (ICTB)**, as depicted in Figure 246 below.



**Figure 246: Provider Task – Complete Application, Transfer (ICTB)**

Providers may then open, complete, and submit the Transfer Application according to the instructions provided. Figure 247 below depicts the Transfer (ICTB) Application for privileges.

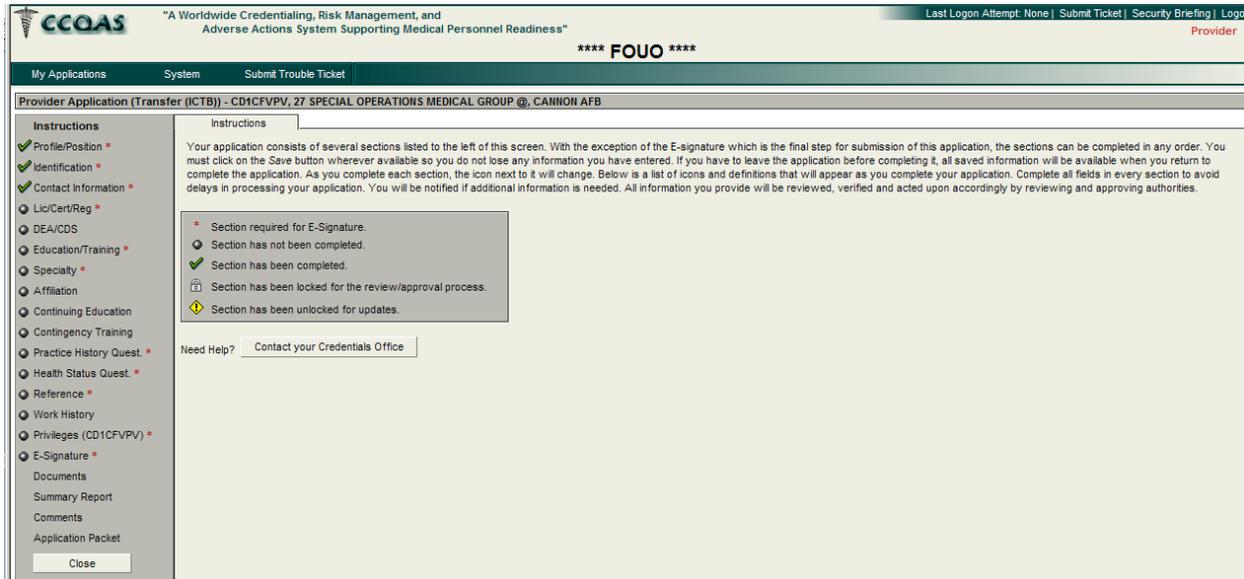


Figure 247: Transfer (ICTB) Application for Privileges



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 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
- 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 ICTB 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 in accordance with Service policy
- Providers may still scan and upload documents to the application, as appropriate

The Transfer (ICTB) email notification is sent to Providers immediately after the ICTB is initiated, if the provider has not submitted the e-app a reminder email every 5 days for 45 days. 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.

## 8.5 Processing an ICTB Transfer Application for Clinical Privileges

When CC/MSSP/CMs at a sending ~~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 248 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.

Provider	Application Type	Status	Provider Phone	Application Task Initiated	Provider Started Completing	Number of Days Completing
BOHETT, JOSH	Transfer (ICTB)	Pending	41614654	10/19/2012		
CRANE, HART	Transfer (ICTB)	Pending	654564	10/19/2012	13/19/2012	0

**Figure 248: 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 249 below.



**Figure 249: Gaining CC/MSSP/CM Task – Transfer (ICTB) Application**

Once submitted by the Provider, the ICTB application is processed the same as any other E-application. See Section 5 for additional details.

After the ICTB application is approved, the system imports the new privileges into the **Privileges** section and the ICTB assignment, **Privileges** tab of a Provider's credentials 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.

## 8.6 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 assignment 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 250 below.



Figure 250: Cancel ICTB Menu Item

When the ICTB is cancelled by the sending location, the ICTB assignments at both locations are deleted and will not be available in system queries or reports. If privileges were awarded at the gaining ICTB location, they will be auto-terminated and only the PA Review Complete snapshot will remain. An ICTB assignment and privileges, if awarded, may not be recovered after it has been cancelled.

## 8.7 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 assignment; the status of the ICTB assignment 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 **Assignment Status = Inactive** in their search and reporting criteria. The inactive ICTB assignment also becomes a read-only record at both locations.

If the ICTB ends prior to the end date established when the ICTB assignment was created or if the ICTB is extended, CCQAS users at issuing facilities may manually end or extend the ICTB transaction by selecting **End ICTB** from the menu of actions on the **Search Results** screen, as depicted in Figure 251 below.

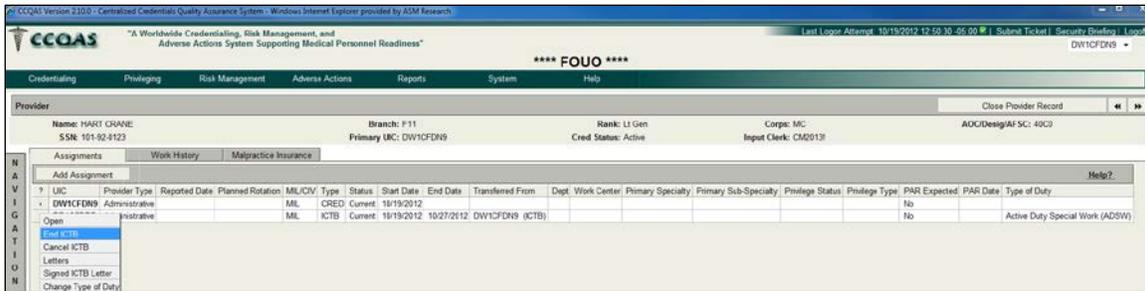


Figure 251: End ICTB Menu Item

An ICTB assignment may only be extended up to the privilege expiration date at the sending location. Once the ICTB End Date has been extended, any privileges awarded at the ICTB location need to be reviewed and extended by the gaining location.

## 8.8 PAR for ICTB Duty

CCQAS automatically initiates the PAR process for any ICTB duty that is greater than three 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 252 below.

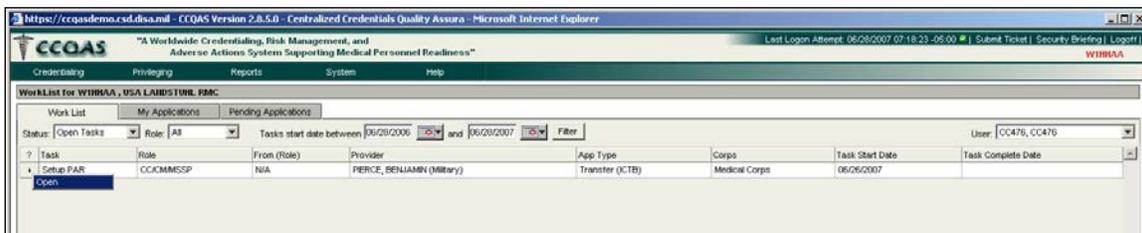


Figure 252: Gaining CC/MSSP/CM Task – Setup PAR

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.

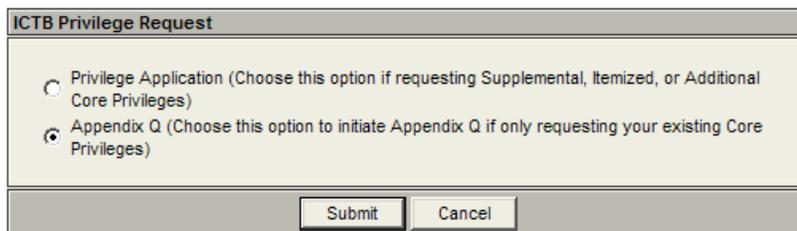
## 8.9 The ICTB Process for Navy Facilities

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 are only applicable for ICTB transfers from one Navy facility to another Navy facility. 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 253 below.



The screenshot shows a dialog box titled "ICTB Privilege Request". Inside the dialog, there are two radio button options. The first option is "Privilege Application (Choose this option if requesting Supplemental, Itemized, or Additional Core Privileges)" and is unselected. The second option is "Appendix Q (Choose this option to initiate Appendix Q if only requesting your existing Core Privileges)" and is selected. At the bottom of the dialog, there are two buttons: "Submit" and "Cancel".

**Figure 253: 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 254 below.

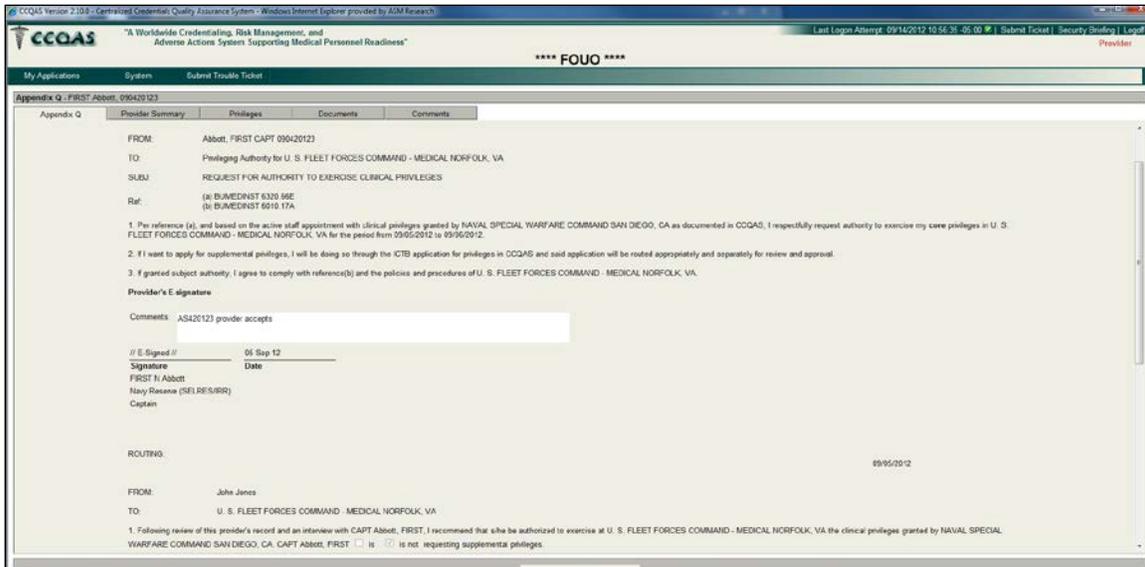


Figure 254: Appendix Q Letter

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 255 below.



Figure 255: 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, is 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 Permanent Change of Station (PCS) is the permanent transfer of a military or civil service Provider from one duty location to another. Military and civil service 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 current CRED assignment at the ‘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 Transfer (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 current privileging period at the sending location
- When a PCS date becomes effective, CCQAS inactivates the assignment at the sending location and sets the assignment status to current at the gaining location.
- When a PCS transaction is performed, the sending facility is given the option to Transfer Custody of the credentials record to the gaining facility, the default is Yes
- When users elect to perform a custody transfer concurrently with the PCS, the PCS transfer and the custody transfer have the same date, the PCS Effective Date

These processes are described in more detail in the following sections.

### 9.1 Requesting a PCS by the Gaining Location

CCQAS 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 locate the Provider’s credentials record, select **Provider Search** from the **Credentialing** drop-down menu. Enter the last name, first name or SSN 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 for, select **Assignment** from the hidden menu of actions on the **Search Results** tab as depicted in Figure 79.

**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 **All Primary UIC or Assignment UIC** radio button is selected, CCQAS only searches for the Provider among those that are already performing duty at the user’s location.

Credentiaing		Privileging		Reports		System		Help	
Provider Search		Advanced Credentials Search		Search Results		Add Credentials Provider			
?	Name	SSN	Primary UIC	Start Date	Branch	Corps	Statu		
▶	JONES, HANNANH	428-35-7439	HL0RFC23	10/23/2012			CIV		
▶	JONES, NORA	510-16-2012	ED1MFND9	10/16/2012	F11	MC	MIL		
▶	JONES, SABRINA	100-72-4444	CD1CFVPV	12/13/2012	F11	NC	MIL		
▶	JONES, TOM	800-08-0808	W2P0AA	10/23/2012	A12	MS	MIL		
	Assignment	219-88-1212	W0Q1AA	09/24/2012			MIL		
	Request Custody Transfer	218-11-2222	S30MFLRY	09/21/2012			MIL		
	Letters	999-33-8758	N00183	09/07/2012			CIV		

**Figure 256: Assignment Menu Item on the ‘Provider Locator’ Tab**

The Provider’s Assignment screen of his or her credentials record displays, as depicted in Figure 257. CC/MSSP/CMs then click the hidden menu of actions and select **Request PCS** on the Provider’s current CRED assignment.

Credentiaing		Privileging		Reports		System		Help				
Provider												
Name: Jon Jones SSN: 219-88-1212				Branch: Primary UIC: W0Q1AA			Rank: Cred Status: Active					
Assignments		Work History		Malpractice Insurance								
Add Assignment												
?	UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date	Transferred From	Dept	Work C
	W0Q1AA	Armed Duty Staff (non Training)			MIL	CRED	Current	09/24/2012				
	Request PCS											

**Figure 257: Request PCS Action on Assignment tab**

CC/MSSP/CMs must enter the **PCS RNLT Date** (i.e., Report No Later Than), and then click **Send**, as depicted in Figure 81. A message displays, which indicates the request was sent.

Subject: PCS Transfer Requested

PCS RNLT Date: 02/20/2013

Message Preview: CC103 CC103 is requesting that the credentialing record for Jones, Jon (219-88-1212) be PCS'd to W2DLAA, ARMED FORCES INSTITUTE OF PATHOLOGY, WASHINGTON NLT 02/20/2013.

My contact information is as follows:  
 Username: CC103  
 Email: ctest@asmr.com  
 Phone: (111) 222-3333 (Home)

Send Close

**Figure 258: Request PCS Broadcast Message at Requesting Location**

CC/MSSP/CMs at PCS sending (i.e., losing) facilities or units receive the request through the **Broadcast Message** function within CCQAS. 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. See Section 15.9 for more on Broadcast Messages.

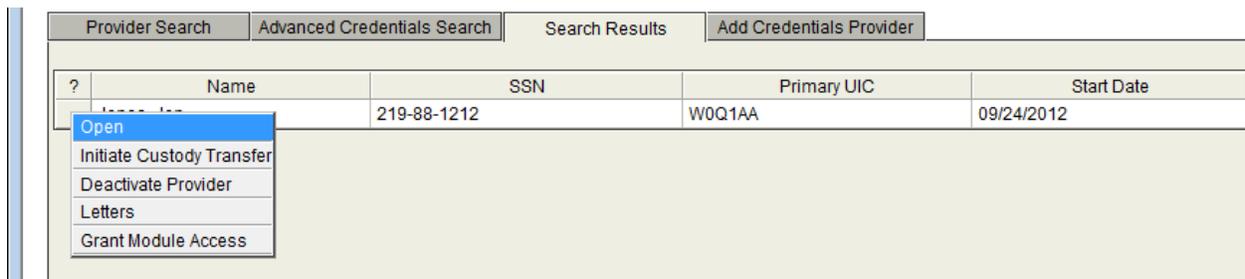
## 9.2 Initiating the PCS at the Sending Location

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:** Only locations with a current CRED assignment may initiate a PCS transaction. A Provider's assignment may not be PCSed if the Provider has an active ICTB. See Section 8.8 for more on **Ending an ICTB**.

A PCS transaction is initiated through the Credentialing module. To initiate a PCS, select **Provider Search** from the **Credentialing** drop-down menu. Enter the last name, first name or SSN of the Provider, select the **All (Primary UIC or Assignment UIC)** radio button, and 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.



**Figure 259: Open Menu Item**

Navigate to the **Work History** section of the credentials record by selecting **Work History** from the **Navigation** bar on the left. Select **Initiate PCS** from the hidden menu of actions next to the current assignment, as depicted in Figure 260.

Provider										
Name: Jon Jones					Branch:					
SSN: 219-88-1212					Primary UIC: W0Q1AA					
N A V I G A T I O N	Assignments		Work History			Malpractice Insurance				
	Add Assignment									
	?	UIC	Provider Type	Reported Date	Planned Rotation	MIL/CIV	Type	Status	Start Date	End Date
		W0Q1AA	Active Duty Staff (non Training)			MIL	CRED	Current	09/24/2012	
		<ul style="list-style-type: none"> <li>Open</li> <li style="background-color: #e0e0e0;">Initiate PCS</li> <li>Initiate ICTB</li> <li>End Assignment</li> <li>Cancel Assignment</li> <li>Letters</li> <li>Initiate Application</li> <li>Reactivate Privileges</li> </ul>								

**Figure 260: Initiate PCS Menu Option**

CC/MSSP/CMs enter the **Gaining UIC**, **Effective Date**, and click **Submit** to initiate the PCS transaction, as depicted in Figure 261.

**Note:** When PCS's are initiated by the Primary UIC, the **Transfer Custody** radio button is automatically defaulted to "Yes" to transfer custody and responsibility for maintaining the provider's credentials record to the gaining facility.

Initiate PCS - Jon, Jones	
Gaining UIC: W2DLAA 	Effective Date: 02/20/2013 
Provider's AKO Email: anthony.d.roberts12.civ@mail.mil	Transfer Custody: Yes <input checked="" type="radio"/> No <input type="radio"/>
<small>Email notifications to this provider are currently sent to this primary email address. Changes or corrections to this email address should be made prior to initiating this PCS transaction.</small>	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

**Figure 261: Initiate PCS Prompts Screen**

The **Initiate PCS** screen, depicted in Figure 262, appears differently if Providers do not have a user account. Additional data fields are present to capture a Provider's primary email address and phone information, both of which are required to create the new user account for Providers.

Initiate PCS - TRACY, POPE	
<small>A user account for the provider will be created as part of the PCS process. This will allow the provider to be able to use CCQAS to complete his application online.</small>	
Gaining UIC: <input type="text"/> 	Effective Date: <input type="text"/> 
Provider's Phone Type: Home 	Provider's Phone Number: <input type="text"/>
Provider's Primary Email: <input type="text"/>	Transfer Custody: Yes <input checked="" type="radio"/> No <input type="radio"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

**Figure 262: Initiate PCS Screen for additional fields for Provider User Account**

Providers then receive their user ID and temporary password information, which are required to access CCQAS, via email messages sent to the address entered on the **Initiate PCS** screen.

Immediately after the sending location initiates a PCS transaction, the following actions automatically occur:

- CCQAS generates a Transfer (PCS) 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. See Section 11 for more information
- Note: Refer to Service guidance for utilization of the electronic PAR
- A transaction is written to the Transaction Table at both the sending and gaining facility. The Transaction Table is explained in Section 6.
- If the PCS Effective Date is today or a prior date:
  - A new CRED assignment with a **Status** of “*Current*” is created at the gaining location
  - The **Status** of the CRED assignment at the sending location is set to “*Inactive*”
  - Any current privileges at the sending location are auto-expired with the PCS Effective Date
  - If **Transfer Custody** = *Yes*, primary custody of the credentials record is transferred to the gaining UIC
  - Information from the Provider's assignment at the losing facility is maintained as a read-only record in the **Work History, Assignments** tab of the credentials record
- If the PCS Effective Date is a future date, CCQAS generates a new CRED assignment with a **Status** of “*Pending*” at the gaining location  
**Note:** Pending PCS transactions can only be initiated 30 days in advance.
  
- For future dated PCSs, at 0001 (Central Time) on the PCS Effective Date:
  - The **Status** of the CRED assignment at the gaining facility changes to “*Current*”
  - The **Status** of the CRED assignment at the sending location changes to “*Inactive*”.
  - Any current privileges at the sending location are auto-expired with the PCS Effective Date.
  - If **Transfer Custody** = *Yes*, primary custody of the credentials record is transferred to the gaining UIC
  - The Providers module access for the sending UIC is removed.
- Information from the Provider's assignment at the losing facility is maintained as a read-only record in the **Work History, Assignments** tab of the credentials record

CC/MSSP/CMs at receiving (i.e., gaining) facilities or units receives a New Message Alert as depicted in Figure 89. See [Section 6](#), Transaction Table.

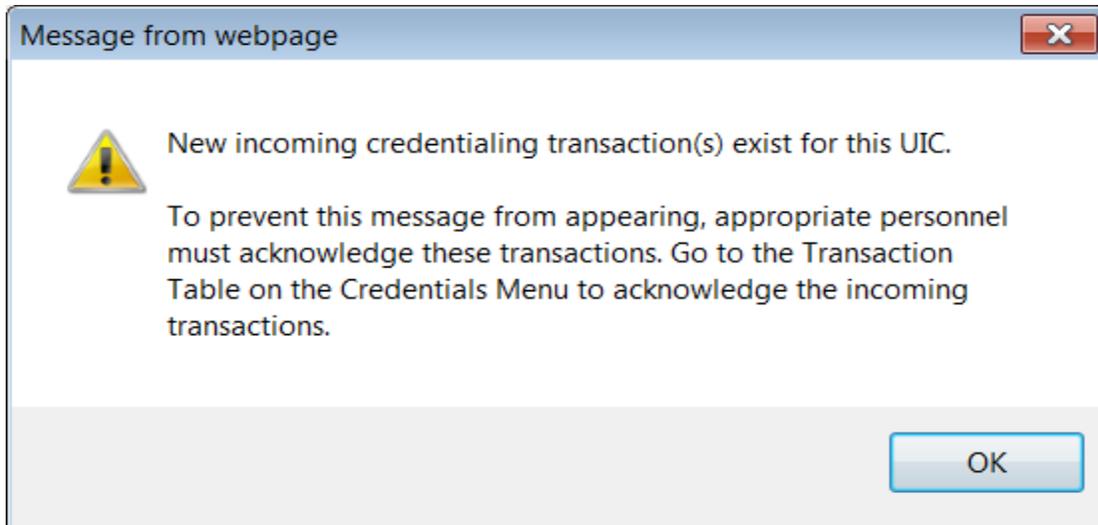


Figure 263: New Incoming Message Alert

### 9.3 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 264.

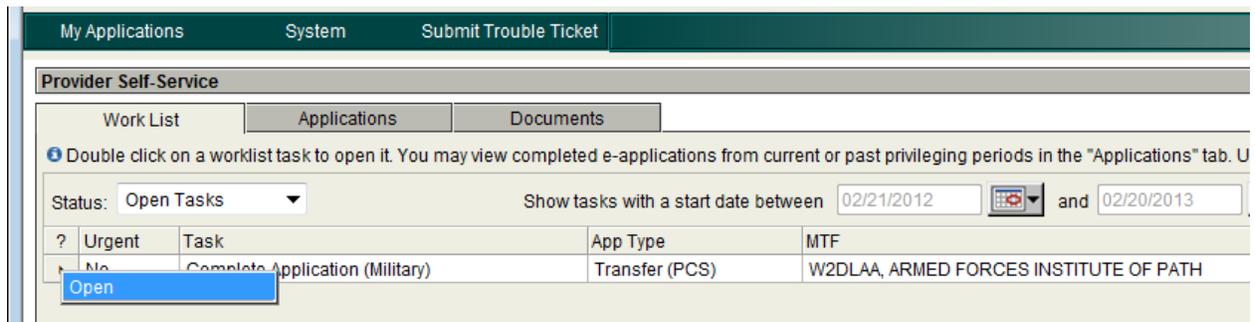


Figure 264: Provider Task – Complete Application, Transfer (PCS)

Providers may then open, complete, and submit the Transfer (PCS) Application according to the instructions provided, as depicted in Figure 265.

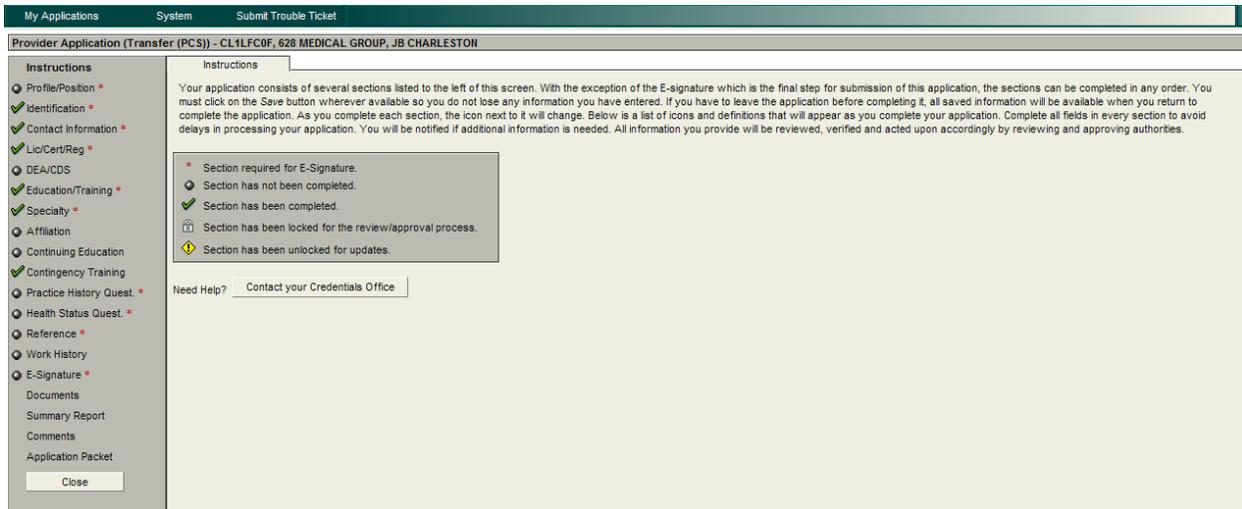


Figure 265: Transfer (PCS) Application for Privileges

See [Section 5](#) for how to process an e-App.

#### 9.4 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 266.

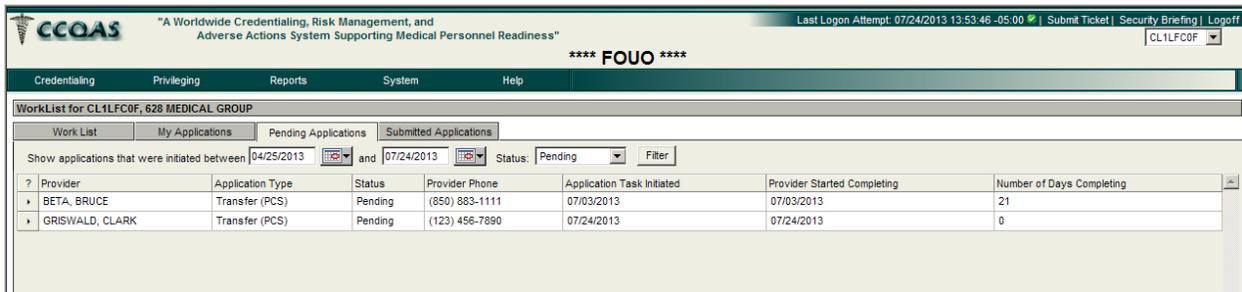
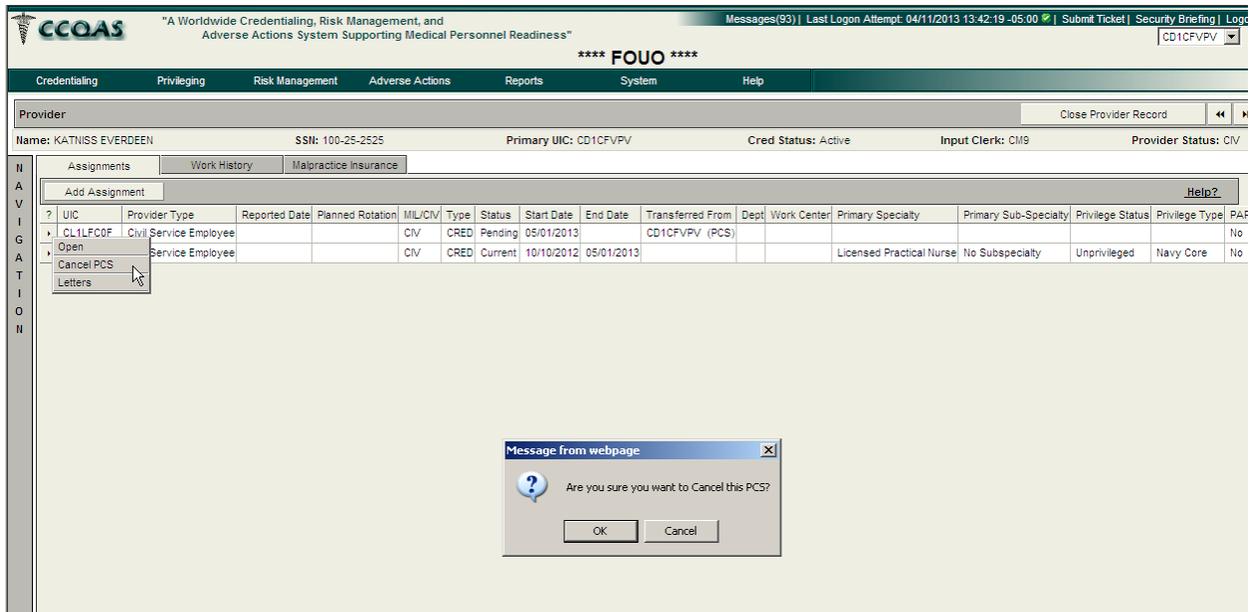


Figure 266: Gaining CC/MSSP/CM ‘Pending Applications’ Tab

See [Section 5](#) for further details on Processing the E-Application for Clinical Privileges

#### 9.5 Cancelling a PCS

The Record Movement - PCS role is required to cancel a PCS transaction. If a PCS transaction was initiated in error and needs to be cancelled, the sending CC/MSSP/CM can cancel the PCS by selecting **Cancel PCS** from the hidden menu of actions, on the Work History, Assignment tab, for the UIC of the gaining facility. The Cancel PCS Menu is depicted in Figure 93.



**Figure 267: Cancel PCS Menu**

**Note: Use with Caution as process cannot be undone.** When the PCS is cancelled, any associated e-Apps are deleted.

## 9.6 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 268.

If users click **Cancel**, the PCS transaction is cancelled. If users click **OK**, the PCS transaction proceeds.



**Figure 268: 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.

**Note:** At the time of the PCS, Dual Module users will lose all Module roles at their current UIC.

## 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 number of days prior to privilege expiration on the **Command Parameters** screen. See [Section 15.2](#) for more about Command Parameters.

### 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. See [Section 6](#) for further details.

### 10.3 The Renewal Application

After a renewal application is generated the provider will open, complete, and submit the Renewal Application, according to the instructions provided, as depicted in Figure 95.

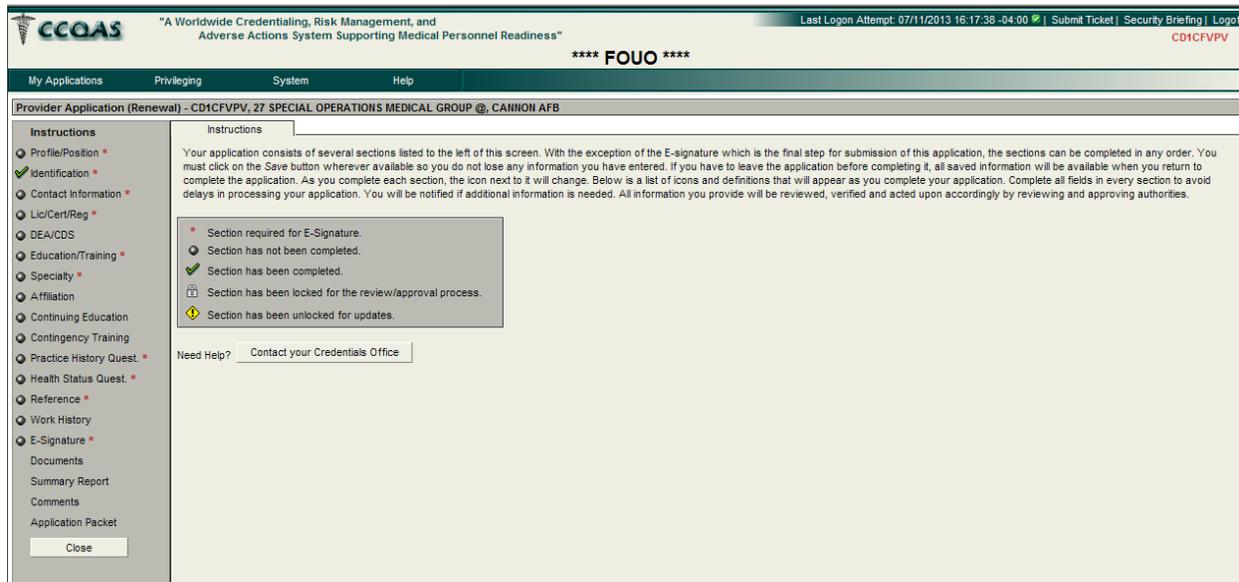


Figure 269: Provider Application (Renewal)

### 10.4 Processing an Application for Renewal of Clinical Privileges

See [Section 5](#) for Processing the E-Application for Clinical Privileges.

