

HCLSoftware

HCL iAutomate

Installation Guide
Version 6.5



The data contained in this document shall not be duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded to chosen parties because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client's or prospective client's right to use the information contained in the data if it is obtained from another source without restriction. The data subject to this restriction is contained in all marked sheets.

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Copyright © 2025 HCL Technologies Limited.

Table of Contents

1	Preface	19
1.1	Intended Audience	19
1.2	About this Guide	19
1.3	Related Documents	19
1.4	Conventions	19
2	iAutomate Overview	20
3	iAutomate Installation	22
3.1	Environment Planning	22
3.2	Environment Preparation	23
3.2.1	iAutomate Components	23
3.2.2	Deployment Identification Mode	24
3.2.3	Component Installation Prerequisites	39
3.3	Prerequisites to Run the Installer	40
3.3.1	Installer	41
3.4	iAutomate Installation	41
3.4.1	Run the Installer	41
3.4.2	Install iAutomate	41
3.4.3	Database Setup	42
3.4.4	Component Setup	44
3.4.5	Server Configuration	47
3.4.6	Run Pre-Requisite Checker	50
3.4.7	Configure Admin Details	52
3.4.8	Install	53
3.5	iAutomate Upgradation	57
3.5.1	Install iAutomate	57
3.5.2	Database Setup	59
3.5.3	Component Setup	60
3.5.4	Server Configuration	61
3.5.5	Run Pre-Requisite Checker	63
3.5.6	Install	64
3.6	Post Installation Activities	68
3.6.1	Enable Secure Communication (Changing HTTP to HTTPS)	69
3.6.2	Configuration Changes – Certificate Name Change (Type – PFX)	112
3.6.3	Configuration Changes – Certificate Name Change for PEM/CRT/KEY Certificates	150
3.6.4	Load Balancer Configuration	151
3.6.5	Configuration Changes – Access iAutomate without Certificate (Type – PFX)	158
3.6.6	Configuration Changes – Access iAutomate with Certificate (Type – PFX)	164
3.6.7	Configuration Changes - Access iAutomate without Certificate (Type – PEM)	168
3.6.8	Configuration Changes – SaaS based Ticket Analysis	174
3.6.9	Configuration Changes - Run BASEUI and WEBAPI on Same Port	180
3.6.10	Configuration Changes in Apache – For Python Components	183
4	Appendix	188
4.1	List of Abbreviations	188
5	Support	189

Table of Figures

Figure 1 - iAutomate Workflow	20
Figure 2 - Run the Installer	41
Figure 3 - iAutomate Implementation	42
Figure 4 - iAutomate Implementation	42
Figure 5 - Select Authentication	43
Figure 6 - Test Connection	43
Figure 7 - Component Setup	44
Figure 8 - Configure Mongo DB and Solr	47
Figure 9 - Check Mongo DB and Solr Connection Status	47
Figure 10- Server Configuration	48
Figure 11 - Successful Validation	48
Figure 12- Server Configuration	49
Figure 13 - Successful Validation	49
Figure 14 - Prerequisite Checker	50
Figure 15 - Pre-Requisite Checking in Progress	51
Figure 16 - Pre-Requisite Checker Status	51
Figure 17 - Prerequisite Checker Report	52
Figure 18 - Configure Admin Details	53
Figure 19 – Installation	54
Figure 20 - Installation Progress	54
Figure 21 - Installation Progress (In case of failure)	55
Figure 22 - Installation Successful	55
Figure 23 - Message on Launching iAutomate	56
Figure 24 - iAutomate Login Page	56
Figure 25 - iAutomate Login Page (Cont.)	56
Figure 26 - iAutomate Login Page (Cont.)	57
Figure 27 - iAutomate Login Page (Cont.)	57
Figure 28 - iAutomate Implementation	58
Figure 29 - iAutomate Upgradation	58

Figure 30 - Database Details.....	59
Figure 31 – Database Setup.....	59
Figure 32 – Database Setup(cont.)	60
Figure 33 – Component Setup.....	60
Figure 34 – Server Configuration.....	61
Figure 35 - Server Configuration (cont.)	61
Figure 36- Server Configuration	62
Figure 37 - Successful Validation.....	62
Figure 38 - Prerequisite Checker	63
Figure 39 - Pre-Requisite Checking in Progress	63
Figure 40 - Pre-Requisite Checker Status	64
Figure 41 - Prerequisite Checker Report	64
Figure 42 – Installation	65
Figure 43 - Installation Progress.....	65
Figure 44 - Installation Progress (In case of failure)	66
Figure 45 - Installation Successful	66
Figure 46 - Message on Launching iAutomate	67
Figure 47 - iAutomate Login Page	67
Figure 48 - iAutomate Login Page (Cont.)	67
Figure 49 - iAutomate Login Page (Cont.) License Key	68
Figure 50 - iAutomate Login Page (Cont.) License Key	68
Figure 51 - Hosting KRS from HTTP to HTTPS.....	69
Figure 52 - Hosting KRS from HTTP to HTTPS (cont.)	70
Figure 53 - Hosting KRS from HTTP to HTTPS (cont.)	70
Figure 54 - Hosting KRS from HTTP to HTTPS (cont.)	70
Figure 55 - Hosting KRS from HTTP to HTTPS (cont.)	71
Figure 56 - Hosting KRS from HTTP to HTTPS (cont.)	71
Figure 57 - Hosting KRS from HTTP to HTTPS (cont.)	71
Figure 58 - Hosting Base user interface from HTTP to HTTPS	72
Figure 59 - Hosting Base user interface from HTTP to HTTPS (cont.).....	72

Figure 60 - Hosting Base User Interface from HTTP to HTTPS (cont.)	72
Figure 61 - Hosting Base user interface from HTTP to HTTPS (cont.).....	73
Figure 62 - Hosting Base user interface from HTTP to HTTPS (cont.).....	73
Figure 63 - Hosting Base user interface from HTTP to HTTPS (cont.).....	73
Figure 64 - Hosting Base user interface from HTTP to HTTPS (cont.).....	74
Figure 65 - Hosting Base user interface from HTTP to HTTPS (cont.).....	74
Figure 66 - Hosting Base user interface from HTTP to HTTPS (cont.).....	74
Figure 67 - Hosting Web API from HTTP to HTTPS	74
Figure 68 - Hosting Web API from HTTP to HTTPS (Cont.)	75
Figure 69 - Hosting Web API from HTTP to HTTPS (Cont.)	75
Figure 70 - Hosting Web API from HTTP to HTTPS (Cont.)	75
Figure 71 - Hosting Web API from HTTP to HTTPS (Cont.)	75
Figure 72 - Hosting Listener from HTTP to HTTPS	75
Figure 73 - Hosting Listener from HTTP to HTTPS	76
Figure 74 - Hosting Listener from HTTP to HTTPS (cont.).....	76
Figure 75 - Hosting Listener from HTTP to HTTPS (cont.).....	77
Figure 76 - Hosting Listener from HTTP to HTTPS (cont.).....	77
Figure 77 - Hosting Listener from HTTP to HTTPS (cont.).....	77
Figure 78 - Hosting Listener from HTTP to HTTPS (cont.).....	78
Figure 79 - Changing LB IP via GUI from HTTP to HTTPS	78
Figure 80 - Identify Thumbprint of the Certificate	78
Figure 81 - Identify Thumbprint of the Certificate (cont.).....	79
Figure 82 - Identify Thumbprint of the Certificate (cont.).....	79
Figure 83 - Identify Thumbprint of the Certificate (cont.).....	80
Figure 84 - Identify Thumbprint of the Certificate (cont.).....	80
Figure 85 - Identify Thumbprint of the Certificate (cont.).....	81
Figure 86 - Identify Thumbprint of the Certificate (cont.).....	81
Figure 87 - Hosting Listener from HTTP to HTTPS	82
Figure 88 - Hosting Listener from HTTP to HTTPS (cont.).....	82
Figure 89 - Hosting Listener from HTTP to HTTPS (cont.).....	83

Figure 90 - Hosting Listener from HTTP to HTTPS (cont.).....	84
Figure 91 - Hosting Listener from HTTP to HTTPS (cont.).....	84
Figure 92 - Hosting Listener from HTTP to HTTPS (cont.).....	84
Figure 93 - Hosting Listener from HTTP to HTTPS (cont.).....	84
Figure 94 - Hosting Listener from HTTP to HTTPS (cont.).....	85
Figure 95 - Hosting Data Collector from HTTP to HTTPS	85
Figure 96 - Hosting Data Collector from HTTP to HTTPS (cont.).....	86
Figure 97 - Hosting Data Collector from HTTP to HTTPS (cont.).....	86
Figure 98 - Hosting Data Collector from HTTP to HTTPS (cont.).....	87
Figure 99 - Hosting Data Collector from HTTP to HTTPS (cont.).....	87
Figure 100 - Hosting Data Collector from HTTP to HTTPS (cont.).....	87
Figure 101 - Hosting Data Collector from HTTP to HTTPS (cont.).....	87
Figure 102 - Hosting Data Collector from HTTP to HTTPS (cont.).....	88
Figure 103 - Hosting Data Collector from HTTP to HTTPS (cont.).....	88
Figure 104 - Hosting Generic Service from HTTP to HTTPS	89
Figure 105 - Hosting Generic Service from HTTP to HTTPS (Cont.)	89
Figure 106 - Hosting Generic Service from HTTP to HTTPS (Cont.)	90
Figure 107 - Hosting Generic Service from HTTP to HTTPS (Cont.)	90
Figure 108 - Hosting Generic Service from HTTP to HTTPS (Cont.)	91
Figure 109-Hosting Generic Service from HTTP to HTTPS (Cont.)	91
Figure 110 - Hosting Generic Service from HTTP to HTTPS (Cont.)	91
Figure 111 - Hosting Generic Service from HTTP to HTTPS (Cont.)	91
Figure 112 - Hosting Generic Service from HTTP to HTTPS (Cont.)	91
Figure 113 - Hosting RBA Component from HTTP to HTTPS	92
Figure 114 - Hosting RBA Component from HTTP to HTTPS	92
Figure 115 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	93
Figure 116 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	93
Figure 117 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	94
Figure 118 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	94
Figure 119 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	94

Figure 120 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	94
Figure 121 - Hosting RBA Component from HTTP to HTTPS (Cont.).....	94
Figure 122 - Hosting Release Service from HTTP to HTTPS	95
Figure 123 - Hosting Release Service from HTTP to HTTPS (Cont.)	95
Figure 124 - Hosting Release Service from HTTP to HTTPS (Cont.)	96
Figure 125 - Hosting Release Service from HTTP to HTTPS (Cont.)	96
Figure 126 - Hosting Release Service from HTTP to HTTPS (Cont.)	97
Figure 127 - Hosting Release Service from HTTP to HTTPS (Cont.)	97
Figure 128 - Hosting Release Service from HTTP to HTTPS (Cont.)	97
Figure 129 - Hosting Release Service from HTTP to HTTPS (Cont.)	97
Figure 130 - Hosting Release Service from HTTP to HTTPS (Cont.)	97
Figure 131 - Hosting AD Sync from HTTP to HTTPS	98
Figure 132 - Hosting AD Sync from HTTP to HTTPS (cont.)	98
Figure 133 - Hosting AD Sync from HTTP to HTTPS (cont.)	99
Figure 134 - Hosting AD Sync from HTTP to HTTPS (cont.)	99
Figure 135 - Hosting AD Sync from HTTP to HTTPS (cont.)	99
Figure 136 - Hosting AD Sync from HTTP to HTTPS (cont.)	100
Figure 137 - Hosting AD Sync from HTTP to HTTPS (cont.)	100
Figure 138 - Hosting AD Sync from HTTP to HTTPS (cont.)	100
Figure 139 - Hosting AD Sync from HTTP to HTTPS (cont.)	101
Figure 140 - Hosting Email Service from HTTP to HTTPS.....	101
Figure 141 - Hosting Email Service from HTTP to HTTPS (cont.)	102
Figure 142 - Hosting Email Service from HTTP to HTTPS (cont.)	102
Figure 143 - Hosting Email Service from HTTP to HTTPS (cont.)	103
Figure 144 - Hosting Email Service from HTTP to HTTPS (cont.)	103
Figure 145 - Hosting Email Service from HTTP to HTTPS (cont.)	103
Figure 146 - Hosting Email Service from HTTP to HTTPS (cont.)	103
Figure 147 - Hosting Email Service from HTTP to HTTPS (cont.)	104
Figure 148 – Hosting Email Service from HTTP to HTTPS (cont.)	104
Figure 149 - Hosting DAG Service from HTTP to HTTPS	104

Figure 150 - Hosting DAG Service from HTTP to HTTPS (cont.)	105
Figure 151 - Hosting DAG Service from HTTP to HTTPS (cont.)	105
Figure 152 - Hosting DAG Service from HTTP to HTTPS (cont.)	106
Figure 153 - Hosting DAG Service from HTTP to HTTPS (cont.)	106
Figure 154 - Hosting DAG Service from HTTP to HTTPS (cont.)	106
Figure 155 - Hosting DAG Service from HTTP to HTTPS (cont.)	106
Figure 156 - Hosting DAG Service from HTTP to HTTPS (cont.)	107
Figure 157 – Hosting DAG Service from HTTP to HTTPS (cont.)	107
Figure 158 - Hosting Email Service from HTTP to HTTPS.....	107
Figure 159 - Hosting Email Service from HTTP to HTTPS (cont.)	108
Figure 160 - Hosting Assignment Service from HTTP to HTTPS (cont.)	108
Figure 161 - Hosting Assignment Service from HTTP to HTTPS (cont.)	109
Figure 162 - Hosting Service from HTTP to HTTPS (cont.)	109
Figure 163 - Hosting Service from HTTP to HTTPS (cont.)	109
Figure 164 - Hosting Service from HTTP to HTTPS (cont.)	109
Figure 165 - Hosting Service from HTTP to HTTPS (cont.)	110
Figure 166 – Hosting Service from HTTP to HTTPS (cont.)	110
Figure 167 - Configuration Changes via GUI from HTTP to HTTPS	110
Figure 168 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)	111
Figure 169 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)	111
Figure 170 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)	111
Figure 171 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)	112
Figure 172 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)	112
Figure 173 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)	112
Figure 174 - Certificate Name Change – KRS.....	113
Figure 175 - Certificate Name Change – KRS (Cont.).....	113
Figure 176 - Certificate Name Change – KRS (Cont.).....	113
Figure 177 - Certificate Name Change – KRS (Cont.).....	114
Figure 178 - Certificate Name Change – KRS (Cont.).....	114
Figure 179 - Certificate Name Change – BaseUI.....	114

Figure 180 - Certificate Name Change – BaseUI (Cont.).....	114
Figure 181 - Certificate Name Change – BaseUI (Cont.).....	115
Figure 182 - Certificate Name Change – BaseUI (Cont.).....	115
Figure 183 - Certificate Name Change – BaseUI (Cont.).....	115
Figure 184 - Certificate Name Change – Web API.....	115
Figure 185 - Certificate Name Change – Web API (cont.)	116
Figure 186 - Certificate Name Change – Web API (cont.)	116
Figure 187 - Certificate Name Change – Web API (cont.)	116
Figure 188 - Certificate Name Change – Web API (cont.)	116
Figure 189 - Certificate Name Change – Listener	117
Figure 190 - Certificate Name Change – Listener (cont.)	117
Figure 191 - Certificate Name Change – Listener (cont.)	118
Figure 192 - Certificate Name Change – Listener (cont.)	119
Figure 193 - Certificate Name Change – Listener (cont.)	119
Figure 194 - Certificate Name Change – Listener (cont.)	119
Figure 195- Certificate Name Change – Listener (cont.)	119
Figure 196 - Certificate Name Change – Data Collector	120
Figure 197 - Certificate Name Change – Data Collector (Cont.)	120
Figure 198 - Certificate Name Change – Data Collector (Cont.)	121
Figure 199 - Certificate Name Change – Data Collector (Cont.)	121
Figure 200 - Certificate Name Change – Data Collector (Cont.)	121
Figure 201 - Certificate Name Change – Data Collector (Cont.)	122
Figure 202 - Certificate Name Change – Data Collector (Cont.)	122
Figure 203 - Certificate Name Change – Data Collector (Cont.)	122
Figure 204 - Certificate Name Change – Generic Service	123
Figure 205 - Certificate Name Change – Generic Service (cont.)	123
Figure 206 - Certificate Name Change – Generic Service (cont.)	124
Figure 207 - Certificate Name Change – Generic Service (cont.)	124
Figure 208- Certificate Name Change – Generic Service (cont.)	125
Figure 209 - Certificate Name Change – Generic Service (cont.)	125

Figure 210 - Certificate Name Change – Generic Service (cont.)	125
Figure 211- Certificate Name Change – Generic Service (cont.)	125
Figure 212 - Certificate Name Change – RBA Component	126
Figure 213 - Certificate Name Change – RBA Component (cont.).....	126
Figure 214 - Certificate Name Change – RBA Component (cont.).....	127
Figure 215 - Certificate Name Change – RBA Component (cont.).....	127
Figure 216 - Certificate Name Change – RBA Component (cont.).....	128
Figure 217 - Certificate Name Change – RBA Component (cont.).....	128
Figure 218 - Certificate Name Change – RBA Component (cont.).....	128
Figure 219 - Certificate Name Change – RBA Component (cont.).....	128
Figure 220 - Certificate Name Change – Release Service	129
Figure 221 - Certificate Name Change – Release Service (cont.)	129
Figure 222 - Certificate Name Change – Release Service (cont.)	130
Figure 223 - Certificate Name Change – Release Service (cont.)	130
Figure 224 - Certificate Name Change – Release Service (cont.)	131
Figure 225 - Certificate Name Change – Release Service (cont.)	131
Figure 226 - Certificate Name Change – Release Service (cont.)	131
Figure 227 - Certificate Name Change – Release Service (cont.)	131
Figure 228 - Certificate Name Change – AD Sync Service	132
Figure 229 - Certificate Name Change – AD Sync Service (cont.).....	132
Figure 230 - Certificate Name Change – AD Sync Service (cont.).....	132
Figure 231 - Certificate Name Change – AD Sync Service (cont.).....	133
Figure 232 - Certificate Name Change – AD Sync Service (cont.).....	133
Figure 233 - Certificate Name Change – AD Sync Service (cont.).....	133
Figure 234 - Certificate Name Change – AD Sync Service (cont.).....	133
Figure 235 - Certificate Name Change – AD Sync Service (cont.).....	134
Figure 236 - Certificate Name Change – Email Service.....	134
Figure 237 - Certificate Name Change – Email Service (cont.).....	135
Figure 238 - Certificate Name Change – Email Service (cont.).....	135
Figure 239 - Certificate Name Change – Email Service (cont.).....	136

Figure 240 - Certificate Name Change – Email Service (cont.)	136
Figure 241 - Certificate Name Change – AD Sync Service (cont.)	136
Figure 242 - Certificate Name Change – Email Service (cont.)	136
Figure 243 – Certificate Name Change – Email Service (cont.)	137
Figure 244 - Certificate Name Change – DAG Service	137
Figure 245 - Certificate Name Change – DAG Service (cont.)	137
Figure 246 - Certificate Name Change – DAG Service (cont.)	138
Figure 247 - Certificate Name Change – DAG Service (cont.)	138
Figure 248 - Certificate Name Change – DAG Service (cont.)	139
Figure 249 - Certificate Name Change – DAG Service (cont.)	139
Figure 250 - Certificate Name Change – DAG Service (cont.)	139
Figure 251 – Certificate Name Change – DAG Service (cont.)	139
Figure 252 - Certificate Name Change – Assignment Service	139
Figure 253 - Certificate Name Change – Assignment Service (cont.)	140
Figure 254 - Certificate Name Change – Assignment Service (cont.)	140
Figure 255 - Certificate Name Change – Assignment Service (cont.)	141
Figure 256 - Certificate Name Change – Assignment Service (cont.)	141
Figure 257 - Certificate Name Change – Assignment Service (cont.)	141
Figure 258 - Certificate Name Change – Assignment Service (cont.)	141
Figure 259 – Certificate Name Change – Assignment Service (cont.)	142
Figure 260 - Certificate Name Change – iRecommend	142
Figure 261 - Certificate Name Change – iRecommend (Cont.)	142
Figure 262 - Certificate Name Change – iRecommend (Cont.)	143
Figure 263 - Certificate Name Change – iRecommend (Cont.)	143
Figure 264 - Certificate Name Change – iRecommend (Cont.)	144
Figure 265 - Certificate Name Change – iRecommend (Cont.)	144
Figure 266 - Certificate Name Change – iParse	144
Figure 267 - Certificate Name Change – iParse (Cont.)	145
Figure 268 - Certificate Name Change – iParse (Cont.)	145
Figure 269 - Certificate Name Change – iParse (Cont.)	146

Figure 270 - Certificate Name Change – iParse (Cont.)	146
Figure 271 - Certificate Name Change – iScrape	146
Figure 272 - Certificate Name Change – iUnique	147
Figure 273 - Certificate Name Change – iUnique	147
Figure 274 - Certificate Name Change – iUnique	148
Figure 275 - Certificate Name Change – iUnique	148
Figure 276 - Certificate Name Change – iUnique	149
Figure 277 - Certificate Name Change – Knowledge	149
Figure 278 - Certificate Name Change – Knowledge (Cont.)	149
Figure 279 - Certificate Name Change – Knowledge (Cont.)	149
Figure 280 - Certificate Name Change – Knowledge (Cont.)	150
Figure 281 - Certificate Name Change – Knowledge (Cont.)	150
Figure 282 - Certificate Name Change – Knowledge (Cont.)	150
Figure 283 - Certificate Name Change (PEM / CRT / Key Certificate).....	151
Figure 284 - Load Balancer Configuration	151
Figure 285 - Load Balancer Configuration (cont.).....	151
Figure 286 - Load Balancer Configuration (cont.).....	152
Figure 287 - Load Balancer Configuration (cont.).....	152
Figure 288 - Load Balancer Configuration (cont.).....	152
Figure 289 - Load Balancer Configuration (cont.).....	153
Figure 290 - Load Balancer Configuration (cont.).....	153
Figure 291 - Load Balancer Configuration (cont.).....	153
Figure 292 - Load Balancer Configuration (cont.).....	153
Figure 293 - Load Balancer Configuration (cont.).....	154
Figure 294 - Load Balancer Configuration (cont.).....	154
Figure 295 - Load Balancer Configuration (cont.).....	154
Figure 296 - Load Balancer Configuration (cont.).....	155
Figure 297 - Load Balancer Configuration (cont.).....	156
Figure 298 - Load Balancer Configuration (cont.).....	156
Figure 299 - Load Balancer Configuration (cont.).....	156