## 11 The Electronic 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. The PAR process may also be manually initiated 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 canceled, when appropriate. These processes are addressed in Sections 11.7 through 11.9.

**Note:** Refer to Service guidance for utilization of the electronic PAR.

### 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 initiating CC/MSSP/CM (sending UIC) entitled, **Task = Setup PAR**, as depicted in Figure 270.



The screenshot shows the CCQAS Work List interface for WZDNAA, BROOKE ARMY MED CTR. The interface includes a navigation menu with options like 'Credentialing', 'Privileging', 'Reports', 'System', and 'Help'. Below the menu, there are tabs for 'My Applications', 'Pending Applications', and 'Submitted Applications'. The 'Status' is set to 'Open Tasks' and the 'Role' is 'All'. A filter is applied for tasks starting between 02/28/2012 and 02/22/2013. The table below shows a single task entry:

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv Expiration
No		Setup PAR	CC/MSSP	N/A	SMITH, ROB (Military)	1st E-App	Medical Corps	02/22/2013		10/29/2014

**Figure 270: 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, while 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.

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 271.



**Figure 271: 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 272.

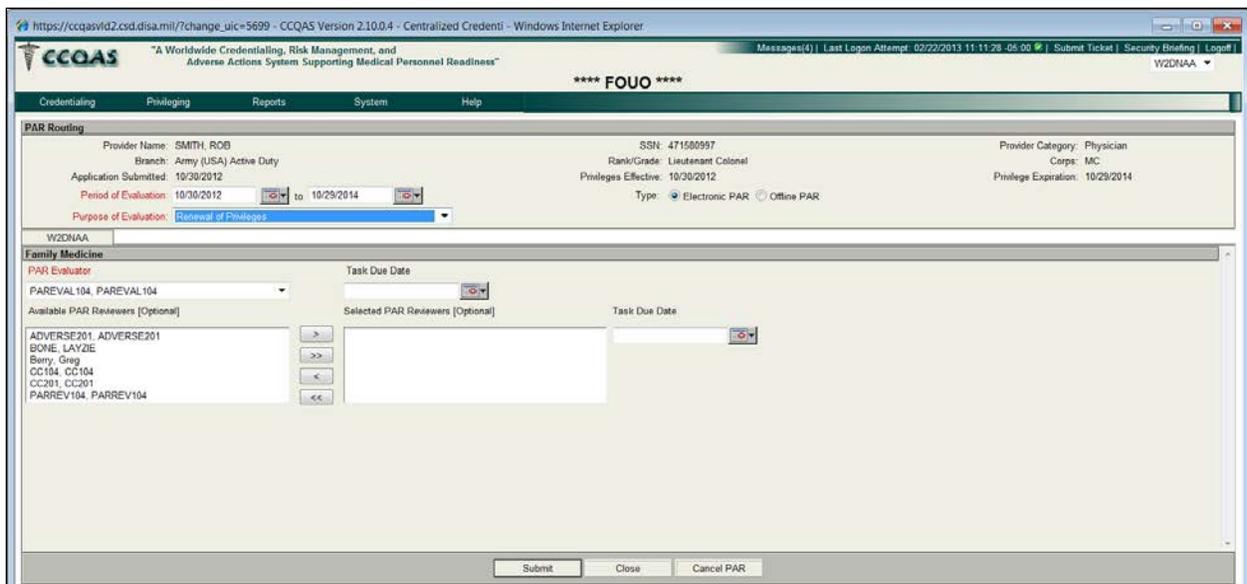


Figure 272: PAR Routing Screen

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 Privilege Category 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 Privilege Category, then one PAR Evaluator should be assigned for each Privilege Category 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

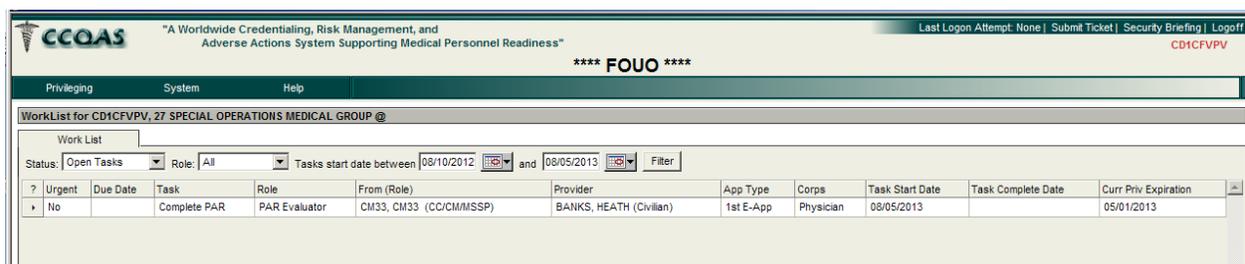
CC/MSSP/CMs may perform one of the following actions on the **PAR Routing** screen:

- 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 273.



The screenshot shows the CCQAS Work List 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, there is a navigation bar with "Privileging", "System", and "Help" options. The main content area is titled "WorkList for CD1CFVPV, 27 SPECIAL OPERATIONS MEDICAL GROUP @". It features a "Work List" section with a "Status" dropdown set to "Open Tasks", a "Role" dropdown set to "All", and a date range filter for "Tasks start date between 08/10/2012 and 08/05/2013". Below this is a table with the following data:

Urgent	Due Date	Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date	Curr Priv Expiration
No		Complete PAR	PAR Evaluator	CM33, CM33 (CC/CM/MSSP)	BANKS, HEATH (Civilian)	1st E-App	Physician	08/05/2013		05/01/2013

**Figure 273: 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 274.

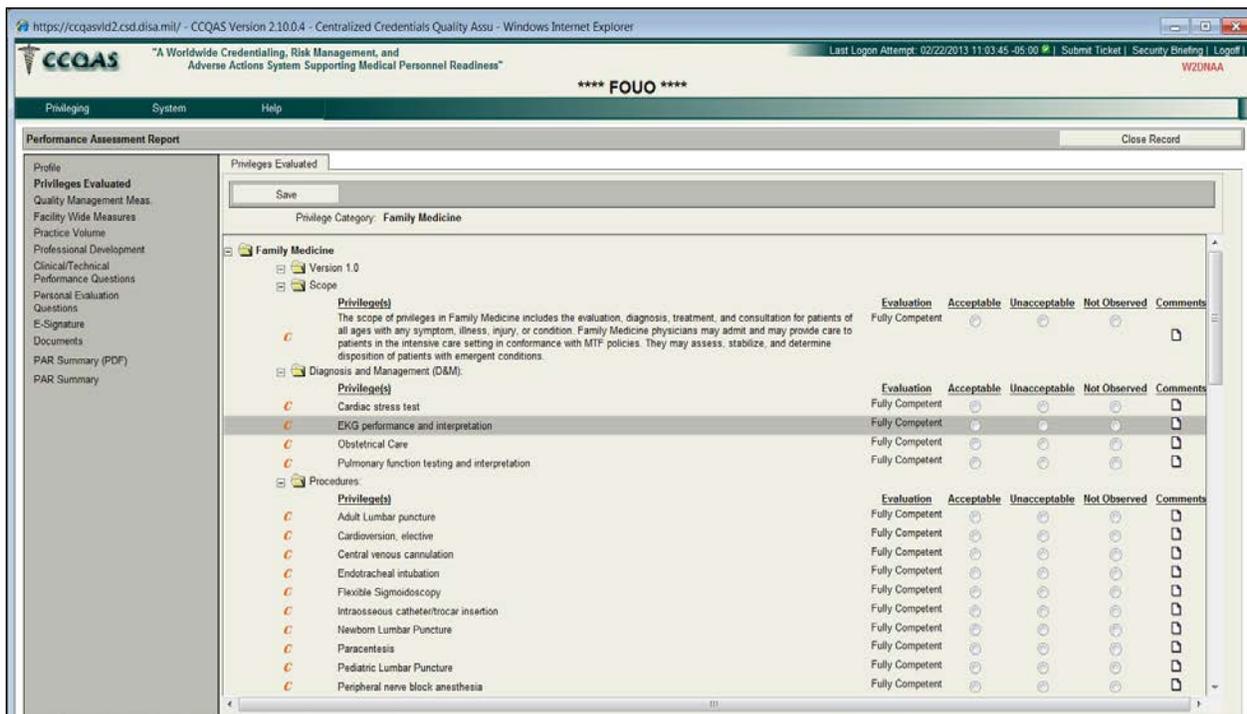
The **Profile** section provides demographic information about the Provider and the location, time period, and Provider's privilege category (i.e., specialty) that require evaluation. PAR Evaluators may navigate between different sections of the application by clicking the desired section of the form 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 274: Profile Section of the PAR**

The next section of the PAR form is the **Privileges Evaluation** section, as depicted in Figure 275.



**Figure 275: Privileges Evaluated Section for 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 276.

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 276: Privileges Evaluated Section for the PAR with Unacceptable

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, as depicted in Figure 277. PAR Evaluators, however, must render a general assessment of the Provider's competency at the end of the PAR form.

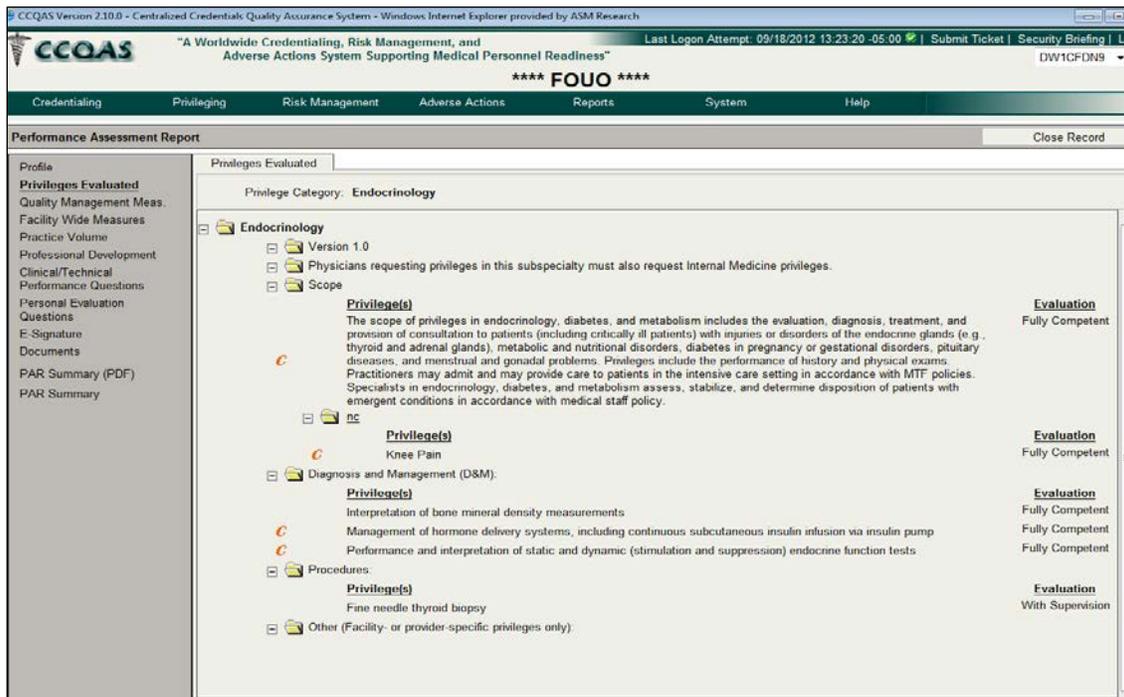


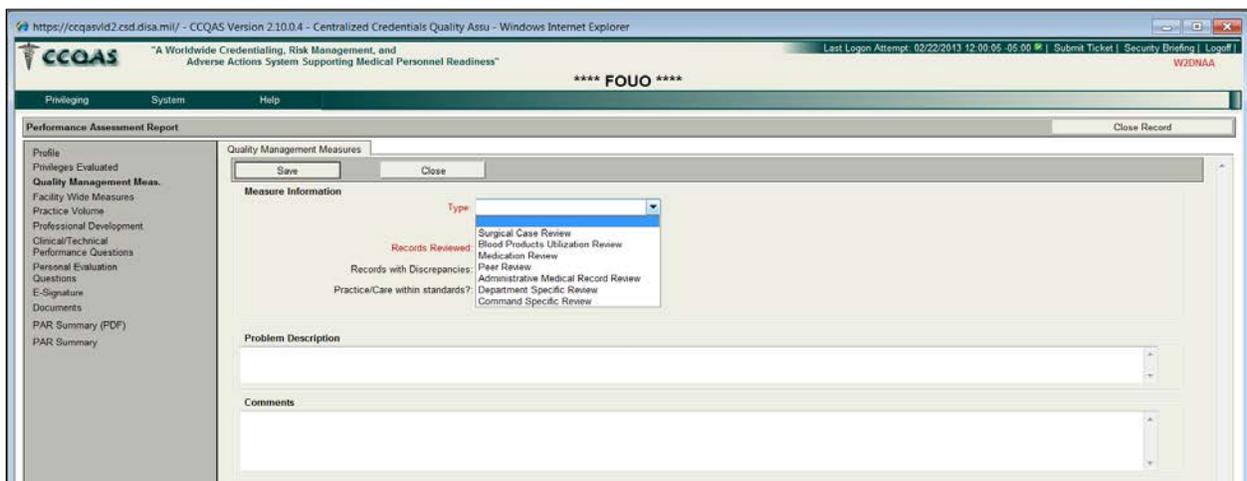
Figure 277: Privileges Evaluated Section for the PAR

The next section of the PAR form is the **Quality Management Measures** section, as depicted in Figure 278. When PAR Evaluators first open the PAR, this screen contains no data. To add a measure, click **Add**.



**Figure 278: Quality Management Measures Section of the PAR**

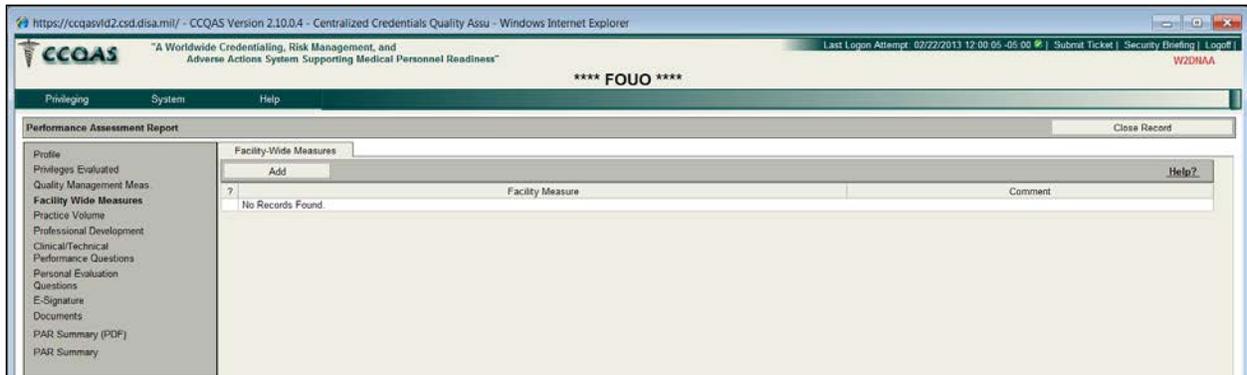
A screen appears with a pick list of different types of measures to select, as depicted in Figure 279. For each type of measure selected, different data fields are enabled to collect the appropriate information for the measure.



**Figure 279: 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 justify a Provider's performance, may be assessed and entered in the Quality Management Measures section of the PAR.

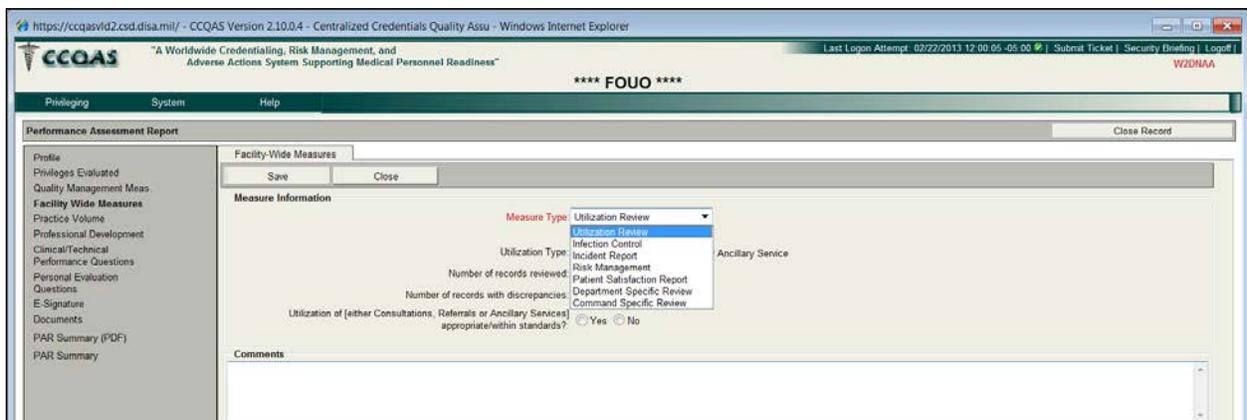
The next section of the PAR form is the **Facility Wide Measures** section, as depicted in Figure 280. The information entered into this section of the PAR depends on the measures being monitored over the period of evaluation or the standard measures used by the Service or facility for performing PARs. When PAR Evaluators first open the PAR, this screen contains no data. To add a measure, click **Add**.



**Figure 280: 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 281. 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 justify a Provider's performance, may be assessed and entered in the **Facility Wide Measures** section of the PAR. The next section of the PAR form is the **Practice Volume** section, as depicted in Figure 282. 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.



**Figure 281: Types of Facility-Wide Measures**

The screenshot shows the 'Practice Volume' section of the PAR form. It includes the following data entry fields:

- Procedures:**
  - Number of Diagnostic Procedures in Radiology:
  - Number of Operating Room Procedures:
  - Number of Invasive Ambulatory Procedures:
  - Number of Non-invasive Ambulatory Procedures:
  - Total Number of Procedures: 0
- Monthly Data:**
  - Average Monthly Admissions:
  - Average Monthly Outpatients Seen:
  - Average Monthly Emergency Room Patients Seen:
  - Percentage of Time in Direct Patient Care:  %
- Leave/Absence Data:**
  - TAD/TDY Days:
  - Leave Days:
  - Sick Days:
  - Other (e.g. Administrative Duties):
  - Total Number of Days Unavailable: 0

At the bottom, there is a 'Comments' text area and a 'Save' button.

**Figure 282: Practice Volume Section of the PAR**

The next section of the PAR is the **Professional Development** section, as depicted in Figure 283. 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**.

The screenshot shows the 'Professional Development' section of the PAR form. It includes the following data entry fields:

- Number of Credit Hours this Period of Evaluation:**

Category	Evaluation Period	Last 3 Years
Credit Category 1	0	20
Credit Category 2	0	0
Credit Category 3	0	0
Credit Category 4	0	0
Credit Category 5	0	0
- Summary Fields:**
  - Number of Papers published during this evaluation period:
  - Number of Professional Presentations during this evaluation period:
  - Number of other Recognitions of Professional Achievements:
- Course Details Table:**

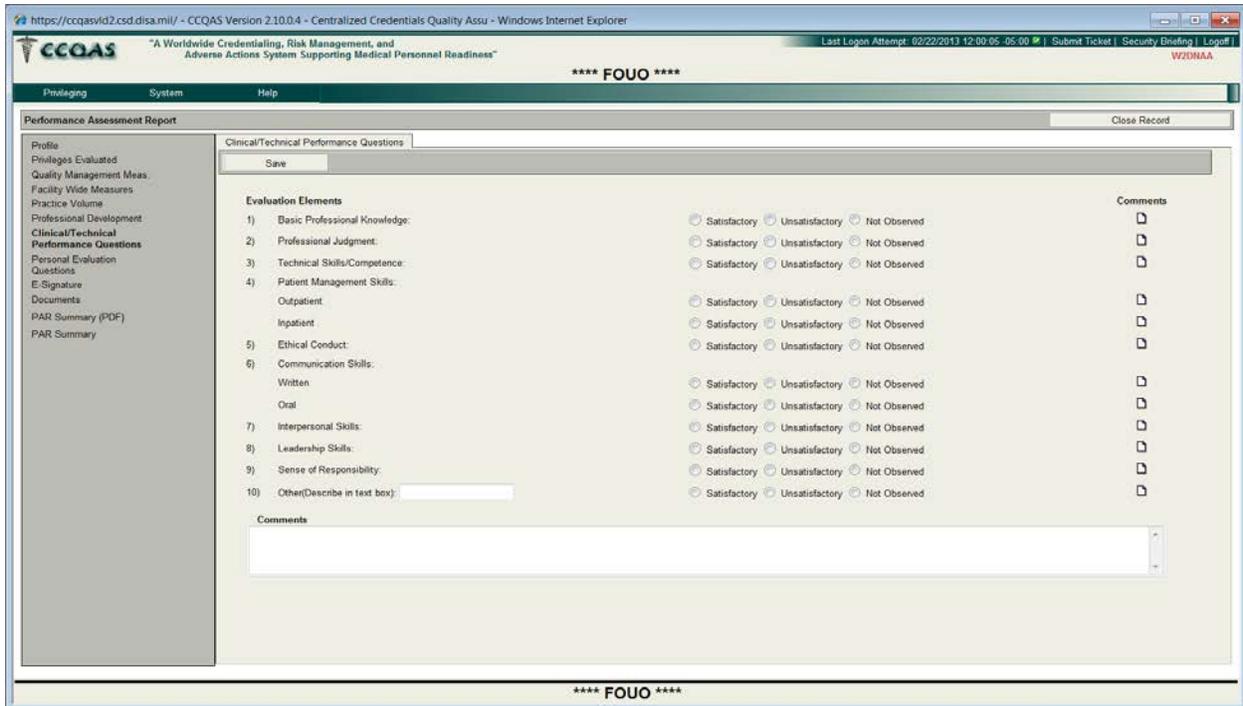
Credit Category	Course Title	Date	Location	Sponsor	Credit Hours
Credit Category 1	SPORTS	05/04/2012	HOUSTON	ROBERTS	10
Credit Category 1	WOMEN	01/30/2012	FT SAM HOUSTON	ANTHONY	10

At the bottom, there is a 'Comments' text area and a 'Save' button.

**Figure 283: Professional Development Section of the PAR**

The next section of the PAR form is the **Clinical/Technical Performance Questions** section, as depicted in Figure 284. 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 284: 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 285. 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**.

https://ccqasvld2.csd.disa.mil/ - CCQAS Version 2.10.0.4 - Centralized Credentials Quality Assu - Windows Internet Explorer

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Login Attempt: 02/22/2013 12:00:05 -05:00 Submit Ticket | Security Briefing | Logout | WZDNAA

\*\*\*\* FOUO \*\*\*\*

Privileging System Help

Performance Assessment Report Class 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

Personal Evaluation Questions

Save

To the best of your knowledge

Question	Yes	No	N/A	Comments
1) Is there any aspect of the provider's health that should be considered when granting privileges?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
2) Is the provider's attendance and participation in staff and committee meetings acceptable?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
3) Has this provider had privileges or staff appointment adversely denied, suspended, limited or revoked?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
4) Has this provider been the subject of an investigation?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
5) Has this provider had substandard care substantiated through one of the actions in (4) above?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
6) Has this provider required counseling, additional training, or special supervision related to clinical practice?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
7) Has this provider failed to obtain appropriate clinical consultation?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
8) Has this provider been the subject of disciplinary action?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
9) Has this provider been diagnosed with alcohol dependency or substance abuse or having an organic mental disorder or psychotic disorder?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
10) Has this provider required modification of practice due to health status?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>
11) Other: <input type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="text"/>

Comments

\*\*\*\* FOUO \*\*\*\*

**Figure 285: 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 286, which contains all information that was entered to date by the PAR Evaluator.

https://ccqasvld2.csd.disa.mil/ - CCOAS Version 2.10.0.4 - Centralized Credentials Quality Assu - Windows Internet Explorer

CCOAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Logon Attempt: 02/22/2013 12:00:05 -05:00 Submit Ticket | Security Briefing | Logout W2DNAA

\*\*\*\* FOUO \*\*\*\*

Privileging 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

**SECTION I - PROFILE**

<b>NAME (Last, First MI)</b>	<b>RANK/GRADE</b>	<b>NPI</b>
SMITH, ROB	LTC	N/A
<b>POSITION</b>	<b>SPECIALTY</b>	<b>DEPT-SERVICE</b>
Physician	Family Practice	Family Medicine

**REPORTING ACTIVITY/FACILITY**  
W2DNAA, BROOKS ARMY MED CTR

<b>PURPOSE OF EVALUATION</b>	<b>PERIOD OF EVALUATION</b>
Renewal of Staff Appointment/Privileges	10/30/2012 to 10/29/2014

**Comments**

**SECTION II - PRIVILEGES BEING EVALUATED**

Version 1.0

Scope

PRIVILEGE ITEM (S)	REQUESTED	APPROVED
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 settings in conformance with HIF policies. They may assess, stabilize, and determine disposition of patients with emergent conditions.	Fully Competent	Fully Competent

**Diagnosis and Management (D&M):**

PRIVILEGE ITEM (S)	REQUESTED	APPROVED
Cardiac stress test	Fully Competent	Fully Competent
EKG performance and interpretation	Fully Competent	Fully Competent
Obstetrical Care		

\*\*\*\* FOUO \*\*\*\*

Figure 286: PAR Summary Form

The same form may be generated as a read-only 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 287. PAR Evaluators then enter an overall assessment of the Provider's performance, add any supporting comments, selects their specialty from the Evaluator Specialty picklist and then click **Submit** to complete the **PAR** task.

My Applications Credentialing Privileging 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

**E-Signature**

**Evaluator Specialty**  
Specialty: Audiologist

**Evaluator Statement**  
I reviewed this provider's clinical performance data and credentials file and found them to be  Within  Not Within standards.  
This provider's performance data  Demonstrates  Does Not Demonstrate current competency.

**Comments:**

Figure 287: E-Signature Section of the PAR

A confirmation screen appears, as depicted in Figure 288. 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.

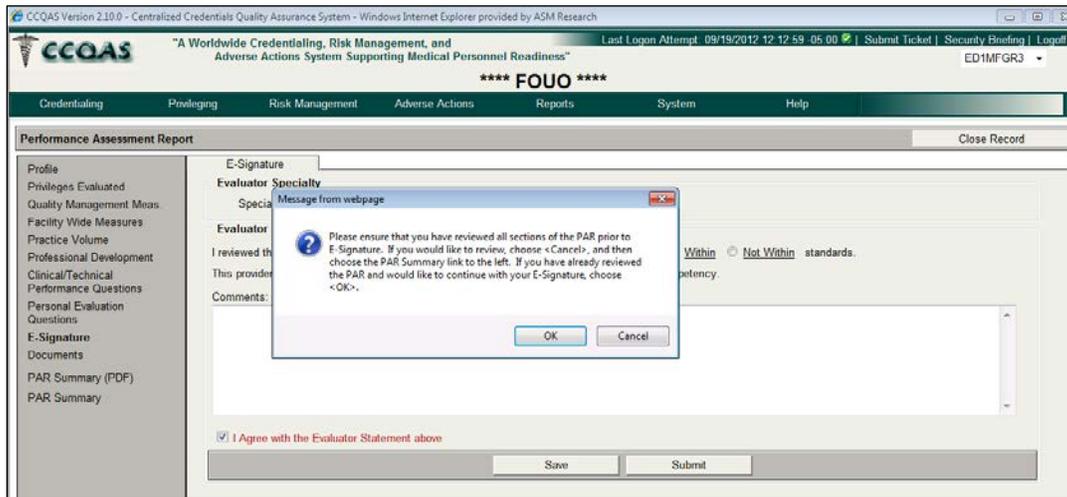


Figure 288: E-Signature Confirmation Screen

### 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 289.

**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.

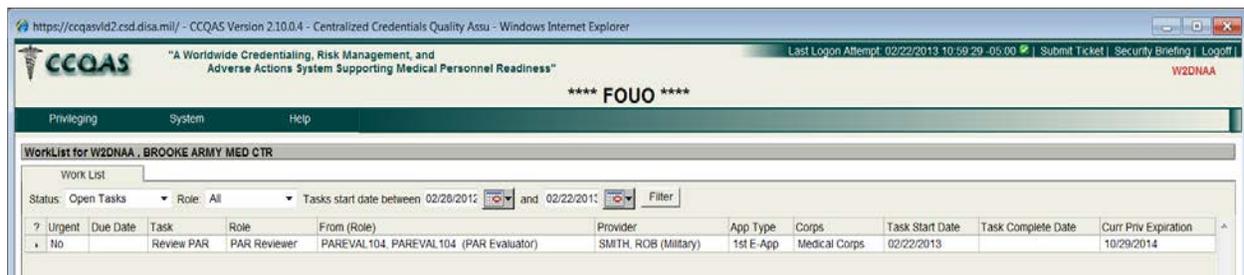
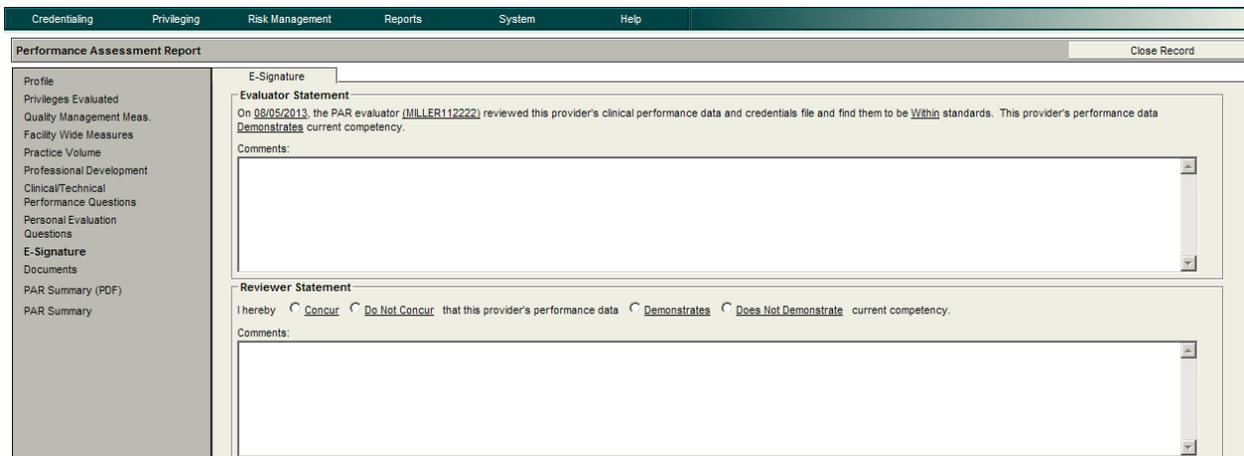


Figure 289: PAR Reviewer Work List Task – Review PAR

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 290.



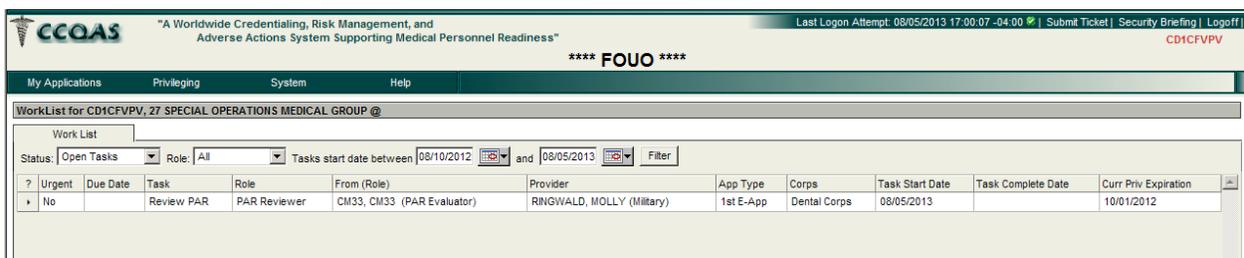
**Figure 290: PAR Reviewer E-Signature Screen**

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.

### 11.6 Reviewing the PAR-The Provider Role

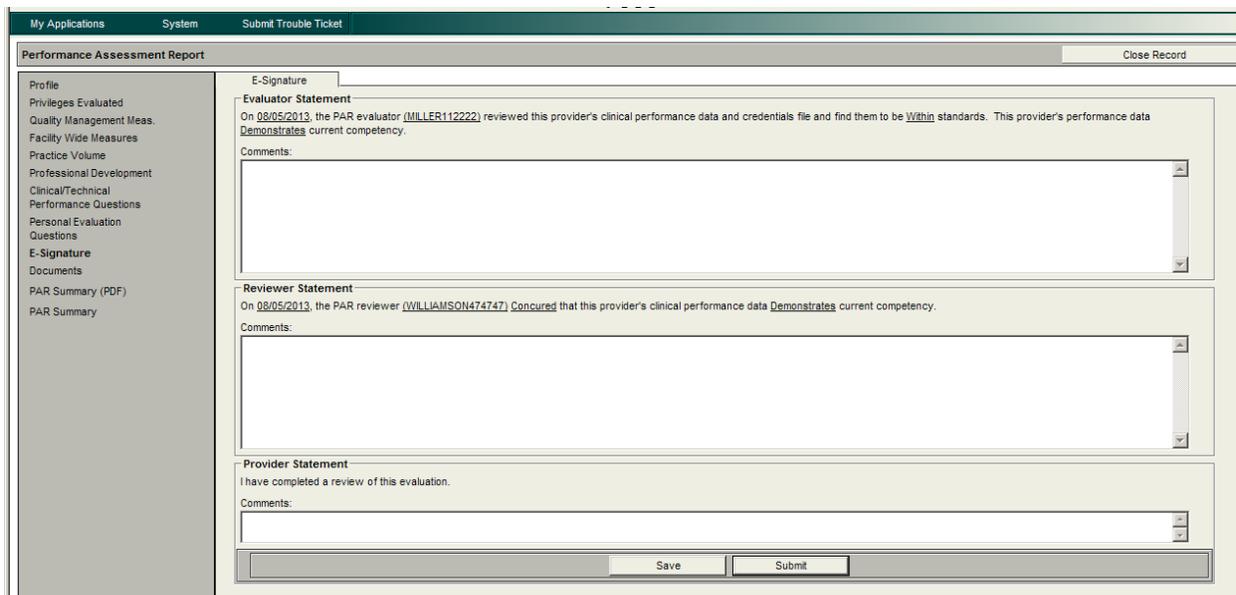
After PAR Evaluators submit a completed PAR, the Provider receives a new work list item with **Task = Review PAR**, as depicted in Figure 291.

**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 291: 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 292.



**Figure 292: Provider E-Signature Screen**

On the **E-Signature** screen, the overall evaluation and comments submitted 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.

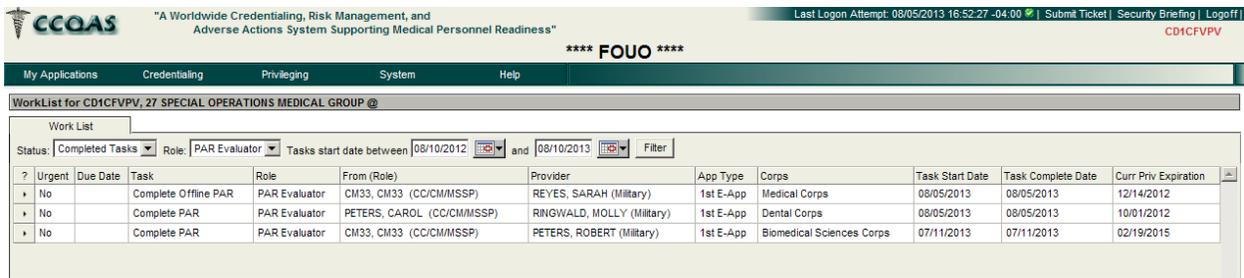
### 11.7 Bypassing the Automated PAR Process

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 293, and then click **Submit**.



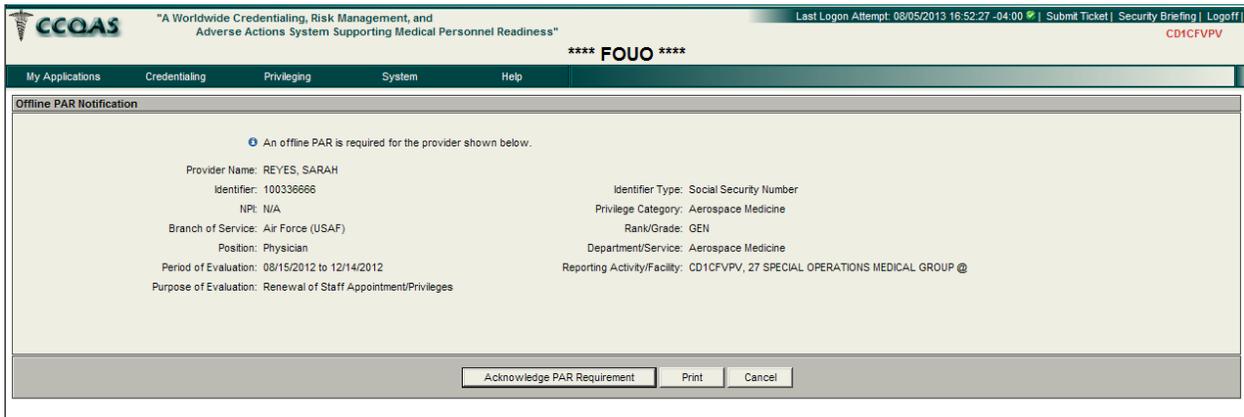
**Figure 293: ‘Offline PAR’ Radio Button**

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 294.



**Figure 294: 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 295. 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 295: Offline PAR Notification**

The offline PAR should be uploaded as a “Provider Document” as **Type = Clinical Performance Evaluation/Performance Assessment Reports**. Individuals who wish 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 296.



**Figure 296: ‘Cancel PAR’ Button**

This action closes the **Setup PAR** task in the CC/MSSP/CM's work list, 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](#))

### 11.9 Canceling or Reassigning a PAR In-Process

Occasions may arise when a PAR needs to be reassigned or canceled 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 cancel 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 cancel 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 297.

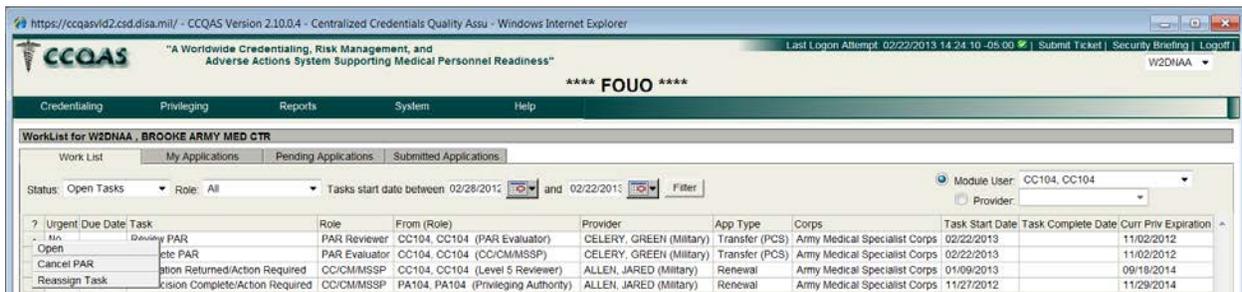


Figure 297: Complete PAR Task Menu Options

A warning message displays, asking CC/MSSP/CMs to confirm their intent to cancel the PAR, as depicted in Figure 298.

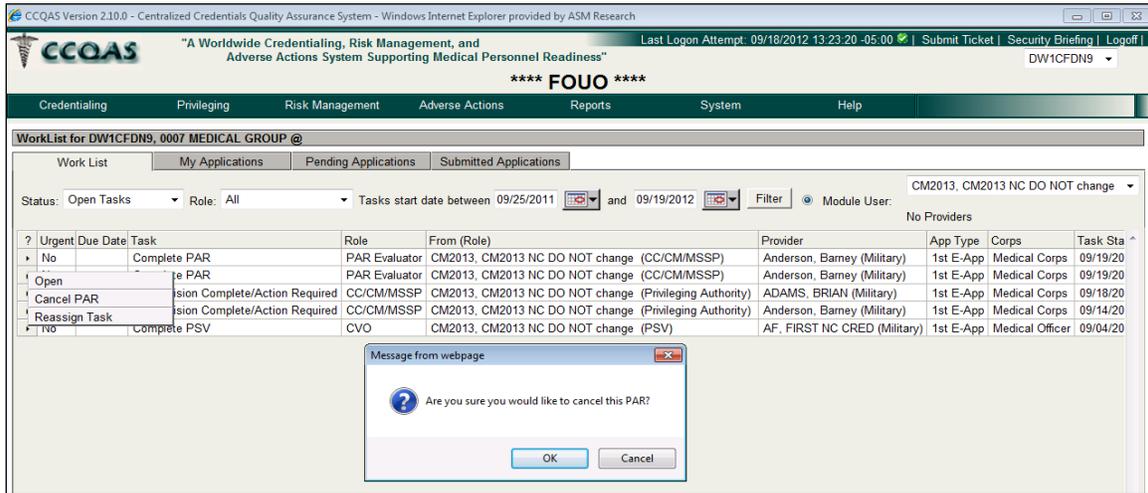


Figure 298: Cancel PAR Warning Message

When CC/MSSP/CMs click **OK**, the **PAR** task is canceled. 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 297 above. The **Re-assign Task** window opens, as depicted in Figure 299.

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.

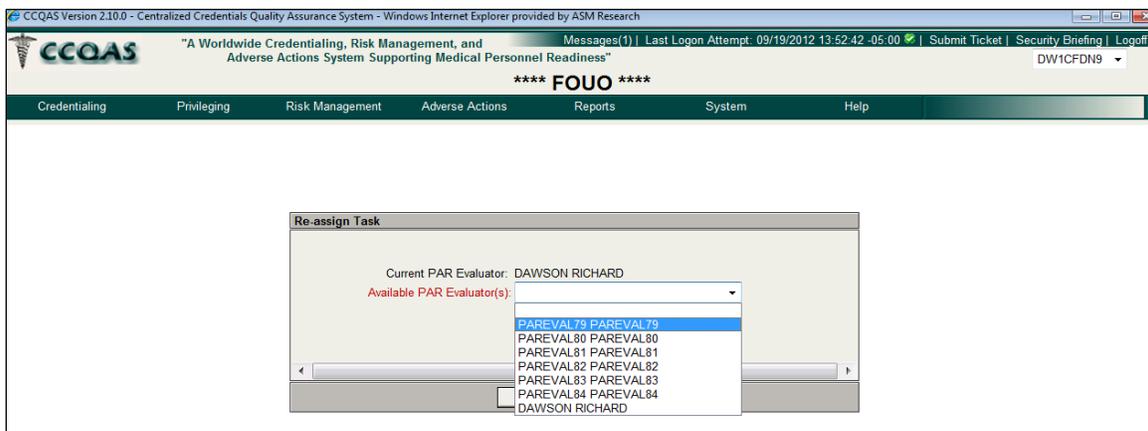


Figure 299: Re-assign Task Window

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 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.

### 12.1 Command Parameters and MTF Contact Information for Letter Generation

Proper use of the Letters functionality requires that the information in the provider's electronic credentials file and the **Command Parameters** and **MTF Contacts** screens in the CCQAS application be accurate and up-to-date (Refer to Section 15.2 for Command Parameters and Section 15.3 for MTF Contacts).

### 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

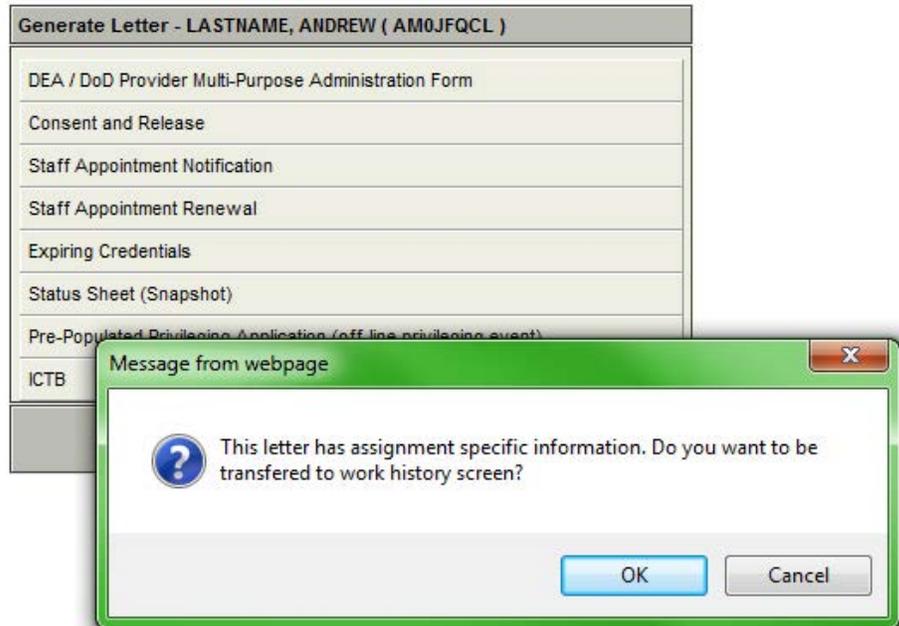
Users may access letters either from the Provider Search or Work History section. Letters may be generated for an individual Provider by searching for the Provider's record and selecting **Letters** from the Hidden Menu of Actions on the **Search Results** screen, as depicted in Figure 300.

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 is a navigation bar with tabs for "Credentialing", "Privileging", "Reports", "System", and "Help". The main content area displays a table of search results. The table has columns for Name, SSN, Primary UIC, Start Date, Branch, Corps, Status, Cred Status, NPI, and Active Assignments. The "Letters" menu item is highlighted in a red circle. Below the table, there is a "Record Count: 28" and buttons for "Search", "Clear Screen", and "Add Provider".

Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
10802, CRS	100-22-4444	CD1CFVPV	08/15/2012	F11	MC	MIL	Active		1
9518, SIR	100-66-5555	CD1CFVPV	08/17/2012			MIL	Active		1
100-76-6666	100-76-6666	CD1CFVPV	10/09/2012	F11	BSC	MIL	Active		1
100-80-8888	100-80-8888	CD1CFVPV	08/20/2012			MIL	Active		1
127-66-7777	127-66-7777	CD1CFVPV	11/27/2012	F11	MC	MIL	Active		1
100-99-5656	100-99-5656	CD1CFVPV	01/09/2013	F11	MC	MIL	Active		1
000-66-5555	000-66-5555	CD1CFVPV	11/29/2012	F11	MC	MIL	Active		1
DYLAN, BOB A	100-11-1111	CD1CFVPV	07/02/2012	F11	MC	MIL	Active		1
EVERDEEN, CATNISS	100-10-1111	CD1CFVPV	03/27/2013	F11	MC	MIL	Active		1
JONES, TAMMY A	100-85-8585	CD1CFVPV	02/25/2013			CIV	Active		1
KENT, TRACY	700-11-9999	N00060	08/16/2012			Dual	Active		2
KENT, TRACY L	123-00-9999	CD1CFVPV	10/09/2012	F11	DC	MIL	Active		1
KIMMEL, JOHN	100-66-5454	CD1CFVPV	01/17/2013			MIL	Active		1
LENNON_1, JOHN	100-99-2222	CD1CFVPV	07/18/2012			CIV	Active		1
MILLER, KELLIE	100-11-2222	CD1CFVPV	07/02/2012			MIL	Active		1
NOPRIVS, JOEY	100-22-5555	CD1CFVPV	08/16/2012	F11	NC	Dual	Active		2
O'SHEA, PATTY	800-99-7777	CD1CFVPV	01/17/2013			MIL	Active		1

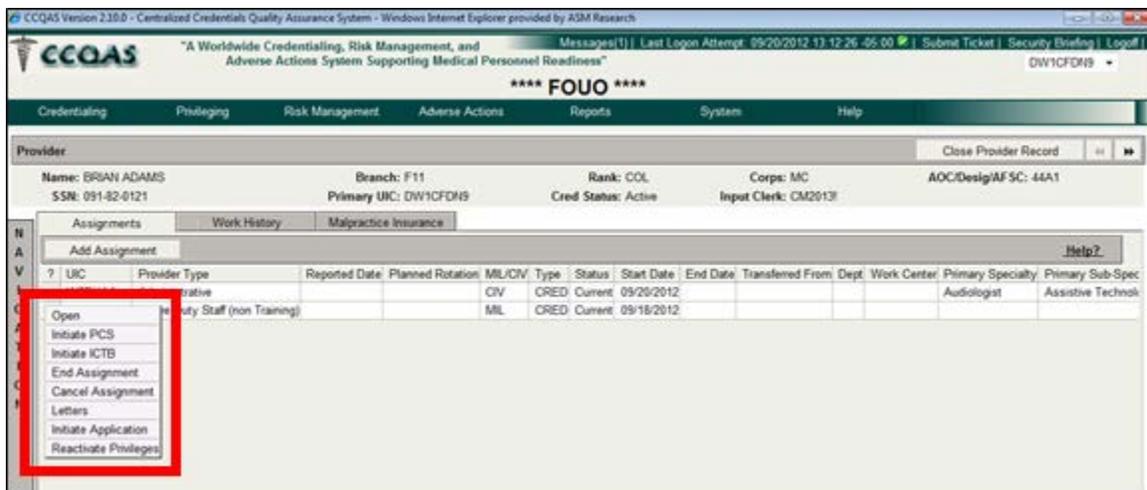
Figure 300: Letters Menu Item, Provider Search

Letters containing assignment-specific information, automatically transfer the user to the Work History section where the Letter can be generated from the specific Assignment. Figure 98 depicts the message displayed when the **Pre-Populated Privileging Application** letter is selected from the Search Results screen. Click **OK** to open the **Work History** screen.



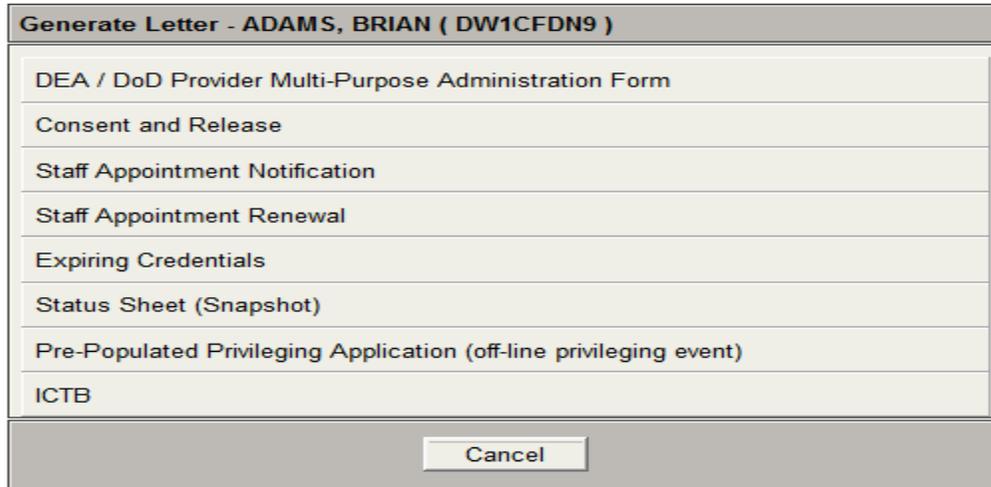
**Figure 301: Pre-Populated Privileging Application Letter Transfer Message**

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. Figure 302 depicts the **Work History, Assignments tab Letters** menu option.



**Figure 302: Letters Menu item, Work History, Assignments Tab**

Once selected, users then view the complete list of letters, as depicted in Figure 303.

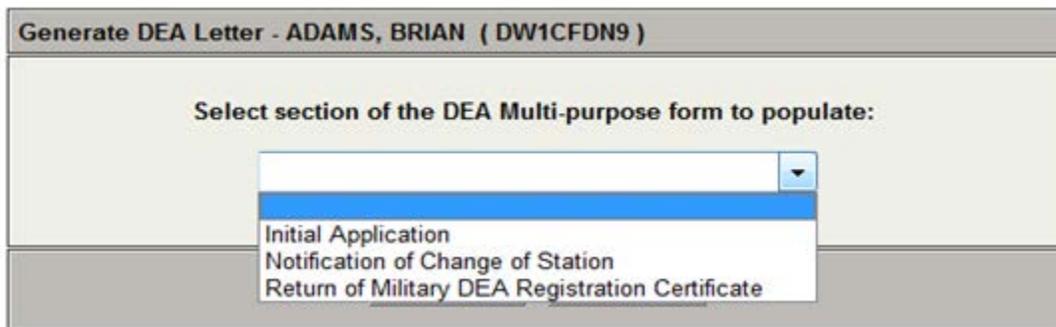


**Figure 303: Generate Letter Menu**

Users may run the desired letter by clicking the letter name. Most letters are automatically generated after they are selected and pre-populated with data from the Provider’s current credentials record.

#### **12.2.1.1 DEA/DoD - Initial Application Letter**

The DEA/ DoD Multi-purpose Administration Form is comprised of 3 sections, as depicted in Figure 304 below. Select the **Initial Application** letter from the drop-down menu.



**Figure 304: DEA Multi-Purpose Letters**

The **DEA License Selection** screen appears, as depicted in Figure 305. Select the radio button next to the appropriate license, and then click **Submit**.

	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

**Figure 305: DEA Initial Application Form License Selection**

The **Initial Application Letter** is generated, as depicted in Figure 306. Notice that the top section of the letter is pre-populated with provider, MTF and contact information.

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: ANDREW LASTNAME Rank/Series: \_\_\_\_\_  
Unit/Facility: 0097 MEDICAL GROUP  
Unit Address: 97 MDG/SGHQ 301 NORTH FIRST STREET ALTUS AFB OK 73523-contacts  
Social Security Number: XXX-XX-6666  
Medical/Dental License Number: 43253245 State of: KY Expiration Date: 04/16/2014

Applicant Signature: \_\_\_\_\_  
Date: \_\_\_\_\_

Credentiaing Authority Signature: \_\_\_\_\_ Date: \_\_\_\_\_  
Name: Mrs. Cred Coordinator (SGHQ)  
Title: Credentiaing Authority  
Address: \_\_\_\_\_  
123command  
Phone Number (Commercial): (703) 555-4321

**Figure 306: Initial Application Letter**

### 12.2.1.2 DEA/DoD - Notification Change of Station Letter

Select the **Notification of Change of Station** letter from the **Generate DEA Letter** drop-down menu (refer to Figure 304), and then select the radio button next to the appropriate DEA information, as depicted in Figure 307.

Generate DEA Letter - LASTNAME, ANDREW ( AM0JFQCL )

Select section of the DEA Multi-purpose form to populate:

Notification of Change of Station

To Command: AY0DFBV3

	DEA Number	DEA Type	Expiration Date
<input checked="" type="radio"/>	45456	DEA (Fee Exempt)	12/31/2014

Submit Cancel

Figure 307: Notification of Change of Station

The **Notification of Change of Station** is generated, as depicted in Figure 306. Notice that the middle section of the letter is now pre-populated with provider, MTF and contact information.

(X)Notification of Change of Station **(Upon Military Transfer/Relocation Only)**

Name of Registrant: ANDREW LASTNAME

DEA Number of Registrant: 45456

Old Unit/Facility: 0097 MEDICAL GROUP 97 MDG/SGHQ  
301 NORTH FIRST STREET ALTUS AFB OK, 73523-contacts

New Unit/Facility: 0031 MEDICAL GROUP 31 MDG / SGH  
UNIT 6180 BOX 245 (APO) AVIANO AB AE, 09604-0245

Registrant Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Credentialing Authority Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name: Mrs. Cred Coordinator (SGHQ)

Phone Number (Commercial): (703) 555-4321

Figure 308: Notification of Change of Station Letter

### 12.2.1.3 DEA/DoD - Return of Military DEA Registration Certificate Letter

Select the **Return of Military DEA Registration Certificate** letter from the **Generate DEA Letter** drop-down menu (refer to Figure 304). Users then select the radio button for the appropriate DEA information, depicted in Figure 104, and then click **Submit**.

Generate DEA Letter - LASTNAME, ANDREW ( AM0JFQCL )			
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"/>	45456	DEA (Fee Exempt)	12/31/2014
Submit		Cancel	

Figure 309: Return of Military DEA Registration Certificate

The **Return of Military DEA Registration Certificate** is generated, as depicted in Figure 306. Notice that the bottom section of the letter is pre-populated with provider and contact information.

-----

---

(X) Surrender of DEA Registration Certificate **(Upon Separation from Military Service Only)**

I surrender my DEA certificate of registration. Certificate of registration is attached.

Name of Registrant: ANDREW LASTNAME

DEA Number of Registrant: 45456

Registrant Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Credentialing Authority Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name: Mrs. Cred Coordinator (SGHQ)

Phone Number (Commercial): (703) 555-4321

Figure 310: Return of Military DEA Registration Certificate Letter

#### 12.2.1.4 Generate Expiring Credentials Letter

When users select the **Expiring Credentials** letter from the Letters menu (refer to Figure 105 above), the **Generate Expiring Credentials Letter** screen appears, as depicted in Figure 106. Users select the appropriate items for the letter, and then click **Submit** to generate the pre-populated letter.

Generate Expiring Credentials Letter - EVERDEEN, CATNISS ( CD1CFVPV )							
Credentials that have or will expire within next <input type="text" value="90"/> days. <input type="button" value="Filter"/>							
<input checked="" type="checkbox"/> State License/Certification/Registration							
<input type="checkbox"/>	Type	State	Number	Field	Status	Expires	ADM Waiver
<input checked="" type="checkbox"/>	License	OR	12365	Podiatrists	Active	09/01/2013	No
<input checked="" type="checkbox"/> National Certification/Registration							
<input type="checkbox"/>	Type	Number	Field	Status	Expires		
<input checked="" type="checkbox"/>	Certification	123	Podiatrists	Active	09/01/2013		
<input checked="" type="checkbox"/> Specialty Board Certification							
<input type="checkbox"/>	Specialty/Subspecialty			Agency Board		Expires	
<input checked="" type="checkbox"/>	Surgery/Plastic & Reconstructive Surgery			American Board of Podiatric Surgery		09/01/2013	
<input checked="" type="checkbox"/> Contingency Training							
<input type="checkbox"/>	Type					Expires	
<input checked="" type="checkbox"/>	ATLS-Advanced Trauma Life Support					09/02/2013	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>							

Figure 311: Expired Credentials Letters Selections

### 12.2.1.5 Pre-Populated Privileging Application Letter

When users select a specific assignment and **Pre-Populated Privileging Application** letter, a list of Privilege Categories display for Allied Health providers, as depicted in Figure 312. To reset the Privilege Category list, select the desired Provider Category and click the **Filter** button. Next, select the appropriate Privilege Category(ies) and click **Submit** to generate the Pre-Populated Privileging Application.

**Figure 312: Pre-Populated Privileging Letter with Privilege 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 As** or **Save Electronic Copy** 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.

#### 12.2.1.6 ICTB Letter

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 ICTB letter. Refer to Section 8 for additional information on the ICTB Process.

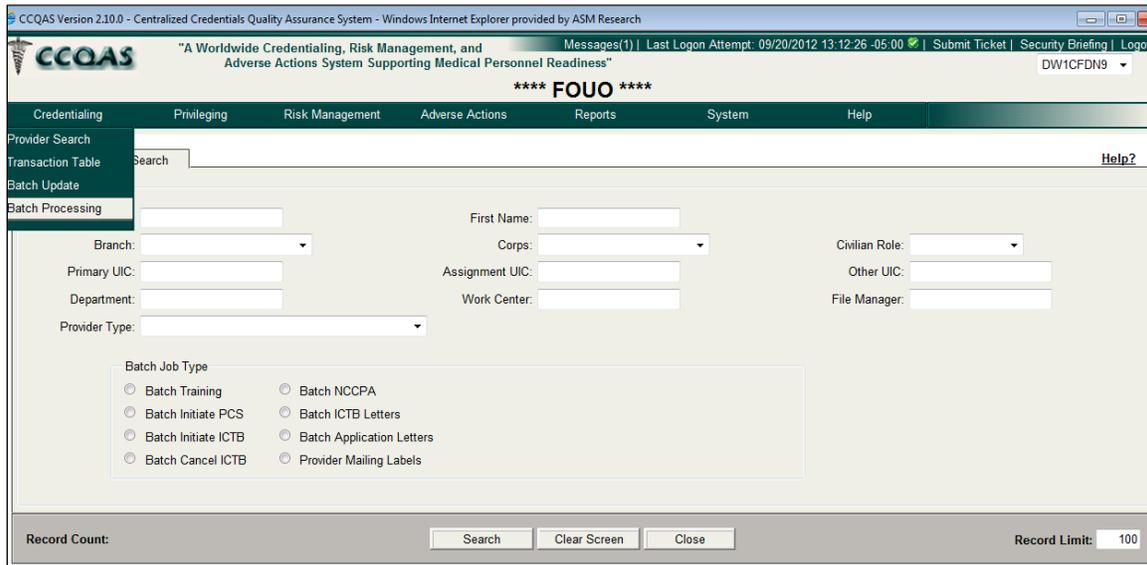
### 12.3 Generating Batch Letters

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 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 313 below. Provider records may be batch-processed by selecting the appropriate batch action in the **Action** section of the screen.

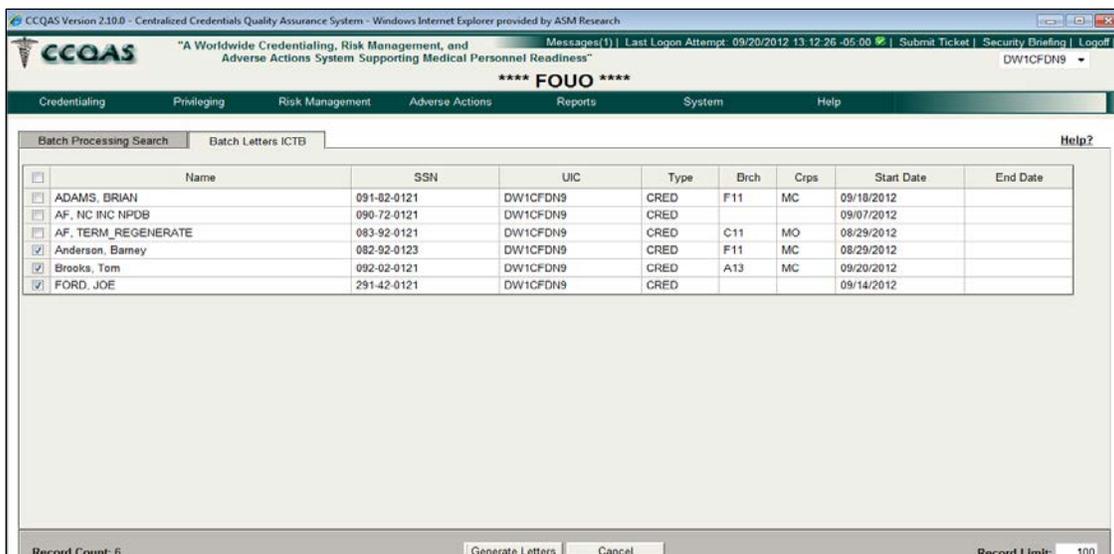
Additional search criteria may be entered in the upper portion of the **Credentials Provider Search** screen if users wish to limit the batch action to only certain groups of records (e.g., only Providers in a specific **Department, Work Center, Corps, or UIC**). After users enter all appropriate search criteria and select the desired batch action, they click **Search**.

Additional details on how to use Batch Processing can be found in [Section 6.4](#) of this guide.



**Figure 313: Action Section of the Credentials Provider Search Screen**

A list of Providers who meet the search criteria specified is displayed, as depicted in Figure 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 **Generate Letters** at the bottom of the screen.



**Figure 314: Batch ICTB Letter Screen**

On the next screen, depicted in Figure 315 below, users are prompted to enter information regarding the ICTB location and dates, and additional text for the ICTB letter.

**Figure 315: 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 316 below. The letters may then be printed directly from the CCQAS application or saved.