Figure 300 - Load Balancer Configuration (cont.).....	157
Figure 301 - Load Balancer Configuration (cont.).....	157
Figure 302 - Load Balancer Configuration (cont.).....	157
Figure 303 - Load Balancer Configuration (cont.).....	158
Figure 304 - Configuration Changes – Access iAutomate without Certificate (Type – PFX).....	158
Figure 305 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	159
Figure 306 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	159
Figure 307 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	160
Figure 308 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	160
Figure 309 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	160
Figure 310 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	160
Figure 311 - Configuration Changes – Access iAutomate without Certificate (Type – PFX).....	161
Figure 312 - Configuration Changes – Access iAutomate without Certificate (Type – PFX).....	161
Figure 313 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	161
Figure 314 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	162
Figure 315 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	162
Figure 316 – Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	163
Figure 317 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	163
Figure 318 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	164
Figure 319 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	164
Figure 320 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	165
Figure 321 Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	165
Figure 322 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	165
Figure 323 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	165
Figure 324 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	166
Figure 325 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	166
Figure 326 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)	166
Figure 327 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	167
Figure 328- Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	167
Figure 329 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	168

Figure 330 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.).....	168
Figure 331 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	168
Figure 332 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	169
Figure 333 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	169
Figure 334 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	169
Figure 335 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	170
Figure 336 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	170
Figure 337 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	171
Figure 338 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	171
Figure 339 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	171
Figure 340 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	172
Figure 341 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	172
Figure 342 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	173
Figure 343 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)	173
Figure 344- Manage Proxy.....	174
Figure 345 - Password in plaintext	175
Figure 346 - Password from Key Vault (CyberArk)	175
Figure 347 - Password from Internal Secret Manager	175
Figure 348- Build Models.....	176
Figure 349- Build Models (cont.)	176
Figure 350- Build Models (cont.)	176
Figure 351- Build Models (cont.)	177
Figure 352- Build Models (cont.)	177
Figure 353- Build Models (cont.)	177
Figure 354- Build Models (cont.)	177
Figure 355- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis	178
Figure 356- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.)	178
Figure 357- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.)	178
Figure 358- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.)	179
Figure 359- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.)	179

Figure 360- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.) 180

Figure 361- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.) 180

Figure 362 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 181

Figure 363 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 181

Figure 364 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 182

Figure 365 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 182

Figure 366 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 183

Figure 367 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 183

Figure 368 - Configuration Changes - Run BASEUI and WEBAPI on Same Port..... 183

Figure 369 -Apache Upgradation 184

Figure 370 - Apache Upgradation (cont.) 185

Figure 371 - Apache Upgradation (cont.) 186

Figure 372 - Screenshot of the Apache Python Services 187

List of Tables

Table 1 - Conventions	19
Table 2 - Environment Categorization	22
Table 3 - Types of Servers	23
Table 4 - Minimal Deployment	25
Table 5 - Small Environment without High Availability (HA)	27
Table 6 - Medium Environment without HA	28
Table 7 - Large Environment without HA	30
Table 8 - Small Environment with HA	32
Table 9 - Medium Environment with HA	35
Table 10 - Large Environment with HA	37
Table 11 - Component Installation Prerequisites	39
Table 12 - Prerequisites to Run the Installer	40
Table 13 - iAutomate Components	44
Table 14 - MongoDB Configuration Parameters	46

Document Revision History

This guide is updated with each release of the product or when necessary.

This table provides the revision history of this Installation Guide.

Version Date	Description
October, 2019	HCL_iAutomate_v4.0_Installation_Guide
May, 2020	HCL_iAutomate_v5.0_Installation_Guide
September, 2020	HCL_iAutomate_v6.0_Installation_Guide
November, 2020	HCL_iAutomate_v6.0.1_Installation_Guide
January, 2021	HCL_iAutomate_v6.0.2_Installation_Guide
April, 2021	HCL_iAutomate_v6.0.3_Installation_Guide
October, 2021	HCL_iAutomate_v6.1_Installation_Guide
March, 2022	HCL_iAutomate_v6.1.1_Installation_Guide
October, 2022	HCL_iAutomate_v6.2_Installation_Guide
November, 2022	HCL_iAutomate_v6.2.1_Installation_Guide
October, 2023	HCL_iAutomate_v6.3_Installation_Guide
December, 2023	HCL_iAutomate_v6.3.2_Installation_Guide
June, 2024	HCL_iAutomate_v6.4_Installation_Guide
August, 2024	HCL_iAutomate_v6.4.1_Installation_Guide
November, 2024	HCL_iAutomate_v6.4.2_Installation_Guide
February, 2025	HCL_iAutomate_v6.4.2_Installation_Guide

1 Preface

This section provides information about the HCL iAutomate Installation Guide and includes the following topics.

- [Intended Audience](#)
- [About This Guide](#)
- [Related Documents](#)
- [Conventions](#)

1.1 Intended Audience

This information is intended for administrators responsible for installing iAutomate and infrastructure administrators responsible for provisioning infrastructure required for installation of iAutomate.

1.2 About this Guide

This guide provides instructions to install iAutomate. It includes the pre-installation and the installation procedures for iAutomate.

This guide also provides summary material about additional servers and optional post- installations and references to the other documents for detailed information.

1.3 Related Documents

The following documents can be referenced in addition to this guide for further information on the iAutomate platform.

- iAutomate User Guide
- iAutomate Pre-Requisite Guide
- iAutomate Troubleshooting Guide

1.4 Conventions

The following typographic conventions are used in this document:

Table 1 - Conventions

Convention	Element
Boldface	Indicates graphical user interface elements associated with an action, or terms defined in text or the glossary
Underlined Blue Face	Indicates cross-reference and links
Italic	Indicates document titles, occasional emphasis, or glossary terms
Courier New (Font)	Indicates commands within a paragraph, URLs, code in examples, and paths including onscreen text and text input from users
Numbered lists	Indicates steps in a procedure to be followed in a sequence
Bulleted lists	Indicates a list of items that is not necessarily meant to be followed in a sequence

2 iAutomate Overview

iAutomate is an Intelligent Runbook Automation product which is equipped with Artificial Intelligence, Machine Learning and Natural Language Processing capabilities for simplifying and automating the IT Operations issues resolution lifecycle including incidents, service request tasks, change request tasks and events. It leverages its NLP capabilities for analyzing and understanding the context of a specific issue, recommends the most relevant solution and even triggers the execution, thereby enabling Zero Touch Automated Remediation. It also provides AI-driven Knowledge Recommendation by suggesting relevant knowledge articles from various repositories, both internal and external, as and when required by human agents.

When no runbook is available for automated remediation, it searches & downloads relevant executable codes and scripts for subject matter expert to validate, customize, approve and publish for the future use.

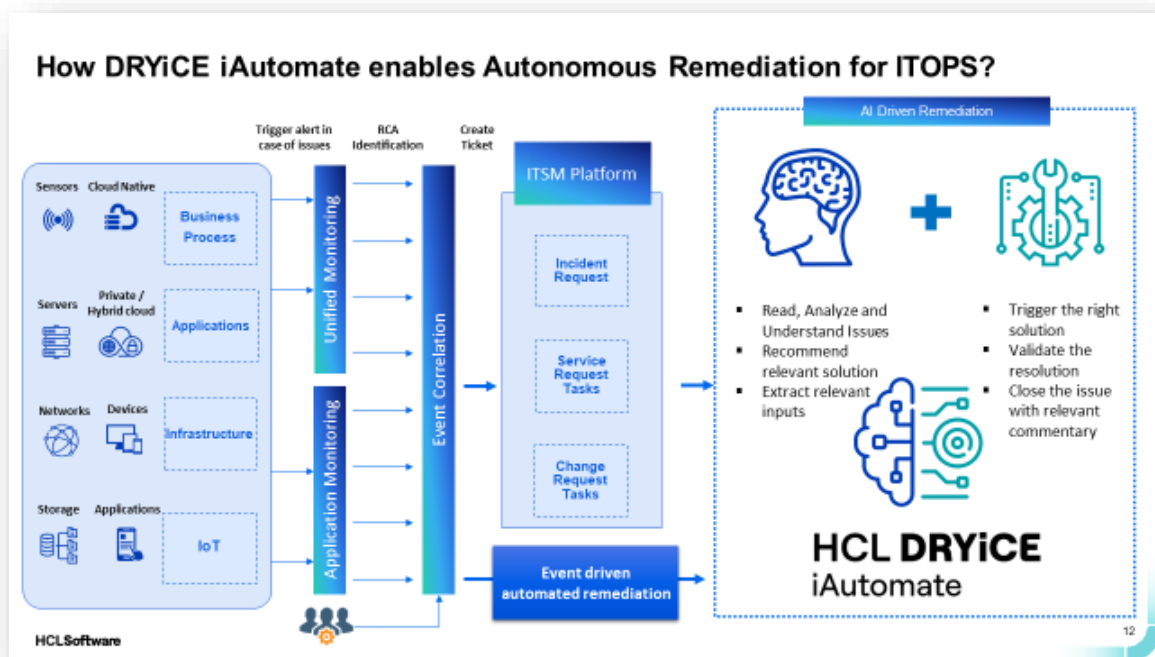


Figure 1 - iAutomate Workflow

Intelligent automation powered by HCL iAutomate can make a tremendous impact in an enterprise adjusting to the New Normal:

- **Reduces Costs**
 - Achieves up to 30% reduction in service desk related costs.
 - Quick and High ROI
- **Mitigates Risks**
 - Avoids operational risks and ensures compliance by avoiding critical outages.
 - Reduces escalations and improves SLA compliance by up to 20%.
 - Achieves up to 85% reduction in MTTR.
- **Drives Efficiency**

- Automates redundant tasks and lets employees focus on more creative activities.
- Reduces manual effort by 30% to 60%.
- Improves customer satisfaction by up to 50% by providing faster incident and service request resolutions.

– **Rapid Time to Value**

- Quick implementation in 6 to 8 weeks*
- Leverages 3000+ reusable and configurable runbooks out of the box
- Achieves zero-touch automation state in 4 to 5 months*

*Conditions Apply

3 iAutomate Installation

This section describes the detailed iAutomate installation procedure, and the various stages involved in this process.

The iAutomate installation process comprises the following steps:

1. Plan and Prepare Your Environment

Prior to installing iAutomate, the environment, hardware, and networking components must be prepared and configured. The relevant software dependencies must be installed. For more information about preparing components for installation, see Environment Planning.

2. Complete Pre-installation Tasks

Lists tasks the user needs to complete before installing iAutomate.

3. Installation

After the environment has been prepared and the relevant databases and servers have been provisioned, user can install the iAutomate product.

4. Complete Post Install Checks

After installing the iAutomate product, complete the post installation tasks. These tasks include specific steps required for iAutomate Configuration. For more information about the post-installation tasks, see Configure iAutomate.

The complete installation of iAutomate includes databases, a web interface, and a set of services including iRecommend, iParse, iUnique, iScrape, iKnowledge and others.

This section includes the following topics:

- [Environment Planning](#)
- [Environment Preparation](#)
- [Prerequisites to Run the Installer](#)
- [iAutomate Installation](#)
- [iAutomate Upgradation](#)
- [Post-Installation Activities](#)

3.1 Environment Planning

Before preparing the deployment environment, see the environment categorization table and plan accordingly.

Environments are classified in three categories based on the parameters listed below:

Table 2 - Environment Categorization

Environment Indicator	Number of Tickets (per month)	Number of Unique Tickets (per month)	Number of Documents Processed	Number of Search Queries (per month)	Concurrent Executions	Data Retention
Small	Less than 30,000	Less than 500	Less than 1,000	Less than 5,000	up to 100	6 months
Medium	30,000 to 60,000	500 to 1,000	1,000 to 3,000	5,000 to 10,000	up to 200	6 months

Environment Indicator	Number of Tickets (per month)	Number of Unique Tickets (per month)	Number of Documents Processed	Number of Search Queries (per month)	Concurrent Executions	Data Retention
Large	60,000 to 1,50,000	1,000 to 3,000	3,000 to 5,000	10,000 to 30,000	up to 400	6 months

Data Retention is only applicable for ticket data.

Search Queries and Document Process is only applicable when iKnowledge module is installed.

Concurrent Executions have been arrived at based on the limitation of the RBA tool for runbook executions and the ITSM tool for pushing tickets into iAutomate.

3.2 Environment Preparation

This section details how to prepare the environment to perform the physical installation and configuration of iAutomate. Before proceeding, users should familiarize themselves with the different components of iAutomate.

3.2.1 iAutomate Components

iAutomate follows a multi-tier architecture and includes the following components:

- **Web Components-** This includes the user interface that enables the configuration, management, and quick resolution of tickets.
- **Service Components-** It is divided into two categories:
 - **Application Components-** This includes essential services that work together to achieve the core functionality of iAutomate.
 - **Advanced AI Components-** This includes features like Solution Creation; Natural Language Processing (NLP) based assisted services, and so on.

The following table lists the components available on different servers.

Table 3 - Types of Servers

Server Type	Components	Description
Web Component	Web UI	Web User Interface for Admin, Configuration, Operations Console, Dashboards and Knowledge Analysis and Search functionalities
	Web API	It is an API in the iAutomate web module that can be accessed using the HTTP protocol.
	KRS	The Key Rotation Service component serves the purpose of providing additional security through rotation of keys on a periodic basis.
Application Component	iRecommend	It leverages Natural Language Processing and is responsible for recommending the best-suited runbook for resolving the issue based on the ticket description
	iParse	It serves the purpose of analyzing the ticket description and summary for extracting relevant parameters to be passed to configurable runbooks
	iUnique	It helps in clustering the ticket data (incident, service requests, change requests) into different categories for identification of automation opportunities
	Data Collector	It is responsible for collecting ticket information from the ITSM tool

Server Type	Components	Description
	Generic Executor	It is used for data processing at the DB layer for enabling backend processes.
	RBA Executor	It helps in triggering the identified runbook for automatic resolution using an underlying RBA tool
	Release	It is used to release the ticket in case an appropriate runbook is not recommended OR runbook execution for a ticket fails. In the latter case, the ticket is released and assigned to a human agent to investigate it.
	Generic Listener	Ticket passes through multiple stages during the resolution lifecycle using iAutomate. Generic Listener module is responsible for ensuring the ticket is moved to the next stage based on the outcome. Its job is to identify the status of the present stage and based on success / failure, move the ticket to the consequent stage in the lifecycle
	AD Sync	It is responsible for fetching LDAP user from LDAP Server.
	Email Service	It is responsible for sending mail-based notifications to user.
	DAG Service	It is responsible for triggering network related use cases.
	Assignment Service	It is used to assign tickets to the group fetched from Gen AI Studio.
Ansible Inside Wrapper Component	Ansible SDK Wrapper	It is responsible for triggering Ansible Inside Tool
Advanced AI Component	Advanced Knowledge	It returns a list of relevant documents for a query that have been crawled from different repositories like SNOW KB, Web URL, Satori repository, and internal files and folders.
	iKnowledge	It returns a list of relevant results from Google for a query, if no relevant document exists in the organization's repository.
	Knowledge rating	It enables users to provide feedback as a rating for the document search corresponding to the ticket summary.
	iScrape	It helps in automated runbook creation for ticket categories for which runbooks don't exist by exploring various internal and external data sources for relevant executable code snippets and scripts.

Before starting the installation, identify the components that user needs to install based on the requirement. Also, the user needs to identify the deployment mode from the below list based on the Environment categorization identified earlier.

3.2.2 Deployment Identification Mode

iAutomate can be installed in the following deployment modes using the installer.

3.2.2.1 Minimal Deployment Mode

In this mode, the following iAutomate servers are deployed:

- **Web and Application Server:** This server hosts the Web UI and the Application components.

- **Advanced AI Server, MongoDB and Solr:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components along with the Document Storage (MongoDB) and Indexer (Solr).
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate.

The following table describes the hardware and software requirements for this installation.

Table 4 - Minimal Deployment

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
Web Server + Application Server	Web Component	- Web UI - Web API - KRS	NA	One Virtual Server with 2vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	100 GB
	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service - Assignment Service					
	Application Component - Python	- iParse - iUnique - iRecommend					
Advanced AI Server + MongoDB + Solr	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	One Virtual Server with 2vCPU, 8 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	100 GB

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
	Document Storage	MongoDB	NA			Mongo DB + Solr	
	Indexer	Solr	NA				
Database Server	Database	Transactional Database	Microsoft SQL Server 2016 - Standard Edition	One Virtual Server with 4vCPU, 8 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. If Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

Alternate Database options:

1. AWS Relational Database Service (RDS)
2. GCP SQL Server 2017 PaaS service

For Document storage, MongoDB as a service can be used from AWS and GCP marketplace.

Ansible Inside Wrapper Component install on Ansible inside server, it can be installed from any server.

3.2.2.2 Small Environment without High Availability (HA)

In this mode, the following iAutomate servers are deployed:

- **Web and Application Server:** This server hosts the Web UI and the Application components.
- **Advanced AI Server:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components.
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate.
- **MongoDB and Solr:** This server hosts the Document Storage (MongoDB) and Indexer (Solr).

The following table describes the hardware and software requirements for this installation.

Table 5 - Small Environment without High Availability (HA)

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
Web Server + Application Server	Web Component	- Web UI - Web API - KRS	NA	One Virtual Server with 2vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB
	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service - Assignment Service					
	Application Component - Python	- iParse - iUnique - iRecommend					
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	One Virtual Server with 2vCPU, 4 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	50 GB
Database Server	Database	Transactional Database	Microsoft SQL Server 2016, 2019 - Standard Edition	One Virtual Server with 4vCPU, 8 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
MongoDB and Solr	Document Storage	MongoDB	NA	One Virtual Server with 4vCPU, 8 GB RAM	2 GB RAM	Operating System - Windows Server 2016, 2019 , 64-bit	100 GB
	Indexer	Solr	NA				

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. In case Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

- Alternate Database options

1. AWS Relational Database Service (RDS)
2. GCP SQL Server 2017 PaaS service

- For Document storage, MongoDB as a service can be used from AWS and GCP marketplace.

Ansible Inside Wrapper Component install on Ansible inside server, it can be installed from any server.

3.2.2.3 Medium Environment without High Availability (HA)

In this mode, the following iAutomate servers are deployed:

- **Web Server:** This server hosts the Web User Interface.
- **Application Server:** This server hosts the Application components.
- **Advanced AI Server:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components.
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate.
- **MongoDB and Solr:** This server hosts the Document Storage (MongoDB) and Indexer (Solr).

The following table describes the hardware and software requirements for this installation.

Table 6 - Medium Environment without HA

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
Web Server	Web Component	- Web UI - Web API - KRS	NA	One Virtual Server with 2vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016,	50 GB

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
						2019,2022 64-bit	
Application Server	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service - Assignment Service	NA	One Virtual Server with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	100 GB
	Application Component - Python	- iParse - iUnique - iRecommend					
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	One Virtual Server with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	100 GB
Database Server	Database	Transactional Database	Microsoft SQL Server 2016, 2019 - Standard Edition	One Virtual Server with 4vCPU, 8 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019,2022 64-bit	300 GB

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
MongoDB and Solr	Document Storage	MongoDB	NA	One Virtual Server with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019 , 64-bit	100 GB
	Indexer	Solr	NA				

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. If Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

- Alternate Database options

1. AWS Relational Database Service (RDS)

2. GCP SQL Server 2017 PaaS service

- For Document storage, MongoDB as a service can be used from AWS and GCP marketplace.

Ansible Inside Wrapper Component install on Ansible Inside server, it can be installed from any server.

3.2.2.4 Large Environment without High Availability (HA)

In this mode, the following iAutomate servers are deployed:

- **Web Server:** This server hosts the Web User Interface.
- **Application Server:** This server hosts the Application components.
- **Advanced AI Server:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components.
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate.
- **MongoDB and Solr:** This server hosts the Document Storage (MongoDB) and Indexer (Solr).

The following table describes the hardware and software requirements for this installation.

Table 7 - Large Environment without HA

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
Web Server	Web Component	- Web UI - Web API - KRS	NA	One Virtual Server with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016,	100 GB

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
						2019,2022 64-bit	
Application Server	Application Component - Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service - Assignment Service	NA	One Virtual Server with 4vCPU, 16 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	100 GB
	Application Component - Python	- iParse - iUnique - iRecommend					
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	One Virtual Server with 4vCPU, 16 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	100 GB
Database Server	Database	Transactional Database	Microsoft SQL Server 2016, 2019 - Standard Edition	One Virtual Server with 8vCPU, 16 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019,2022 64-bit	500 GB

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage (Local)
MongoDB and Solr	Document Storage	MongoDB	NA	One Virtual Server with 4vCPU, 16 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019, 64-bit	150 GB
	Indexer	Solr	NA				

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. If Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

Alternate Database options:

1. AWS Relational Database Service (RDS)
2. GCP SQL Server 2017 PaaS service

For Document storage, MongoDB as a service can be used from AWS and GCP marketplace.

Ansible Inside Wrapper Component install on Ansible Inside server, it can be installed from any server.

3.2.2.5 Small Environment with High Availability (HA)

In this mode, the following iAutomate servers are deployed:

- **Web and Application Server:** This server hosts the Web UI and the Application components.
- **Advanced AI Server:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate
- **MongoDB:** This server hosts the Document Storage Database (MongoDB)
- **Solr:** This server hosts the Indexer (Solr)

The following table describes the hardware and software requirements for this installation.