Type	Degree/Field of Study	Institution	Attended To	Completed	Date of PSV
Qualifying Degree	MD	Uniformed Services University of Health Sciences	Y	Y	09/18/2012
Internship (PGY-1)	1343	3 MDG	Y	Y	09/18/2012

**Figure 316: ICTB Batch Letter**

## 13 Generating Standard Credentials and Privileging Reports

A number of standard credentialing and privileging reports are available from CCQAS. Access to these reports is based on Roles/Permissions. 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 317 below. Users then select **Standard and Credentialing**.



Figure 317: Accessing the CCQAS Standard Credentialing Reports

A list of standard reports is displayed, as depicted in Figure 318 below. Users may run a selected report by clicking the report name.

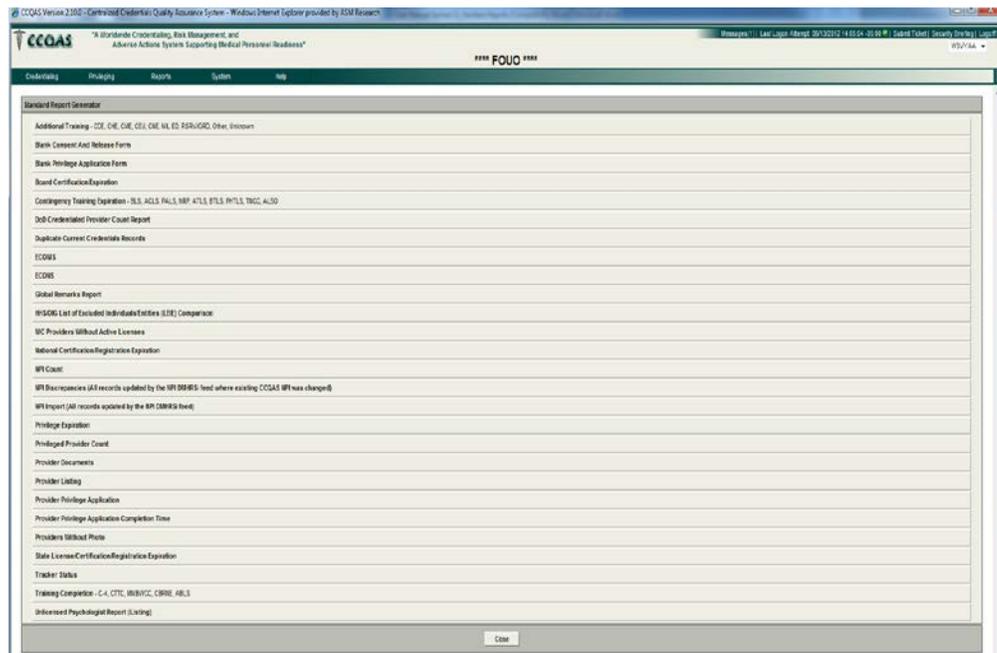
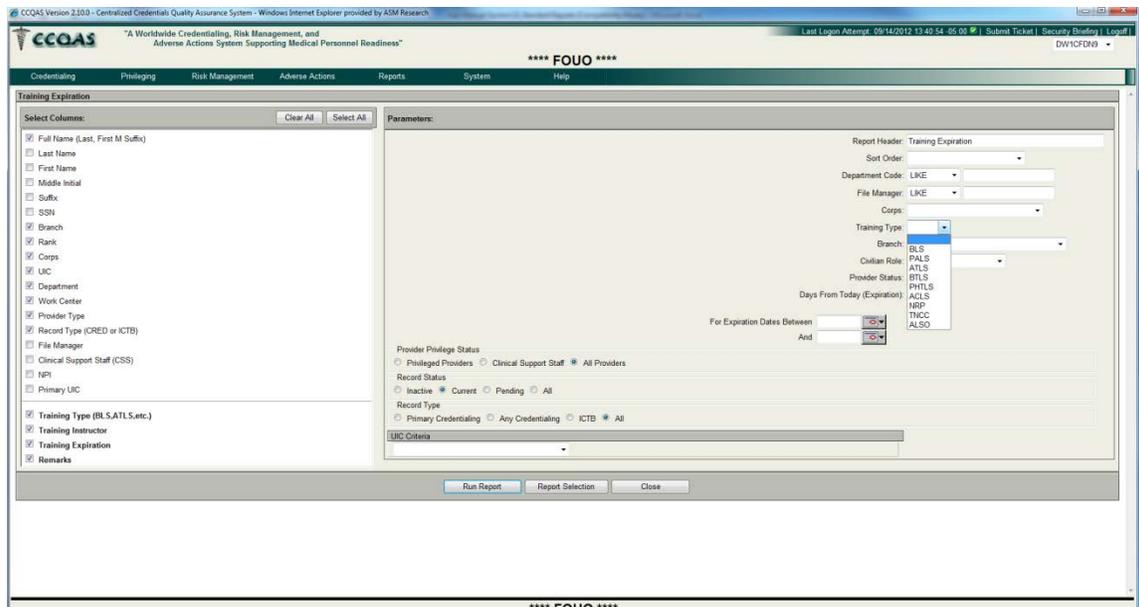


Figure 318: List of Standard Credentials Reports

The **Contingency Training Expiration** report is depicted in Figure 319 as an example.



**Figure 319: Parameter Screen for the Contingency 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 display in their report by selecting or deselecting 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 the Provider’s name if another sort option is not selected. (**Note:** If users select **Rank** for the sort order, the report is sorted alphabetically by 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 text “ped” included in their **Department Code** field, such as “pediatric clinic” or “pediatrics” would be queried to generate the report. This filter is not case sensitive.

- 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  
**NOTE:** the filters “Like” and “Not Like” act as wildcards to the “**ped**” and “**Smi**” samples above
- **Provider Privilege Status**
  - Privileged Providers – filter includes all privileged and unprivileged providers, where the Clinical Support Staff checkbox is NOT checked for the Assignment.
  - Clinical Support Staff – filter includes all providers who have the Clinical Support Staff checkbox checked for the Assignment.
  - All Providers – filter includes all providers
- A **Record Status** indicator that enables only Inactive, Current, Pending, or All assignment types to be included in the report query
- A **Record Type** indicator that enables only Primary Credentials Status, Any Credentials (CRED only) assignment, ICTB assignment, or All record types to be included in the report query  
**NOTE:** Selection of **All Record Types** may result in an individual Provider being listed multiple times, if they have multiple assignments.
- **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.  
**NOTE:** CC/MSSP/CMs with access to multiple UICs must have report Role/Permissions at each UIC in order to be able to create reports for that UIC.
- **Expiration Dates** filter that allows users to enter applicable date ranges that should be used to generate the report

For the **Contingency 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 do not select a **Training Type** value, then all training types are included in the report. If Training Type=BLS is selected, in addition to training for specified expiration dates, records missing BLS training will also be 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:

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Additional Training	Date range; Record Status; Record Type, SSN (if Single Provider is selected)	<p>UIC Criteria</p> <p>If “Date Range” (default) is selected the “For Completion Dates Between:” then a date range is required.</p> <p>If “All Dates” is selected the “For Completion Dates Between:” is disabled.</p> <p>If multiple training CE’s are selected as columns for the report, all Providers that meet any one of the completion date criteria are included on the report, unless Single Provider is selected.</p>	<p>Lists Providers who have CDE, CHE, CME CEU, CNE, MIL ED, PSRV/GRD Other or Unknown - training completion dates between the date range specified.</p> <p><b>NOTE:</b> This report is not available for export to Word or Excel.</p>
Blank Consent and Release Form		None	Consent and Release Provider liability empty statement.
Blank Privilege Application Form	Provider Category, Privilege Category	<p>Duty Section, Duty Phone, Assignment Date, Station Date (data entered into these fields will not appear on the Form)</p> <p>NOTE: CC/MSSP/CM must select a Provider Category and click the Filter button to see available MPLs.</p>	A blank Privilege Application Form based on selected Privilege Categories.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Board Certification /Expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps; Branch, Civ Role, Provider Status UIC Criteria	Lists Providers who's ABMS, AOA, ADA or other 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 <b>Specialties</b> tab of the electronic credentials record.
Contingency Training Expiration	Expiration Date range; Record Status; Record Type	Department Code; File Manager; Corps; Training Type; Branch: Civilian Role; Provider Status; Days from Today (Expiration); 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.  <b>NOTE:</b> If Training Type BLS is selected, Providers without BLS training will also be listed on the report.
DoD Credentialed Provider Count	Group By, Contractors Only, Include	UIC , Provider Status	Lists a count of all Providers by selected Group By with additional filters available.  <b>NOTE:</b> Count Report available at Service level and DoD level only.
Duplicate Current Credentials	Search Criteria	None	Lists Providers who have more than one current CRED assignment.
ECOMS		Region, Provider Status	Lists the Providers with the specified Provider Status and the person with whom their file currently resides. The report enables users to submit comments and recommendations for each Provider included in the report. This report queries on CRED assignments only (not ICTB assignments) and looks at only the most recent status entered for the Provider.  <b>NOTE:</b> The ECOMS report lists Providers who are not Clinical Support Staff.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
ECONS		Region, Provider Status	<p>Lists the Providers with the specified Provider Status and the person with whom their file currently resides. The report enables users to submit comments and recommendations for each Provider included in the report. This report queries on CRED assignments only (not ICTB assignments) and looks at only the most recent status entered for the Provider.</p> <p><b>NOTE:</b> The ECONS report lists Clinical Report Staff.</p>
Global Remarks Report	Provider Remark; Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; 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 range.
U.S. Department of Health and Human Services/Office of Inspector General (HHS/OIG) List of Excluded Individuals/Entities (LEIE) Comparison	This report is generated automatically upon selection; no query criteria are entered by users.	None	<p>This report provides a listing of all Department of Defense (DoD) Providers assigned to, or working at the user's facility, who have been DHHS-sanctioned (TRICARE-sanctioned).</p> <p><b>NOTE:</b> Provider's returned via this report warrant further review.</p>
MC Providers Without Active Licenses	Record Status; Record Type;	UIC Criteria	Lists all Medical Corps Providers who do not have at least one active state license.
National Certification/Registration/Expiration	Expiration Date range; Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps, Branch, Civilian Role, Provider Status, UIC Criteria	<p>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. This report is generated from data entered on the National tab of the <b>Licenses/Certifications/Registration</b> section of the electronic credentials record.</p>

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
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.
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 Credentials Records that have had their NPI changed by DMHRSi.
NPI Import	NPI Import Date Range; Provider Privilege Status; Record Status; Record Type	Department code; File Manager; Corps; Branch; Civilian Role; Provider Status; UIC Criteria	Lists Records updated by the NPI DMHRSi feed.
Privilege Expiration	Expiration Date range; Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; 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 counts of Providers by UIC, command, and location for the specified Record Type and Record Status: <ul style="list-style-type: none"> <li>• All Providers</li> <li>• CSS Providers</li> <li>• Non-CSS Providers</li> <li>• Privileged Providers</li> </ul>
Provider Documents	Upload Date Range; Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; Document Type; UIC Criteria;	The report displays a list of Provider documents uploaded within the specified date range.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Provider Listing	Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; UIC Criteria	Lists all Providers who are assigned to the user's UIC.
Provider Privilege Application	Created Date Range; Completed Date Range	Provider Last Name; Application Status: Assigned CC/CM/MSSP; UIC Criteria	<p>Lists all Providers with E-Applications who currently have, or have had, an assignment in a facility. Report includes:</p> <ul style="list-style-type: none"> <li>• Total Number of Applications</li> <li>• Number of Completed Applications</li> <li>• Average Days to Complete</li> </ul> <p><b>NOTE:</b> If Application Status is not specified, Offline Privileges will be included.</p>
Provider Privilege Application Completion Time Report	PA Decision Created Date Range	Provider Last Name; Provider First Name; Application Status; Corps; Branch; Civilian Role; Provider Status; Assigned CC/CM/MSSP; UIC Criteria	<p>Lists all Providers with E-Applications who have an assignment in a facility with completion times. Report includes:</p> <ul style="list-style-type: none"> <li>• Total Number of Applications</li> <li>• Number of Completed Applications</li> <li>• Average Days to Complete</li> </ul> <p><b>NOTE:</b> If Application Status is not specified, Offline Privileges will be included.</p>
Providers Without Photo	Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; UIC Criteria	Lists Providers who do not have a photo loaded into the <b>Profile</b> section.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
State License/ Certification/ Registration Expiration	Provider Privilege Status; Expiration Date Range; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; Field of Licensure; Days From Today (Expiration); UIC Criteria	Lists Providers whose state license, certification, or registration expires within the specified date range. If a Provider holds multiple State Lic/Cert/Regs that meet the expiration date criteria, each State Lic/Cert/Reg is reported as a separate row on the report. This report is generated from data entered in the <b>State</b> section of the <b>Licenses/Certifications/Registration</b> tab of the electronic credentials record.
Tracker Status	Provider Privilege Status; Record Status; Record Type; Privilege Expiration Date Range (if Privilege Expiration Date is checked under Selected Columns)	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; Most Recent Tracker Status; Tracker Status; Tracker Status Date Range; UIC Criteria	Lists specified Providers and their relevant tracker status.  <b>NOTE:</b> This report is not available for export to Word or Excel.
Training Completion	Completion Date Range; Provider Privilege Status; Record Status; Record Type	Department Code; File Manager; Corps; Branch; Civilian Role; Provider Status; UIC Criteria	Lists Providers who have training completion dates within the date range specified.

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
Unlicensed Psychologist Report	Record Type	UIC Criteria	Lists Providers with a Specialty of Psychologist, who do not have an active, unexpired Psychologist State License.

**Table 4: Descriptions of CCQAS Standard Credentialing Reports**

**Example:** Robert runs the **Training Expiration Report** to determine which Air Force Active Duty 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 August 2, 2013. Robert's **Contingency Training Expiration** report Parameter screen would look like the one depicted in Figure 320.

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.

**Figure 320: Example of Contingency 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 321.

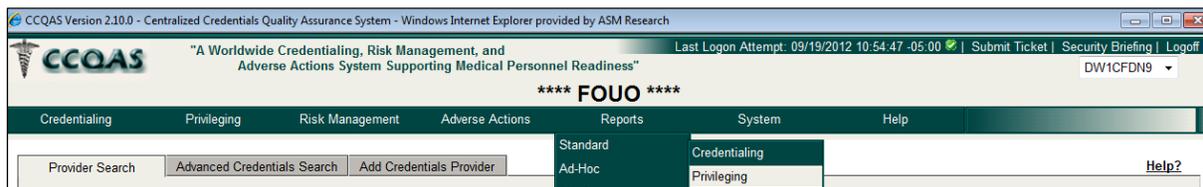


**Figure 321: Reporting Options**

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 322.



**Figure 322: Accessing the CCQAS Standard Privileging Reports**

A list of standard reports display, as depicted in Figure 323. Users may run a report by clicking the report name.



**Figure 323: List of Standard Privileging Reports**

The available reports are listed in Table 5 below:

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. Report includes: <ul style="list-style-type: none"> <li>• Concept Code</li> <li>• Creation Date</li> <li>• Last Update Date</li> </ul>
Provider Privilege	Provider	Privilege Category; Privilege Code Description; Effective Date	This report displays a list of a Provider's privileging actions. Clicking on an entry displays the privilege list that corresponds to the selecting privileging action. <b>NOTE:</b> The Privilege Code Description includes a Privilege

Standard Report Title	Required Query Parameters	Optional Query Parameters	Description of Report
		Range; Privilege Expiration Date Range	Lookup button.
Privilege Finder	Privilege Description or Privilege Lookup	Provider Types; Delineation	This report lists Providers with selected Privilege(s) for the selected Provider Type(s).

**Table 5: Descriptions of CCQAS Standard Privileging Reports**

Example of the Provider Privilege Report:

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Last Login Attempt: 08/02/2013 08:44:52 -04:00 | Submit Ticket | Security Briefing | Log Out [CD1CFVPV]

\*\*\*\* FOUO \*\*\*\*

Credentialing Privileging Risk Management Reports System Help

Privilege Management - Privilege Provider Information Report

Provider: DELEON, KATIE

Privilege Category: Select a Privilege Category

Privilege Code Description:  Privilege Lookup

Effective Date Between:  And

Privilege Expiration Date Between:  And

Search Close

?	Provider	Civ/Mil	Branch	Corps	Type	Status	Effective Date	Privilege Expiration Date
+	DELEON, KATE	ML	Air Force (USAF)	Medical Corps	1st E-App	Closed	12/13/2012	12/12/2014

**Figure 324: Provider Privilege report Parameters Screen**

\*\*\*\* FOUO \*\*\*\*

Name: PETERS, ROBERT, Appointment: Affiliate Priv. Granted Date: 13 Dec 12  
 Mil/Civ: Military Corps: BSC Privileges: Regular Priv. Expiration Date: 12 Feb 13

PRIVILEGED PROVIDER INFORMATION REPORT

<b>SERVICE: Air Force</b>			
<b>UIC: CD1CFVPV MTF: 27 SPECIAL OPERATIONS MEDICAL GROUP @</b>			
<b>PROVIDER</b>		<b>SSN</b>	<b>MILITARY/CIVILIAN</b>
PETERS, ROBERT		XXX-XX-1111	Military
<b>ORGANIZATION UNIT</b>		<b>MILITARY/CIVILIAN ADMITTING</b>	<b>TYPE OF PRIVILEGES</b>
27 SPECIAL OPERATIONS MEDICAL GROUP @		Military	No Regular
<b>PRIVILEGE CATEGORY: Dietitian</b>			
Version 1.0			
<b>Scope</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
The scope of privileges for dietitians includes the nutritional assessment, evaluation, diagnosis, education, counseling and collaborative treatment of patients of all ages with a variety of nutritional needs. Dietitians provide a range of individual, family, unit, and community services and programs in multiple settings including outpatient, inpatient and the community. Dietitians participate in transitions of care and refer patients to other healthcare providers, community agencies, and programs.	Fully Competent	Not Supported	
<b>Diagnosis and Management (D&amp;M):</b>			
<b>Nutrition Assessment / Monitoring / Evaluation:</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
Assessment for food allergy/intolerance or alternate dietary plan	Fully Competent	Not Supported	
Prevent and mitigate disease to include but not limited to: drug-nutrient and diet-drug interactions, substance abuse and feeding problems	Fully Competent	Not Supported	
Order laboratory tests: albumin/prealbumin, blood glucose, HgA1C, lipid profile, 24-hour UUN, thyroid function, fasting insulin, vitamin/mineral levels, iron studies, fecal fat/fecal elastase, liver function, albumin/creatinine, fructosamine, CRP, PTH	Fully Competent	Not Supported	
Order swallow study	Fully Competent	Not Supported	
<b>Nutrition Intervention:</b>			
<b>PRIVILEGE ITEM (S)</b>	<b>REQUESTED</b>	<b>APPROVED</b>	
Develop feeding regimens for nutritional support of trauma, critical care, burn, transplantation and bariatric and other major surgeries, to include fluid and electrolyte requirements	Fully Competent	Not Supported	
Develop nutritional care plans and dietetic support for psychiatric eating disorders, e.g. anorexia, bulimia	Fully Competent	Not Supported	
Recommend nutritional care plans for advanced nutrition intervention for conditions in the pediatric patient to include malabsorption, endocrine abnormalities, failure to thrive, congenital abnormalities, or inborn errors of metabolism	Fully Competent	Not Supported	
Develop nutritional care plans for the oncology and hematology patient to include drug-nutrient interaction	Fully Competent	Not Supported	
Order and/or maintain enteral feeding devices in accordance with MTF policies	Fully Competent	Not Supported	

This document is protected by 10 USC 1102

\*\*\*\* FOUO \*\*\*\*

Page

Figure 325: Sample Provider Privilege report results

After a report is generated, users may either click **Print** or **Cancel**. 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 CCQAS application by clicking the **Print** button. 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** button. 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

**Note:** Users should have Microsoft® Word or Excel open prior to copying report data.

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 121.



Figure 326: Exporting a Report to Word or Excel

Users must read and acknowledge a QA pop-up message, and then a Data Copied Message by clicking **OK**, as depicted in Figures 122 and 123.

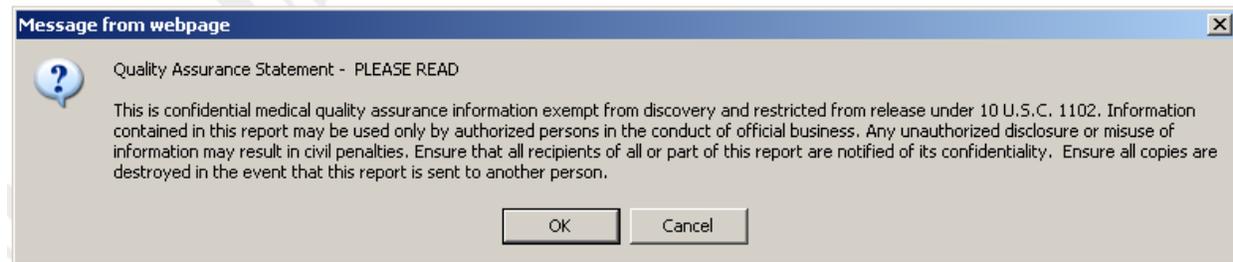


Figure 327: QA Statement

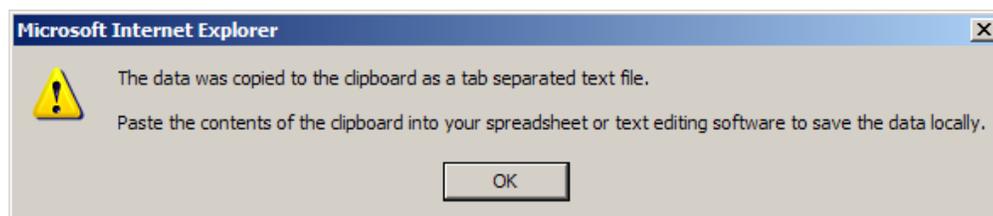


Figure 328: Data Copied Message Window

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 329. 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 Assistant	Active	9/1/2013
4	Clarkson, KELLY	A11	LTG	Medical Corps	W2DHAA			ADM	CRED	23		Allopathic Physician	Active	10/6/2012
5														

**Figure 329: 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, to include the QA/1102 statement.

## 14 Generating Ad-Hoc Credentials Reports

The CCQAS ad-hoc report tool may be used to answer business questions that cannot be addressed using the CCQAS standard reports. Access to Ad Hoc reports is based on Roles/Permissions. This tool enables users to generate reports using most data fields in the electronic credentials file. It provides a robust query capability that supports the use of multiple criteria to populate a desired report. Mastery of this tool requires a good working knowledge of CCQAS data, an understanding of the limitations of the tool, and practice. Users are encouraged to review the following sections and sample problems to ensure appropriate use of the ad-hoc tool.

### 14.1 Generating an Ad-Hoc Credentials Report

As with the CCQAS standard reports, ad-hoc reports are created by first selecting the data fields to build the columns of the report, and then selecting the query or filter criteria for populating the rows of the report. The ad-hoc report tool for Credentials is accessed by clicking **Reports** on the main menu bar, selecting **Ad-hoc** from the drop-down menu, and then selecting **Credentialing**. Figure 330 depicts the **Ad-hoc Reporting** menu.

The screenshot shows the CCQAS Version 2.10.0 interface in a Windows Internet Explorer browser. The page title is "CCQAS Version 2.10.0 - Centralized Credentials Quality Assurance System - Windows Internet Explorer provided by ASM Research". The main header includes the CCQAS logo, the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness", and a "\*\*\*\* FOUO \*\*\*\*" warning. The navigation menu has tabs for "Credentialing", "Privileging", "Reports", "System", and "Help". The "Reports" tab is active, and a dropdown menu is open, showing options: "Standard", "Ad-Hoc", "Admin", "NPDB Query", and "MTF". The "Ad-Hoc" option is selected, and a sub-menu is open, showing "Credentialing" as the selected option. The main content area contains a "Provider Search" section with fields for "Last Name", "Alias Last Name", "Branch", "Primary UIC", "Department", "Provider Type", "Sort By" (set to "Last Name"), "First Name", "Alias First Name", "Corps", "Assignment UIC", and "Work Center". There are also checkboxes for "Assignment Status" (Inactive, Current, Pending) and "Search Type" (All (Primary UIC or Assignment UIC), Primary UIC, Assignment UIC, ICTB, Provider Locator).

Figure 330: Ad-hoc Reporting Menu for Credentialing

The following example will be used throughout this section to illustrate the ad-hoc report functionality.

**Example:** Robert, an experienced CCQAS user, is asked to provide a listing of all physicians Board Certified in Family Practice whose Board Certification is due to expire within the next 12 months. To generate this report, Robert needs to query CCQAS for Providers who are Specialty Board Certified in Family Practice or Internal Medicine, and whose Board Certification is expiring within a defined date range. He determines that the Provider's name, SSN (now reported in the **Person ID Type** and **Person ID** fields), and **Department** should be included on the report. For the purposes of this example, assume that the current date is August 6, 2013. In the **Select Detail** section of this screen, users specify the categories of data to include in their ad-hoc report, as depicted in Figure 331. This is also the screen where the user would indicate Record Status and Record Type:

- A **Record Status** indicator that enables only Inactive, Current or Pending assignment types to be included in the report query
- A **Record Type** indicator that enables only Credentialing (Primary), Credentialing (Any/CRED and ICTB), ICTB assignment, or All record types to be included in the report query
- **NOTE:** Include **Record ID** as a column in the Ad Hoc report to assist in identifying orphaned records (sub records). Every sub record associated with one provider will share the same Record ID.

The screenshot shows the 'Ad Hoc Report Wizard' interface. At the top, there is a navigation bar with tabs for 'Credentialing', 'Privileging', 'Risk Management', 'Reports', 'System', and 'Help'. Below this, the main window is titled 'Ad Hoc Report Wizard - Select the detail you would like to view for each provider record'. The window is divided into three columns. The first column, 'Select Detail', contains a list of checkboxes: License/Certification/Registration, DEA/CDS, Education/Training, Specialty (checked), Affiliation, Continuing Education, Contingency Training, References, Databank Queries, Custody History, Assignments/Work History (checked), and Remarks. The second column, 'Record Status', contains radio buttons for Inactive, Current (checked), and Pending. The third column, 'Record Type', contains radio buttons for Credentialing (Primary), Credentialing (Any), ICTB, and All (checked). At the bottom of the window, there are three buttons: 'Close', 'Recall Saved Query', and 'Next >>'.

**Figure 331: First Screen of the Ad-hoc Report Wizard**

The categories listed are similar, but not identical, to the sections that comprise the electronic credentials record. The selection of data categories on this screen determines the data fields that are returned on the next screen for building the columns of the report. The following mapping (refer to Table 6) 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.

Credentials File Section	Example Data Fields	Ad-Hoc Report Wizard
Profile	First Name, Last Name, Alias Last Name, Branch, Rank, Corps	Provider Tab (Default), Profile Column
Identification	Identification Type, Number	Provider Tab (Default), Identification Column
Contact Information	Address, Phone Number, Email	Provider Tab (Default), Contact Column
Lic/Cert/Reg	Number, State, Field	Lic/Cert/Reg Tab, Columns: <ul style="list-style-type: none"> <li>• State License</li> <li>• National Certification</li> <li>• Unlicensed Information</li> </ul>
DEA/CDS	Number, Expiration Date	DEA/CDS Tab, DEA/CDS Column
Education/Training	Degree, Institution	Education/Training Tab, columns: <ul style="list-style-type: none"> <li>• Professional Education</li> <li>• Post Graduate Training</li> <li>• ECFMG</li> </ul>
Specialty	Specialty, Board Certification	Specialty Tab, Specialty column
Affiliation	Affiliation Type	Affiliation Tab, Provider Affiliation column
Continuing Education	Type, Course, Credits	Continuing Education Tab, Continuing Education column
Contingency Training	Training Type, Completion and Expiration	Contingency Training Tab, Contingency Training column
References	Reference Name, Address	References Tab, References column
Databank Queries	NPDB Last Query Date, HIPDB Last Query Date, FSMB Last Query Date	Databank Queries Tab, Databank Queries column
Custody History	Credentialing facility	Custody History Tab, Custody History column
Work History	Assignment, Malpractice, Civilian, Credentialing Facility, Primary Business Address, Current Appointment, Provider Privileges, Tracker Status	Assignments/Work History Tab, columns: <ul style="list-style-type: none"> <li>• Assignments</li> <li>• Work History</li> <li>• Provider Malpractice</li> </ul>
Privileges		Not available
Documents		Not available
Remarks	Remark Type, Remark	Remarks Tab, Remarks column

**Table 6: Mapping from the Credentials Record to Ad-hoc Report Wizard**

Users should note that data fields associated with the categories **Profile**, **Identification**, and **Contact Information**, will automatically be presented on the next screen, regardless of the other categories of data selected.

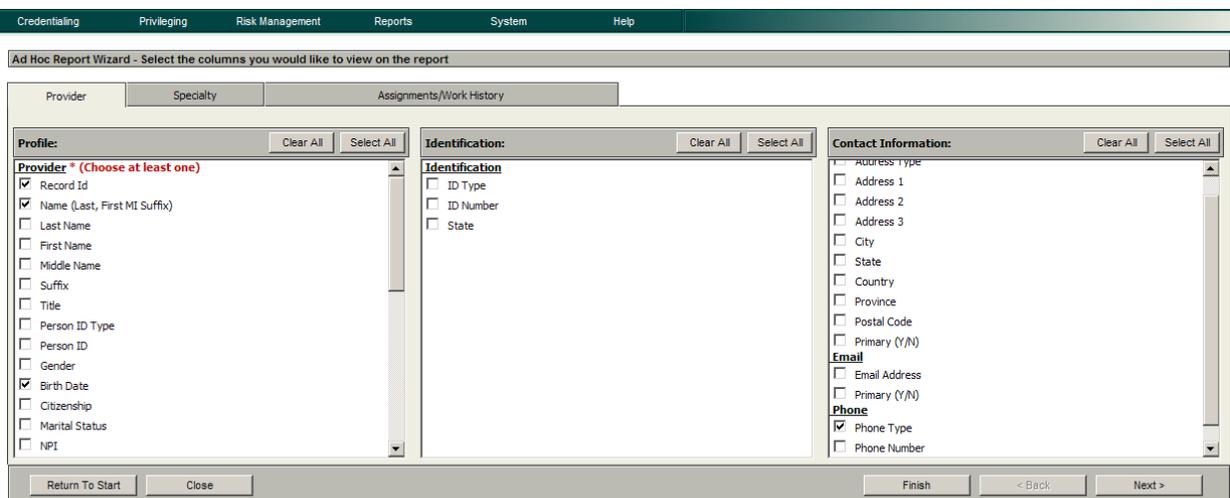
**Example:** On the first screen of the ad-hoc report tool, Robert has checked **Assignments/Work History**, since he wants a report that includes Department code (refer to Figure 331 above). Robert also needs demographic information about the Provider on his report, but does not need to select any additional categories, since Provider information from the **Profile** section of the credentials record is automatically presented on the following screen.

On this screen users also select the status and type of records to be included in the report. CCQAS defaults its search to records with **Record Status (Assignment) = Current** and **Record Type = All**, unless users change the default settings on this screen (refer to Figure 331 above). After selecting the categories, type, and status of records that should be queried, users click **Next >>**. The second screen displays a series of tabs that reflect the categories selected on the previous screen. The **Provider** tab is automatically presented on this screen, regardless of the categories selected on the previous screen. The **Provider** tab is separated into three subsections. The **Profile** subsection includes data fields from the **Profile, Identification, and Contact Information** sections of the Provider’s credentials record.

Users build the columns of the report by selecting data fields on these tabs. Users may move to the next tab by clicking **Next >>** or by clicking the label of the tab. Users may move back and forth between tabs, and tabs may be left blank if users determine that no data elements from that tab are needed. The data fields may be selected in any order, but will appear on the report in the order in which they appear on the tabs.

**Example:** Robert selects **Record ID**, provider **Name (Last, First, MI, Suffix)**, and **Birth Date** in the **Profile** column and **Phone Type** in the **Contact Information** column of the **Provider** tab (refer to Figure 332).

**Hint:** Always include data fields used for query criteria as a column on the report.



**Figure 332: Provider Tab of the Ad-Hoc Report Wizard**

Robert then selects the **HPTC Specialty, Level, Board Name, Expiration Date** and **Expiration Indefinite** columns on the **Specialty** tab, as depicted in Figure 333. Robert then clicks **Next >**.

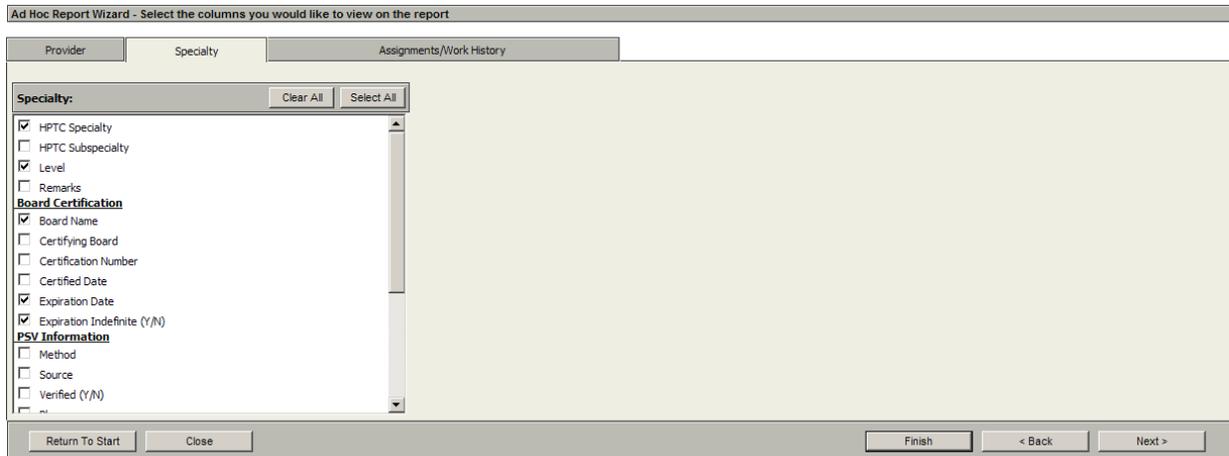


Figure 333: The Specialty Tab of the Ad-Hoc Report Wizard

The **Assignments/Work History** subsections are contained within the **Assignments**, **Assignment/Work History**, and **Provider Malpractice** sections of the Provider’s credentials record, respectively. Robert selects **Assignment UIC**, **Department**, **Record Type**, **Civ. Role**, **Credentialing UIC** as a column for query criteria on the report, and then clicks **Finish**. Figure 334 depicts the **Assignment/Work History** section of the ad-hoc report wizard.

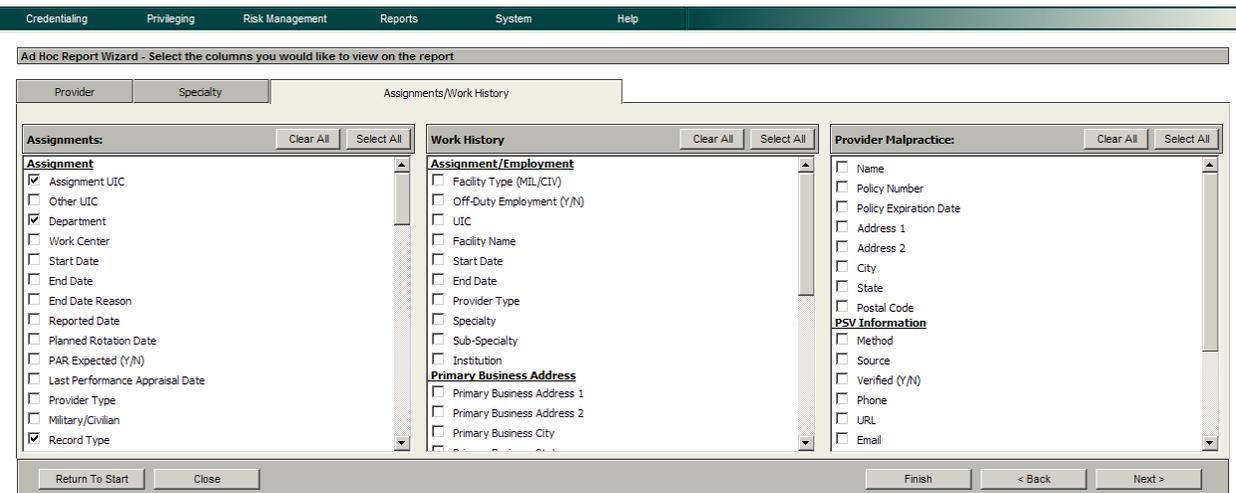


Figure 334: The Assignment/Work History Tab of the Ad-Hoc Report Wizard

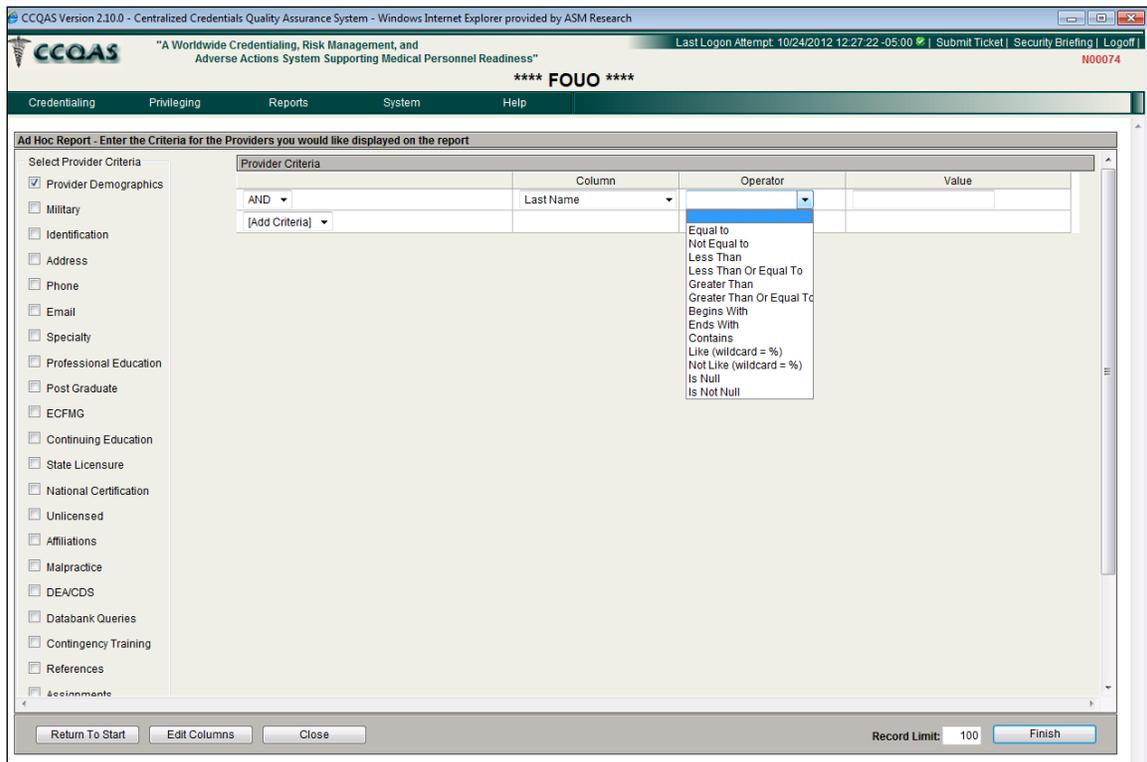
After users select the desired data fields from the tabs, the following actions may be taken:

- If users realize that the wrong data categories were selected on the previous screen, they may click the **Return to Start** button to begin again
- Clicking the **Close** button closes the ad-hoc report generator and returns users to the **Credentials Provider Search** screen
- Clicking the **Finish** button automatically moves users to the final screen of the ad-hoc report tool
- Clicking the **< Back** button moves users to the previous tab on the second screen of the ad-hoc report wizard. The **< Back** button is disabled if the **Provider** tab is displayed

- Clicking the **Next >** button from the last tab also moves users to the third screen of the ad-hoc report tool

On the third screen of the ad-hoc report tool, depicted in Figure 335, users specify criteria for populating the rows of the report. When a category of data is selected, a window opens that enables users to select the desired data field, operator, and value for the query.

**Note:** The **Demographics** checkbox in the **Select Provider Criteria** section enables users to use the data fields present in the **Profile, Identification, and Contact Information** sections of the credentials record as query criteria for the search.



**Figure 335: Third Screen of the Ad-hoc Report Wizard**

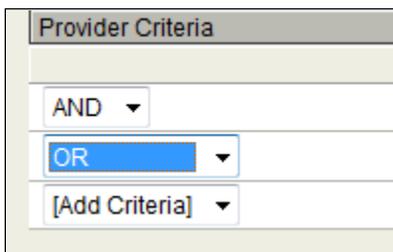
A listing and description of available operators are provided in Table 7 below.

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

Operator	Data Types	Description
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 numbers and any additional characters where the % is placed

**Table 7: Operators for Ad-hoc Query Criteria**

If users wish to use more than one data field to query the CCQAS database, another query criteria from a different category may be added by checking the second category. Other query criteria from the same category may be added by clicking **Add Criteria**, as depicted in Figure 336.



**Figure 336: 'AND' and 'OR' Operators Selections**

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 query criteria from different categories are applied, CCQAS automatically applies **AND** logic for the query.

**Example:** Robert needs to use multiple query criteria to generate this report. He wants to identify Providers who are Board Certified in Family Practice or Internal Medicine, and whose Board Certification will expire within the next year. He uses **OR** to query Providers who are Board Certified in either Family Practice or Internal Medicine as depicted in Figure 337. Since the Expiration Date is in the same section, Robert needs enter the date range after each respective Specialty.

(Family Practice **OR** Internal Medicine) **AND** Date between specified Dates range.

The screenshot shows the 'Ad Hoc Report - Enter the Criteria for the Providers you would like displayed on the report' window. On the left, a list of criteria categories is shown, with 'Specialty' selected. The main area contains a table for defining query criteria:

	Column	Operator	Value
AND	HPTC Specialty	Equal to	Family Practice
AND	Expiration Date	Between	08-06-2013 And 08-06-2014
OR	HPTC Specialty	Equal to	Internal Medicine
AND	Expiration Date	Between	08-06-2013 And 08-06-2014
[Add Criteria]			

At the bottom of the window, there are buttons for 'Return To Start', 'Edit Columns', and 'Close'. On the right side, there is a 'Record Limit' set to 100 and a 'Finish' button.

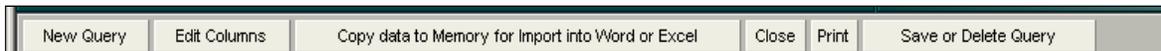
**Figure 337: Example of Multiple Query Criteria, Ad-hoc Report Wizard**

**Note:** Robert could also run two separate reports to get the same result. He could run one report to identify all Providers Board Certified in Family Practice whose certification is expiring within a 12 month range. He would then run a second report to identify all Providers Board Certified in Internal Medicine whose certification is expiring within a 12 month range.

After the query criteria are specified, users may take the following actions:

- Clicking the **Return to Start** button returns users to the first screen of the ad-hoc report tool and clears all selected data fields and query criteria
- Clicking the **Edit Columns** button returns users to the second screen of the ad-hoc report tool. Previously selected data fields will be displayed and may be edited
- Clicking the **Close** button closes the ad-hoc report generator and returns users to the **Credentials Provider Search** screen
- Clicking the **Finish** button generates the ad-hoc report up to the specified **Record Limit**

After all query criteria have been specified, the report is generated by clicking **Finish**. The report may take some time to generate depending on its size and complexity. After a report is generated, users may select one of the options at the top of the report, as depicted in Figure 338 below.



**Figure 338: Action Options for a Report**

- Clicking the **New Query** button returns users to the first screen of the ad-hoc report tool and clears all selected data fields and query criteria
- Clicking the **Edit Columns** button returns users to the second screen of the ad-hoc report tool. Previously selected data fields will be displayed and may be edited
- Clicking the **Copy Data to Memory for Import into Word or Excel** button allows users to export the report to Microsoft® Word or Microsoft® Excel (refer to Section 14.6)
- Clicking the **Close** button cancels the report and closes the ad-hoc report generator
- Clicking the **Print** button allows users to print the report directly from the CCQAS application (refer to Section 14.5)
- Clicking the **Save or Delete Query** button allows users to save the report criteria to a file so that it may run again in the future. If the report was generated using a saved query, the query may also be deleted (refer to Sections 14.2–14.4)

Reports cannot be saved in the CCQAS application. To save their report, users must either print a hardcopy or export it to Microsoft® Word or Microsoft® Excel so that the report may be saved as a file on their workstation. For reports that are run routinely, users should consider saving their query in CCQAS and recalling it each time the report is run, to ensure the report is run using the same reporting criteria each time.

## 14.2 Saving an Ad-Hoc Report Query for Future Use

Users may save a report query in the CCQAS application by clicking **Save or Delete Query**, located at the top of the ad-hoc report. A window opens that enables users to assign a name and description to the query prior to saving it. A well-documented query includes a listing of the data fields that comprise the report columns and a description of the query criteria that are used to populate the rows of the report. All CCQAS users who hold permissions to run ad-hoc reports for a given UIC have access to report queries saved for that UIC.

**Hint:** If any of the reporting criteria are date-sensitive, it may be necessary to change the dates used in the query. It is advised to note this requirement in the description for the saved query.

**Example:** Robert documents both the data fields and query criteria used to generate his report. Since the specific dates in the date range will change for future reports, he also notes that in the description, as depicted in Figure 339 below.

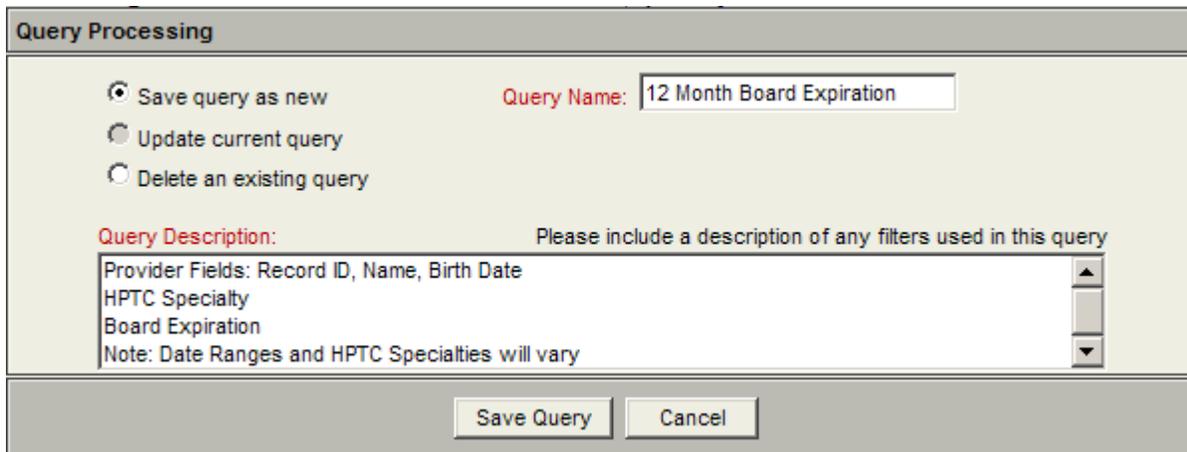


Figure 339: Query Processing Screen to Save or Delete Query

### 14.3 Running an Ad-Hoc Report from a Saved Query

A query may be recalled from the first screen of the ad-hoc report tool by clicking **Recall Saved Query**, as depicted in Figure 340.



Figure 340: Recall Saved Query Screen

The **Select Query Name** screen appears, as depicted in Figure 341. This screen allows users to select the **Query Name** from a list of queries that have been saved for that UIC. After selecting it, click **Submit**. The information from the saved query automatically populates all three screens of the ad-hoc report tool. A new report may be generated using the saved query information, or users may edit the columns or query criteria prior to running the report. Any changes to the reporting criteria may then be saved to the existing query, saved as a new query, or not saved at all. A saved query may be run as often as needed until it is deleted by a user.

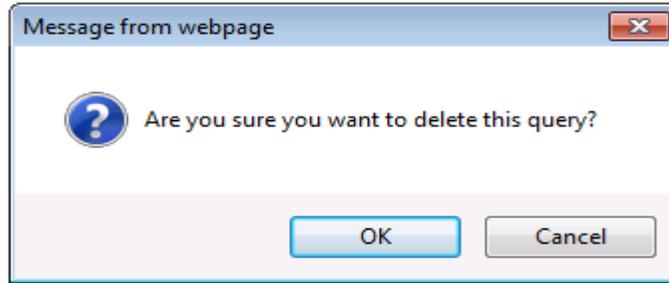


Figure 341: Recall Saved Query Name Screen

**Example:** Robert does not need to change original data fields included in the original query, but he does change the date range in the query criteria for reports that are run on a different date. Note that the report description reminds him that this is necessary.

### 14.4 Deleting a Saved Query

A saved query may be deleted in two ways. When a saved query is recalled from the first screen of the ad-hoc report tool, users may select **Delete** to delete the query. A confirmation message is then generated by system, as depicted in Figure 342.



**Figure 342: Delete Query Confirmation Message**

Users may also delete a saved query after a report is generated by clicking **Delete An Existing Query** (refer to Figure 339). Users are then allowed to select from the list of available queries for their UIC. Users who have permissions to use the ad-hoc report tool are able to save or delete a query for their UIC.

### 14.5 Printing an Ad-Hoc Report

Users may print the ad-hoc report directly from the CCQAS 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 the user's browser settings. Alternatively, many users prefer to export the report to Microsoft® Word or Excel to format their report prior to printing.

### 14.6 Exporting an Ad-hoc Report to Microsoft® Word or Excel

Users may export an ad-hoc 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.

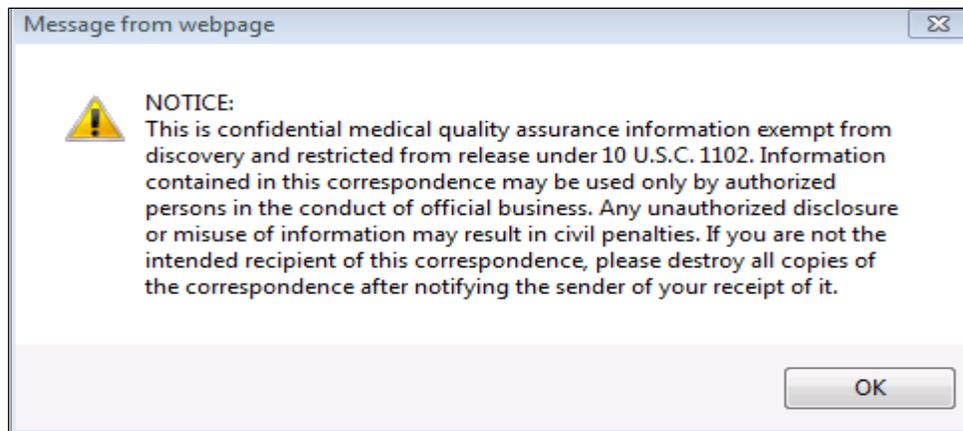
Provider		Provider Phone		Provider Assignment				Specialty				
Record Id	Name	Birth Date	Phone Type	Assignment UIC	Department	Record Type	Civ. Role	UIC	HPTC Specialty	Board Name	Expiration Date	Expiration Indefinite (Y/N)
122	SMITH, PAUL	07/03/1980	Home	CD1CFVPV		CRED		CD1CFVPV	Family Practice	American Academy of Family Physicians	12/20/2013	No

Record Count: 1

This is confidential medical quality assurance information exempt from discovery and restricted from release under 10 U.S.C. 1102. Information contained in this report may be used only by authorized persons in the conduct of official business. Any unauthorized disclosure or misuse of information may result in civil penalties. If you are not the intended recipient of this report, please destroy all copies of the report after notifying the sender of your receipt of it.

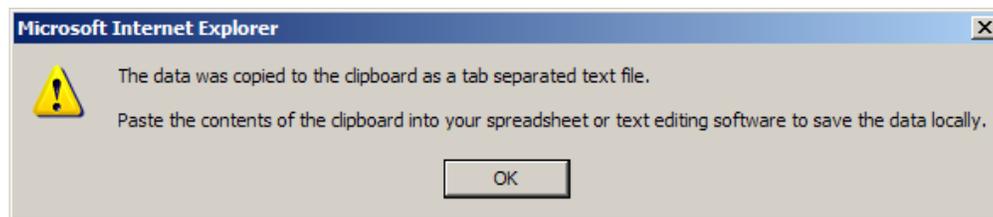
**Figure 343: Copy Data to Memory for Import into Word or Excel**

CCQAS generates a QA statement that users must accept by clicking **OK**, as depicted in Figure 344.



**Figure 344: QA Statement**

A second **Data Copied** pop-up window opens, as depicted in Figure 345. Click **OK**.



**Figure 345: Data Copied Message Window**

Users may now 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 then pasted into a column and a row, respectively in a Microsoft® Word or table or a Microsoft® Excel spreadsheet. The report may then be manipulated, saved, and printed as a regular Microsoft® Word or Excel file.

**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 will have to create a new report header and other descriptive information manually, as needed.

## 14.7 Sample Ad-hoc Reports

Three sample ad-hoc reports are provided on the following pages (refer to Table 8, Table 9, and Table 10). These sample ad-hoc reports are designed to demonstrate important features and limitations of the ad-hoc report tool, as well as appropriate use of operators.

## Ad-hoc Training Scenario 1: Providers Licensed in California

**Purpose:** This exercise will demonstrate the generation of an ad-hoc query with one filter.

**Scenario:** Robert receives notification from the State of California that his procedures for license renewal are changing. He wants to identify all Providers who will be affected by this change, so he runs an ad-hoc report to identify all Providers who are licensed in California.

Ad-hoc Report Screen	Columns and Query Criteria	Comments/Notes
First screen	Under <b>Select Detail</b> , select: <ul style="list-style-type: none"> <li>License/Certification/ Registration</li> </ul>	Unless the user specifies otherwise, CCQAS automatically searches records with <b>Record Status = Current</b> and <b>Record Type = All</b> .
Second screen, <b>Provider</b> tab	Under the <b>Provider</b> tab/ <b>Profile</b> section, select: <ul style="list-style-type: none"> <li>Record ID</li> <li>Name</li> </ul>	These are the columns that will be included in Robert's report.
Second screen, <b>State Licensure</b> tab	On the <b>Lic/Cert/Reg</b> tab, select: <ul style="list-style-type: none"> <li>License Number</li> <li>State Code</li> </ul>	These are the columns that will be included in Robert's report.
Third screen, <b>Select Provider Criteria</b>	Under <b>Provider Criteria</b> , select: <ul style="list-style-type: none"> <li>State Licensure</li> </ul>	
Third screen, <b>State Licensure Criteria</b>	Under <b>State Licensure Criteria</b> , select: <ul style="list-style-type: none"> <li><b>Column = State</b></li> <li><b>Operator = Equal to</b></li> <li><b>Value = CA</b></li> </ul>	By specifying CA, only those Providers with California licenses will be included in your report.
Resulting report		Multiple records will be returned for Providers who are licensed in CA.

**Table 8: Training Scenario 1**

When users generate an ad-hoc report that includes Providers with more than one sub-record (e.g., multiple subspecialties, state licenses, certifications, DEA/CDS, etc.), all sub-records associated with those Providers are returned on an ad-hoc report, if any one of the sub-records meets the reporting criteria.

Robert included **Record ID** as a column on his report, so that each sub-record could be linked back to the Provider to which it belonged. The **Record ID** is CCQAS-generated and unique to each Provider. Every sub-record associated with one Provider shares the same **Record ID**.

## Ad-hoc Training Scenario 2: BLS and ACLS Training Expiration

**Purpose:** This exercise will demonstrate the generation of an ad-hoc query with filters on multiple data elements.

**Scenario:** Robert has been asked to identify those Providers assigned to a mobilization UIC/UTC whose BLS or ACLS expire within the next 10 months. For purposes of illustration, this request was made on 1/02/2012.

Ad-hoc Report Screen	Columns and Query Criteria	Comments/Notes
First screen	Under <b>Select Detail</b> , select: <ul style="list-style-type: none"> <li>Contingency Training</li> <li>Assignment Work History</li> </ul>	Unless the user specifies otherwise, CCQAS automatically searches records with <b>Record Status = Current</b> and <b>Record Type = All</b> .
Second screen, <b>Provider</b> tab	On the <b>Provider tab/Profile</b> section, select: <ul style="list-style-type: none"> <li>Record ID</li> <li>Name</li> <li>Person ID Type</li> <li>Person ID</li> </ul>	The BLS and ACLS details and dates are found on the <b>Provider</b> tab, rather than the <b>Education</b> or <b>Training</b> tabs.
Second screen, <b>Contingency Training</b> tab	On the <b>Contingency Training</b> tab, select: <ul style="list-style-type: none"> <li>Training Type</li> <li>Training Expiration</li> </ul>	
Second screen, <b>Assignment/Work History</b> tab	On the <b>Assignment/Work History</b> tab, select: <ul style="list-style-type: none"> <li>Assignment UIC</li> </ul>	This is the column that will be included in Robert's report.
Third screen, <b>Select Provider Criteria</b>	Select <b>Contingency Training</b> .	
Third screen, <b>Contingency Training Criteria</b>	Under <b>Contingency Training Criteria</b> , select: <ul style="list-style-type: none"> <li><b>Column = Training type</b></li> <li><b>Operator = Equal To</b></li> <li><b>Value BLS</b></li> <li><b>Column = Training Expiration</b></li> <li><b>Operator = Between</b></li> <li><b>Values 01-01-2012 and 10-01-2012</b></li> </ul>	This filter will select those Providers with BLS training
Third screen, <b>Add Criteria</b>	Under <b>Add Criteria</b> , select: <ul style="list-style-type: none"> <li>OR</li> </ul>	Robert wants Providers with BLS or ACLS.
Third screen, <b>Contingency Training Criteria</b>	Under <b>Contingency Training Criteria</b> , select: <ul style="list-style-type: none"> <li><b>Column = Training type</b></li> <li><b>Operator = Equal To</b></li> <li><b>Value ACLS</b></li> <li><b>Column = Training Expiration</b></li> <li><b>Operator = Between</b></li> <li><b>Value = 01-01-2012 and 10-31-2012</b></li> </ul>	This filter will select those Providers whose BLS or ACLS are due to expire.

Ad-hoc Report Screen	Columns and Query Criteria	Comments/Notes
Third screen, <b>Assignment</b>	Under <b>Assignment Criteria</b> , select: <ul style="list-style-type: none"> <li>• <b>Column = Assignment UIC</b></li> <li>• <b>Operator = Is not Null</b></li> </ul>	This queries only those Providers who are assigned to a UIC.
Resulting report. <b>Finish</b> button		The report lists all Providers assigned to a mobilization UIC whose BLS or ACLS will expire within 10 months.

**Table 9: Training Scenario 2**

Operator **OR** was used because Robert wanted to identify Providers with an upcoming BLS or ACLS expiration.

Operator **AND** was automatically applied when filters from different categories (e.g., **Demographics** and **Assignment UIC**) were used.

**Example:** All Providers whose BLS or ACLS Contingency Training expired within 10 months **AND** were assigned to a UIC.

By using the operator **IS NOT NULL**, users are able to capture all records for which a UIC has been assigned. Any records that do not have a value in that data field will not be included on the report.

**Note:** There is also a Standard Contingency Training Report available (See [Section 13](#)).

### Ad-hoc Training Scenario 3: ECFMG Status

**Purpose:** This exercise will demonstrate the generation of an ad-hoc query with filters on multiple data elements.

**Scenario:** Robert has been directed to screen all unlicensed, foreign trained physicians to ensure their ECFMG is currently valid.

Ad-hoc Report Screen	Columns and Query Criteria	Comments/Notes
First screen	Under <b>Select Detail</b> , select: <ul style="list-style-type: none"> <li>• Licensure/Certification/ Registration</li> <li>• Education/Training</li> </ul>	
Second screen, <b>Provider</b> tab	On the <b>Provider</b> tab/ <b>Profile</b> section, select: <ul style="list-style-type: none"> <li>• Record ID</li> <li>• Name</li> </ul>	
Second screen, <b>State License</b> tab	On the <b>Lic/Cert/Reg</b> tab, select: <ul style="list-style-type: none"> <li>• Status</li> <li>• Expiration Date</li> </ul>	These are the columns that will be included in Robert's report.

Ad-hoc Report Screen	Columns and Query Criteria	Comments/Notes
Second screen, <b>Education/Training</b> tab	On the <b>Education/Training</b> tab, under <b>Professional Education</b> subheading, select: <ul style="list-style-type: none"> <li>Foreign Medical Graduate (Y/N)</li> </ul> Under <b>ECFMG</b> subheading, select: <ul style="list-style-type: none"> <li>Expiration Date</li> </ul>	These are the columns that will be included in Robert's report.
Third screen, <b>Select Provider Criteria</b>	Select <b>Professional Education</b> .	
Third screen, <b>Education/Training Criteria</b>	Under <b>Professional Education Criteria</b> , select: <ul style="list-style-type: none"> <li><b>Column = Foreign Medical Graduate (Y/N)</b></li> <li><b>Operator = Equal to</b></li> <li><b>Value = Yes</b></li> </ul>	This will identify all Providers that are foreign trained.
Resulting Report		The report will list ECFMG data for all Providers who are foreign trained and the status of any licenses they hold.

**Table 10: Training Scenario 3**

This report included the licensure status as a column, but did not use licensure status as query criteria. Ad-hoc reports cannot be used to identify Providers who have never held a state license. If a Provider never held a state license, no license record was ever created for that Provider. If no licensing record exists, CCQAS cannot run a query against it. Two standard reports, **Unlicensed Credentials Record Report** or **Unlicensed Provider Report**, should be used to identify unlicensed and uncertified Providers.

## 15 System Management

System management is an important part of CCQAS and Module users at both the MTF and Service Level have varying levels of access to the **System** menu, and its functionality. The **System** menu, depicted in Figure 346 is located in the main tool bar. The options within the menu vary based on the module user's roles, set via the **System Admin** tab in User Processing (refer to [Section 3](#)).

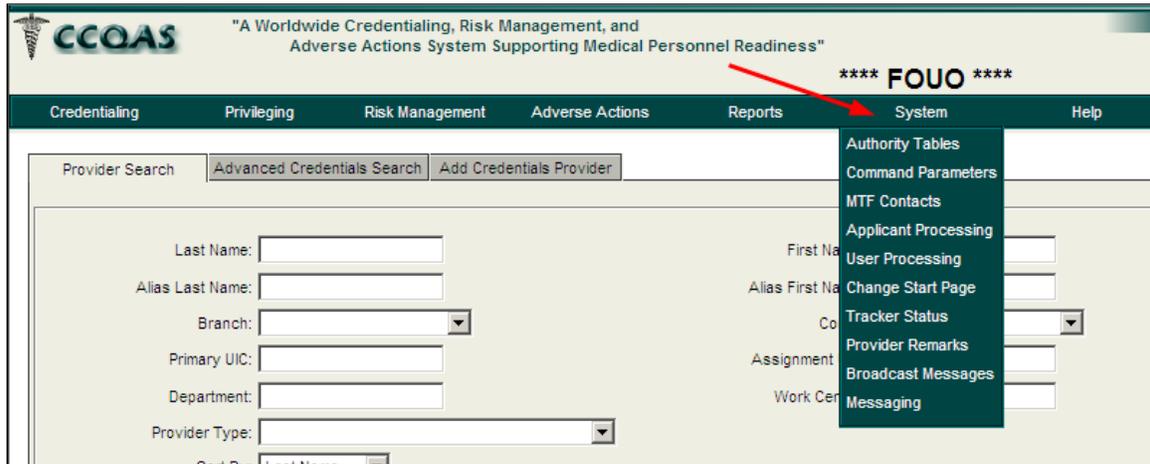


Figure 346: System Menu

### 15.1 Authority Tables

The **Authority Tables** section of the **System** menu, depicted in Figure 347, provides a Crosswalk (CW) mapping of values within CCQAS, and Lookup (LU) text descriptions of those values in the crosswalk mapping.

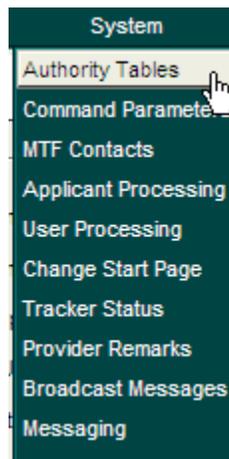


Figure 347: Authority Tables Menu Option

After users open the **Authority Tables** page, they select either CW mappings or LU values, and then click the Display button to see the database properties. Figure 348 below depicts the **Authority Tables** page.