Table 8 - Small Environment with HA

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
Web Server	Web Component	- Web UI - Web API - KRS	NA	Two Virtual Servers with	4 GB RAM	Operating System - Windows	50 GB (Additional D:

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
+ Application Server	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service - Assignment Service		2vCPU, 8 GB RAM		Server 2016, 2019,2022 64-bit	Drive) and 50GB shared storage (SAN / File Folder)
	Application Component - Python	- iParse - iUnique - iRecommended					
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	Two Virtual Servers with 2vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019,2022 64-bit	50 GB (Additional D: Drive) and 50GB shared storage (SAN / File Folder)

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
Database Server*	Database	Transactional Database	Microsoft SQL Server 2016, 2019 - Standard Edition	Two Virtual Servers with 4vCPU, 8 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB Shared storage (SAN / File Folder)
MongoDB**	Document Storage	MongoDB	NA	One Virtual Server with 2vCPU, 4 GB RAM	2 GB RAM	Operating System - Windows Server 2016, 2019, 64-bit	50 GB (Additional D: Drive)
Solr***	Indexer	Solr	NA	One Virtual Server with 2vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019, 64-bit	50 GB (Additional D: Drive)

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. If Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

- Alternate Database options

1. AWS Relational Database Service (RDS)
2. GCP SQL Server 2017 PaaS service

- For Document Storage, if *MongoDB must be made available in HA, then 3 servers will have to be provided as per the best practices. Alternately, MongoDB as a service can be used from AWS and GCP marketplace.

- For Indexer, if Solr has to be made available in HA, then 5 servers will have to be provided as per the best practices

Ansible Inside Wrapper Component install on Ansible Inside server, it can be installed from any server.

3.2.2.6 Medium Environment with High Availability (HA)

In this mode, the following iAutomate servers are deployed:

- **Web Server:** This server hosts the Web User Interface
- **Application Server:** This server hosts the Application components.
- **Advanced AI Server:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate

- **MongoDB:** This server hosts the Document Storage Database (MongoDB).
- **Solr:** This server hosts the Indexer (Solr)

The following table describes the hardware and software requirements for this installation.

Table 9 - Medium Environment with HA

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
Web Server	Web Component	- Web UI - Web API - KRS	NA	Two Virtual Servers with 2vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	50 GB (Additional D: Drive) and 50GB shared storage (SAN / File Folder)
Application Server	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service - Assignment Service	NA	Two Virtual Servers with 4vCPU, 8 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB (Additional D: Drive) and 50GB shared storage (SAN / File Folder)
	Application Component - Python	- iParse - iUnique - iRecommend					

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	Two Virtual Servers with vCPU, 8 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB (Additional D: Drive) and 50GB shared storage (SAN / File Folder)
Database Server*	Database	Transactional Database	Microsoft SQL Server 2016, 2019 - Standard Edition	Two Virtual Servers with 4vCPU, 16 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019, 2022 64-bit	300 GB shared storage (SAN / File Folder)
MongoDB*	Document Storage	MongoDB	NA	One Virtual Server with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019 64-bit	100 GB (Additional D: Drive)
Solr***	Indexer	Solr	NA	One Virtual Server with 4vCPU, 8 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019 64-bit	100 GB (Additional D: Drive)

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. If Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

- Alternate Database options

1. AWS Relational Database Service (RDS)
2. GCP SQL Server 2017 PaaS service

- For Document Storage, if *MongoDB must be made available in HA, then 3 servers will have to be provided as per the best practices. Alternately, MongoDB as a service can be used from AWS and GCP marketplace.

- For Indexer, if Solr has to be made available in HA, then 5 servers will have to be provided as per the best practices

Ansible Inside Wrapper Component install on Ansible Inside server, it can be installed from any server.

3.2.2.7 Large Environment with High Availability (HA)

In this mode, the following iAutomate servers are deployed:

- **Web Server:** This server hosts the Web User Interface
- **Application Server:** This server hosts the Application components.
- **Advanced AI Server:** This server hosts iScrape, iKnowledge, and Advanced iKnowledge components
- **Database Server:** This server hosts the SQL Server database, which is the main transactional database of iAutomate
- **MongoDB:** This server hosts the Document Storage Database (MongoDB).
- **Solr:** This server hosts the Indexer (Solr)

The following table describes the hardware and software requirements for this installation.

Table 10 - Large Environment with HA

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
Web Server	Web Component	- Web UI - Web API - KRS	NA	Two Virtual Servers with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB (Additional D: Drive) and 50 GB shared storage (SAN / File Folder)
Application Server	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener	NA	Two Virtual Servers with 4vCPU, 16 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB (Additional D: Drive) and 50 GB shared storage (SAN /

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
		- AD Sync - Email Service - DAG Service - Assignment Service					File Folder)
	Application Component - Python	- iParse - iUnique - iRecommend					
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	NA	Two Virtual Servers with 4vCPU, 16 GB RAM	8 GB RAM	Operating System - Windows Server 2016, 2019, 2022 64-bit	100 GB (Additional D: Drive) and 50 GB shared storage (SAN / File Folder)
Database Server*	Database	Transactional Database	Microsoft SQL Server 2016, 2019 - Standard Edition	Two Virtual Servers with 8vCPU, 16 GB RAM	Not Applicable	Operating System - Windows Server 2016, 2019, 2022 64-bit	500 GB shared storage (SAN / File Folder)
MongoDB**	Document Storage	MongoDB	NA	One Virtual Server with 4vCPU, 8 GB RAM	4 GB RAM	Operating System - Windows Server 2016, 64-bit	150 GB (Additional D: Drive)
Solr***	Indexer	Solr	NA	One Virtual Server with	8 GB RAM	Operating System -	150 GB (Additio

Server	Component	Sub-Components	Database Requirement	Recommended Hardware Configuration	Minimum RAM Requirement for iAutomate	Software Requirements	Storage
				4vCPU, 16 GB RAM		Windows Server 2016, 2019, 64-bit	Local D: Drive)

The installer needs to be run on individual servers that include Web Component, Base Component, and Advance AI Component server. If Advanced AI components like iKnowledge, Advanced Knowledge and iScrape are not required, only Web Server, Application Server and Database server will be required.

- Alternate Database options

1. AWS Relational Database Service (RDS)
2. GCP SQL Server 2017 PaaS service

- For Document Storage, if *MongoDB has to be made available in HA, then 3 servers will have to be provided as per the best practices. Alternately, MongoDB as a service can be used from AWS and GCP marketplace.

- For Indexer, if Solr has to be made available in HA, then 5 servers will have to be provided as per the best practices.

Ansible Inside Wrapper Component install on Ansible Inside server, it can be installed from any server.

3.2.3 Component Installation Prerequisites

Prior to running the installer, complete all procedures as described in [Environment Planning](#) and ensure that all the software prerequisites for the iAutomate component installation are met.

The following table describes the software requirements to install the components.

Table 11 - Component Installation Prerequisites

Server	Component	Sub-Components	Software Requirements
Web Server	Web Component	- Web UI - Web API - KRS	- IIS 10.0 or above - Dot Net Framework 4.8.x - Microsoft ACE OLEDB 16.0
Application Server	Application Component – Microsoft Dot Net	- Data Collector - RBA Executor - Generic Executor - Release - Generic Listener - AD Sync - Email Service - DAG Service	- Dot Net Framework 4.8.x - Python 3.10.11 64-bit - NLTK - OpenSSL-Win64 - Apache Server 2.4 - VC++ 2022 64-bit Redistributable package - python_prereq

Server	Component	Sub-Components	Software Requirements
		- Assignment Service	
	Application Component - Python	- iParse - iUnique - iRecommend	
Advanced AI Server	Advanced AI Component - Python	- iScrape - iKnowledge - Advanced Knowledge - Knowledge Rating	- Dot Net Framework 4.8.x - Python 3.10.11 64-bit - NLTK - OpenSSL-Win64 - Apache Server 2.4 - VC++ 2022 64-bit Redistributable package - python_prereq - Oracle Distribution of Java JDK 23 (Required only for Solr installation)
Database Server	Database	Transactional Database	MS SQL 2016/2019 /MS SQL 2022 (+) Enterprise / Standard edition 64 bit
MongoDB	- Advanced AI Component - Document Storage	MongoDB	MongoDB 8.0.4
SOLR	- Advanced AI Component - Indexer	SOLR	- SOLR 9.7.0 - nssm 2.24
Certificates (applicable for all tiers)			SSL Certificates

3.3 Prerequisites to Run the Installer

This section provides an overview of the prerequisites to run the installer.

Once the infrastructure is prepared, determine the server where the installer will be run. Prior to running the installer, ensure all prerequisites are ready on the server.

Table 12 - Prerequisites to Run the Installer

Applications	Version
Windows Version	Microsoft® Windows® Server 2012 Standard Edition or Windows Server 2016, 2019 Standard Edition
.Net Framework	.Net Framework 4.8

The requirements mentioned in the following tables indicate the minimum configuration required at the time of installation:

- Table 4 - Minimal Deployment
- Table 6 - Medium Environment without HA
- Table 7 - Large Environment without HA

- Table 8 - Small Environment with HA
- Table 9 - Medium Environment with HA
- Table 10 - Large Environment with HA

Over a period, based on the use of enterprise managed resources, user might have to upgrade to a higher configuration.

3.3.1 Installer

The installer includes an installer executable. This executable enables complete installation of iAutomate and checks the prerequisites for all the servers and components.

3.4 iAutomate Installation

This section explains how to install iAutomate components using the installer on any server or standalone machine. The installer can be further used for deployment of web server, application server, advanced AI server and, database server, and the underlying components.

iAutomate implementation contains the following menus:

- [Run the Installer](#)
- [Install iAutomate](#)

Before running the installer, ensure that the 'write' permission is enabled for the user on the Apache24 folder.

3.4.1 Run the Installer

Review the prerequisites carefully before proceeding with the installation.

After confirming that the system meets the prerequisites to run the iAutomate installer, perform the following steps:

1. To get access to the iAutomate installer package, please get in touch with aiops-pmg-team@hcl-software.com. Copy the zipped installer file to the server where you want to run the iAutomate installer.
2. Unzip and extract all the contents to the default folder.
3. Browse the HCL_iAutomate_v6.5_Installer.exe in the folder and click Run as administrator to start installation.

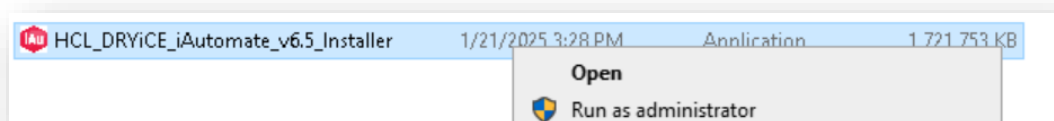


Figure 2 - Run the Installer

3.4.2 Install iAutomate

This section lists the steps to install the iAutomate components on all hosts. Ensure that user meets all requirements in the section [Environment Preparation](#) and [Prerequisites to Run the Installer](#) before starting the installation procedure.

To install iAutomate, perform the following steps:

1. On running the Installer, the following page appears.

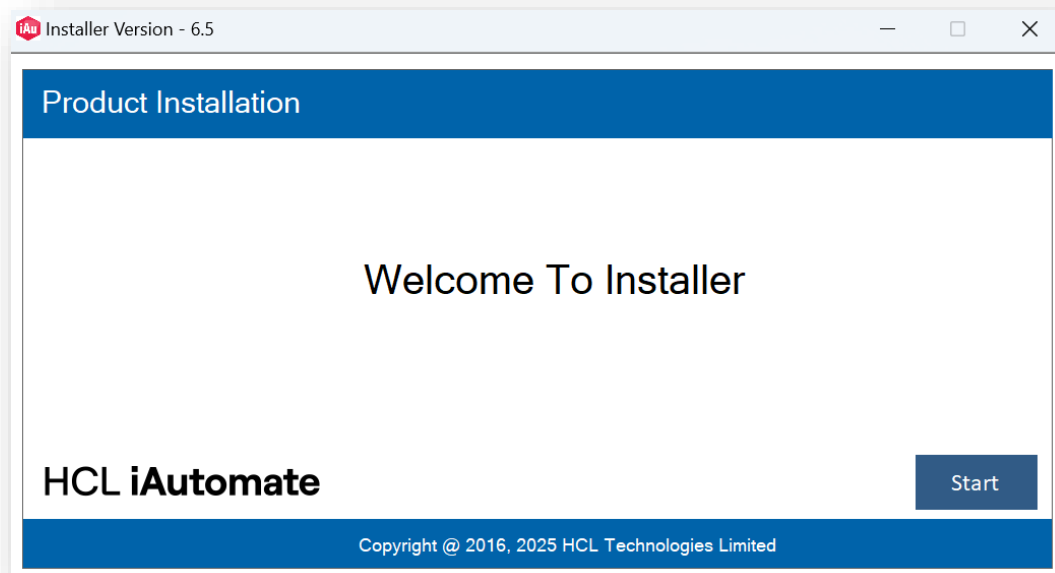


Figure 3 - iAutomate Implementation

2. Click **Start**. It will extract required binaries and the following page appears.

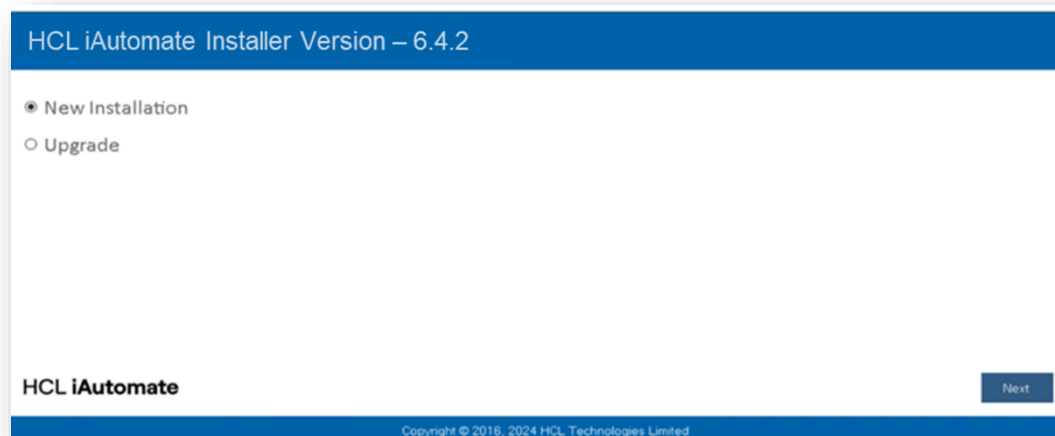


Figure 4 - iAutomate Implementation

3. Click **Next**. The page lists the setup required for installation in the left pane and the details of the selected setup in the right pane.

3.4.3 Database Setup

User can create a customized database using the following steps.

1. On the **Database Details** view, type the **Server Name**, and then the **Database Instance Name**.

Figure 5 - Select Authentication

2. Select the **Authentication** type. The type of login authentication used to configure the database determines the resulting username.
3. There are two types of authentications used for database configuration:
 - Windows Authentication
 - SQL Server Authentication

It is recommended to use windows authentication in production environment.

4. In the **UserName** and **Password** fields, type username and password to access the server.
5. In the **Database Name** field, database is auto filled by default.
6. To check the connectivity to a server using the credentials provided, click **Check Connection**. This displays a message for **Connection Success** or **Connection Failure**.
7. Successful connection to the database enables the **Next** button.

Figure 6 - Test Connection

8. Click **Next**.
The **Component Setup** page appears.

All fields marked with an asterisk (*) are mandatory.

3.4.4 Component Setup

After creating the database, perform the following steps to set up the Web UI components.

1. The **Component Selection** view lists the components, and their corresponding parameters based on the selected component.
2. The following types of components are deployed in iAutomate:
 - **Web Component** - It includes the user interface that enables the configuration, management, and resolution of tickets.
 - **Service Component** - This is further divided into three categories:
 - **Application Component** - This includes essential services that work together to achieve the core functionality of iAutomate.
 - **Ansible Inside Wrapper Component** – This includes wrapper service that works with Ansible inside.
 - **Advanced AI Component** - This includes features like Solution Creation; Natural Language Processing (NLP) based assisted services, and so on.

Component	Parameter	Value	Type
Application Component	Web UI Name	HCLiAutomateBaseUI	Port
	Web API Name	HCLiAutomateWEBAPI	Port
	KRS Name	HCLiAutomateKRS	Port
	iRecommend Name	HCL.iAutomate.iRecomnr	Port
	Entity Name	HCL.iAutomate.EntityMc	Port
	iParse Name	HCL.iAutomate.iParse	Port
	iUnique Name	HCL.iAutomate.iUnique	Port
	Data Collector Name	HCL.iAutomate.DC	Port
	Generic Executor Name	HCL.iAutomate.GenericE	Port
	RBA Executor Name	HCL.iAutomate.RBAComj	Port
	Release Name	HCL.iAutomate.ReleaseS	Port
	AD Sync Name	HCL.iAutomate.ADSyncS	Port
	Email Service Name	HCL.iAutomate.EmailSer	Port

Figure 7 - Component Setup

The administrator can add or remove components based on their environment as decided during the planning phase.

The following table lists the components available on different servers.

Table 13 - iAutomate Components

Server Type	Components	Description
Web Component	Web UI	Web User Interface for Admin, Configuration, Operations Console, Dashboards and Knowledge Analysis and Search functionalities
	Web API	It is an API in the iAutomate web module that can be accessed using the HTTP protocol.

Server Type	Components	Description
	KRS	The Key Rotation Service component which serves the purpose of providing additional security through rotation of keys on a periodic basis.
Application Component	iRecommend	It leverages Natural Language Processing and is responsible for recommending the best suited runbook for resolving the issue based on the ticket description
	iParse	It serves the purpose of analyzing the ticket description and summary for extracting relevant parameters to be passed to configurable runbooks
	iUnique	It helps in clustering the ticket data (incident, service requests, change requests) into different categories for identification of automation opportunities
	Data Collector	It is responsible for collecting ticket information from the ITSM tool
	Generic Executor	It is used for data processing at the DB layer for enabling backend processes.
	RBA Executor	It helps in triggering the identified runbook for automatic resolution using an underlying RBA tool
	Release	It is used to release the ticket in case an appropriate runbook is not recommended OR runbook execution for a ticket fails. In the latter case, the ticket is released and assigned to a human agent.
	Generic Listener	Ticket passes through multiple stages during the resolution lifecycle using iAutomate. Generic Listener module is responsible for ensuring the ticket is moved to the next stage based on the current outcome. Its job is to identify the status of the present stage and based on success / failure, move the ticket to the consequent stage in the lifecycle
	AD Sync	It is responsible for fetching LDAP user from LDAP Server.
	Email Service	It is responsible for sending mail notifications to user
	DAG Service	It is responsible for executing Network Related Use cases.
	Assignment Services	It is used to assign tickets to the group fetched from Gen AI Studio.
Ansible Inside Wrapper Component	Ansible SDK Wrapper	It is responsible for triggering Ansible Inside Tool
Advanced AI Component	Advanced Knowledge	It returns a list of relevant documents for a query that have been crawled from different repositories like SNOW KB, Web URL, Satori repository, and internal files and folders.
	iKnowledge	It returns a list of relevant results from Google for a query, if no relevant documents exist in the organization's repository.
	Knowledge rating	It enables users to provide feedback as a rating for the document search corresponding to the ticket summary.

Server Type	Components	Description
	iScrape	It helps in automated runbook creation for ticket categories for which runbooks don't exist by exploring various internal and external data sources for relevant executable code snippets and scripts.

3. Select the components as planned for the server configuration.
4. Select the **Web Component**, **Application Component**, **Ansible Inside Wrapper Component** or **Advanced AI Component** check boxes to install all the components listed under the servers simultaneously or select a single component to install it individually.
5. After component selection, their corresponding details are auto filled and enables user to select the **Port** for each component.
6. On selecting **Advance AI Components**, user must provide the MongoDB and Solr database details else the setup will display the **Server Configuration** page.
7. To continue with the installation, click Next.
This enables the **Configure MongoDB** and **Solr** tab on the left navigation pane. Type the following details to set up the MongoDB and Solr databases:
8. On the Configure MongoDB page:
 - a. Type the **MongoDB Server Name** (including the port details).
 - b. In the **User ID** and **Password** fields, type username and password to access the server.
 - c. Select the Version Type.
 - d. Select the **HA** mode.
 - e. Based on the selected "**Version Type**" and **HA** mode (selected / unselected), please follow the below steps:

Table 14 - MongoDB Configuration Parameters

Version Type	HA Mode	Number of Servers Required*	CA File Required	PEM File Required
Community	Enabled	At least 3	Not Required	
Community	Disabled	1	Not Required	
Enterprise	Enabled	At least 3	Depends**	Required
Enterprise	Disabled	1	Depends**	Required

* - As per the best practices, number of servers required should be odd in numbers. Provide the list of all MongoDB instances as comma separated pairs of hostname and port.

** -. CA File is only required if and only if MongoDB installation mandates use of CA file

9. On the **Configure Solr** page:
 - a. Type the **Solr Server**.
 - b. In the **User ID** and **Password** fields, type user ID and password to access the server.
 - c. The default port is auto filled in the **PORT** field next to each component.
 - d. Click **Next**.

Configure MongoDB

MongoDB Server *

User ID * Password *

Version Type * Community HA ☐

Pem File

CA file available ☐

CA File

Configure Solr

Solr Server *

User ID * Password *

ZooKeeper Port * Port *

Figure 8 - Configure Mongo DB and Solr

- e. User will be prompted to check the connection status. Click **Yes** to proceed with checking the connection status or **No** to continue with the Installation.

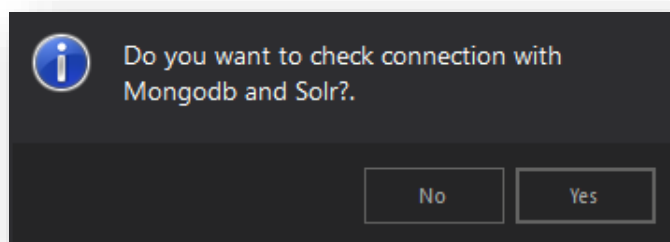


Figure 9 - Check Mongo DB and Solr Connection Status

The Server Configuration page appears.

All fields marked with an asterisk (*) are mandatory.

3.4.5 Server Configuration

This section describes how to set up and configure a server for iAutomate installation.

To configure servers, provide the following details:

1. The **IP Address/Host Name**, where user wants to install the components.

The installer automatically detects the host name where the installer is running and auto-fills the information in the text box.