**Note:** Authority Tables are exclusively used by the Service Level Representatives.

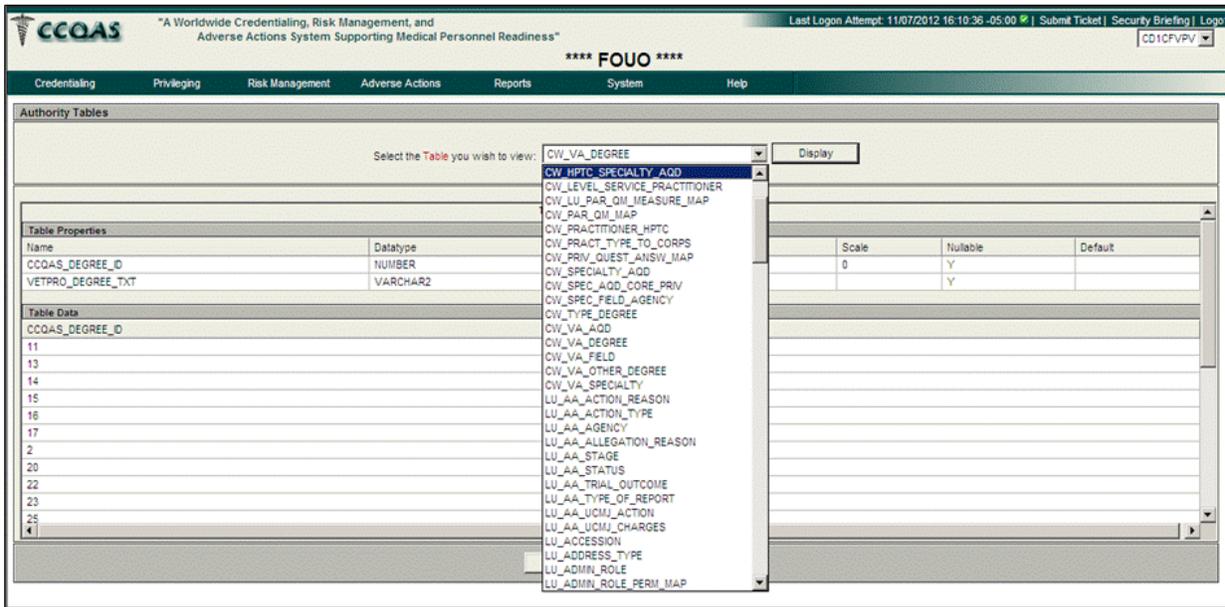


Figure 348: CW and LU Mappings/Values for Display

## 15.2 Command Parameters

When users select **Command Parameters** from the **System** menu, they may view and edit (with proper role) various contact and personnel information for their assigned MTF. Figure 349 depicts the **Commands Parameters** menu option.

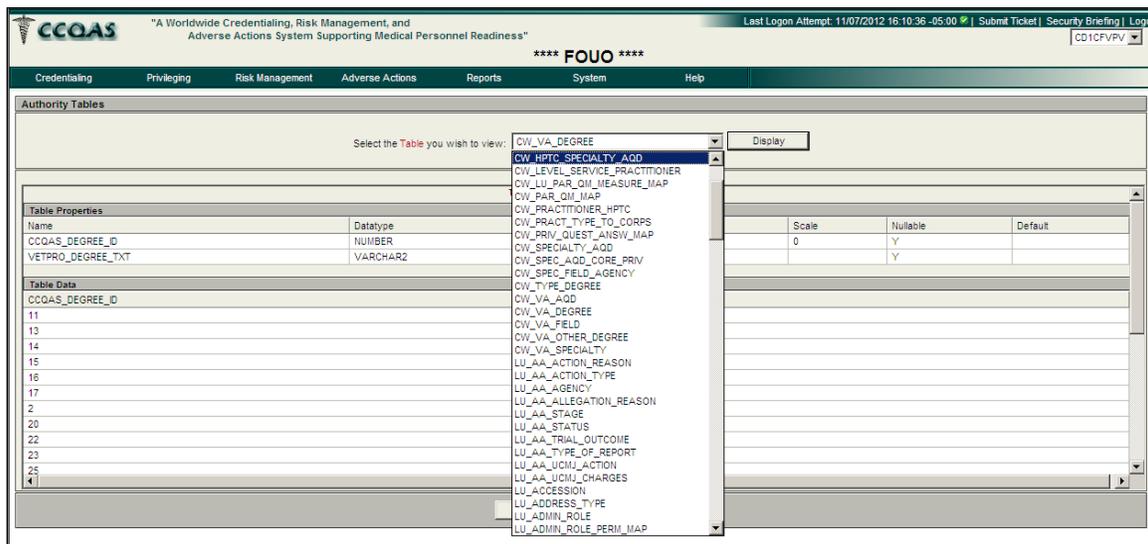


Figure 349: Command Parameters Menu Option

**Command Parameters** includes demographic data for the Credentials Signature Authority, Risk Management Signature Authority, POC for ECOMS/ECONS, Certification Authority, and First, Second, and Third POCs for the facility. Figure 350 depicts the **Command Parameters** page.

**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 pre-populate credentialing and privileging letters and forms. Refer to [Section 12](#) for detailed information on the letter generation process.

**Command Parameters** also displays, whether or not the MTF has the Privileging Module activated, and allows the Privileging Authority UIC, Active Renewal Days Notice, Reserve/Guard Renewal Days Notice, Expiration Credentials 1st Notice Days and 2nd Notice Days values to be set or updated on this page.

**Figure 350: Command Parameters Page**

Users may add or edit command and contact information by typing in the information and clicking save 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 the respective 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
- 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

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 351.

The screenshot shows a web form with two main 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 four fields:  
 - "Privileging Module Activated:" with the value "Yes".  
 - "Privileging Authority UIC:" with the value "W2H810" and a small icon of three people.  
 - "Active Renewal Notice Days:" with the value "30".  
 - "Reserve/Guard Renewal Notice Days:" with the value "90".

**Figure 351: 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.

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 352.

**Note:** Auto renewal only works if the previous privileges were granted electronically and the provider remains at the same UIC. If an e-application is manually generated and not completed prior to the automated renewal date, a new second e-application is automatically generated and will need to be terminated.

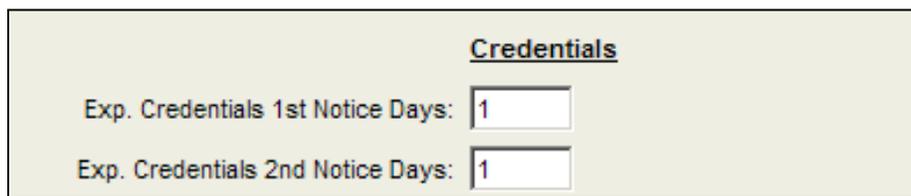
The screenshot shows a "Provider Self-Service" interface with tabs for "Work List", "Applications", and "Documents". Below the tabs is a help message: "Double click on a worklist task to open it. You may view completed e-applications from current or past privileging periods in the 'Applications' tab. U in the 'Documents' tab." Below this is a filter section with "Status: Open Tasks" and a date range "Show tasks with a start date between 10/06/2011 and 10/05/2012". A table below shows a single task:

Urgent	Task	App Type	MTF
No	Complete Application (Military)	Renewal	W2DH78, FORT BELVOIR COMMUNITY HOSPITA

**Figure 352: Provider Work List Item – Complete Renewal Application**

In the Credentials section, the “Exp Credentials 1st Notice Days” and “Exp Credentials 2nd Notice Days” parameters control how many days prior to credential expiration an automated email notification will be sent to the provider. Expiring credential notification emails are sent for expiring (1) State Licenses/Certifications/ Registrations, (2) National Certifications/Registrations, (3) Contingency Training (i.e., BLS, etc.) and (4) Specialty Board Certifications.

**Note:** The email notification is sent to the provider’s primary email address so ensure that the primary email addresses are always kept up-to-date in CCQAS. Email addresses may be updated in either the CCQAS record or the CCQAS User account and an email update to one will automatically update the other.



Credentials

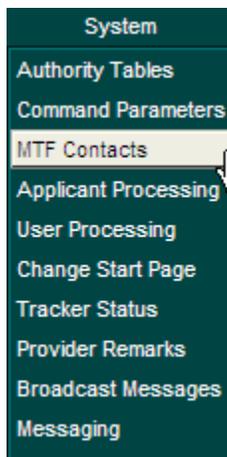
Exp. Credentials 1st Notice Days:

Exp. Credentials 2nd Notice Days:

**Figure 353: Exp. Credentials Notice Days on the Command Parameters Screen**

### 15.3 MTF Contacts

When users select the **MTF Contacts** option from the **System** menu, the contact information defaults to the UICs for that service. There are radio buttons to display All MTFs, or just Air Force, Army, or Navy. Figure 354 depicts the **MTF Contacts** menu option.



**Figure 354: MTF Contacts Menu Option**

Outside of a user’s own MTF, the contact information is read-only. At the user’s MTF, he or she can edit and update this information with appropriate role.

The **MTF Contacts** page is depicted in Figure 355.

MTF		Branch Clinics							
UIC: CD1CFVPV Privileging: Yes Service: Air Force Activate Privileging Module: Privileging Module Activated MTF Name: 27 SPECIAL OPERATIONS MEDICAL GROUP @ Address 1: 27 MDG/SGHC Address 2: 208 W. CASABLANCA AVE City: CANNON AFB State: NM - New Mexico Zip: 88103-5014 Country: United States - US DMIS: 85 Head Officer: HEAD OFFICER		UIC: <input type="text"/> Add Branch Clinic <table border="1"> <thead> <tr> <th>UIC</th> <th>Name</th> <th>Location</th> </tr> </thead> <tbody> <tr> <td>FFL0L0</td> <td>0161 MDG @</td> <td>Phoenix, AZ</td> </tr> </tbody> </table>		UIC	Name	Location	FFL0L0	0161 MDG @	Phoenix, AZ
UIC	Name	Location							
FFL0L0	0161 MDG @	Phoenix, AZ							
Credentials Coordinator Name: Mrs. Jessica Smith Commercial Phone: 575.555.6608 DSN Phone: 555.6608 Fax Phone: 2345 Email Address: Jessica.Smith.Test@us.af.mil		Risk Manager Name: Mr. Mark Jones Commercial Phone: 575.555.4009 DSN Phone: 555.4009 Fax Phone: 234 Email Address: Mark.Jones.Test@cannon.af.mil							
Remarks Priv Activated: 4/10/2008 Updated 23 May 2005 Change E-mail in Contacts maybe giving odd message 06/09/08TR									
<input type="button" value="Save"/> <input type="button" value="Cancel"/>									

**Figure 355: Editable MTF Contacts Screen**

The Activate Privileging Module field indicates if the MTF has been activated on the Privileging Module or not.

MTF and Credentials Coordinator data is used to pre-populate various Letters and automated CCQAS email notifications.

This is only place where Branch Clinics can be associated with a parent MTF. This is the first step in the Branch Clinic Management Process. See [Section 16.1](#) for more details.

## 15.4 Applicant Processing

Refer to [Section 3.2](#)

## 15.5 User Processing

Refer to [Section 3.2](#)

## 15.6 Change Start Page

When users select **Change Start Page** from the **System** menu, they can set which screen they would like to see when they log in to CCQAS. Figure 356 depicts the **Change Start Page** menu option.

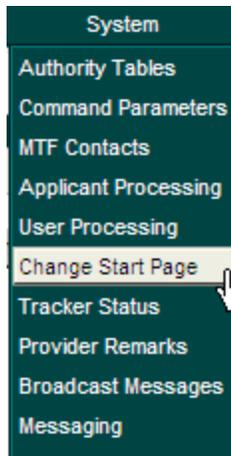


Figure 356: Change Start Page Menu Option

To change the start page, select one of the options from the **Change Start Page** drop-down menu, as depicted in Figure 357. The start page options are **Credentials Search**, **Privileging Worklist**, **Incident Management Search**, **Claim Management Search**, **Disability Management Search** and **Adverse Actions Search**.

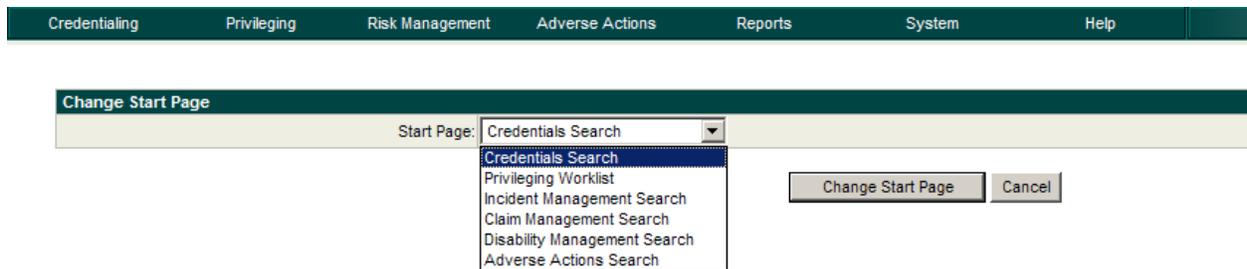
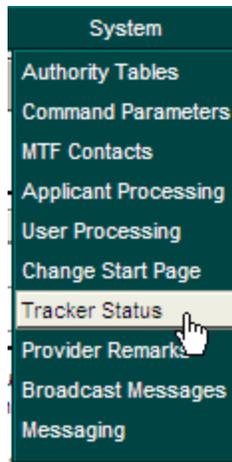


Figure 357: 'Change Start Page' Drop-down Menu Options

Click **Change Start Page** to confirm the selection. The selected change will take effect the next time users log in to CCQAS. Click **Cancel** to return to the main page.

## 15.7 Tracker Status

Users can insert, delete, update, and edit MTF Tracker Status entries by selecting **Tracker Status** from the **System** menu, as depicted in Figure 358 below.



**Figure 358: Tracker Status Menu Option**

The MTF Tracker Status entries managed here appear in the **Tracker Status** drop-down menu, as depicted in Figure 359. CCQAS users can view the MTF Tracker Status entries at the associated MTF.

		Tracker Status		Description
Delete	Update	1	test	
Delete	Update	1	Creating a Tracker Status type	
Delete	Update	1	Adding in a tracker status	
Delete	Update	1	Tracker Status #1	
Delete	Update	2	yawn	
Delete	Update	2ND	Second Notice Letter Sent	
Delete	Update	2ND	test no	
Delete	Update	2NDQP	PR missing information	
Delete	Update	3	blah blah	
Delete	Update	ABC	ABC	
Delete	Update	ACDU	Member sent permanent Active Duty	
Delete	Update	ADMIN1	General Administrative Records (We hold privileges in temporary abeyance.)	
Delete	Update	ADMIN2	REDCOM Records Review (NPQ 30 day follow-up required (Med Boards)	
Delete	Update	ADMIN3	DIRECTOR ONLY (Pending Administrative Action - Full and Fair Hearing)	
Delete	Update	ADMIN4	ECOMS Kickback	
Delete	Update	ARCHIVED	Date file was Archived by CCPD Staff	
Delete	Update	CCPR	Cred comm peer review	
Delete	Update	CR+1/APR	Committee Ready / April of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/AUG	Committee Ready / August of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/DEC	Committee Ready / December of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/FEB	Committee Ready / February of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/JAN	Committee Ready / January of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/JUL	Committee Ready / July of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/JUN	Committee Ready / June of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/MAR	Committee Ready / March of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/MAY	Committee Ready / May of ECOM/DS (ready for ECOMS)	
Delete	Update	CR+1/NOV	Committee Ready / November of ECOM/DS (ready for ECOMS)	

**Figure 359: Tracker Status Screen**

**Note:** Refer to Section [6.3.12.1](#) for further details on how to maintain Tracker Status entries in the provider's credentials record.

## 15.8 Provider Remarks

Users can insert, delete, update, and edit MTF Provider remarks entries by selecting **Provider Remarks** from the **System** menu, as depicted in Figure 360.

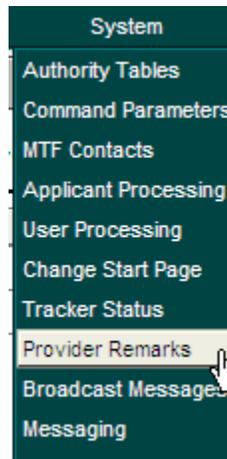


Figure 360: Provide Remarks Menu Option

The **Provider Remarks Type** window opens, as depicted in Figure 361. The pick list options for **Provider Remarks** are created when CC/MSSP/CMs click **Insert** in the upper left-hand corner of the screen.

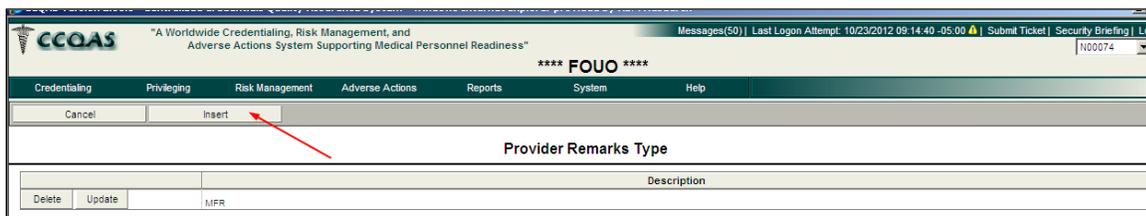


Figure 361: Provider Remarks Screen

After CC/MSSP/CMs enter a free-text **Description** and click **Add**, the **Provider Remarks Type** displays one new entry. Figure 362 depicts the **Provider Remarks Type (Description)** screen.

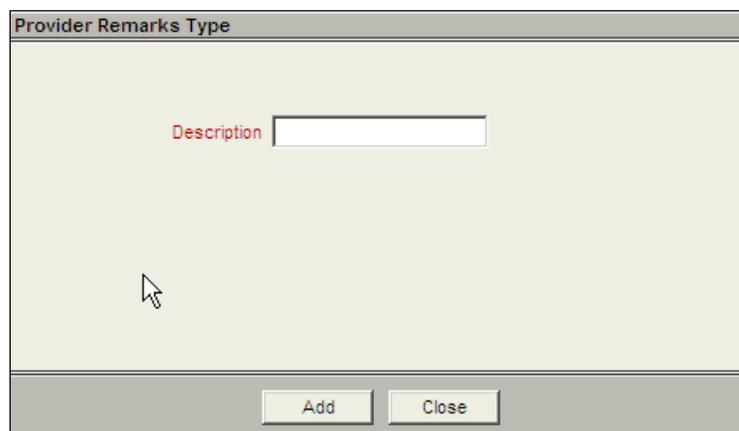


Figure 362: Provider Remarks Type Screen (Description)

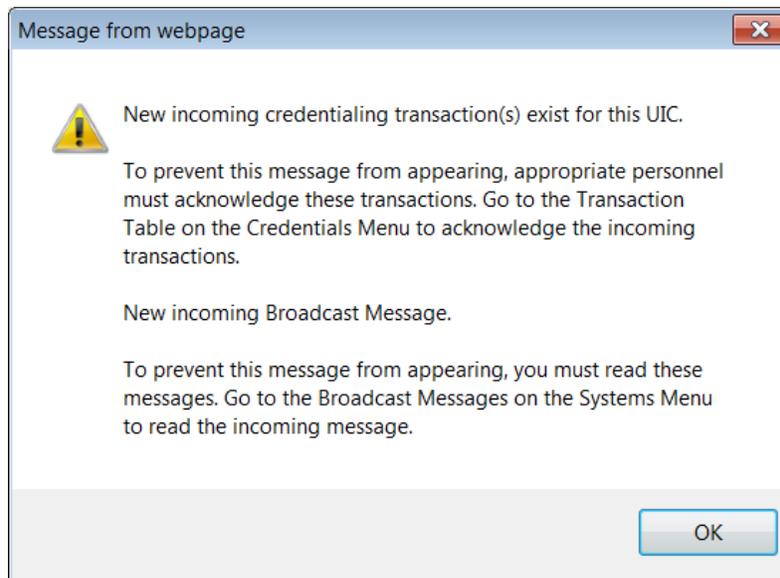
Additional remarks types may be entered by repeating this process until the complete list of pick list values have been created, as depicted in Figure 363. After all desired values have been created, CC/MSSP/CMs click **Cancel** to complete the configuration process.

		UIC	Description
Delete	Update	FFMSJ0	Record review accomplished 9/14/2011 by EKP
Delete	Update	FFL910	License
Delete	Update	FFMKW0	2 YR TOUR WITH THE ARMY, PCF IS TEMP. INACTIVE
Delete	Update	FFL440	NPI
Delete	Update	FFMMF0	Licensure
Delete	Update	FFTMW0	retired
Delete	Update	FFMFH0	Details
Delete	Update	FFLOL0	Memo
Delete	Update	FFTDQ0	DEA Number
Delete	Update	KF0FCB6	test May 15
Delete	Update	BP2ZFBL5	Testing for User guide
Delete	Update	CD1CFVPV	testing
Delete	Update	ED1MFND9	local
Delete	Update	HL0RFC23	Pending CF Review
Delete	Update	CD1CFVPV	TRAINING 15_OCT
Delete	Update	BP2WFP05	PAC Initial Remark
Delete	Update	DM1LFC0N	AFTER PCS
Delete	Update	DM1LFC0N	VAL2 test
Delete	Update	CD1CFVPV	Example for user Guide
Delete	Update	CL1LFC0F	Review Notes
Delete	Update	CL1LFC0F	Credentials Update
Delete	Update	CL1LFC0F	New Assignment
Delete	Update	CL1LFC0F	Privileging event

**Figure 363: Provider Remarks Type Screen**

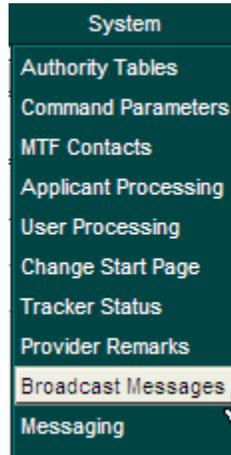
## 15.9 Broadcast Messaging

Broadcast messages are system-wide messages and notifications that are meant to be viewed by anyone that logs into the application. If there is an unread broadcast message users can see a notification message about the incoming message when they log in to CCQAS as depicted in Figure 364.



**Figure 364: New Incoming Broadcast Message Alert**

To view incoming messages, select **Broadcast Messages** from the **System** menu, as depicted in Figure 365.

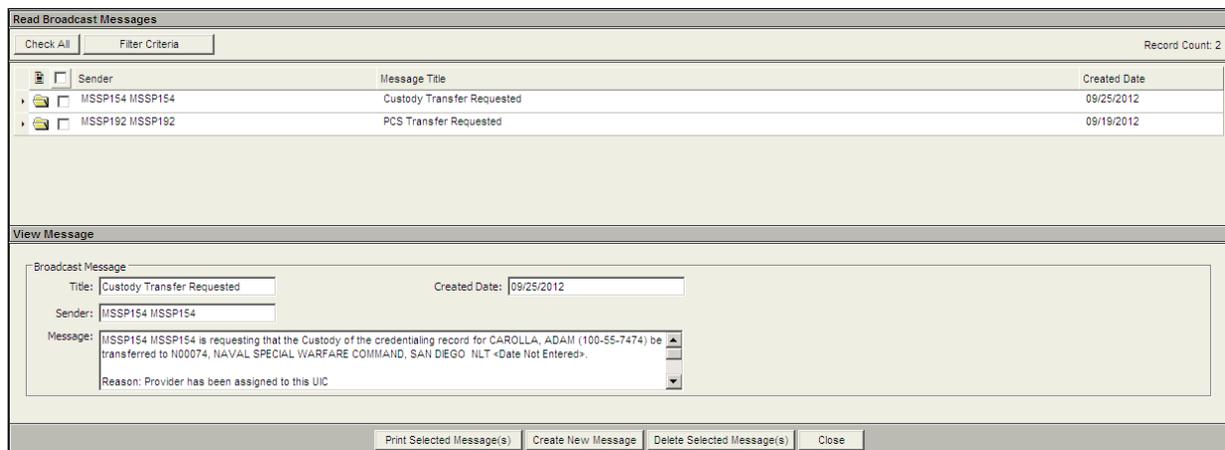


**Figure 365: Broadcast Messages Menu Option**

The **Broadcast Messages** screen opens, as depicted in Figure 366. Unread messages display in the **Read Broadcast Messages** section of the screen. Users have options to **Check All** messages (button), or they can filter these messages by clicking the **Filter Criteria** button. Messages can be filtered in the following manner:

- Message Title
- Read
- Sent From
- Date

The **View Message** section of the screen, depicted in Figure 366, contains the body of the broadcast message. This includes the title of the message, the date the message was created, the sender of the message, and the message itself.



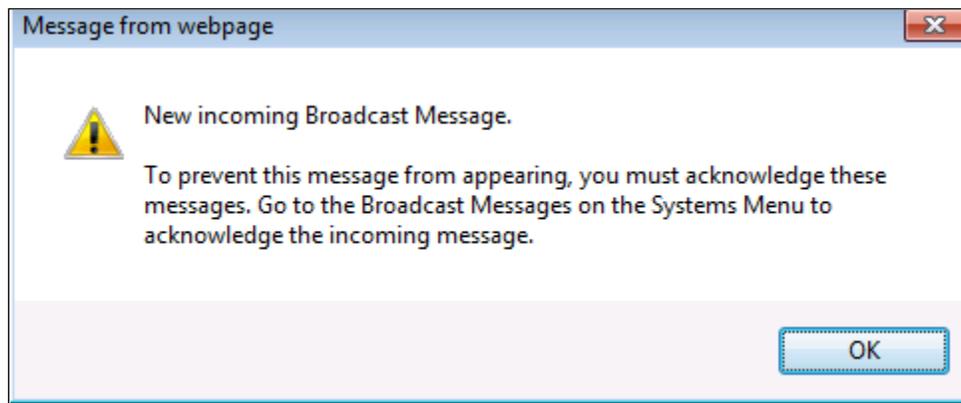
**Figure 366: Broadcast Message Screen**

After CC/MSSP/CMs read the message, they may close it by clicking **Close**, or print it by first clicking the checkbox in the upper portion of the Read Broadcast Messages then clicking **Print Selected Message(s)**, at the bottom of the screen. To delete the message, first click the checkbox in the upper portion of the Read Broadcast Message, then select **Delete Selected Message(s)** at the bottom of the screen.

**Types of Broadcast Messages include:**

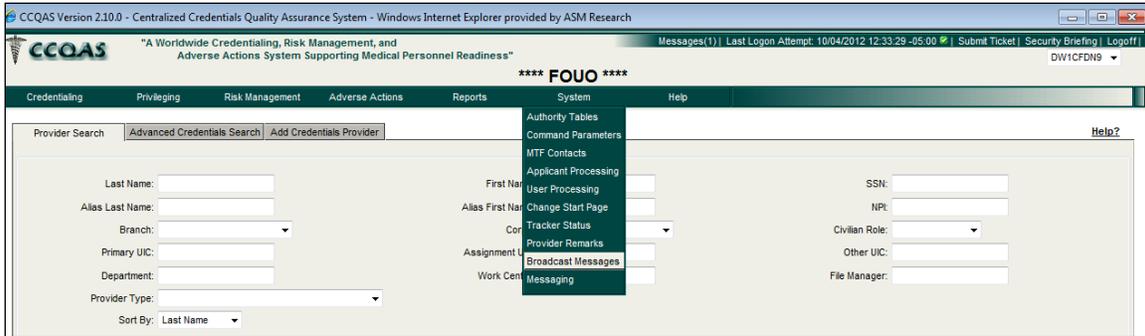
- **ICTB Transfer Requested Broadcast Message** - An automatic notification is sent to the primary CC/MSSP/CM whenever a non-primary UIC performs an ICTB request
- **PCS Transfer Requested Broadcast Message** - An automatic notification is sent to the primary CC/MSSP/CM whenever a non-primary UIC performs an ICTB request
- **Custody Transfer Requested Broadcast Message** - The Broadcast Message for a Custody Transfer includes the name of the requested Provider, the custody NLT date, the reason for custody transfer and POC information of the requesting location.
- **Update of Credentials Requested Broadcast Message** – An automatic notification is sent to the primary CC/MSSP/CM whenever a non-primary UIC uploads a document and requests the primary CC/MSSP/CM take appropriate action
- **Reactivate Account Broadcast Message** – A system message that is sent to the CC/MSSP/CM when a provider account has been deactivated and a provider has an active task that needs to be completed.

### 15.9.1 Incoming Broadcast Messages



**Figure 367: New Incoming Broadcast Message Alert for Sending Location**

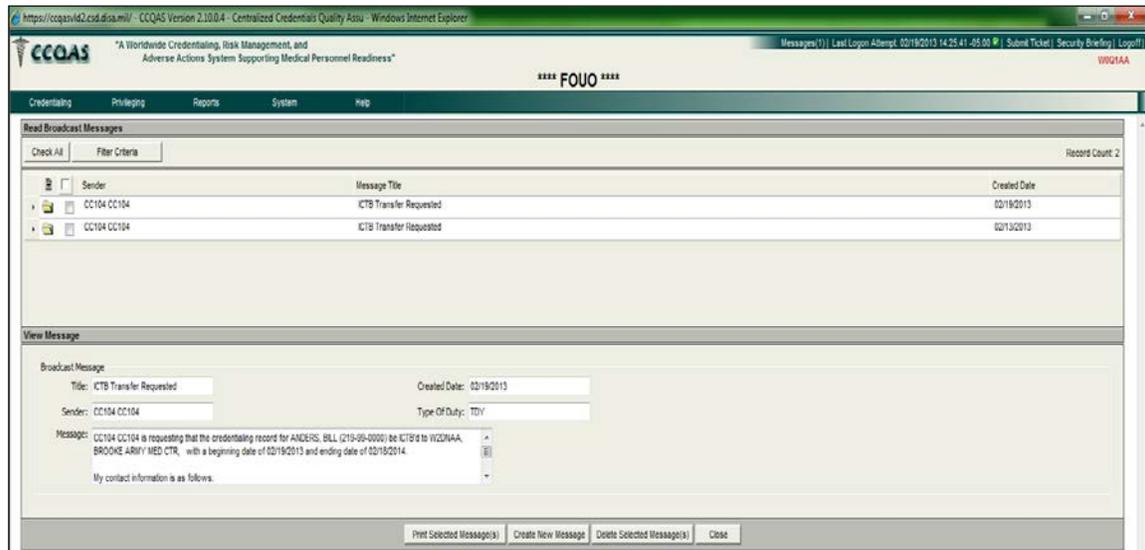
To view incoming messages, select **Broadcast Messages** from the **System** drop-down menu, as depicted in Figure 368 below.



**Figure 368: Broadcast Messages Menu Item at the Sending Location**

An automatic notification is sent to the sending ICTB UIC whenever an ICTB request is entered. Fields include: Title, Created Date, Sender, Type of Duty and Message. Figure 369 below depicts the Broadcast Message screen.

After the CC/MSSP/CM 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 the **Delete Selected Message(s)** button at the bottom of the screen.