2. Select the **Account Type** from the available options:
 - Local Administrator
 - Domain Account
3. Type the Domain Name.

Server Configuration ?

IP Address/HostName *

Account Type * Domain Account ▼ Domain *

User Name * Password *

Installation Path *

Figure 10- Server Configuration

4. In the **UserName** and **Password** fields, type the login credentials to access the application server.
5. Click **Check User Validity** to validate the user to connect to the server.
6. Click **Browse** to specify the appropriate **Installation Path** to install the server components.
7. On successful connection to the server, a **Validation Successful** message appears beside the Password field.

Server Configuration ?

IP Address/HostName *

Account Type * Domain Account ▼ Domain *

User Name * Password * **Validation Successful**

Installation Path *

Figure 11 - Successful Validation

8. Click **Next**.
The **Pre-Requisite Checker** page appears.

All fields marked with an asterisk (*) are mandatory.

9. If “Ansible Inside Wrapper Component” has been chosen below screen appear,

The image shows two windows from a software installation process. The top window, titled "Server Configuration", contains fields for "IP Address/HostName", "Account Type" (set to "Domain Account"), "Domain", "User Name", and "Password". A "Check User Validity" button is located below the "User Name" and "Password" fields. The "Installation Path" field has a "Browse" button next to it. The bottom window, titled "Ansible Wrapper Component Server Configuration", contains fields for "IP Address/HostName", "User Name", and "Password", with a "Check User Validity" button below the "User Name" and "Password" fields. Both windows have "Back" and "Next" buttons at the bottom.

Figure 12- Server Configuration

10. Ansible Wrapper Component Server Configuration: -

- a. The **IP Address/Host Name**, where user wants to install the components.

The Ansible Inside Wrapper install on server where Ansible Wrapper is installed.

- b. In the User Name and Password fields, type the login credentials to access the server.
- c. Click Check User Validity to validate the user to connect to the server.
- d. On successful connection to the server, a Validation Successful message appears beside the **Password** field.

This image shows the same two windows as Figure 12, but with a green "Validation Successful" message displayed below the "Password" field in both the "Server Configuration" and "Ansible Wrapper Component Server Configuration" windows. The "Check User Validity" buttons are no longer visible, indicating they have been clicked.

Figure 13 - Successful Validation

11. Click **Next**.

The Pre-Requisite Checker page appears.

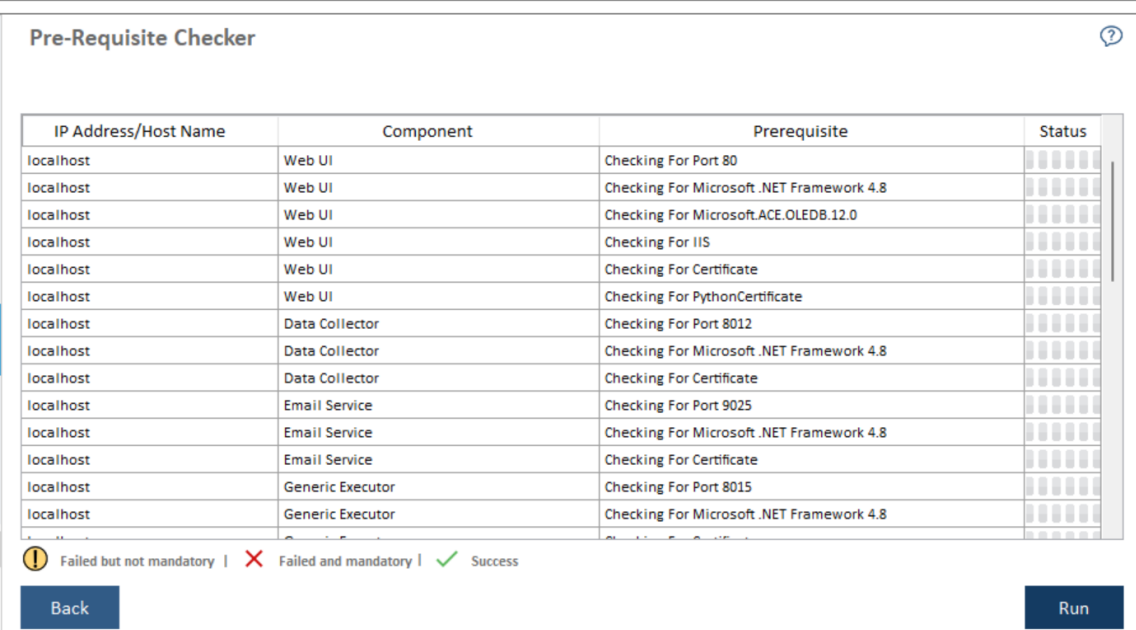
All fields marked with an asterisk (*) are mandatory.

3.4.6 Run Pre-Requisite Checker

This section describes the procedure to check if all iAutomate installation prerequisites have been met before the installation. The Prerequisite Checker identifies all the missing pre-requisite software and utilities. User will have to ensure that the identified prerequisites are installed manually before proceeding further.

To run the **Prerequisite Checker**, perform the following steps:

1. Click **Run**.



The screenshot shows the 'Pre-Requisite Checker' window. It contains a table with four columns: 'IP Address/Host Name', 'Component', 'Prerequisite', and 'Status'. The table lists various components like Web UI, Data Collector, Email Service, and Generic Executor, along with their respective prerequisites such as Port 80, .NET Framework 4.8, and Microsoft.ACE.OLEDB.12.0. The status column shows progress bars for each prerequisite. Below the table, there is a legend: a yellow warning icon for 'Failed but not mandatory', a red X for 'Failed and mandatory', and a green checkmark for 'Success'. At the bottom, there are 'Back' and 'Run' buttons.

IP Address/Host Name	Component	Prerequisite	Status
localhost	Web UI	Checking For Port 80	
localhost	Web UI	Checking For Microsoft .NET Framework 4.8	
localhost	Web UI	Checking For Microsoft.ACE.OLEDB.12.0	
localhost	Web UI	Checking For IIS	
localhost	Web UI	Checking For Certificate	
localhost	Web UI	Checking For PythonCertificate	
localhost	Data Collector	Checking For Port 8012	
localhost	Data Collector	Checking For Microsoft .NET Framework 4.8	
localhost	Data Collector	Checking For Certificate	
localhost	Email Service	Checking For Port 9025	
localhost	Email Service	Checking For Microsoft .NET Framework 4.8	
localhost	Email Service	Checking For Certificate	
localhost	Generic Executor	Checking For Port 8015	
localhost	Generic Executor	Checking For Microsoft .NET Framework 4.8	

⚠ Failed but not mandatory | ✖ Failed and mandatory | ✔ Success

Back Run

Figure 14 - Prerequisite Checker

The **Pre-requisite Checker** always runs as part of the iAutomate setup.

2. A progress bar appears while the **Pre-Requisite Checker** runs.

IP Address/Host Name	Component	Prerequisite	Status
localhost	Web UI	Checking For Certificate	✓
localhost	Web UI	Checking For PythonCertificate	✓
localhost	Data Collector	Checking For Port 8012	✗
localhost	Data Collector	Checking For Microsoft .NET Framework 4.8	✓
localhost	Data Collector	Checking For Certificate	✓
localhost	Email Service	Checking For Port 9025	✗
localhost	Email Service	Checking For Microsoft .NET Framework 4.8	✓
localhost	Email Service	Checking For Certificate	✓
localhost	Generic Executor	Checking For Port 8015	✗
localhost	Generic Executor	Checking For Microsoft .NET Framework 4.8	✓
localhost	Generic Executor	Checking For Certificate	✓
localhost	iKnowledge	Checking For Port 8024	✗
localhost	iKnowledge	Checking For Python 3.6.0	✓
localhost	iKnowledge	Checking For Apache 2.4	✓

Failed but not mandatory |
 Failed and mandatory |
 Success

Back Re-Run

Figure 15 - Pre-Requirement Checking in Progress

- In the **Status** column, each prerequisite is marked a success or a failure.

IP Address/Host Name	Component	Prerequisite	Status
localhost	Web UI	Checking For Certificate	✓
localhost	Web UI	Checking For PythonCertificate	✓
localhost	Data Collector	Checking For Port 8012	✗
localhost	Data Collector	Checking For Microsoft .NET Framework 4.8	✓
localhost	Data Collector	Checking For Certificate	✓
localhost	Email Service	Checking For Port 9025	✗
localhost	Email Service	Checking For Microsoft .NET Framework 4.8	✓
localhost	Email Service	Checking For Certificate	✓
localhost	Generic Executor	Checking For Port 8015	✗
localhost	Generic Executor	Checking For Microsoft .NET Framework 4.8	✓
localhost	Generic Executor	Checking For Certificate	✓
localhost	iKnowledge	Checking For Port 8024	✗
localhost	iKnowledge	Checking For Python 3.6.0	✓
localhost	iKnowledge	Checking For Apache 2.4	✓

Failed but not mandatory |
 Failed and mandatory |
 Success

Back Re-Run

Figure 16 - Pre-Requirement Checker Status

- In case of failure, Re-Run button appears.
- Please ensure that the identified issue is resolved and re-run the pre-requisite checker.

- Upon successful validation of all the pre-requisites, **Next** button is enabled.
- Click **Export** to export the **Pre-Requirement Checker** report, if required.

Pre-Requisite Checker			
Total No of Request 46 Successful 46 Failed 0			
Export			
IP Address/Host Name	Component	Prerequisite	Status
localhost	Web UI	Checking For Microsoft.ACE.OLEDB.12.0	✓
localhost	Web UI	Checking For IIS	✓
localhost	Web UI	Checking For Certificate	✓
localhost	Web UI	Checking For PythonCertificate	✓
localhost	Data Collector	Checking For Port 8014	✓
localhost	Data Collector	Checking For Microsoft .NET Framework 4.8	✓
localhost	Data Collector	Checking For Certificate	✓
localhost	Email Service	Checking For Port 9026	✓
localhost	Email Service	Checking For Microsoft .NET Framework 4.8	✓
localhost	Email Service	Checking For Certificate	✓
localhost	Generic Executor	Checking For Port 8016	✓
localhost	Generic Executor	Checking For Microsoft .NET Framework 4.8	✓
localhost	Generic Executor	Checking For Certificate	✓
localhost	iParse	Checking For Port 8007	✓

 Failed but not mandatory |
  Failed and mandatory |
  Success

Back

Next

Figure 17 - Prerequisite Checker Report

Use **Back** to go to the previous page.

6. Click Next. The **Configure Admin Details** page appears.

3.4.7 Configure Admin Details

Administrative roles provide controlled decentralization of administrative responsibilities and the functionality to add or manage more administrators or users, manage settings, and perform governance actions.

This section describes the steps involved to configure the Super Administrator which is required after the initial setup of iAutomate.

To configure **Super Administrator** details, perform the following steps:

1. On the **Configure Admin Details** page, type the new administrator's **Name**, **Email** and **Password**.

Configure Admin Details

Name *

Email *

Password *

Re-enter Password *

Password Policy: Password must contain at least 1 capital letter, 1 small letter, 1 number and 1 special character and 8-15 characters length. Space not allowed. Only !, @, #, \$, % Special characters are allowed.

Figure 18 - Configure Admin Details

If the database provided in the [Database Setup](#) already exists at the time of installation, then the **Configure Admin Details** page will remain unavailable.

2. Post installation, the administration console can be accessed by this **Super Administrator** account to configure iAutomate.
3. Click **Next** to review the information provided on previous pages.

Click **Reset** to reset the admin credentials. Click **Back** to navigate to the previous pages for making any changes. All fields marked with an asterisk (*) are mandatory.

3.4.8 Install

This section describes the installation of iAutomate after all components and admin configuration is completed.

1. Before proceeding with the Installation, review the information on the **Installation** page and, if required, click **Back** to make any changes.
2. Click **Run** to start the installation.

Installation Overall Status : Not yet started ?

Server Type : Database

Server Details

IP/Hostname Address :

Database

Database Instance: ■■■■■■■■■■

Database Name:

Server Type : Web | Application

Server Details

IP Address : User Name :

Web UI

Component Name: Web UI ■■■■■■■■■■

Site Name: HCLiAutomateBaseUI

Path : C:\NewFolder

Back Run

Figure 19 – Installation

The progress bar displays the installation progress.

Installation OverAll Status In Progress ?

Server Type : DataBase

Server Details

IP/Hostname Address :

DataBase

DataBase Instance: ■■■■■■■■■■

Database Name:

Server Type : Web

Server Details

IP Address : User Name :

Web UI

Component Name: Web UI ■■■■■■■■■■

Site Name: HCLiAutomateBaseUI

Path : C:\iAutomateComponent

Exit

Figure 20 - Installation Progress

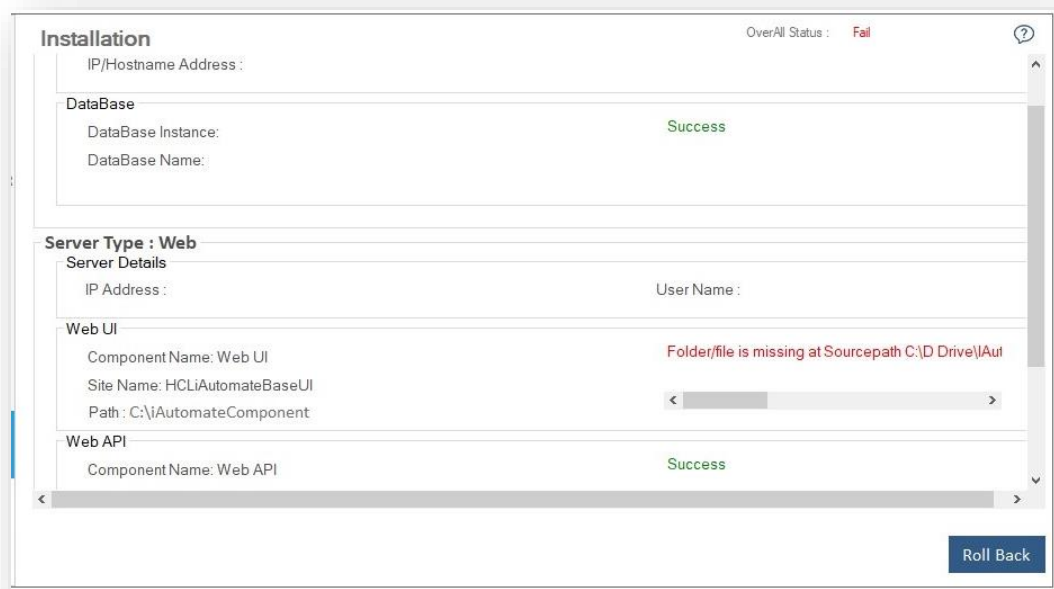


Figure 21 - Installation Progress (In case of failure)

In case of installation failure, error messages for the corresponding component appear on the screen. Click **Rollback** button to uninstall the components and re-run the Installer after resolving the issues. To perform the cleanup, delete all the folders manually on the server installation path provided earlier. Contact the product team administrator for further assistance.

- After successful installation, the **Launch Application** button appears. Click **Exit** to exit the installer.

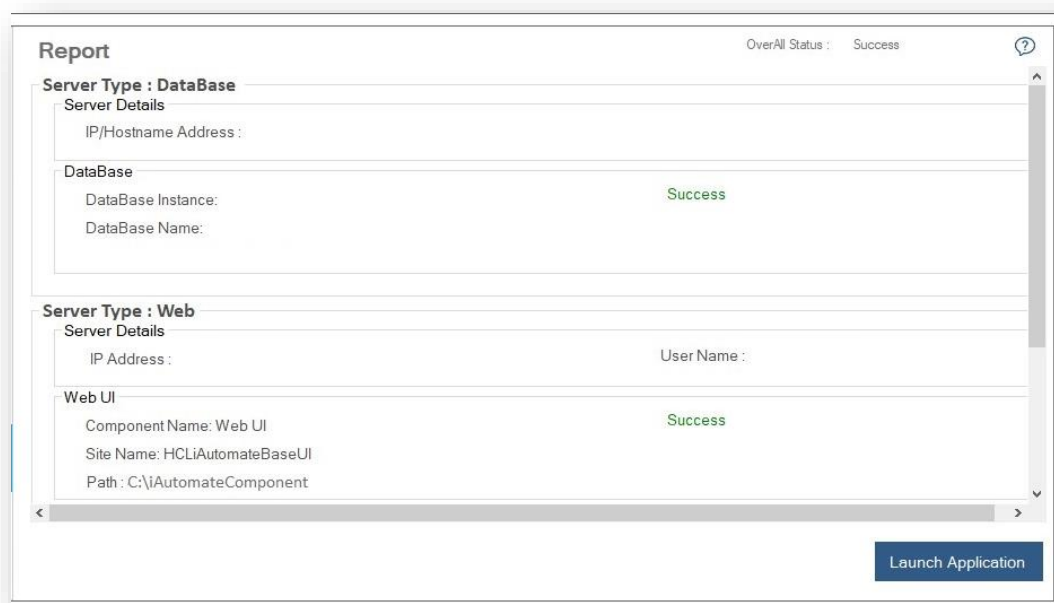


Figure 22 - Installation Successful

- Click **Launch Application** button to start iAutomate.

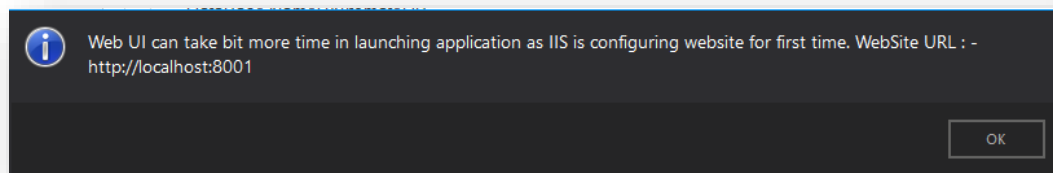


Figure 23 - Message on Launching iAutomate

5. Click **OK** to navigate to the **iAutomate Login Page**.

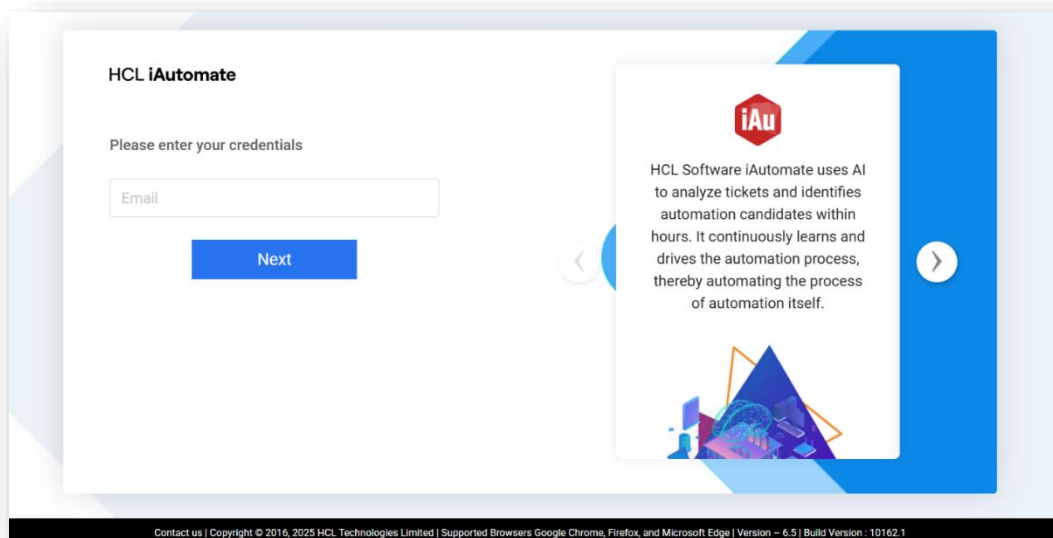


Figure 24 - iAutomate Login Page

6. After the login page is opened, it asks for the **License key**.

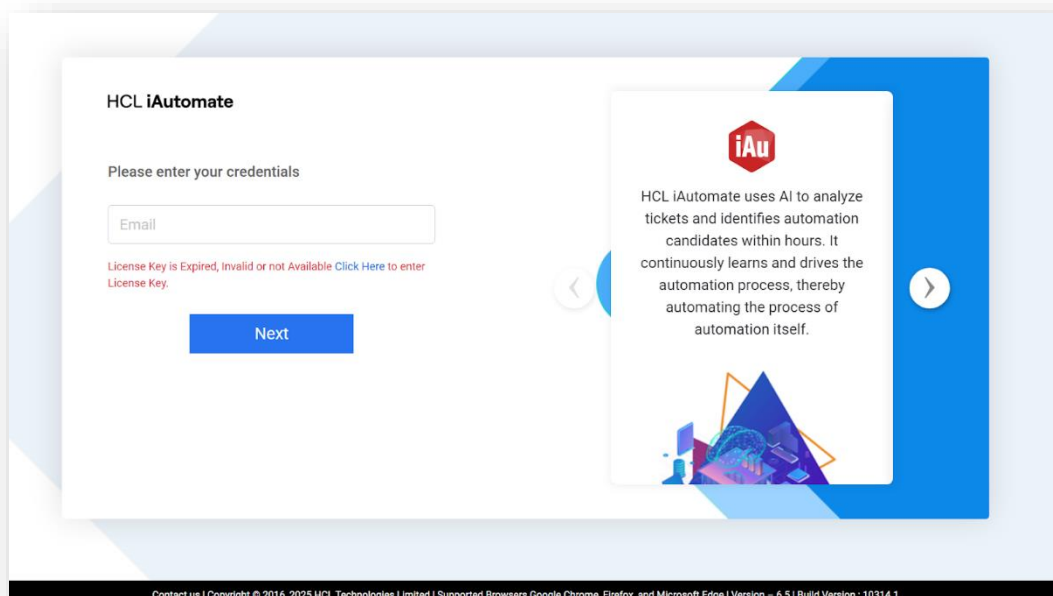


Figure 25 - iAutomate Login Page (Cont.)

7. Click on '**Click Here**' hyperlink to enter the license key.

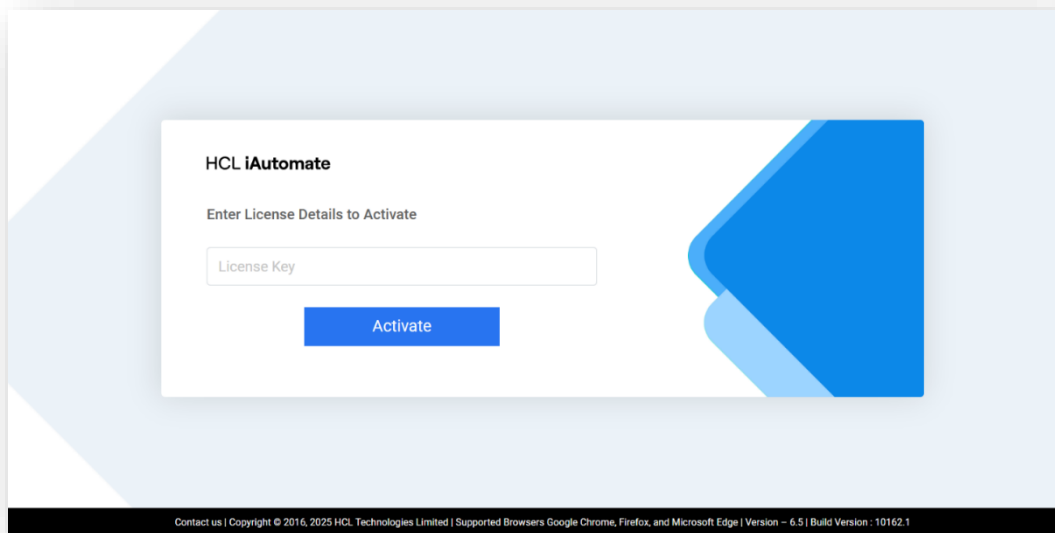


Figure 26 - iAutomate Login Page (Cont.)
License Key

8. Submit the license key.

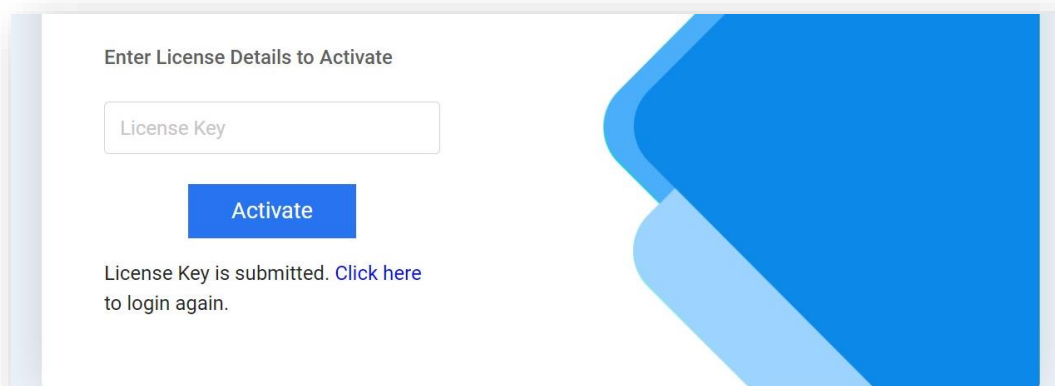


Figure 27 - iAutomate Login Page (Cont.)
License Key

9. Click on the **Click Here** link again to login again.

3.5 iAutomate Upgradation

This section lists the steps to upgrade iAutomate components on all hosts.

3.5.1 Install iAutomate

To upgrade iAutomate, perform the following steps:

1. On running the Installer, the following page appears.

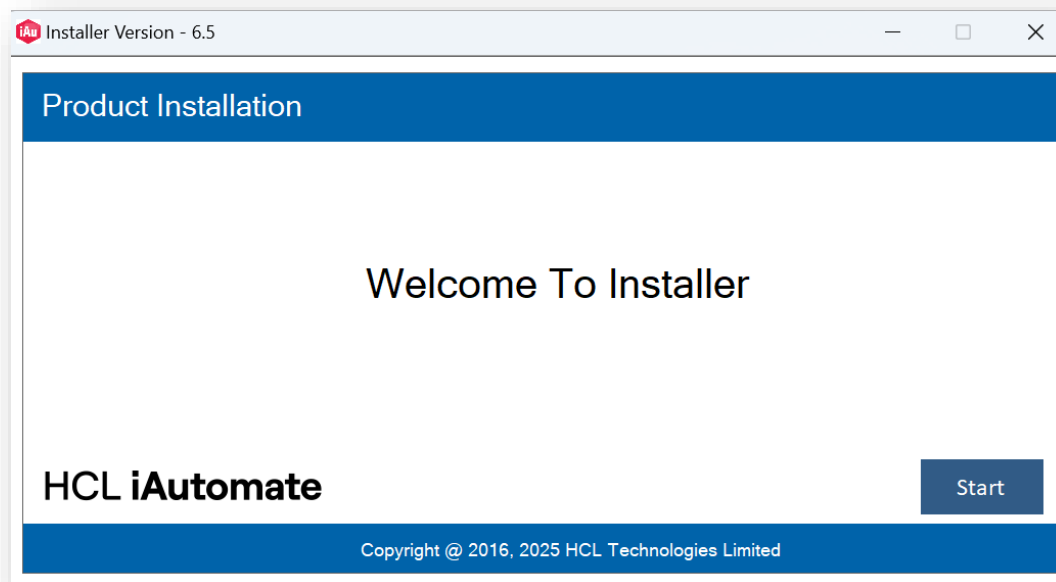


Figure 28 - iAutomate Implementation

2. Click **Start**. It will extract required binaries and the following page appears.
3. Select **Upgrade**.

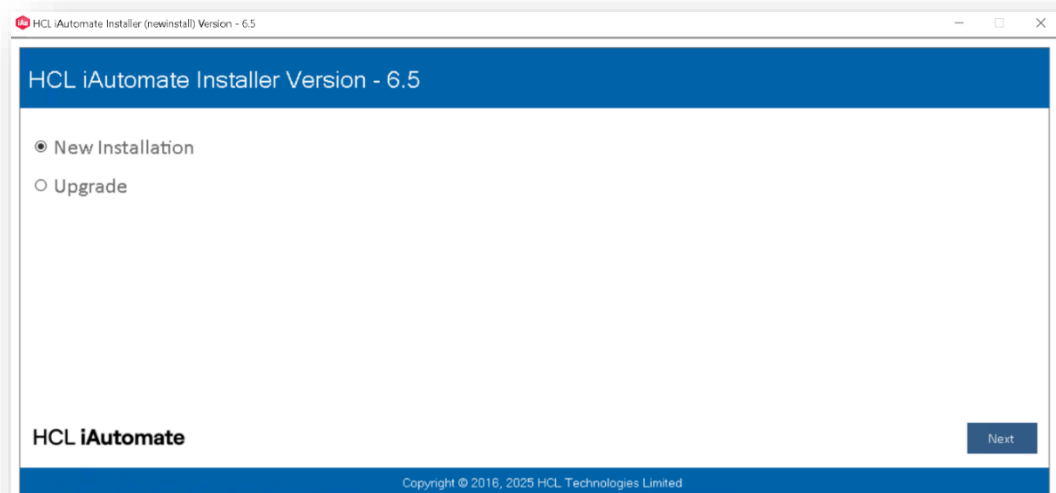


Figure 29 - iAutomate Upgradation

4. Click **Next**.
5. The page lists the setup required for installation in the left pane and the details of the selected setup in the right pane.

Figure 30 - Database Details

The next step is to update the database.

3.5.2 Database Setup

1. On the **Database Details** view, type the **Server Name**, and the **Database Instance Name**.

Figure 31 – Database Setup

2. Select the **Authentication** type. The type of login authentication used to configure the database determines the resulting username.
3. There are two types of authentications used for database configuration:
 - Windows Authentication
 - SQL Server Authentication

It is recommended to use windows authentication in production environment.

4. In the **UserName** and **Password** fields, type username and password to access the server.
5. In the **Database Name** field is auto filled by default.
6. To check the connectivity to a server using the credentials provided, click **Check Connection**.
7. On successful connection to the database, below screen appears.

Figure 32 – Database Setup(cont.)

8. Select **ServerHost/IP** on which the upgrade is required.
9. Click **Next**. The **Component Setup** page appears.

All fields marked with an asterisk (*) are mandatory.

3.5.3 Component Setup

After creating the iAutomate database, perform the following steps to set up the Web UI components.

1. The **Component Selection** view lists the components and their corresponding parameters based on the selected component. A ★ is displayed against each component which was installed earlier on previously selected server host/IP.

Web UI Name	Web API Name	KRS Name	iRecommend Name	Entity Name	iParse Name	iUnique Name	Data Collector Name	Generic Executor Name	RBA Executor Name	Release Name	AD Sync Name	Email Service Name
HCLiAutomateBaseUI	HCLiAutomateWEBAPI	HCLiAutomateKRS	HCLiAutomate.iRecomm	HCLiAutomate.EntityMc	HCLiAutomate.iParse	HCLiAutomate.iUnique	HCLiAutomate.DC	HCLiAutomate.GenericE	HCLiAutomate.RBACom	HCLiAutomate.ReleaseS	HCLiAutomate.ADSyncS	HCLiAutomate.EmailSer
Port	Port	Port	Port	Port	Port	Port	Port	Port	Port	Port	Port	Port
80	8080	8085	9000	9003	8006	8009	8012	8015	8018	8021	9022	9025

Figure 33 – Component Setup

2. Select the components as planned for the server configuration.
3. Select the **Web Component**, **Application Component**, **Ansible Inside Wrapper Component** or **Advanced AI Component** check boxes to install all the components listed under the servers simultaneously or select a single component to install it individually.
4. After component selection, their corresponding details are auto filled and enables user to select the Port for each component.

5. Click **Next**. The **Server Configuration** page appears.

All fields marked with an asterisk (*) are mandatory.

3.5.4 Server Configuration

This section describes how to set up and configure a server for iAutomate installation.

To configure servers, provide the following details:

1. All the server configuration is pre-populated based on the previously selected previously selected server host/IP.

User can only change the username and password.

The screenshot shows the 'Server Configuration' window. It contains several input fields: 'IP Address/HostName' with a dropdown arrow, 'Account Type' with a dropdown menu set to 'Domain Account', 'User Name', 'Password', 'Domain' (with placeholder 'Enter Domain'), and 'Installation Path' (with a 'Browse' button). A 'Check User Validity' button is positioned below the 'User Name' and 'Password' fields. All fields have a red asterisk indicating they are mandatory.

Figure 34 – Server Configuration

2. Enter Password and Click **Check User Validity** to validate the user to connect to the server.
3. On successful connection to the server, a **Validation Successful** message appears beside the **Password** field.

This screenshot shows the 'Server Configuration' window after validation. A green 'Validation Successful' message is displayed next to the 'Password' field. The 'Installation Path' field now contains the text 'C:\AutomateInstaller'. The 'Back' and 'Next' buttons are visible at the bottom of the window.

Figure 35 - Server Configuration (cont.)

4. Click **Next**. The **Pre-Requirement Checker** page appears.

All fields marked with an asterisk (*) are mandatory.

5. If “Ansible Inside Wrapper Component” has been chosen below screen appear,

Server Configuration

IP Address/HostName *

Account Type * Domain Account Domain *

User Name * Password *

Installation Path *

Ansible Wrapper Component Server Configuration

IP Address/HostName *

User Name * Password *

Figure 36- Server Configuration

6. Ansible Wrapper Component Server Configuration: -
 - a. The IP Address/Host Name, where user wants to install the components.

The Ansible Inside Wrapper install on server where Ansible Wrapper is installed.

- b. In the User Name and Password fields, type the login credentials to access the server.
 - c. Click Check User Validity to validate the user to connect to the server.
 - d. On successful connection to the server, a Validation Successful message appears beside the Password field.

Server Configuration

IP Address/HostName *

Account Type * Domain Account Domain *

User Name * Password *

Installation Path *

Ansible Wrapper Component Server Configuration

IP Address/HostName *

User Name * Password *

Figure 37 - Successful Validation

7. Click **Next**.
The Pre-Requisite Checker page appears.

All fields marked with an asterisk (*) are mandatory.

3.5.5 Run Pre-Requisite Checker

This section describes the procedure to check if all iAutomate installation prerequisites have been met before the installation. The Prerequisite Checker identifies all the missing pre-requisite software and utilities. User will have to ensure that the identified prerequisites are installed manually before proceeding further.

To run the **Prerequisite Checker**, perform the following steps:

1. Click **Run**.

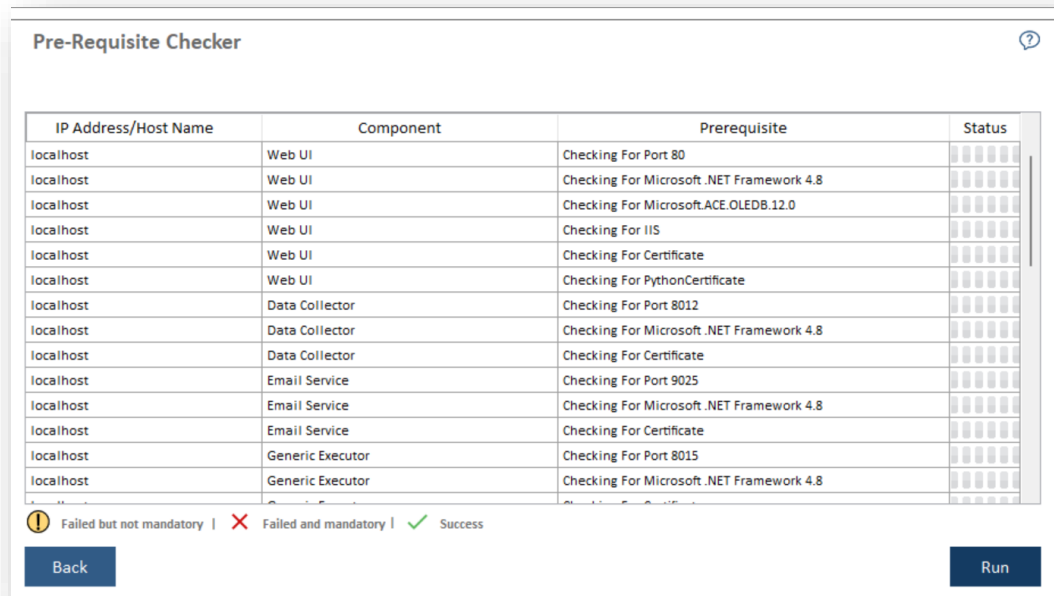


Figure 38 - Prerequisite Checker

The **Pre-requisite Checker** always runs as part of the iAutomate setup.

2. A progress bar appears while the **Pre-Requirement Checker** runs.

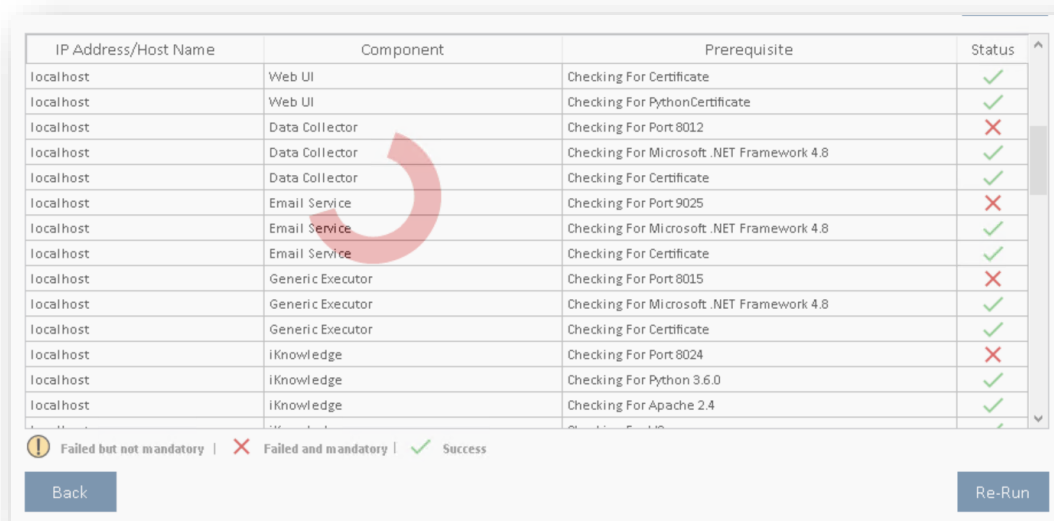


Figure 39 - Pre-Requirement Checking in Progress

3. In the **Status** column, each prerequisite is marked a success or a failure.

IP Address/Host Name	Component	Prerequisite	Status
localhost	Web UI	Checking For Certificate	✓
localhost	Web UI	Checking For PythonCertificate	✓
localhost	Data Collector	Checking For Port 8012	✗
localhost	Data Collector	Checking For Microsoft .NET Framework 4.8	✓
localhost	Data Collector	Checking For Certificate	✓
localhost	Email Service	Checking For Port 9025	✗
localhost	Email Service	Checking For Microsoft .NET Framework 4.8	✓
localhost	Email Service	Checking For Certificate	✓
localhost	Generic Executor	Checking For Port 8015	✗
localhost	Generic Executor	Checking For Microsoft .NET Framework 4.8	✓
localhost	Generic Executor	Checking For Certificate	✓
localhost	iKnowledge	Checking For Port 8024	✗
localhost	iKnowledge	Checking For Python 3.6.0	✓
localhost	iKnowledge	Checking For Apache 2.4	✓

Failed but not mandatory |
 Failed and mandatory |
 Success

[Back](#)
[Re-Run](#)

Figure 40 - Pre-Requirement Checker Status

In case of failure, **Re-Run** button appears.

Please ensure that the identified issue is resolved and re-run the pre-requisite checker.

- Upon successful validation of all the pre-requisites, **Next** button is enabled.
- Click **Export** to export the **Pre-Requirement Checker** report, if required.

IP Address/Host Name	Component	Prerequisite	Status
localhost	Web UI	Checking For Microsoft.ACE.OLEDB.12.0	✓
localhost	Web UI	Checking For IIS	✓
localhost	Web UI	Checking For Certificate	✓
localhost	Web UI	Checking For PythonCertificate	✓
localhost	Data Collector	Checking For Port 8014	✓
localhost	Data Collector	Checking For Microsoft .NET Framework 4.8	✓
localhost	Data Collector	Checking For Certificate	✓
localhost	Email Service	Checking For Port 9026	✓
localhost	Email Service	Checking For Microsoft .NET Framework 4.8	✓
localhost	Email Service	Checking For Certificate	✓
localhost	Generic Executor	Checking For Port 8016	✓
localhost	Generic Executor	Checking For Microsoft .NET Framework 4.8	✓
localhost	Generic Executor	Checking For Certificate	✓
localhost	iParse	Checking For Port 8007	✓

Failed but not mandatory |
 Failed and mandatory |
 Success

[Back](#)
[Next](#)

Figure 41 - Prerequisite Checker Report

Click **Back** to go to the previous page.

- Click **Next**. The **Install** page appears.

3.5.6 Install

This section describes the installation of iAutomate after all components and admin configuration is completed.

- Before proceeding with the Installation, review the information on the **Installation** page and, if required, click **Back** to make any changes.
- Click **Run** to start the installation.

Installation Overall Status : Not yet started ?

Server Type : Database

Server Details

IP/Hostname Address :

Database

Database Instance: ■■■■■■■■■■

Database Name: ■■■■■■■■■■

Server Type : Web | Application

Server Details

IP Address : User Name :

Web UI

Component Name: Web UI ■■■■■■■■■■

Site Name: HCLiAutomateBaseUI

Path : C:\NewFolder

Back Run

Figure 42 – Installation

The progress bar displays the installation progress.

Installation OverAll Status In Progress ?

Server Type : DataBase

Server Details

IP/Hostname Address :

DataBase

DataBase Instance: ■■■■■■■■■■

Database Name: ■■■■■■■■■■

Server Type : Web

Server Details

IP Address : User Name :

Web UI

Component Name: Web UI ■■■■■■■■■■

Site Name: HCLiAutomateBaseUI

Path : C:\iAutomateComponent

Exit

Figure 43 - Installation Progress

Installation OverAll Status : **Fail**

IP/Hostname Address :

DataBase

DataBase Instance: **Success**

DataBase Name:

Server Type : Web

Server Details

IP Address : User Name :

Web UI

Component Name: Web UI **Folder/file is missing at Sourcepath C:\D Drive\IAul**

Site Name: HCLiAutomateBaseUI

Path : C:\iAutomateComponent

Web API

Component Name: Web API **Success**

Roll Back

Figure 44 - Installation Progress (In case of failure)

In case of installation failure, error messages for the corresponding component appear on the screen. Click **Rollback** button to uninstall the components and re-run the Installer after resolving the issues. To perform the cleanup, delete all the folders manually on the server installation path provided earlier. Contact the product team administrator for further assistance.

- After successful installation, the **Launch Application** button appears. Click **Exit** to exit the installer.

Report OverAll Status : **Success**

Server Type : DataBase

Server Details

IP/Hostname Address :

DataBase

DataBase Instance: **Success**

DataBase Name:

Server Type : Web

Server Details

IP Address : User Name :

Web UI

Component Name: Web UI **Success**

Site Name: HCLiAutomateBaseUI

Path : C:\iAutomateComponent

Launch Application

Figure 45 - Installation Successful

- Click **Launch Application** to start iAutomate.