**Figure 369: Broadcast Message Menu Item**

**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 limited email functionality within the CCQAS system only.

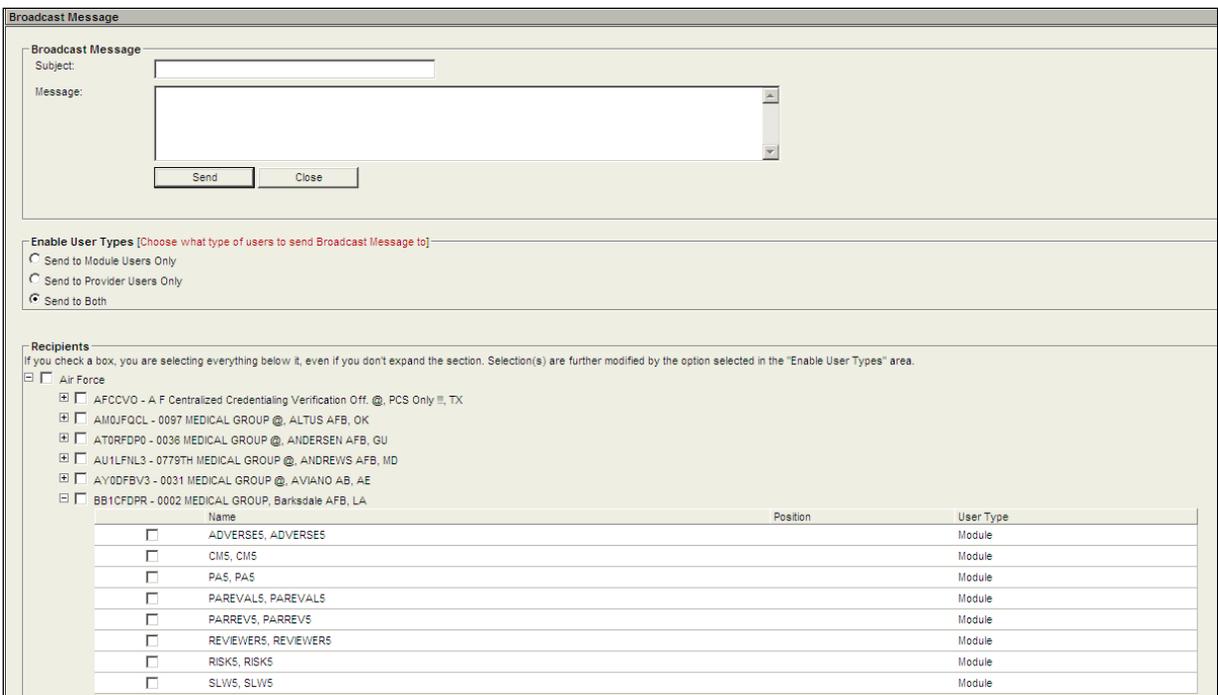
## 15.9.2 Create New Broadcast Message

When users select **Create New Message** at the bottom of the **Broadcast Message** page, a blank message screen appears, as depicted in Figure 370. They fill out the subject and the body of the

message. Users then select which type of users to send the broadcast message to, by selecting one of the **Enable User Types** radio buttons. The available user types are as follows:

- Send to Module Users Only
- Send to Provider Users Only
- Send to Both

Users then select the message recipients by selecting the appropriate **Recipients** check boxes. The list will default to the current user’s service, but can be expanded by clicking the **Plus**  buttons on the left-hand side of the check boxes. The **Plus**  button expands the service list, which allows users to select one or multiple MTFs to receive the message. Users may expand the MTFs further by click the **Plus**  button to select specific users at the UIC. Figure 370 below depicts the **Create Message** page, with the **Recipients** section expanded to the MTF user level.



**Enable User Types** [Choose what type of users to send Broadcast Message to]

Send to Module Users Only  
 Send to Provider Users Only  
 Send to Both

**Recipients**  
 If you check a box, you are selecting everything below it, even if you don't expand the section. Selection(s) are further modified by the option selected in the "Enable User Types" area.

Air Force  
 AFCCVO - A F Centralized Credentialing Verification Off. @, PCS Only III, TX  
 AMQJFQCL - 0097 MEDICAL GROUP @, ALTUS AFB, OK  
 AT0RFDP0 - 0036 MEDICAL GROUP @, ANDERSEN AFB, GU  
 AU1LNL3 - 0779TH MEDICAL GROUP @, ANDREWS AFB, MD  
 AYODFBV3 - 0031 MEDICAL GROUP @, AVIANO AB, AE  
 BB1CFDPR - 0002 MEDICAL GROUP, Barksdale AFB, LA

Name	Position	User Type
<input type="checkbox"/> ADVERSES, ADVERSES		Module
<input type="checkbox"/> CMS, CMS		Module
<input type="checkbox"/> PAS, PAS		Module
<input type="checkbox"/> PAREVALS, PAREVALS		Module
<input type="checkbox"/> PARREVS, PARREVS		Module
<input type="checkbox"/> REVIEWERS, REVIEWERS		Module
<input type="checkbox"/> RISKS, RISKS		Module
<input type="checkbox"/> SLW5, SLW5		Module

**Figure 370: Create Message Page**

**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 limited email functionality within the CCQAS system only.

### 15.9.3 Broadcast Message and Custody Transfers

The Primary UIC receives a broadcast message that another CC/MSSP/CM is requesting the transfer of the Provider’s credentials custody. For more information on broadcast messages, refer to [Section 15](#). The message that the Primary UIC sees includes the following information:

CM28 C28 is requesting that the Custody of the credentialing record for Blue, Carrie (222-11-4444) be transferred to HL0RFC23,15th MEDICAL GROUP, HICKAM AFB NLT 05/07/2013.

*Reason: Provider has been assigned to this UIC*

*My contact information is as follows:*

*Username: CM28*

*Email: email@email.com*

*Phone: (111) 222-3333 (Home)*

*Credentials Coordinator:*

*Name: Cred Coordinator*

*Commercial Phone: (703) 123-4567*

*DSN Phone: 123-4567*

*Fax Phone: (703) 123-0987*

*Email Address: ctest@email.com*

At this point, the request for custody transfer has been made. The Primary UIC now follows the steps in [Section 17.1](#) to initiate the custody transfer to the requesting UIC.

## 15.10 Messaging

When users select the **Messaging** option from the **System** menu, they can then select whether or not to receive email notifications. Figure 371 depicts the **Messaging** menu option.

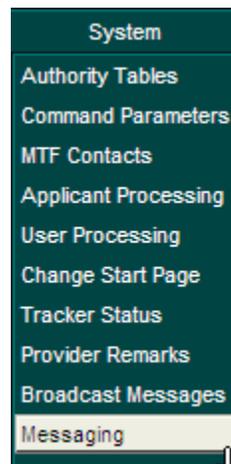


Figure 371: Messaging Menu Option

The **Email Notification** screen opens, where users can select whether or not they would like to receive email notifications by selecting either the **Yes** or **No** radio buttons. If users select **No**, they will no longer receive the Privileging email messages (This option is not recommended for users that do not login to CCQAS on a daily basis). Figure 372 depicts the **Email Notification** screen.

**Note:** If users choose to disable email messages, this does NOT disable broadcast messages.

Credentialing	Privileging	Risk Management	Adverse Actions	Reports	System	Help
Email Notification						
Privileging						
Would you like to receive email notifications? <input checked="" type="radio"/> Yes <input type="radio"/> No						
						Save

**Figure 372: Email Notification Screen**

## 16 Branch Clinic Management

Branch Clinic Management is a new function within CCQAS that allows MTF level users to designate specific UICs as branch clinics to create a hierarchy. MTF 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

Select the **System** menu and, select **MTF Contacts**, which displays all UICS for your service, and then select the MTF UIC, as depicted in Figure 373.

**Note:** CC/MSSP/CMs can then filter by service by selecting the radio button for that service, which is located at the top of the screen.



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 373: MTF Contacts List

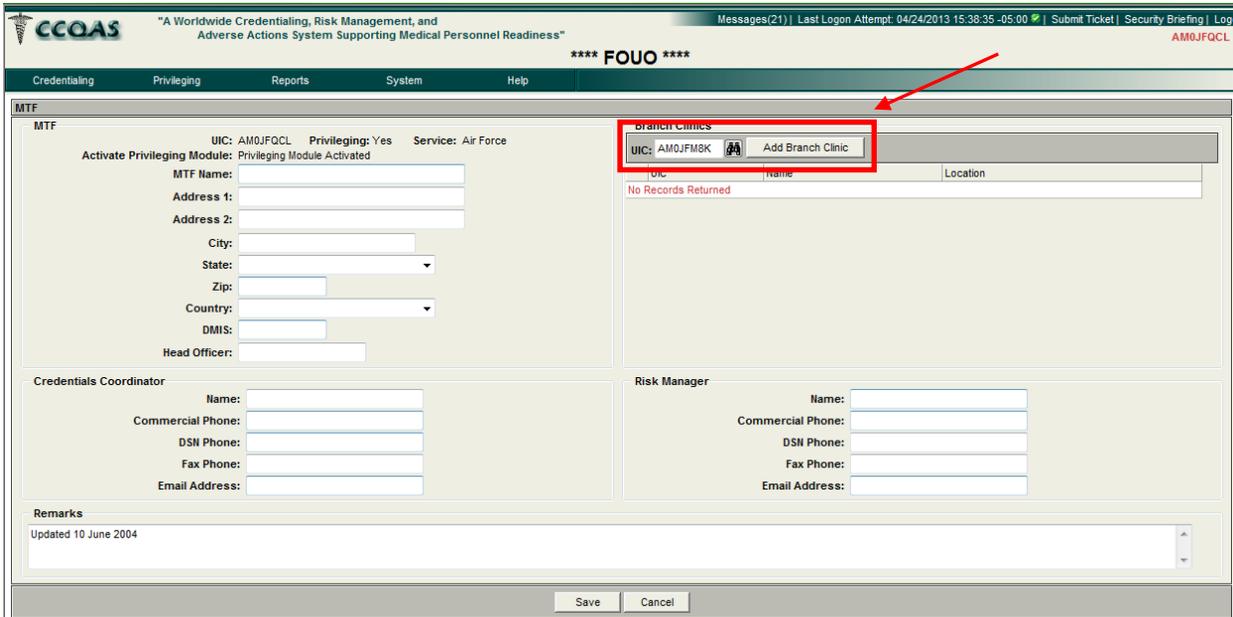
The **MTF** page displays the following sections: **MTF**, **Credentials Coordinator**, **Branch Clinics**, **Risk Manager**, and **Remarks**. To search for a branch clinic, select the **Binoculars** icon, enter the search criteria and click **Search**. **Authorized** users can select the UIC they want to add as a branch clinic, as depicted in Figure 374.

**Note:** At the MTF level you can only alter your own MTF contacts information.

Figure 374: UIC Selection for Branch Clinic

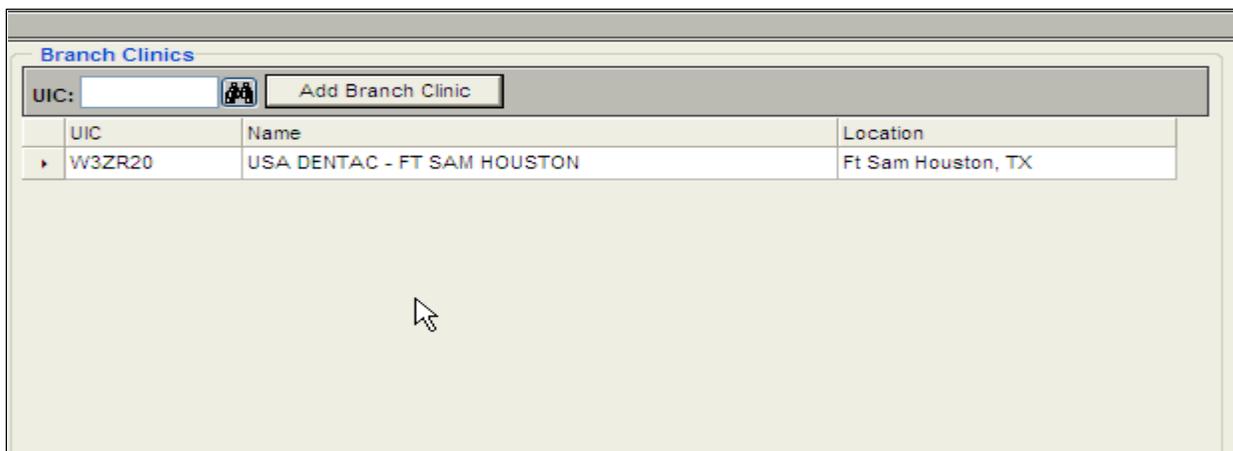


When **authorized** users select the appropriate UIC, it displays in the **UIC** field, as depicted in Figure 375. To add the UIC as a branch clinic, click the **Add Branch Clinic** button.



**Figure 375: Add Branch Clinic**

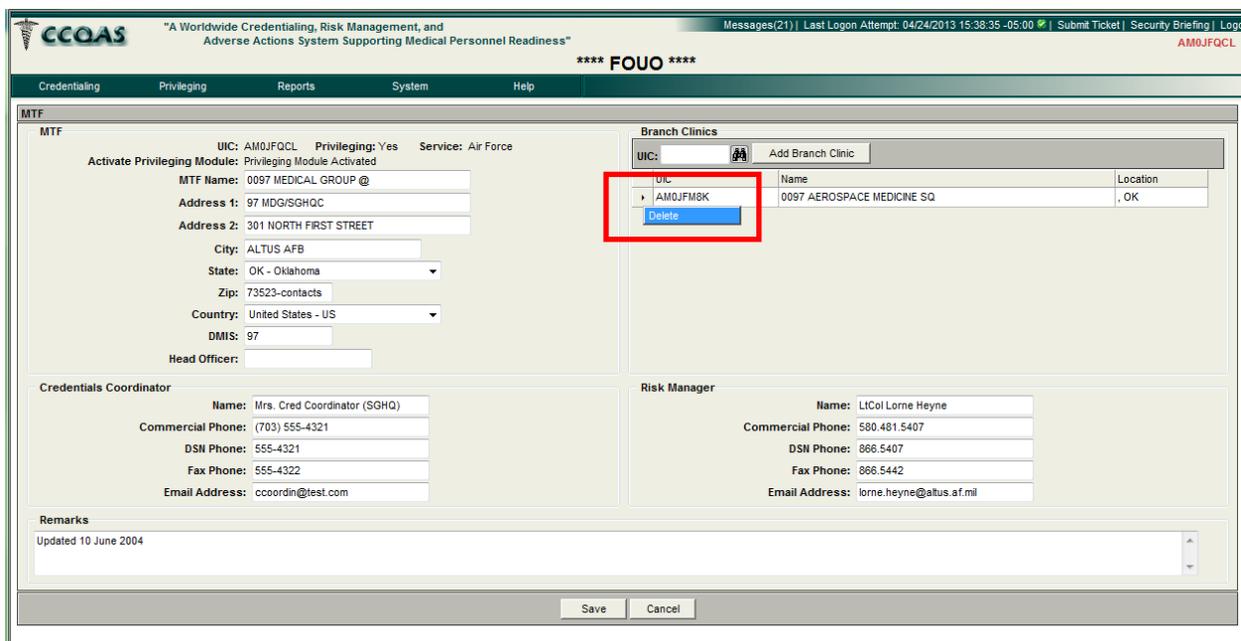
When authorized users click the **Add Branch Clinic** button the new branch clinic displays in the **Branch Clinics** section, as depicted in Figure 376.



**Figure 376: Branch Clinic Record**

**Note:** Authorized users have successfully added a branch clinic to the parent UIC's hierarchy.

Authorized 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 377.



**Figure 377: Delete Branch Clinic**

**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.

## 16.2 Privileging at a Branch Clinic

On the **Position** tab of their electronic application, Providers have the ability to select the parent UIC and/or multiple branch clinics and request privileges not only at the parent UIC, but the corresponding branch UICs.

**Note:** CC/MSSP/CMs must be granted access to Branch Clinic UICs by a Service Level User in order to separately configured each Branch Clinic UIC per the Managing Facility Privilege Lists process in section 4 before providers can request privileges for that Branch Clinic UIC.

Figure 378 depicts a sample Provider's application, which displays parent and branch clinics.

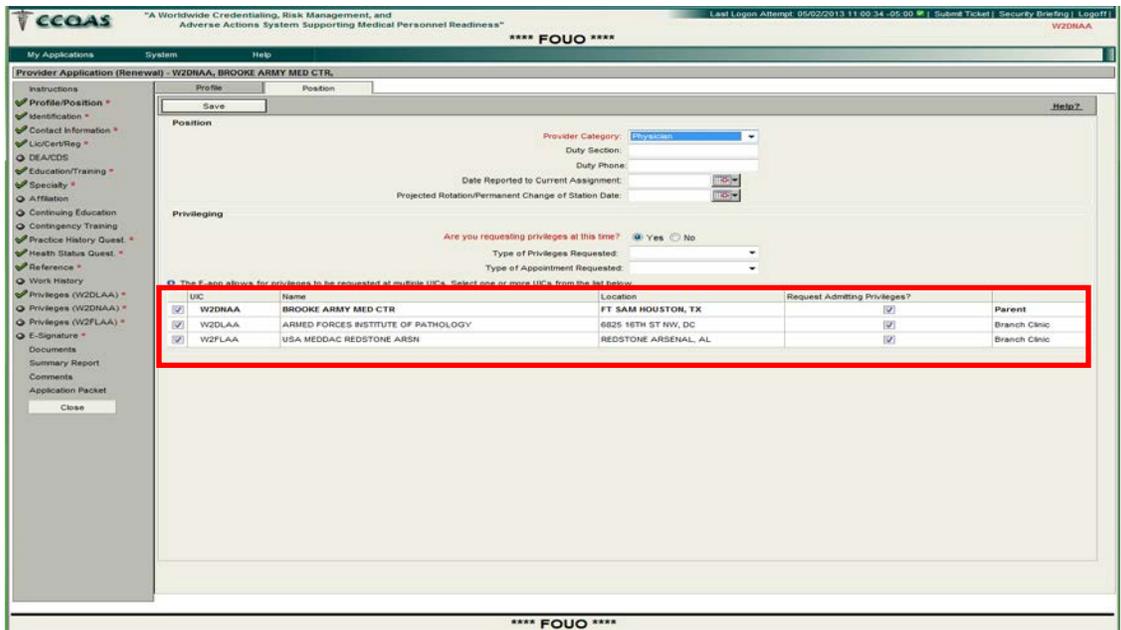


Figure 378: Branch Clinics on 'Position' Tab for Provider E-App

The **Privileges** section for each selected UIC displays on the **Navigation** menu on the left (refer to Figure 379). 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.

**Note:** Level 1 Reviewers must be granted access to the Branch Clinic UICs by a Service Level User before they can be assigned as a Reviewer.

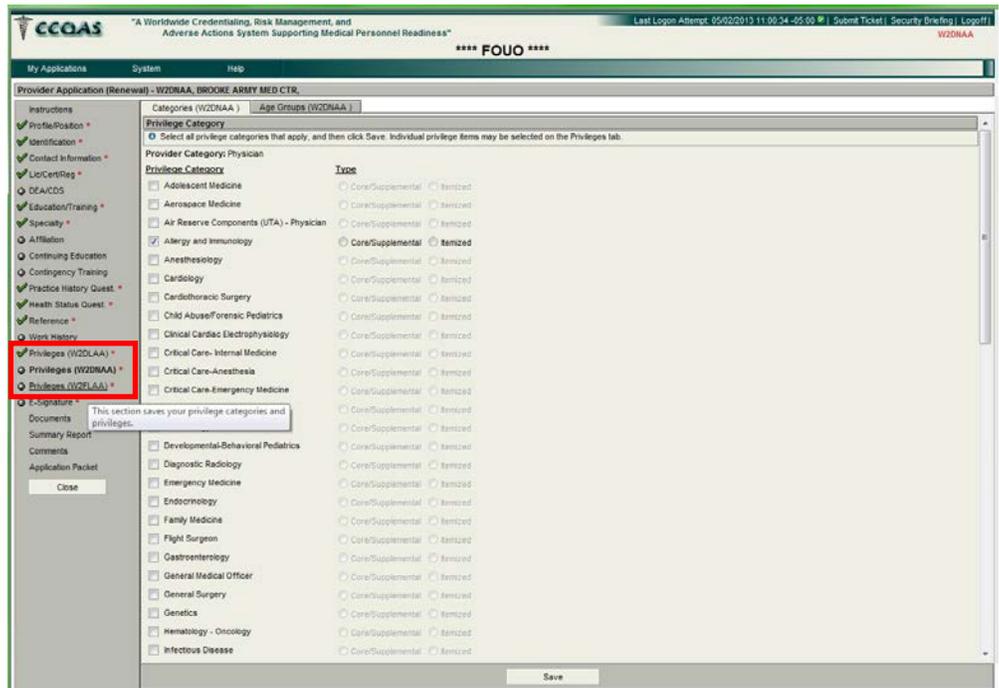


Figure 379: Privileges Section for Branch Clinics

Providers complete and submit their electronic application with requested privileges. The PAC at the parent UIC receives a task notification. After the PSV is completed for the electronic application, the PAC routes it to at least one Level 1 reviewer for each UIC. On the first UIC tab, the levels 2-6 and 5-6 Reviewers/Committee Chairs and the PA are selected once for the entire E-application. Figure 380 and Figure 381 depict the **Routing** page.

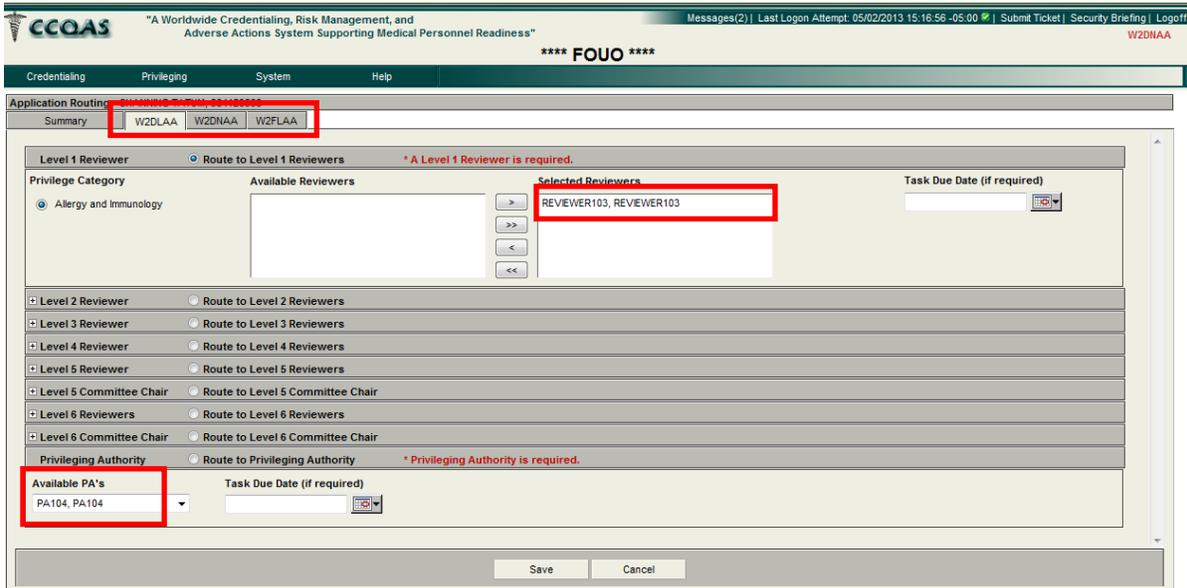


Figure 380: Reviewer Routing Page

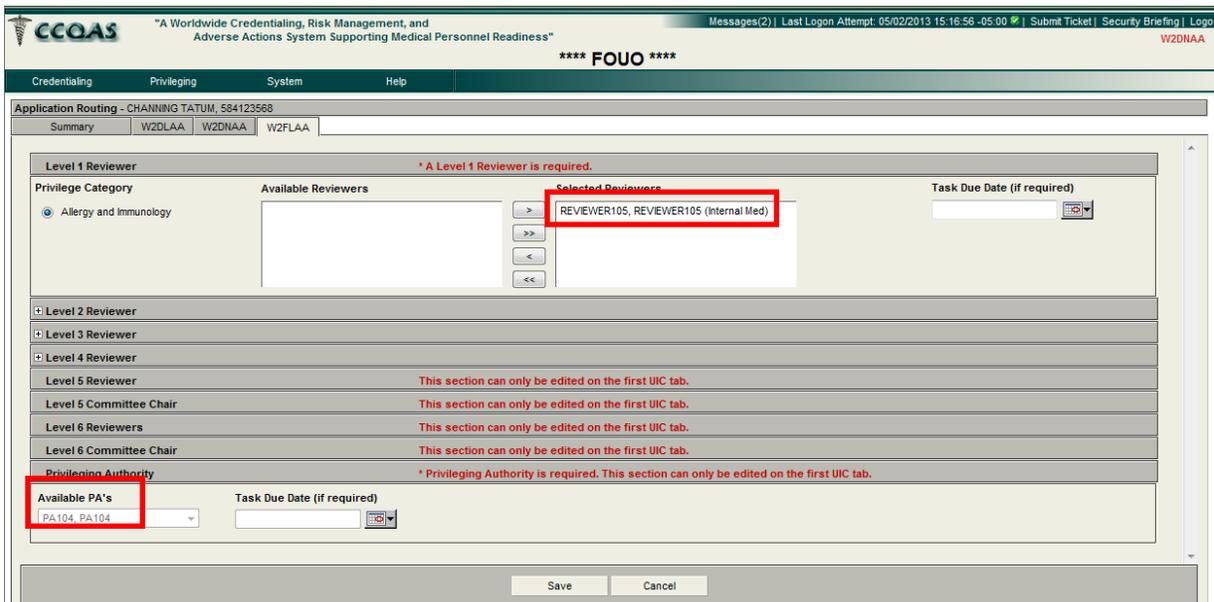


Figure 381: Reviewer Routing Page for Branch Clinic

The PAC can view the summary of the application routing before submitting it. Figure 382 depicts the **Summary** page.

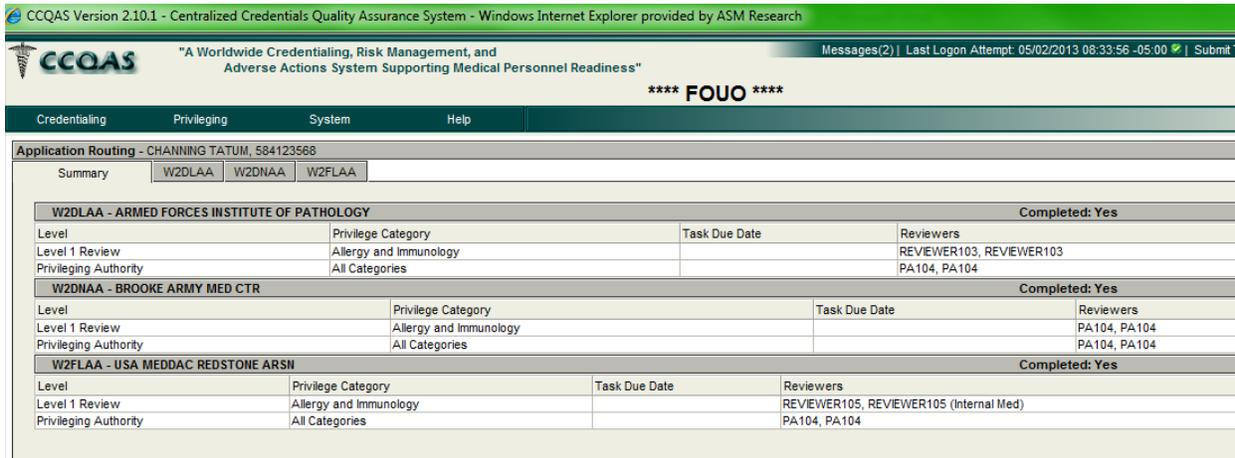


Figure 382: Summary Page for Reviewer Routing

After PACs submit the application for routing, the Reviewers can view new tasks in their Work List. The Branch Clinic Reviewers can only see the privileges that the Provider requested at that Branch Clinic. 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 383.

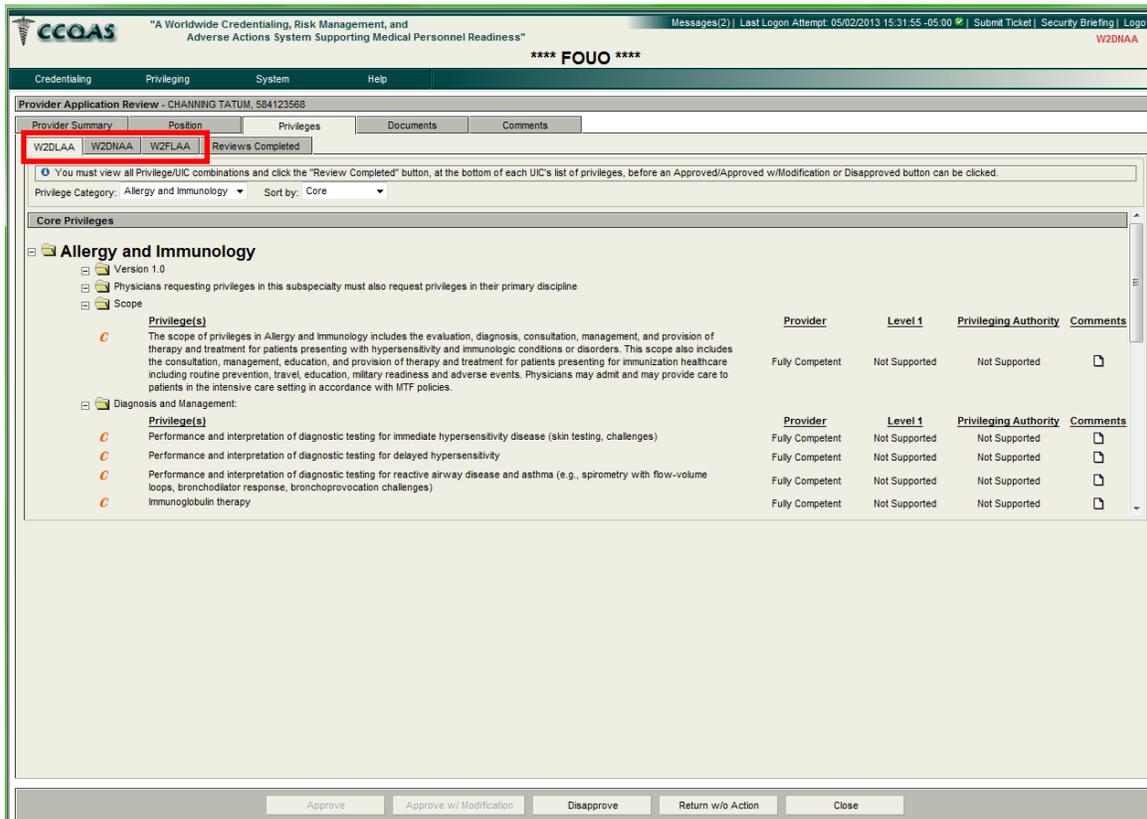
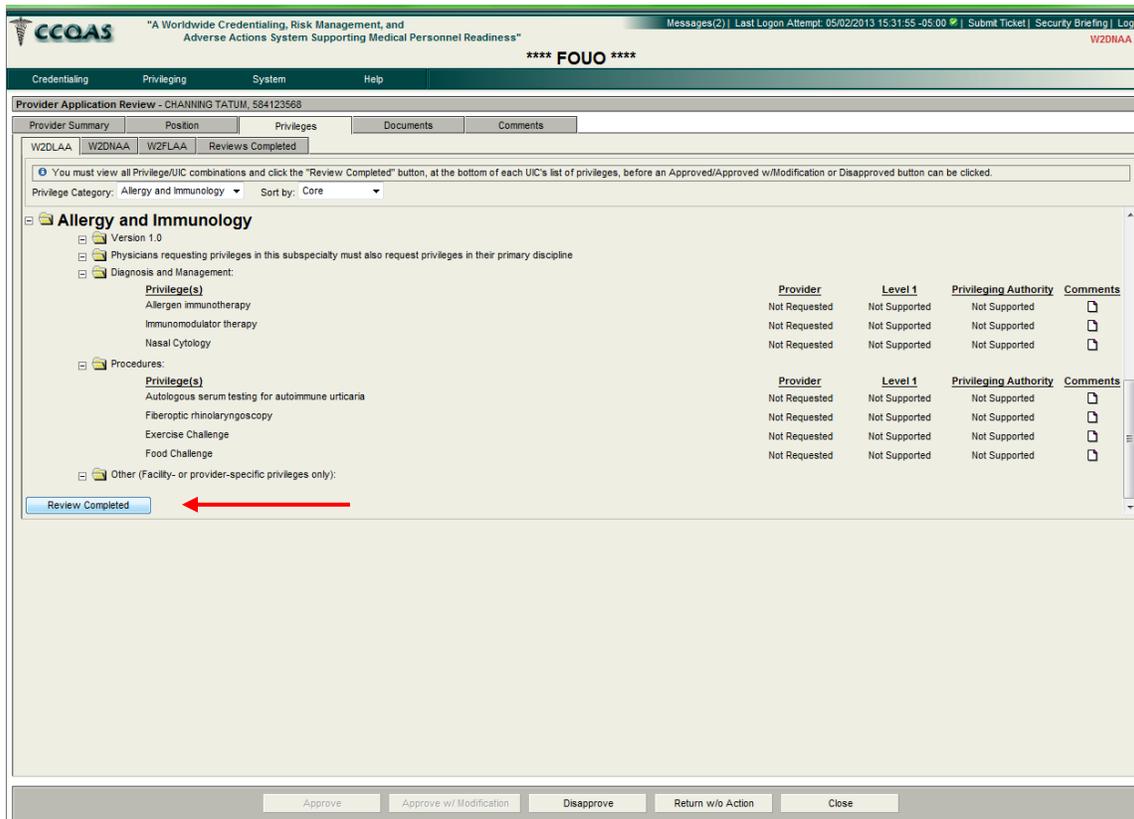


Figure 383: PA Review of Privileges for Parent/Branch Clinics

After PAs review all privileges for each UICs, they must click the **Review Complete** button for each UIC the provider is requesting privileges, before they are able to proceed. The arrow in Figure 384 shows the Review Complete button, which is located at the bottom of the privilege list.