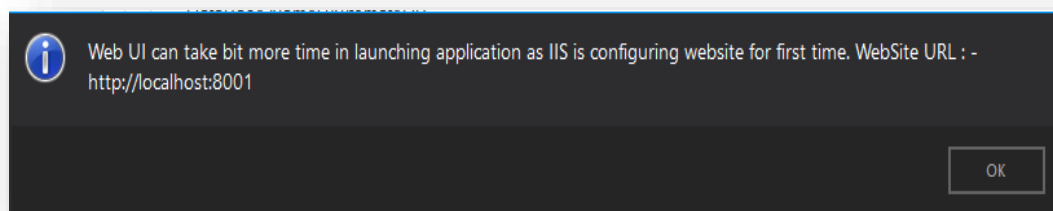


Figure 46 - Message on Launching iAutomate

5. Click **OK** to navigate to the **iAutomate Login Page**.

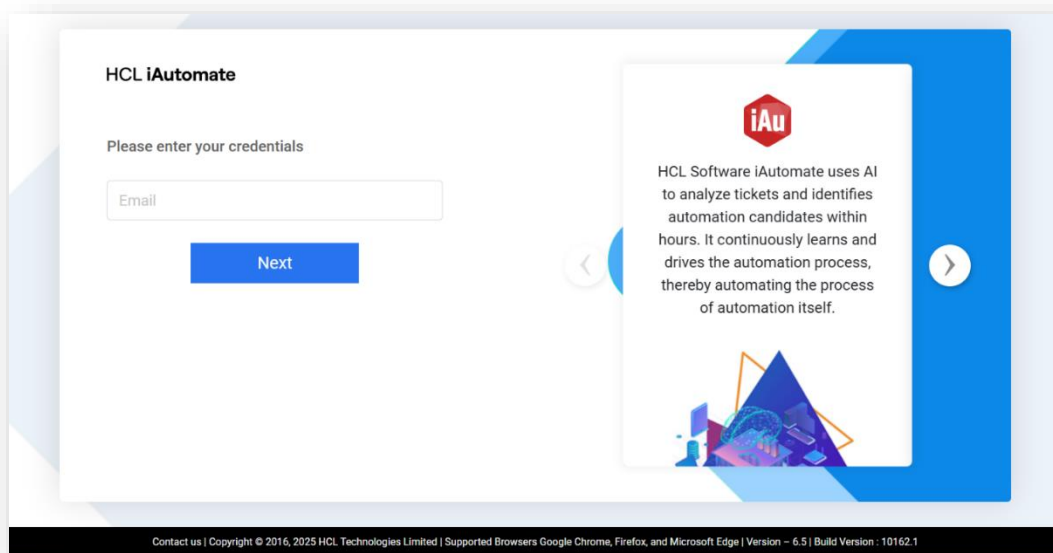


Figure 47 - iAutomate Login Page

6. After login page is opened, its asks for License key.

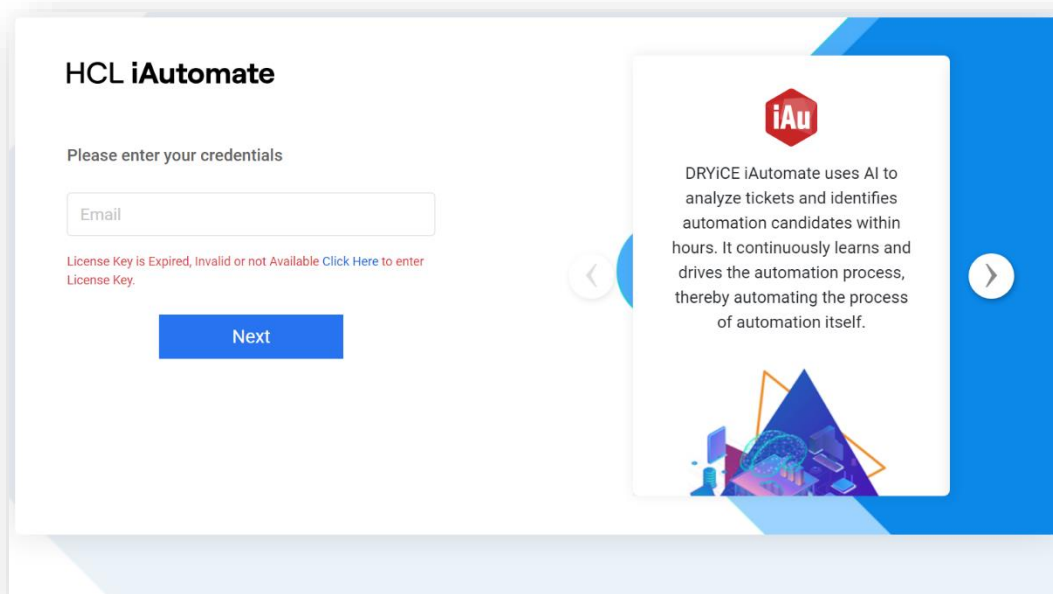


Figure 48 - iAutomate Login Page (Cont.)

7. Click on 'Click Here' hyperlink to enter the license key.

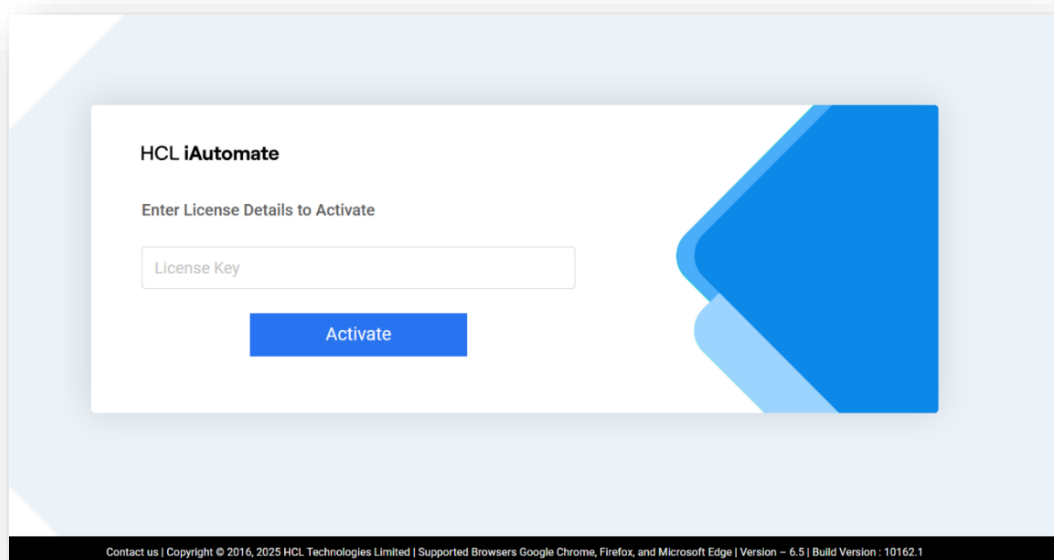


Figure 49 - iAutomate Login Page (Cont.) License Key

8. Submit the license key and login again by clicking on the **Click Here** link.

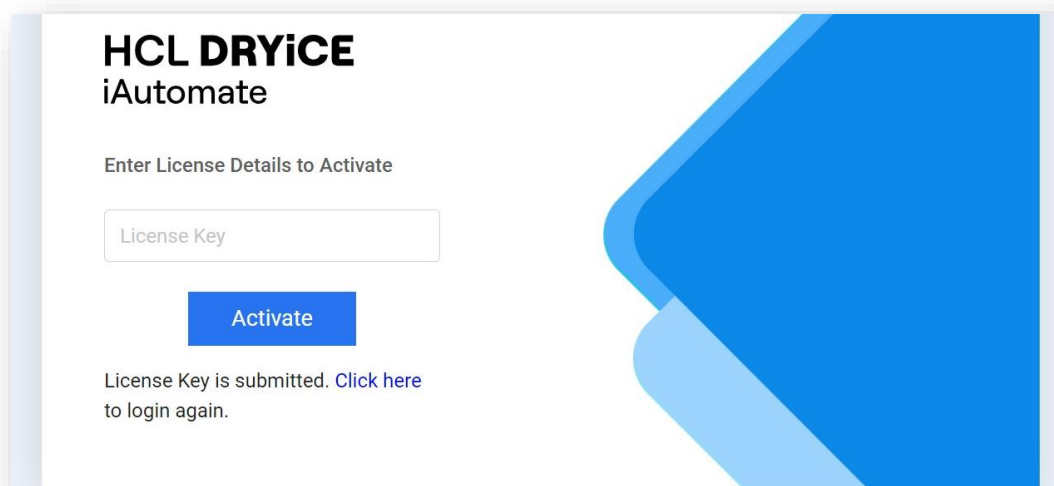


Figure 50 - iAutomate Login Page (Cont.) License Key

After Upgrade, kindly check all configurations (Credentials) on screens (Mange Runbook Tool, Data Source details, Manage SMTP, Mange Proxy, Component Key Value Configuration etc.) are visible, if not kindly enter again and click on save/update button.

3.6 Post Installation Activities

This section describes how to perform certain post installation activities which are strictly dependent on the organization's requirements.

It includes the following:

- [Enable Secure Communication \(Changing HTTP to HTTPS\)](#)
- [Configuration Changes – Certificate Name Change \(Type – PFX\)](#)
- [Configuration Changes – Certificate Name Change \(for PEM/CRT/KEY Certificates\)](#)
- [Load Balancer Configuration](#)

- [Configuration Changes - Access iAutomate without Certificate \(Type – PFX\)](#)
- [Configuration Changes - Access iAutomate with Certificate \(Type – PFX\)](#)
- [Configuration Changes - Access iAutomate without Certificate \(Type – PEM\)](#)
- [Configuration Changes – SaaS based Ticket Analysis](#)
- [Configuration Changes – Run BASEUI and WEBAPI on same port](#)

All the post installation activities listed above are optional.

3.6.1 Enable Secure Communication (Changing HTTP to HTTPS)

This section describes how to enable secure communication by changing HTTP to HTTPS. It can be enabled for both the iAutomate website and the deployed components.

3.6.1.1 Website Only

This section describes how to enable the secure communication by changing HTTP to HTTPS for the iAutomate website.

The following changes are required in the underlying components to achieve the same.

3.6.1.1.1 Key Rotation Service (KRS)

To change the hosting of KRS from HTTP to HTTPS using the existing certificate, for e.g. 'HclTech.iautomate.Web', please follow the below steps:

1. Press **Win+R** and type **inetmgr**.
2. Click **OK** to open **IIS**.

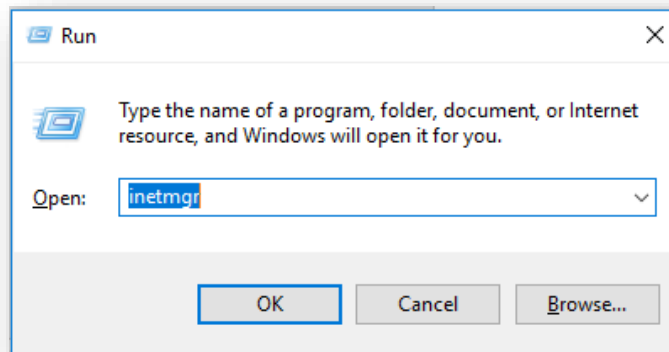


Figure 51 - Hosting KRS from HTTP to HTTPS

3. Expand Sites and click **HCLiAutomateKRS**.

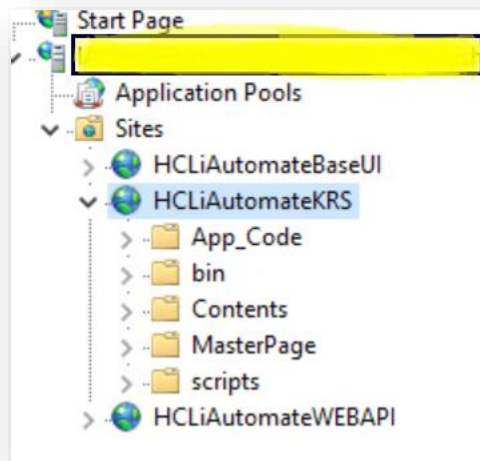


Figure 52 - Hosting KRS from HTTP to HTTPS (cont.)

4. Click on **Bindings** in the **Edit Site** section.

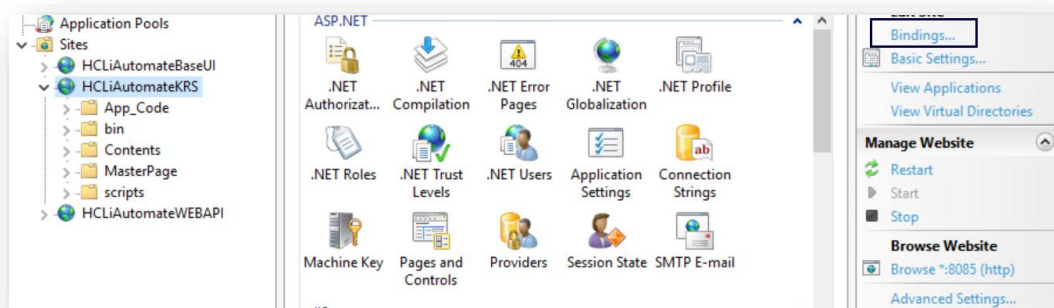


Figure 53 - Hosting KRS from HTTP to HTTPS (cont.)

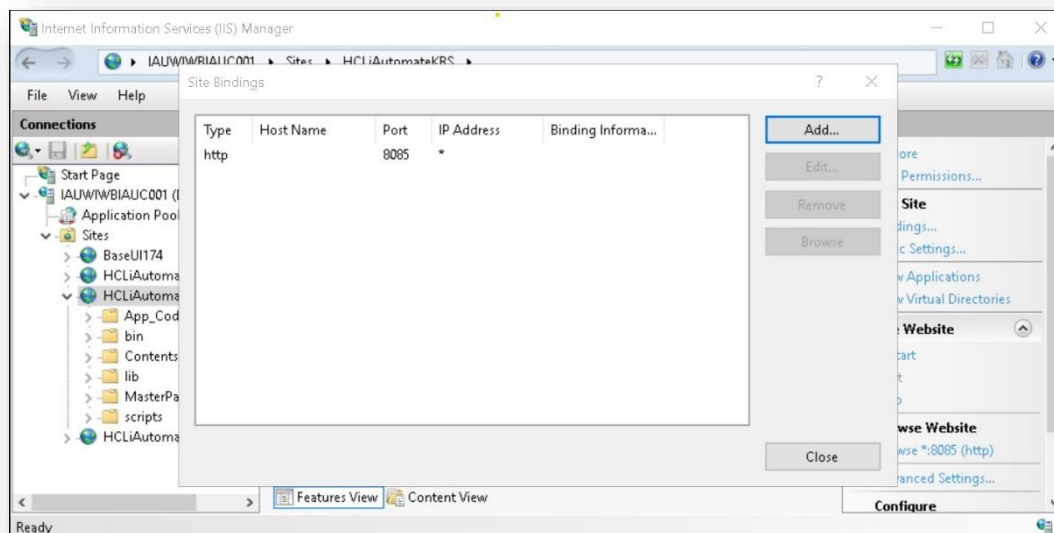


Figure 54 - Hosting KRS from HTTP to HTTPS (cont.)

5. Click **Add New**.
6. Select **Type** as '**https**'. **Port** information gets populated automatically. Select the **SSL Certificate**.
7. Click **OK**.

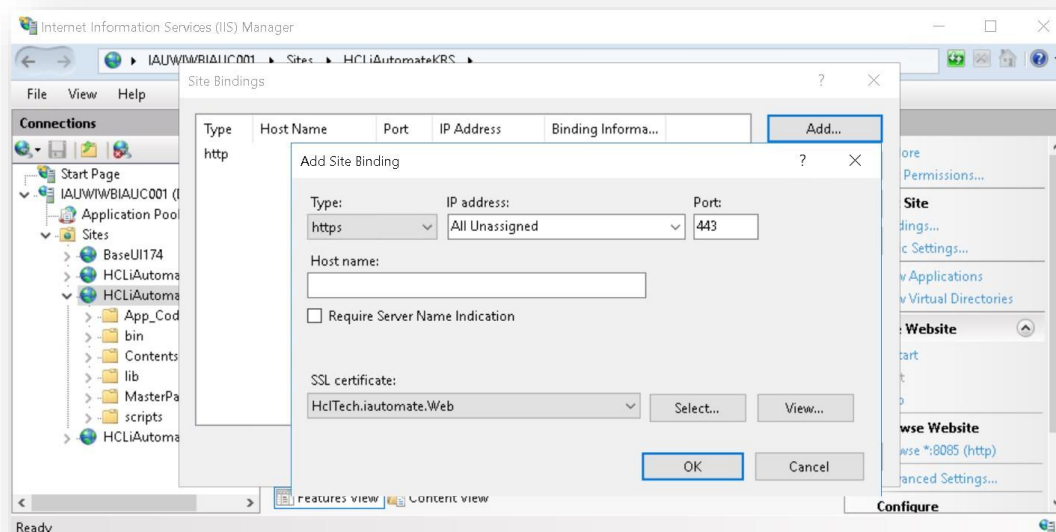


Figure 55 - Hosting KRS from HTTP to HTTPS (cont.)

8. Right click HCLiAutomateKRS .
9. Click **Explore**.
10. Find **Web.config** file and open it in a **Notepad**.



Figure 56 - Hosting KRS from HTTP to HTTPS (cont.)

11. Within the **Web.config** file, find the tag <security> and change it to <security mode="TransportWithMessageCredential">.

```
<security mode="TransportWithMessageCredential">
  <message clientCredentialType="Certificate" />
</security>
```

Figure 57 - Hosting KRS from HTTP to HTTPS (cont.)

12. Save the file for changes to be reflected.
13. Select the service and click **Restart** to restart the services.

3.6.1.1.2 Base User interface

To change the hosting of BaseUI from HTTP to HTTPS using the existing certificate, for e.g. 'HclTech.iautomate.Web', please follow the below steps:

1. Press **Win+R** and type **inetmgr**.
2. Click **OK** to open IIS.

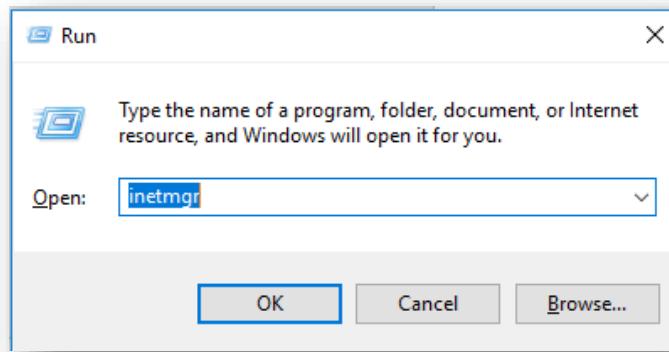


Figure 58 - Hosting Base user interface from HTTP to HTTPS

3. Expand Sites and click **HCLiAutomateBaseUI**.

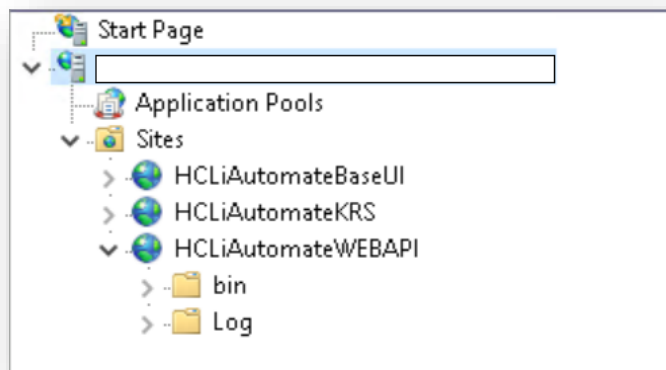


Figure 59 - Hosting Base user interface from HTTP to HTTPS (cont.)

4. Click on **Bindings** in the **Edit Site** section.

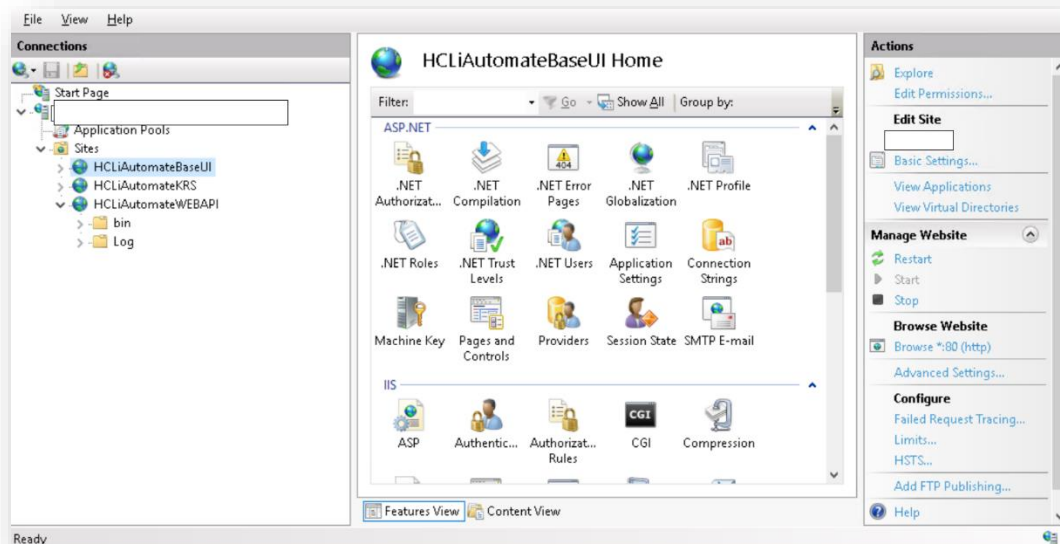


Figure 60 - Hosting Base User Interface from HTTP to HTTPS (cont.)

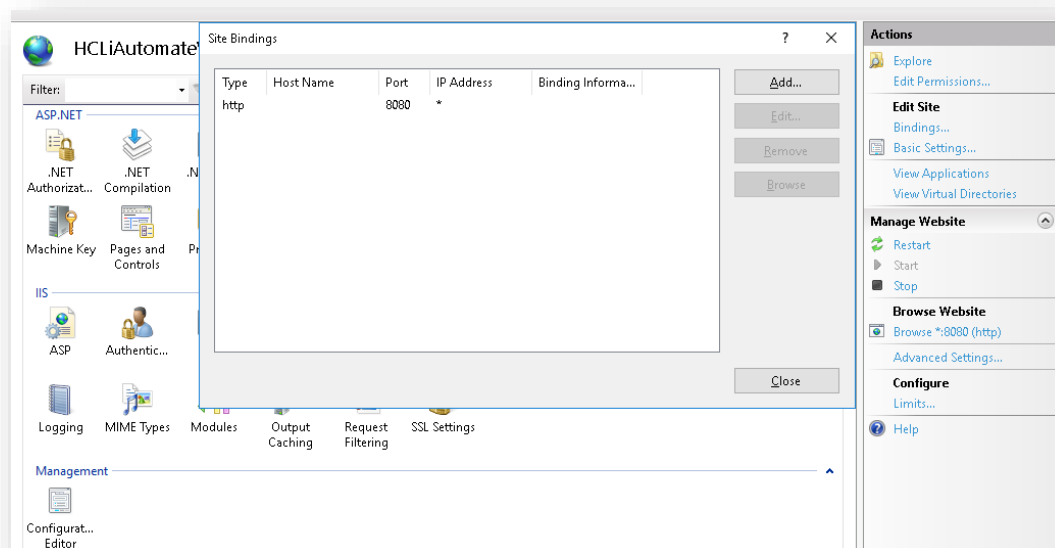


Figure 61 - Hosting Base user interface from HTTP to HTTPS (cont.)

5. Click **Add**.
6. Select **Type** as **https**. **Port** information gets populated automatically. Select the **SSL Certificate**.
7. Click **OK**.

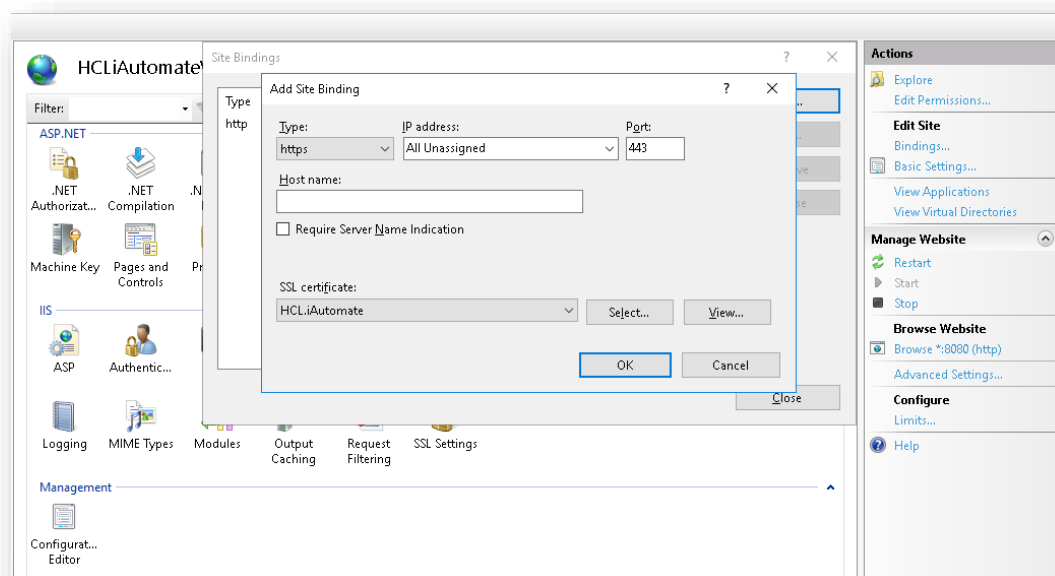


Figure 62 - Hosting Base user interface from HTTP to HTTPS (cont.)

8. Right-click HCLiAutomateBaseUI.
9. Click **Explore**.
10. Find **Web.config** file and open it in a Notepad.

 **Web.config**

Figure 63 - Hosting Base user interface from HTTP to HTTPS (cont.)

11. Within the **Web.config** file, find the key **URL** and change its value from HTTP to HTTPS.

```
<add key="URL" value="https://<ip>:<Port>/KRS/KeyManagement.svc" />
```

Figure 64 - Hosting Base user interface from HTTP to HTTPS (cont.)

12. If the certificate is self-signed, find the key **IsSelfSigned_KRS** and change its value to 'Y'. Else, the value will be 'N'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 65 - Hosting Base user interface from HTTP to HTTPS (cont.)

13. Change the security mode="TransportWithMessageCredential" under <binding> tag.

```
<system.serviceModel>
  <bindings>
    <wsHttpBinding>
      <binding name="Service_WSHttpBinding" maxBufferPoolSize="2147483647" maxReceivedMessageSize="2147483647">
        <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647" maxArrayLength="2147483647" maxBytesPerRead="2147483647" />
        <security mode="TransportWithMessageCredential">
          <message clientCredentialType="Certificate" establishSecurityContext="false" negotiateServiceCredential="false" />
        </security>
      </binding>
    </wsHttpBinding>
  </bindings>
```

Figure 66 - Hosting Base user interface from HTTP to HTTPS (cont.)

14. Select the service and click **Restart** to restart the services.

3.6.1.1.3 Web API

To change the hosting of Web API from HTTP to HTTPS using the existing certificate, for e.g. 'HclTech.iautomate.Web', please follow the below steps:

1. Press **Win+R** and type **inetmgr**.
2. Click **OK** to open IIS.

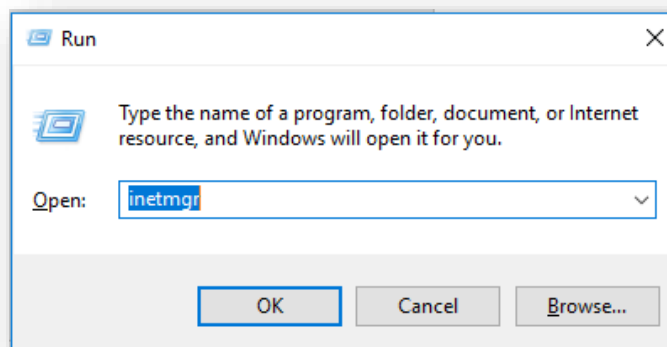


Figure 67 - Hosting Web API from HTTP to HTTPS

3. Expand **Sites** and right-click **HCLiAutomateWEBAPI**.
4. Click **Explore**.

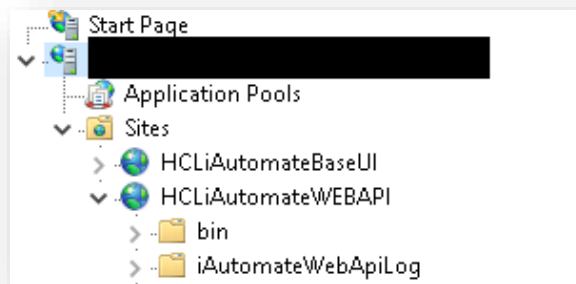


Figure 68 - Hosting Web API from HTTP to HTTPS (Cont.)

5. Find **Web.config** file and open it in a Notepad.

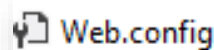


Figure 69 - Hosting Web API from HTTP to HTTPS (Cont.)

6. Within the **Web.config** file, find the key 'URL' and change its value from HTTP to HTTPS.

```
<add key="URL" value="https://<ip>:<Port>/KRS/KeyManagement.svc" />
```

Figure 70 - Hosting Web API from HTTP to HTTPS (Cont.)

7. If the certificate is self-signed, find the key **IsSelfSigned_KRS** and change its value to 'Y'. Else, the value will be 'N'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 71 - Hosting Web API from HTTP to HTTPS (Cont.)

8. **Save** the file for changes to be reflected.
9. Select the service and click **Restart** to restart the services.

3.6.1.1.4 Listener

To change the configuration of the Listener from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

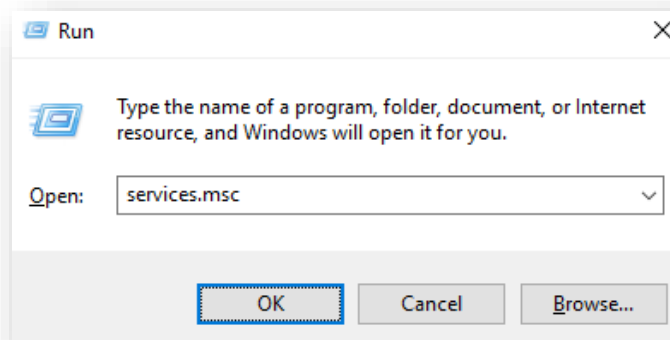


Figure 72 - Hosting Listener from HTTP to HTTPS

- Click **OK** to open the **Windows Services**.

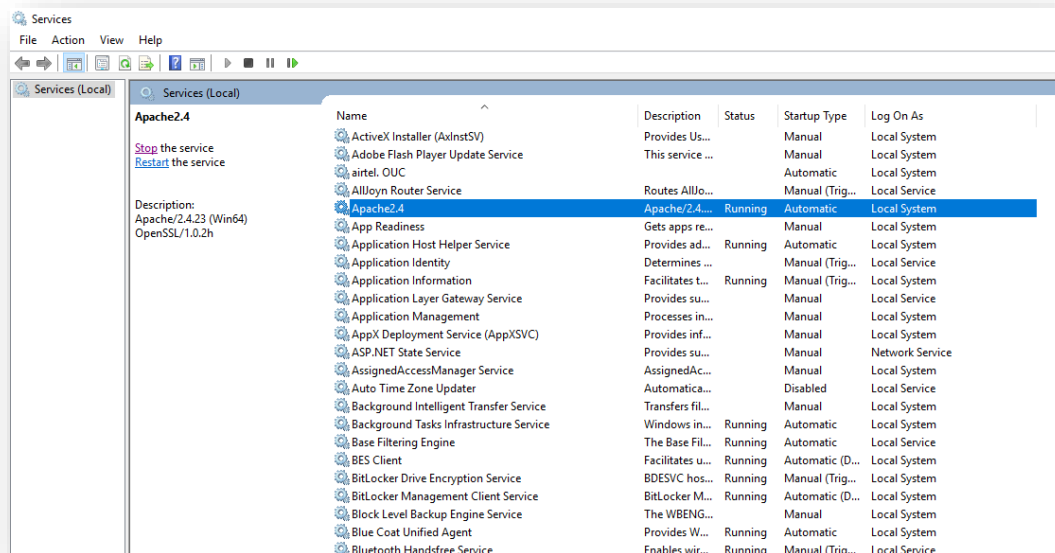


Figure 73 - Hosting Listener from HTTP to HTTPS

- Search for HCL.iAutomate.Listener service and right-click on it.
- Click Properties.

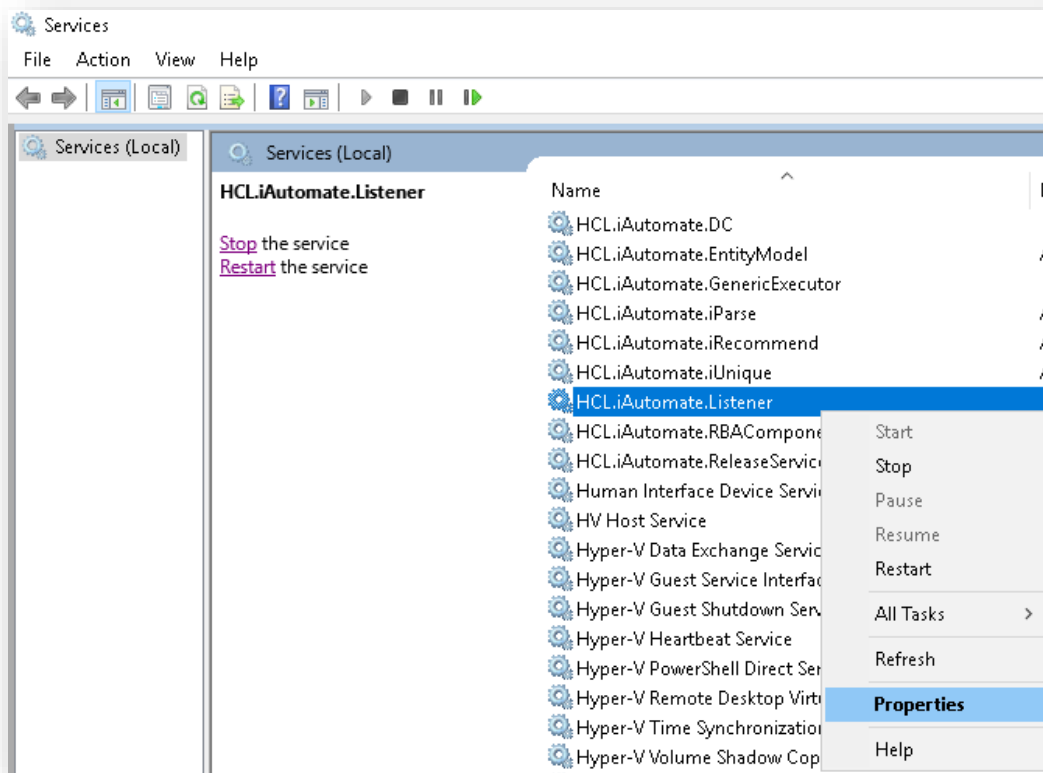


Figure 74 - Hosting Listener from HTTP to HTTPS (cont.)

- Copy the value mentioned in **Path to executable** field as shown in the image below.

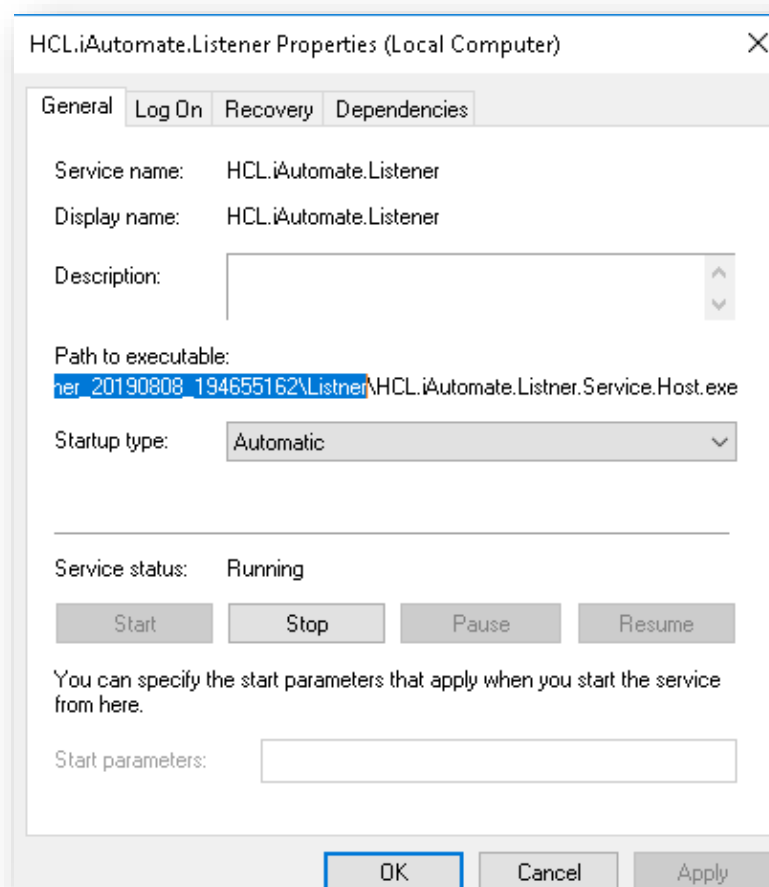


Figure 75 - Hosting Listener from HTTP to HTTPS (cont.)

6. Open **File Explorer**, then paste the **copied path** and press **Enter** to open the desired folder.
7. Search for **HCL.iAutomate.Listener.Service.Host** config file and open it in a Notepad.



Figure 76 - Hosting Listener from HTTP to HTTPS (cont.)

8. Within the **HCL.iAutomate.Listener.Service.Host** config file, find the key **URL** and change its value from HTTP to HTTPS.

```
<add key="URL" value="https://<ip>:<port>" />
```

Figure 77 - Hosting Listener from HTTP to HTTPS (cont.)

9. If the certificate is self-signed, find the key **IsSelfSigned_KRS** and change its value to **'Y'**. Else, the value will be **'N'**.

```
<add key="IsSelfSigned_KRS" value="N" />
```

10. Change the security mode="TransportWithMessageCredential" under <binding> tag.

```
<system.serviceModel>
<bindings>
  <wsHttpBinding>
    <binding name="Service_WSHttpBinding" maxBufferPoolSize="2147483647" maxReceivedMessageSize="2147483647">
      <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647" maxArrayLength="2147483647" maxBytesPerRead="2147483647" ma
      <security mode="TransportWithMessageCredential">
        <message clientCredentialType="Certificate" establishSecurityContext="false" negotiateServiceCredential="false" />
      </security>
    </binding>
  </wsHttpBinding>
</bindings>
<client>
```

Figure 78 - Hosting Listener from HTTP to HTTPS (cont.)

11. Save the file for changes to be reflected.
12. Select the service and click **Restart** to restart the services.

3.6.1.1.5 Configuration Changes via GUI

To change the configuration of Screen from HTTP to HTTPS, please follow the below steps:

1. Login to iAutomate using the **Super Admin** credentials.
2. Roll-over to the Advance Configuration and click Load Balancer Configuration.
3. Select **Component Name** as **Web API**.
4. Change the **Load Balancer URL** from HTTP to HTTPS.

Figure 79 - Changing LB IP via GUI from HTTP to HTTPS

5. Click **Update** to save the changes.

3.6.1.2 Components

This section describes how to enable the secure communication by changing HTTP to HTTPS for the iAutomate Components.

As a prerequisite, user needs to have the Thumbprint of the certificate which can be identified using the below steps:

1. Press **Win+R** and type **mmc**.

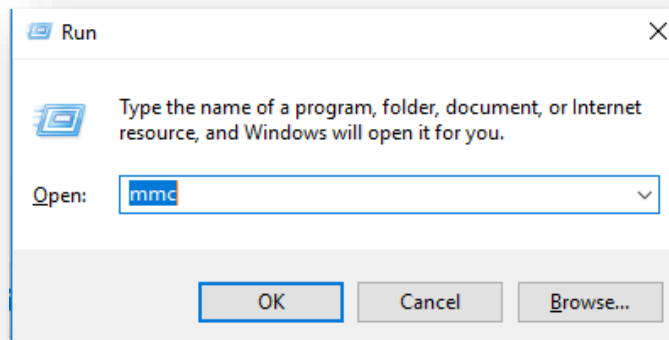


Figure 80 - Identify Thumbprint of the Certificate

2. Click OK to open the Microsoft Management Console.

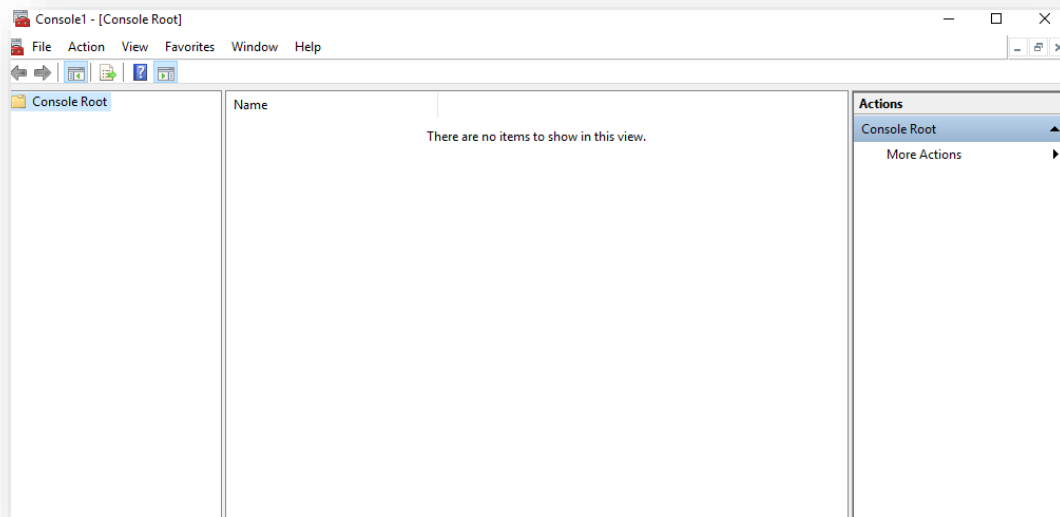


Figure 81 - Identify Thumbprint of the Certificate (cont.)

3. From the **File** menu, select **Add / Remove Snap-in**.

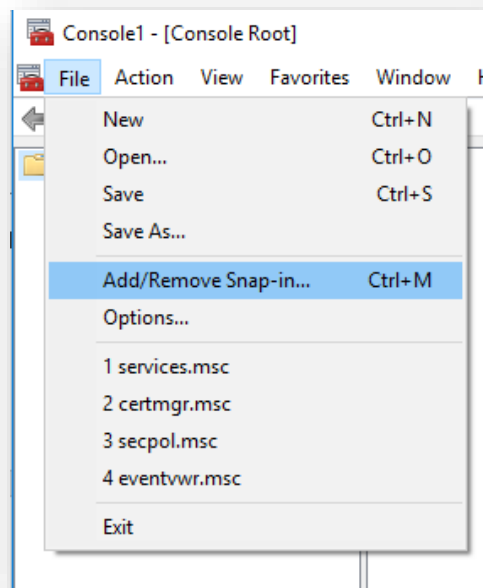


Figure 82 - Identify Thumbprint of the Certificate (cont.)