**Figure 384: PA Decision Review Complete Screen**

On the Reviews Completed tab, PAs must confirm each box is checked, indicating the privileges for each UIC have been reviewed, before approving the application. After all boxes are confirmed checked, the PA clicks either the **Approve** or **Approve with Modification** button at the bottom of the page, as depicted in Figure 385.

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.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" Messages(2) | Last Logon Attempt: 05/02/2013 15:31:55 -05:00 | Submit Ticket | Security Briefing | Logout  
 \*\*\*\* FOUO \*\*\*\* WZDNAA

Credentialing Privileging System Help

Provider Application Review - CHANNING TATUM, 584123568

Provider Summary Position Privileges Documents Comments

WZDLAA WZDNAA WZFLAA Reviews Completed

You must complete the review of all UIC(s) before an Application can be Approved/Approved w/Modification or Disapproved.

reviewed	UIC	Name	Completed Date	By
<input checked="" type="checkbox"/>	W2DLAA	ARMED FORCES INSTITUTE OF PATHOLOGY	05/02/2013	PA104
<input checked="" type="checkbox"/>	W2DNAA	BROOKE ARMY MED CTR	05/02/2013	PA104
<input checked="" type="checkbox"/>	W2FLAA	USA MEDDAC REDSTONE ARSN	05/02/2013	PA104

Approve Approve w/ Modification Disapprove Return w/o Action Close

**Figure 385: PA Decision Screen**

## 17 Custody Transfer

This section outlines the various ways to perform a custody transfer. Providers can have multiple assignments, but only one UIC, their Primary UIC, has custody of the Provider's credentials record.

The Primary UIC is the only UIC that owns the CCQAS Cred record and the only UIC that can directly edit a Provider's CCQAS Cred record.

**Note:** Business rules will dictate custody and custody transfers in accordance with Tri-Service/Service policy.

### 17.1 Custody Transfer without PCS

#### 17.1.1 Initiate Custody Transfer (Primary UIC)

**Note:** Custody transfer can also be accomplished via PCS, refer to [Section 9](#)

When the CC/MSSP/CM at a Provider's primary UIC wants to transfer custody for the credentials record only, he or she can do this by selecting the **Initiate Custody Transfer**. To perform this action, the CC/MSSP/CM runs a credentials search to locate the Provider for whom he or she would like to transfer custody. After the Provider is identified, the CC/MSSP/CM selects **Initiate Custody Transfer** from the hidden menu, as depicted in Figure 386 below.

Name	SSN	Primary UIC	Start Date	Branch	Corps	Status	Cred Status	NPI	Active Assignments
AHL, KENYA	923-92-3923	CL1LFC0F	03/05/2013			CV	Active		1
AIKN, JOHN	101-02-0123	CL1LFC0F	10/10/2012			Dual	Active		2
BANDER, XANDER	111-22-8686	CL1LFC0F	09/08/2012			CV	Active		2
Balk, Lucile	000-12-3456	CL1LFC0F	09/18/2012	F11	MC	Dual	Active		2
Banderz, Xander	222-11-8686	CL1LFC0F	09/08/2012			CV	Active		1
Banderz, Xander	222-11-8686	CL1LFC0F	09/08/2012			CV	Active		1
Blue, Carrie	222-11-4444	CL1LFC0F	02/05/2013	P11	MO	Dual	Active		3
Bunny, Easter	231-74-3333	CL1LFC0F	09/17/2012	F11	MC	Dual	Active		2
Bunny, Benjamin	555-66-4444	CL1LFC0F	08/28/2012			MIL	Active		1
CAROLLA, ADA	204-15-1515	CL1LFC0F	04/09/2013	F11	DC	MIL	Active		1
COLLAZO, LUC	598-14-2200	N00183	03/05/2013	N11	MC	MIL	Active		1
DAYE, BETH	000-00-0168	CL1LFC0F	02/05/2013	N11	MC	MIL	Active		1
DONOTTOUCH, Letters	326-97-2496	CL1LFC0F	02/05/2013			CV	Active		1
DUCK, DAFFY	222-33-4455	CL1LFC0F	02/05/2013	N11	MC	CV	Active		1
Duck, Donald	231-74-0004	CL1LFC0F	08/27/2012			MIL	Active		1
EVERDEEN, KATNISS	100-25-2525	CL1LFC0F	05/01/2013			CV	Active		1
FROG, GREEN	000-12-8765	CL1LFC0F	01/29/2013	A11	MC	MIL	Active		1

Figure 386: Initiate Custody Transfer Option from Hidden Menu

The Initiate Custody Transfer screen appears, as depicted in Figure 387

Initiate Custody Transfer for CAROLLA, ADAM

Transfer Record To: CO0JFSR1 Effective Date: 5/6/2013

Transfer Reason: Provider has been assigned to this UIC

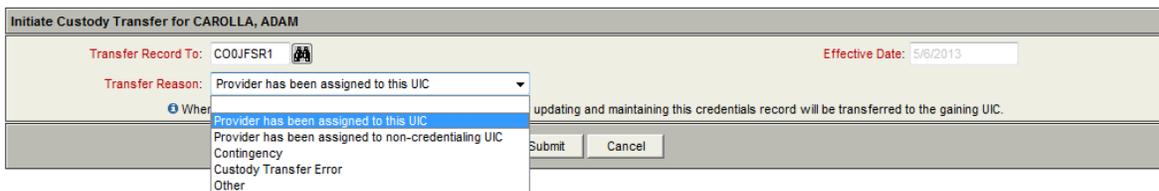
Submit Cancel

Figure 387 below. Select the UIC to transfer custody to and the reason for the custody transfer. The date for the initiate custody transfer function automatically sets to the date of the initiation. This date is NOT editable.

**Note:** Custody Transfer by itself DOES NOT:

- End Assignment at Transferring UIC
- End Privileges at Transferring UIC
- Create Assignment at new Custodial UIC
- Initiate an E-App at new Custodial UIC

**Note:** Custodial Transfer allows new Custodial UIC to change provider profile page when new assignment is created.



**Figure 387: Initiate Custody Transfer Screen**

**Note:** Custodial Transfer CANNOT be cancelled, the gaining UIC must be contacted and custody must be transferred back to previous owner. (For cancelling PCS's, refer to [section 9.8](#)) After CC/MSSP/CM clicks **Submit**, a confirmation message for the transfer displays, as depicted in Figure 388 below. Click **Cancel** to return to the **Custody Transfer** page, or click **OK** to submit the transfer.



**Figure 388: Custody Transfer Confirmations**

After custody is transferred, the appropriate gaining UIC receives a new entry in the Transaction Table as depicted in Figure 389. This entry informs the gaining UIC that a custody transfer to their facility has been initiated.

The screenshot shows the CCQAS interface with the following details:

- Header:** CCQAS logo, "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness", Last Logon Attempt: 05/06/2013 13:40:22 -05:00, Submit Ticket, Security Briefing, Logout, and user ID COUJFSR1.
- Navigation:** Credentiaing, Privileging, Reports, System, Help.
- Security:** \*\*\*\* FOUO \*\*\*\*
- Provider Transactions Section:**
  - Direction:**  Incoming,  Outgoing,  Primary MTF.
  - Status:**  Unacknowledged,  Acknowledged,  Both.
  - Action:**  PCS,  Update of Credentials Requested,  Non-Primary Assignment Created,  Custody Transfer,  ICTB,  All.
- Transaction Table:**

Acknowledged	From MTF	To MTF	Primary MTF	Action	Initiated	Provider Name	SSN	Sender's Name	Sender's Phone
<input checked="" type="checkbox"/>	CL1LFC0F	CO0JFSR1	CO0JFSR1	Custody Transfer	05/06/2013	ADAM CAROLLA	204-15-1515	Mickey Mouse	(703) 123-9876
- Footer:** Search, Save, Close buttons and a note: \*Results showing last 6 months of history

**Figure 389: Custody Transfer in Provider Transaction**

At this point, custody of the record has been transferred. The new Primary CC/MSSP/CM can now search for and update/edit the record.

### 17.1.2 Request Custody Transfer

**NOTE:** If there are questions about Custody transfers between services, contact your service representative.

When a non-primary facility needs access to a Provider's credentials record for updates/editing, the non-primary CC/MSSP/CM can request a custody transfer from the primary UIC. The non-primary CC/MSSP/CM would perform a Provider search via the Provider Locator function, and identify the Provider he or she would like to request a transfer for. The non-primary CC/MSSP/CM would then select **Request Custody Transfer** from the Provider's hidden menu, as depicted in Figure 390 below.

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness" <span style="float: right;">Message</span>									
**** FOUO ****									
Credentialing		Privileging		Reports		System		Help	
Provider Search		Advanced Credentials Search		Search Results		Add Credentials Provider			
▶	AHL, KENYA	923-92-3923	CL1LFC0F	03/05/2013			CIV	Active	628 MEDICAL
▶	AKIN, JOHN	101-02-0123	CL1LFC0F	10/10/2012			Dual	Active	628 MEDICAL
▶	BANDER, XANDER	111-22-6666	CL1LFC0F	09/26/2012			CIV	Active	628 MEDICAL
▶	Ball, Lucille	000-12-3456	CL1LFC0F	09/16/2012	F11	MC	Dual	Active	628 MEDICAL
▶	Banderz, Xander	222-11-6666	CL1LFC0F	09/06/2012			CIV	Active	628 MEDICAL
▶	Banderz, Xander	222-11-6666	CL1LFC0F	09/06/2012			CIV	Active	628 MEDICAL
▶	Blue, Carrie	222-11-4444	CL1LFC0F	02/05/2013	P11	MO	Dual	Active	628 MEDICAL
▶	Bunny, Bernice	5-66-4444	CL1LFC0F	08/28/2012			MIL	Active	628 MEDICAL
▶	Bunny, Easton	1-74-3333	CL1LFC0F	09/17/2012	F11	MC	Dual	Active	628 MEDICAL
▶	DAYE, BETTY	0-00-0168	CL1LFC0F	02/05/2013	N11	MC	MIL	Active	628 MEDICAL
▶	DONOTTOLO, JAMES	5-97-2496	CL1LFC0F	02/05/2013			CIV	Active	628 MEDICAL
▶	DUCK, DAVID	2-33-4455	CL1LFC0F	02/05/2013	N11	MC	CIV	Active	628 MEDICAL
▶	Duck, Donald	231-74-0004	CL1LFC0F	08/27/2012			MIL	Active	628 MEDICAL
▶	EVERDEEN, KATNISS	100-25-2525	CL1LFC0F	05/01/2013			CIV	Active	628 MEDICAL
▶	FROG, GREEN	000-12-8765	CL1LFC0F	01/29/2013	A11	MC	MIL	Active	628 MEDICAL
▶	Hokie, VATECH	222-34-1234	CL1LFC0F	09/15/2012	F11	MC	CIV	Active	628 MEDICAL
▶	Huxtable, Heathcliff	444-55-4444	CL1LFC0F	09/21/2012			CIV	Active	628 MEDICAL

Figure 390: Request Custody Transfer Option in Hidden Menu

The **Request Custody Transfer** screen displays, as depicted in Figure 391 below. The CC/MSSP/CM sets the custody NLT date for the transfer. The date defaults to today's date, but it is editable for future dates. The CC/MSSP/CM then selects a reason for the transfer. The requestor's email address is filled in automatically, but he or she must include a phone number. The CC/MSSP/CM can review the message, but the message body is NOT editable.

**Broadcast Message to CL1LFC0F**

Subject: Custody Transfer Requested

Custody NLT Date: 05/07/2013

Reason: Provider has been assigned to this UIC

Requester's Email: email@email.com

Requester's Phone: (540) 373-2020

Message Preview: CM28 CM28 is requesting that the Custody of the credentialing record for Blue, Carrie (222-11-4444) be transferred to HLORFC23, 15th MEDICAL GROUP, HICKAM AFB NLT 05/07/2013.

Reason: Provider has been assigned to this UIC

My contact information is as follows:  
 Username: CM28  
 Email: email@email.com  
 Phone: (111) 222-3333 (Home)

Credentials Coordinator:  
 Name: Cred Coordinator  
 Commercial Phone: (703) 123-4567  
 DSN Phone: 123-4567  
 Fax Phone: (703) 123-0987  
 Email Address: ctest@email.com

Figure 391: Request Custody Transfer Broadcast Message Screen

Click **Close** to return to the search page, or click **Send** to send the request. After the CC/MSSP/CM clicks **Send**, a confirmation message displays (refer to Figure 392 below), which indicates that the request has been sent. Click **OK** to close confirmation message dialog box.



**Figure 392: Confirmation Message**

## 17.2 Custody Transfer with PCS

A Provider's Primary UIC can also transfer custody with a PCS via the **Initiate PCS** function. This function is outlined in [Section 9](#).

## Appendix A. Frequently Asked Questions (FAQs)

**Q: Can I future date a PCS with outstanding ICTBs? ([CC/MSSP/CM, 9](#))**

A: Yes, as long as the ICTBs end on or prior to the PCS Effective Date.

-----

**Q: The “PA Review Complete” snapshot is missing, why? ([CC/MSSP/CM, 6](#))**

A: Sometimes due to system latency or other technical problems a PDF snapshot may not generate. If you are missing a snapshot contact your Service CCQAS DBA to report the problem and to re-generate the snapshot.

-----

**Q: One of my e-Apps disappeared after the Complete PSV task was completed, why? ([CC/MSSP/CM, 5](#))**

A: To verify the current location of the e-App, go to the Submitted Applications tab and select View Task Log/Comment. If the e-App is in a closed status, the reason is probably because the provider failed to request privileges and complete privilege lists. This can be verified by reviewing the PSV Complete snapshot and/or reviewing closed CCQAS tasks for the e-App in question.

-----

**Q: My Privileging Authority doesn't have an <Approve> button, why? ([PA, 5](#))**

A: The Privileging Authority must select the <Review Completed> button at the bottom of the Privileges tab in order to activate the Approval buttons at the bottom of the screen.

-----

**Q: How do I submit an e-App for Routing? ([CC/MSSP/CM, 5](#))**

A: Once all the Reviewer(s) and the Privileging Authority have been selected and saved for all Privilege Categories on all UIC tabs, select the Summary tab, review and click the <Submit> button.

-----

**Q: I have a contractor who is back after their credentials Record was inactivated last fall when the prior contract ended. I've reactivated the credentials Record but don't know how to initiate an e-App. ([CC/MSSP/CM, 6](#))**

A: Look-up the provider using Provider Search, go to the Work History, Assignment tab and select “Initiate Application” from the hidden action menu to the left of your UIC. If there is no current Assignment at your facility, select the <Add Assignment> button to add a new Assignment and then select “Initiate Application” from the hidden action menu.

-----

**Q: How do I request a Transfer Brief? ([CC/MSSP/CM, 8](#))**

A: Look-up the provider using Provider Locator, go to the Work History, Assignments tab and select “Request ICTB” from the hidden action menu of the current CRED Assignment. This will

send a Broadcast Message. Remember that not all facilities frequent System>Broadcast Messages so if no response don't hesitate to call the Assignment UIC.

-----

**Q: How can I correct the Type of Appointment from “Initial-Active” to “Active” after the e-App has been approved? ([CC/MSSP/CM, 6](#))**

**A:** Look-up the provider using Provider Search, go to the Work History, Assignments tab and open the current Assignment at your facility. Next, select the Privileges tab and update the Type of Appointment and save. CCQAS will prompt the CC/CM/MSSP to enter a reason for the update and a new “appended” PA Review Complete snapshot will automatically generate.

-----

**Q: Provider is completing an e-App and cannot get the green check for the Contact Information section, why? ([Provider, 5](#) or [CC/MSSP/CM, 6](#))**

**A:** The e-App requires that a primary, Home address be entered. BTW: Both the Home and Local Work Address can be designated as Primary.

-----

**Q: I've tried re-routing an e-App five times and it always goes back to the L5 Committee Chair when I need it to go to the L1 Reviewer, why? ([CC/MSSP/CM, 5](#))**

**A:** After selecting the <Routing> button, go to the UIC tab and review the “Route to” radio buttons in the gray separators between Reviewer types. When re-routing the e-App will begin the routing process at the level with the radio button selected.

-----

**Q: I received a Custody Transfer from another facility but I don't have a current Assignment, why? ([CC/MSSP/CM, 9](#))**

**A:** The losing facility must have meant to Initiate a PCS and did a Custody Transfer instead. Contact the losing facility and request that they go to the Work History, Assignment tab and initiate a PCS from the CRED Assignment at their facility.

-----

**Q: How can I make CCQAS screen resolution larger? ([CCQAS User, 1](#))**

**A:** Press the <Ctrl> button and the mouse scroll up for larger and scroll down for smaller or Press the <Ctrl> button with the + (plus) sign to make it larger or the – (minus) sign to make it smaller.

-----

**Q: How can I retrieve an e-App from the L1 Reviewer? ([CC/MSSP/CM, 5](#))**

**A:** On the Work List tab, look to the right where there is a radio button selected to the left of “Module User” and your name. From the drop-down, select the L1 Reviewer and open the e-App to be retrieved. At the bottom of the screen select the <Return w/out Action> button, enter comment and <Submit>. e-App will be returned to the Responsible CC/CM/MSSP.

-----

**Q: How do you know if a provider selected Core or Itemized privileges? ([CC/MSSP/CM, 5](#))**

A: If you open the e-App and the filter is set to “Core” or if all the privileges are listed with “Core” first and then Itemized, then the provider has selected Core Privileges.

-----

**Q: Provider can't submit the e-App and it says the problem is in Contact Information? ([Provider, 5](#))**

A: Make sure all fields are filled in and that the provider has a primary home address, phone, and email.

-----

**Q: Why didn't the “Transaction Table” generate an e-App for the provider after I checked it in? ([CC/MSSP/CM, 6](#))**

A: The “Transaction Table” is only a tracking mechanism to let you know of incoming and outbound actions and has no other purpose then supply a notice.

-----

**Q: The providers showing on my transaction table but the ICTB was canceled, do I check him in or just let it go? ([CC/MSSP/CM, 6](#))**

A: The “Transaction Table” is only a tracking mechanism to let you know of incoming and outbound actions and has no other purpose then supply a notice.

-----

**Q: How do I find an e-App and figure out who has it? ([CC/MSSP/CM, 5](#))**

A: Go to the “Submitted Applications” tab off your work list, find the providers name and double click on it. The “View Task/Comments” screen will come up and look to see who has the “OPEN” Task. The “View Task/Comments” is also available via the “My Applications” tab.

-----

**Q: Can I use my MAC computer to do CCQAS? ([CCQAS User, 1](#))**

A: CCQAS is only compatible with IE6 –IE8, anything else being used will not work properly. Recommended that CCQAS users only use PC based computers.

-----

**Q: I sent a provider on an ICTB to the “DEPLOYED” UIC and they did not receive and e-App, why? ([CC/MSSP/CM, 8](#))**

A: An e-App will only generate if you are doing an ICTB or PCS to a “Privileging UIC” and you can see if the UIC is a privileging from the System > MTF Contacts.

-----

**Q: Do I need to do a “Custody Transfer” for a provider that I deactivate the credentials from my UIC? ([CC/MSSP/CM, 6](#))**

A: No, if the credentials record is reactivated in the future CCQAS will automatically assign the ownership of the credentials to the UIC reactivating it.

-----

**Q: Why can't I see the ECFMG when I PSV the e-App? ([CC/MSSP/CM, 5](#))**

**A:** The ECFMG is not visible during the PSV for the e-App; it is PSVed in the credentials record and recorded for the Qualifying Degree in the e-App.

-----

**Q: Why does my print e-App snapshot have "Pending" on the privileges in the Commander's section and no Commander's signature? ([CC/MSSP/CM, 6](#))**

**A:** You have not printed the "PA Review Complete" snapshot

-----

**Q: My Reviewer has a task on their work list but they can't see it? ([Reviewer, 3](#))**

**A:** Verify Reviewer is in the correct UIC, check their permissions to be sure they have Privileging Module and Reviewer set to Yes.

-----

**Q: Why can't my provider, who is also Reviewer, see his own application? ([Provider, 5](#))**

**A:** Have Providers who are also Reviewers click on "My Applications" to access their own application.

-----

**Q: Why can't I update my provider's credential record (it is all grayed out)? ([CC/MSSP/CM, 6](#))**

**A:** Check the Primary UIC listed at the top of the credentials record, if it is not your UIC, you can only update credentials via the documents section.

-----

**Q: Where do we go now to issue an ICTB or an e-application? ([CC/MSSP/CM, 8](#))**

**A:** ICTBs or e-apps are initiated from hidden menu of options for your UIC in the Work History section of the credentials record.

-----

**Q: Is there a paper application somewhere in CCQAS that I can print for individuals (specifically contractors) who are new to the government (who do not have a CCQAS file)? ([CC/MSSP/CM, 13](#))**

**A:** Yes there is, go to Reports > Standard > Credentialing and select the Blank Privilege Application Form. Then select Provider Category then however many Privilege Categories you want to include in the application then click the Submit button.

-----

**Q: Where are the age groups located on e-applications (i.e. Renewals, Modifications)? ([CC/MSSP/CM, 5](#))**

**A:** Age groups are located in the Position tab of the e-app 2/3 of the way down on the screen. Additionally, Age Groups can be found on Section XII (Clinical Privileges Requested) of the PDF snapshot of the e-app.

-----

**Q: Where are the age groups located on e-applications (i.e. Renewals, Modifications)?** ([Provider, 5](#))

**A:** Age groups are location in a tab off of the Privilege Category Selection.

-----

**Q: How do I add an assignment to a credentials record?** ([CC/MSSP/CM, 6](#))

**A:** Steps to create an assignment at your UIC:

- (1) Select Credentialing > Provider Search
  - (2) Enter providers name or SSN
  - (3) Select the radio button for "Provider Locator" in the Search Type
  - (4) Click search
  - (5) Once the screen refreshes with the provider:
    - (a) Select Assignment from the hidden menu > this now takes you to the Assignment screen of the credentials record but you cannot view anything until you add an assignment.
  - (6) On the Assignments tab:
    - (a) Click the "Add Assignment" button and complete the information where there is red text. Then click save
  - (7) Now you have access to the credentials record and documents or you can issue an e-app for the provider to complete.
- 

**Q: Is it possible to select "Not Supported" on a privilege in one privilege category but then the same privilege can be "Supported" on another privilege category?** ([CC/MSSP/CM with CLP Administrator Role, 4](#))

**A:** Yes, privilege categories are independent of each other and are based on what your facility can support.

-----

**Q: Users getting the "FILE MUST BE LESS THAN 5MB" error.** ([CC/MSSP/CM, Provider, 6](#))

**A:** This error can be because the file being uploaded exceeds the 5MB limit or the naming of the file does not follow Microsoft file extension naming convention. I.e. a document with the following name will produce the 5MB error **Dr. Martin PAR.pdf**. The error is produced because of the ". (dot)" after the Dr. If you re-name it to Dr Martin PAR.pdf the system will accept it and upload the document.

-----

**Q: One of my providers could not sign the e-app after requesting modification of current privileges. When she clicks on SAVE, The system tells her the contact information is incorrect and prevents her for e-signing the application. When she reviews it the contact information appears to be correct.** ([CC/MSSP/CM, Provider, 5](#))

**A:** The Home address must be set as primary in order for the contact information to be considered complete.

-----

**Q: The Internal Medicine Department at my facility has just obtained some new instrumentation that now supports the performance of several new procedures. Several of our providers have requested privileges to perform this procedure in the past, but have not received the requested privileges, since the facility did not support the procedure. Now that our facility can support the procedure, what should I do? ([CC/MSSP/CM, Provider, 4 and 5](#))**

**A:** You can go to the Privileging main menu in CCQAS and click on “Privilege Management”. When the MTF Privilege Management screen is returned, select the privilege category of Internal Medicine from the Privilege Category drop-down list. When the list is displayed, you can change the support designation of those particular privilege items by changing from the “Not Supported” radio button to the “Supported” button, and then click <Save>. The privilege has now been designated as “Supported” and your providers may request the new privilege using a modification application.

-----

**Q: I am a credentials staff member who uses CCQAS every day. Since I check my work list frequently as part of my daily activities, I do not need the email notifications that are filling up my email inbox. Is there any way I can turn my email notifications off? ([CC/MSSP/CM, 15](#))**

**A:** Yes, the notification feature may be turned off for any CCQAS user assigned to the CC/MSSP/CM role by clicking on the System main menu, and selecting “Messaging”, then “Email Notifications”, then follow the instructions on the screen.

-----

**Q: 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? ([CC/MSSP/CM, Provider, 7](#))**

**A:** Contact the CC/MSSP/CM and request that the application be terminated. If the request to terminate the application is not done, after a period of 90 days, the application will become a “non-compliant” application and will be closed, thus disappearing from the 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.

-----

**Q: 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? ([CC/MSSP/CM, Provider, 5](#))**

**A:** Contact the CC/MSSP/CM and request that the application be terminated. If 90 days elapses, the task will become non complaint, will be closed and disappear from his ‘Open’ work list.

-----

**Q: How do I deal with Ghost (what appears to be a duplicate CCQAS task) Application? ([All, 5](#))**

**A:** Work the application on the bottom and the application on the top will disappear.

-----

**Q: How can I select a Specialty Board ([Section 6.3.7](#))**

**A:** You only need to select a Specialty Board for providers who are Board Certified. Using the Board Certification the provider has provided, you go to the Specialty Tab and use the Binoculars to search for the Specialty Board listed. Please note that not all Boards are listed as DoD only recognizes ABMS/AOA/ADA boards for specialty pay purposes.

-----

**Q: How do I reactivate a credentials record? ([CC/MSSP/CM, 6](#))**

**A:** Follow the steps below:

- (1) Enter last and first name > select Inactive and Provider Locator and click search
  - (2) Search results are returned and as you can see this CCQAS record is Inactive
  - (3) From the hidden menu select Activate Provider
  - (4) At this point you have re-activated the CCQAS credentials record for your UIC and have full custody of it. You now need to add an assignment for your UIC
- 

**Q: Why is the “Not Requested” column missing from my privilege list? ([Provider, 5](#))**

**A:** The only time you get the “Not Requested” column is when you select itemized privileges.

-----

**Q: Where do I find the Level 1 Reviewers modifications to privilege items (Recommendations and/or Comments)? ([CC/MSSP/CM, 5](#))**

**A:** Open the e-App task, select the Comments tab, click the hidden menu arrow to the left of the Level 1 Reviewer and select Recommendation Detail. A report listing each privilege with corresponding comment will appear on the screen.

-----

**Q: How can I tell whether or not a privilege is supported or not supported when completing a privilege application? ([CC/MSSP/CM, 5](#))**

**A:** This is a recognized problem but unfortunately at this time there is no way for a provider to tell whether a privilege is Support or Not Supported when selecting privileges. However, regardless of what privileges are selected, Not Supported privileges cannot be Recommended or Approved and therefore will not appear on the final approved privilege list.

-----

**Q: I have a military provider who has retired from my command who has now been hired as a civilian provider. How do I change his/her CCQAS CRED from Military to Civilian and do I have to reprivilege him/her as his/her military privileges do not expire for another year? ([CC/MSSP/CM, 3](#))**

**A:** Go to provider search and locate provider, open provider record and go to Work history and use Left Arrow to End Current Military Assignment (you will need to indicate when assignment

ended and why). Click Add New Assignment to create a New Civilian Assignment. Once you have created a New Civilian Assignment, click on left arrow and select Reactivate Privileges (Must be at same UIC and within 7 days of new current assignment date.) Work history now shows both a Current assignment as a Civilian and an Inactive assignment as a Military provider with all of his previous military information as it existed when provider retired). Go to provider profile and uncheck Military Information. NOTE: You can also change a provider from Military to Civilian by Deactivating Provider and then Reactivating Provider.

-----

**Q: When I go to request privileges how can I tell which ones are Supported or Not Supported at my facility?**

**A:** Unfortunately there is no way to tell which privileges are Supported or Not Supported when requesting privileges. The only way you will know is that any Not Supported privileges you requested cannot be granted, so you must carefully scrutinize your final approved list to determine what privileges were granted.

-----

**Q: I have a provider who is a Reviewer with a Pending PCS however, he/she can't see the pending E-App in order to complete, why?**

**A:** As a Reviewer, his/her opening page defaults to Work List not My Application whereas for a provider user all they can see is My Applications. Have him/her select my applications and they will be able to see and complete their E-App.

-----

**Q: Why can't I as the CC/CM/MSSP assign Branch Clinic Reviewers?**

**A:** The Reviewers for the Branch Medical Clinic can only be assigned at the Service Level.

-----

**Q: If I am a Custodial Record Holder for a provider who does not hold Clinical Privileges at my UIC do I need to make She\He an assignment.**

**A:** No, if the provider is not going to be clinically active at your UIC, you do not have to create an assignment.

-----

**Q: My work list is showing duplicate assignments for my provider one assignment is in review and the other assignment is in my pending applications what do I have to do**

**A:** First of all, go to submitted applications and ensure the EAP is in review, and then you can go to the pending applications and terminate the pending EAP.

-----

**Q: I just added MTF specific privileges in CCQAS for our Family Medicine MPL; how do I mark it as supported?**

**A:** As soon as you add a privilege the system automatically defaults the added privilege to supported, if for any reason you don't see the added privilege as supported check to make sure you added it as a Privilege vice a Privilege list

-----

**Q: How do we process our dual hated providers (Reserve\Civilian)?**

**A:** If you have a civilian provider at your facility that also happens to be a reservist, you are now able to INDEPENDENTLY privilege that provider by adding a new assignment at your facility and then generating an E-App from that assignment for the provider to complete. Once provider has completed the E-App the system will generate renewals automatically based on when those privileges will expire as long as the provider continues to work at your facility. You can also create assignments for any civilian clinical support staff also.

-----

**Q: I just received a file that should have gone to a different command for a provider who recently PCS'd. What can I do to fix this problem?**

**A:** Contact the sending command and have them search for the provider's inactive file and cancel the PCS, custody of the record will return to the sending command and they can PCS the provider to the correct command.

-----

**Q: When an application is in the routing process and there is a non-core privilege that should be checked as supported but was inadvertently overlooked and the first level reviewer sends back to me saying that he cannot go in and check supported, what do I do?**

**A:** The system takes a "snapshot" of the privileges at the time the provider requests them so that any subsequent changes that occur "are not" reflected in the E-App once it is signed by the provider. You have 2 choices, terminate the application and initiate a new one that has the right privileges supported or complete the e-app in progress and then have the provider request a modification. Unfortunately both options require the provider to complete another E-APP.

-----

**Q: I have a provider who completed an application but I had to send it back to him to fix some stuff, the provider is currently deployed and has no CCQAS access, would like to call it back, how do we or can we take these files out of the providers work list like we used to?**

**A:** Unfortunately the answer is no. The CCQAS Service Representatives are restricted from getting in the providers work list, if possible have the provider E-Sign again and re-submit back to her and then the necessary changes can be made by the provider.

-----

**Q: I have a new executive officer. This person is not credentialed LIP. When my commanding officer is unavailable he would be the acting CO and therefore the privileging authority for my command, do I add him as a module user only?**

**A:** Yes, add him as a module user, and give him privileging module, reviewer and Privileging Authority roles.

-----

**Q: I have a provider who is an RN, then was privileged as an Acute Care Nurse Practitioner, then chose not to continue privileges as he\she was not working in those privileges. How do I make CCQAS reflect him as an RN?**

**A:** Add a new assignment for provider due to the system only allows one active military assignment, end the current assignment and then add a new assignment with the start date the same as the provider's last assignment you ended.

-----

**Question: How can I tell whether or not a privilege is supported or not supported when completing a privilege application?**

**A:** This is a recognized problem but unfortunately at this time there is no way for a provider to tell whether a privilege is Support or Not Supported when selecting privileges. However, regardless of what privileges are selected, Not Supported privileges Cannot be Recommended or Approved and therefore will not appear on the final approved privilege list.

-----

**Q: How can I select a Specialty Board?**

**A:** You only need to select a Specialty Board for providers who are Board Certified. Using the Board Certification the provider has provided, you go to the Specialty Tab and use the Binoculars to search for the Specialty Board listed. Please note that not all Boards are listed as DoD only recognizes ABMS/AOA/ADA boards for specialty pay purposes.

-----