4. From the **Available snap-ins** list, select **Certificates**, then click **Add**.

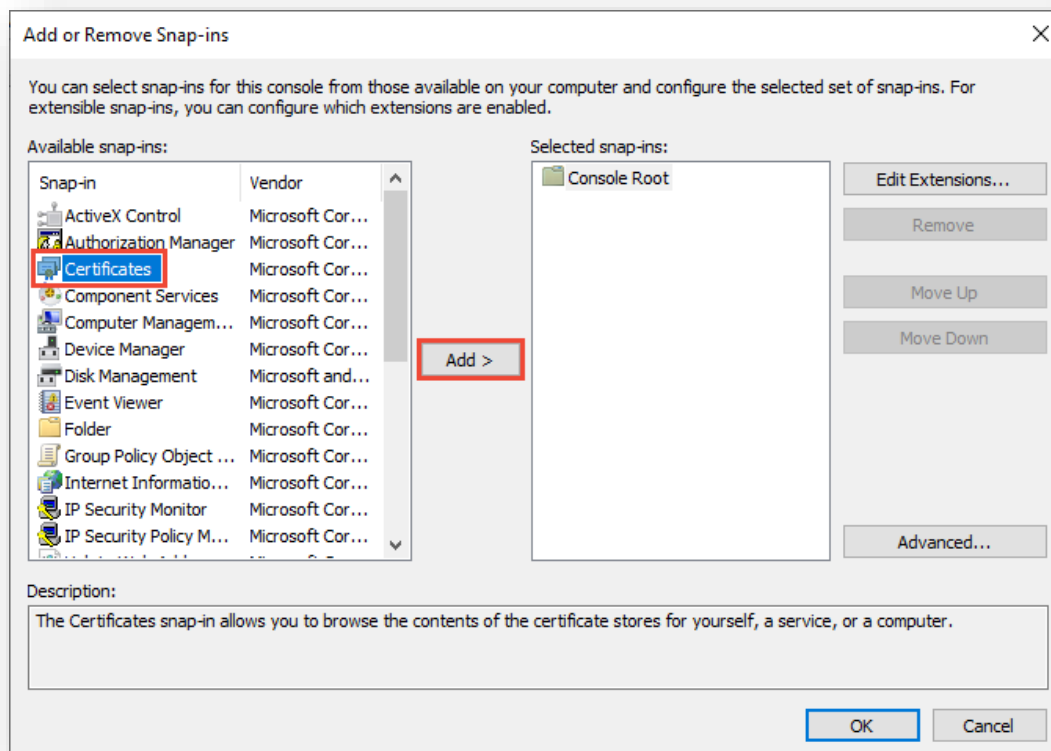


Figure 83 - Identify Thumbprint of the Certificate (cont.)

5. Click **OK**.
6. From the Certificates Snap-In window, select Computer Account and click Next.

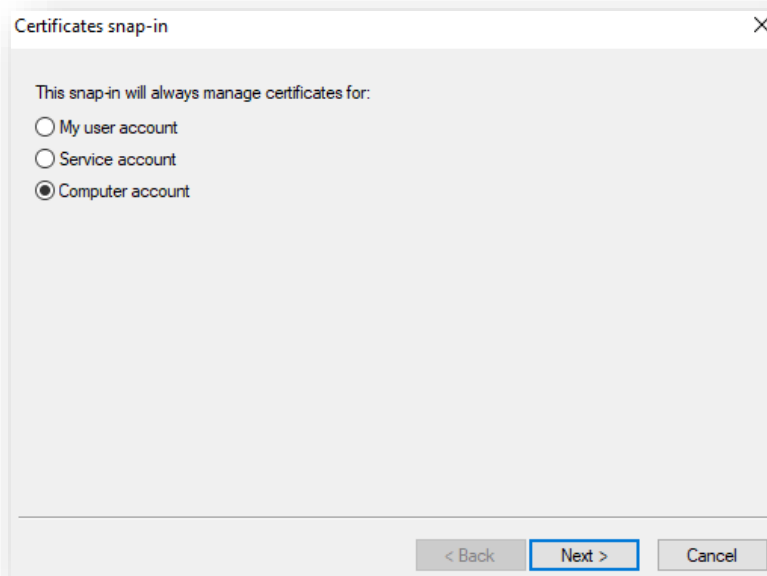


Figure 84 - Identify Thumbprint of the Certificate (cont.)

7. In the left pane, under Console Root, click Certificates (Local Computer).
8. Click **Personal** folder to expand it and then click **Certificates** folder to expand it.

Issued To	Issued By	Expiration Date	Intended Pu
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	4/6/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	3/28/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	7/11/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	4/13/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	3/19/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	6/5/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	6/16/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	5/4/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	8/2/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	7/5/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	4/23/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	3/19/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	3/19/2019	Server Auth...
dfc29558-0f27-4733-9cab-24e5...	MS-Organization-P2P-Access [20...	8/6/2019	Server Auth...

Figure 85 - Identify Thumbprint of the Certificate (cont.)

Please install the certificate through the **Microsoft Management Console** in both **Personal** as well as **Trusted People** folder. Refer to the pre-requisites document for the detailed procedure for certificate installation at required locations.

9. In the list of certificates, find certificate **HclTech.iautomate.Web**.
10. Double-click the certificate to open the **Certificate** dialog box.
11. Scroll through the list of fields and click **Thumbprint** to display the value.

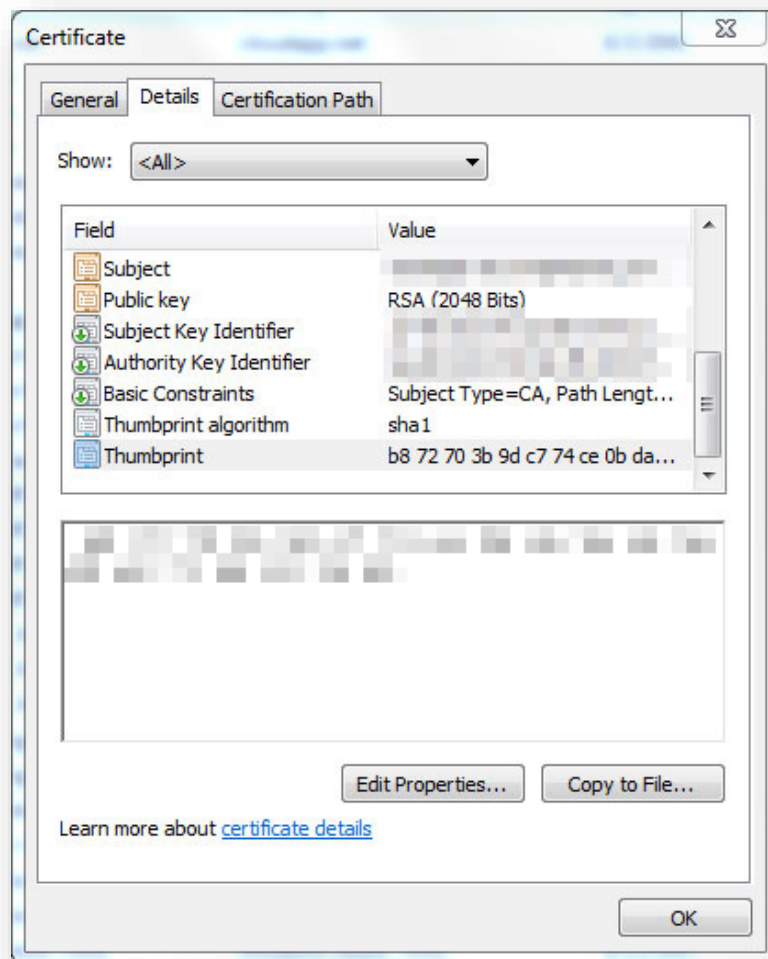


Figure 86 - Identify Thumbprint of the Certificate (cont.)

Following changes are required in the underlying components:

3.6.1.2.1 Listener

To change the configuration of Listener from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

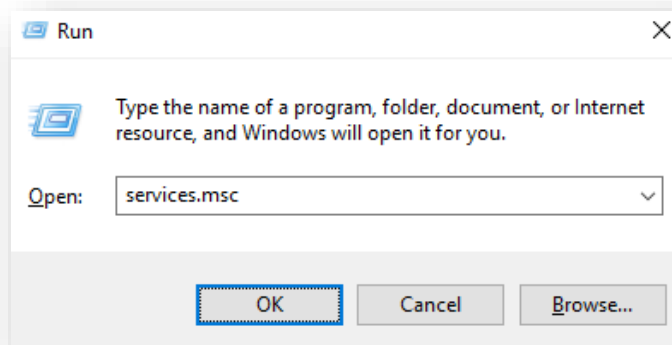


Figure 87 - Hosting Listener from HTTP to HTTPS

2. Click OK to open Windows Services.

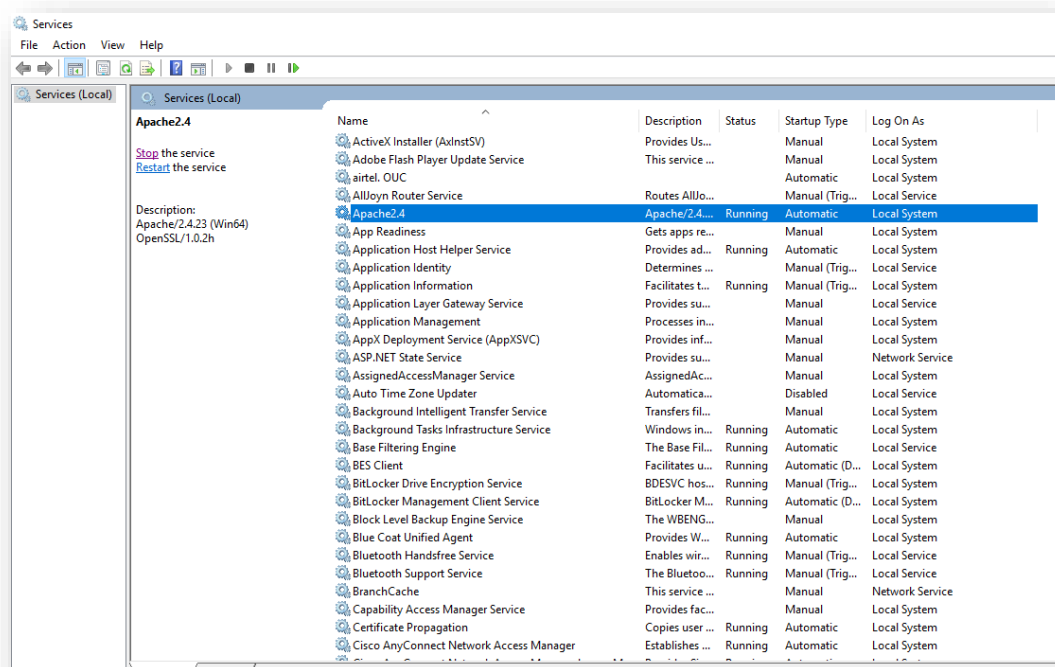


Figure 88 - Hosting Listener from HTTP to HTTPS (cont.)

3. Search for **HCL.iAutomate.Listener** service and right-click on it.
4. Click Properties.

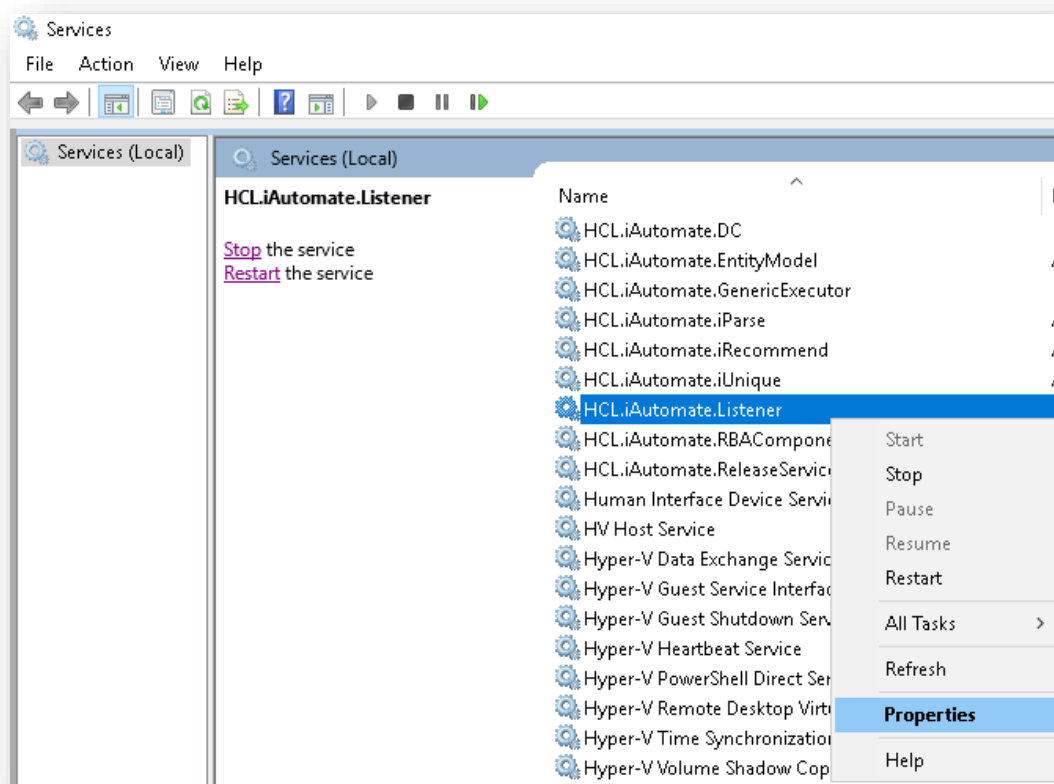


Figure 89 - Hosting Listener from HTTP to HTTPS (cont.)

5. Copy the value mentioned in **Path to executable** as shown in the image below.

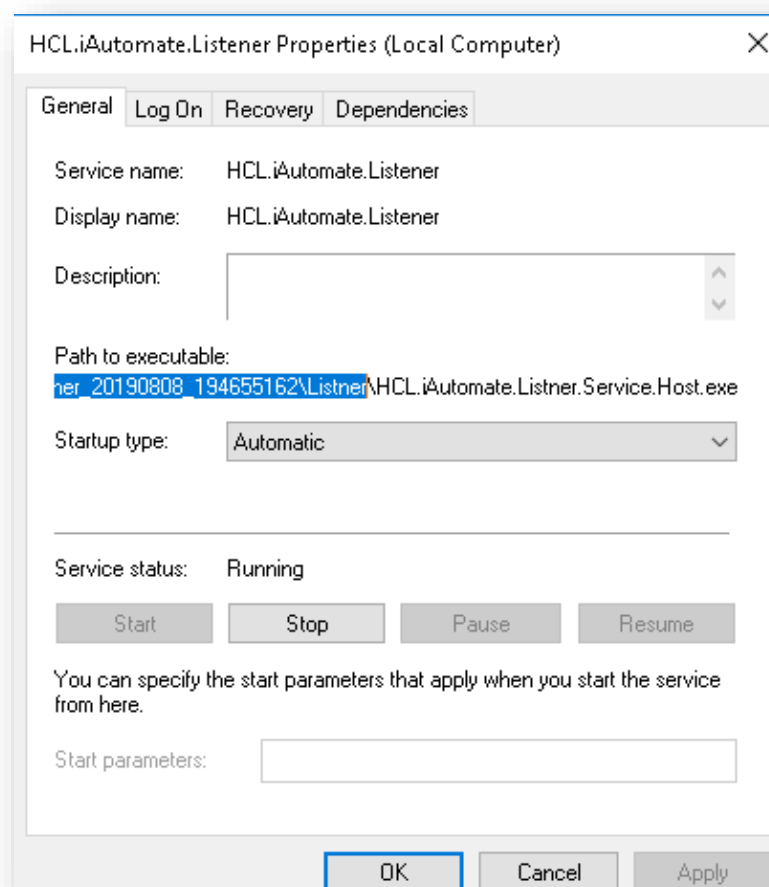


Figure 90 - Hosting Listener from HTTP to HTTPS (cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Search for **HCL.iAutomate.Listener.Service.Host** config file and open it in a Notepad.



Figure 91 - Hosting Listener from HTTP to HTTPS (cont.)

8. Within the **HCL.iAutomate.Listener.Service.Host** config file, find the key **URL** and change its value from HTTP to HTTPS

```
<add key="URL" value="https://<ip>:<port>" />
```

Figure 92 - Hosting Listener from HTTP to HTTPS (cont.)

9. Within the **HCL.iAutomate.Listener.Service.Host** config file, find the key **'IsSelfSigned_Service'** and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 93 - Hosting Listener from HTTP to HTTPS (cont.)

10. Change the security mode="TransportWithMessageCredential" under <binding> tag.

```
<system.serviceModel>
<bindings>
  <wsHttpBinding>
    <binding name="Service_WSHttpBinding" maxBufferPoolSize="2147483647" maxReceivedMessageSize="2147483647">
      <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647" maxArrayLength="2147483647" maxBytesPerRead="2147483647" maxItemsPerChain="2147483647">
      </readerQuotas>
      <security mode="TransportWithMessageCredential">
        <message clientCredentialType="Certificate" establishSecurityContext="false" negotiateServiceCredential="false"
        </security>
      </binding>
    </wsHttpBinding>
  </bindings>
```

Figure 92 - Hosting Listener from HTTP to HTTPS (cont.)

11. Save the changes and open the command prompt as administrator and run the following command.

```
netsh http add sslcert iport=<ip>:<port on which service is
running> appid={fa605232-f580-4d28-895e-3e021ffed82d}
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

12. Select **HCL.iAutomate.Listener** service and click **Restart** to restart the service.

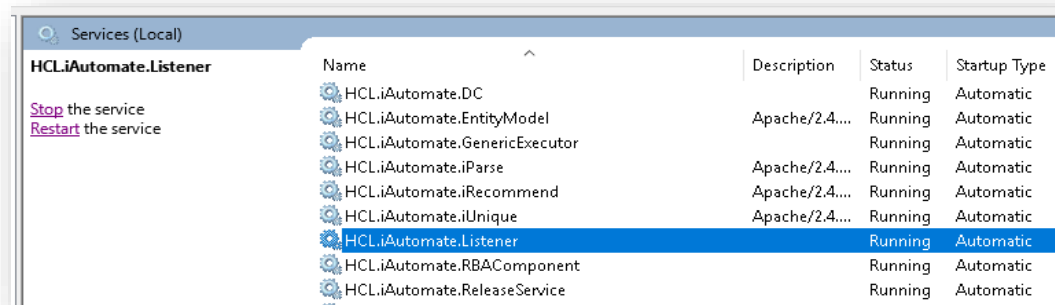


Figure 94 - Hosting Listener from HTTP to HTTPS (cont.)

3.6.1.2.2 Data Collector

To change the configuration of Data Collector from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

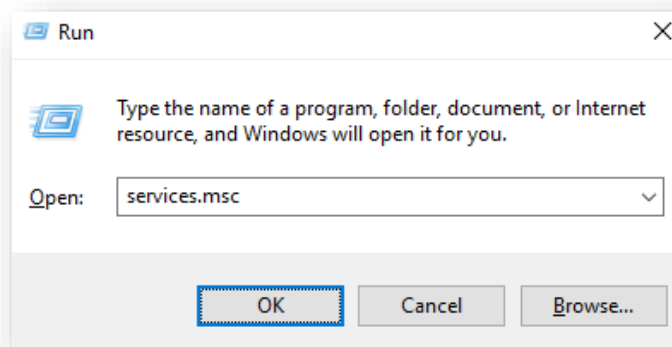


Figure 95 - Hosting Data Collector from HTTP to HTTPS

2. Click OK to open Windows Services.

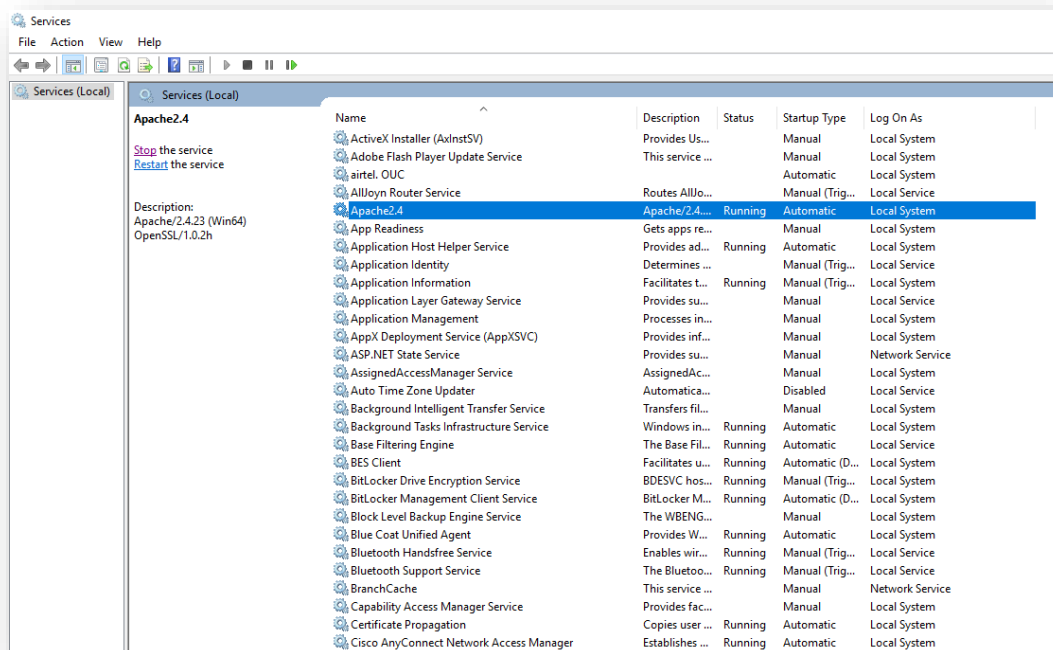


Figure 96 - Hosting Data Collector from HTTP to HTTPS (cont.)

3. Search for **HCLiAutomate.DC** service and right-click on it.
4. Click Properties.

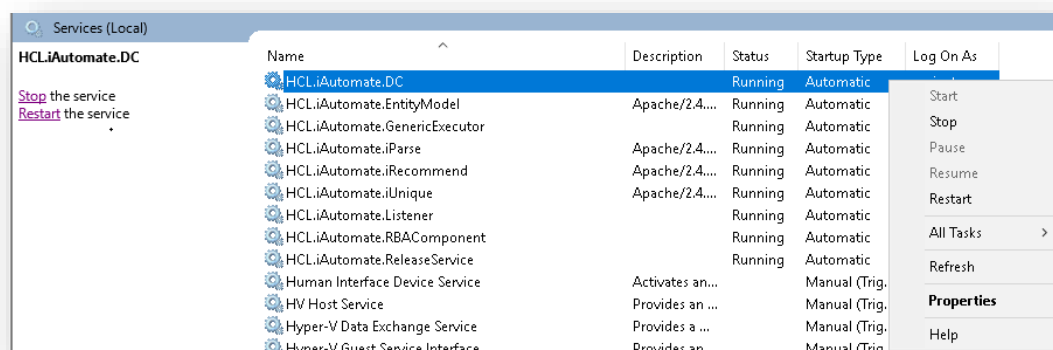


Figure 97 - Hosting Data Collector from HTTP to HTTPS (cont.)

5. Copy the value mentioned in 'Path to executable' as shown in the image below.

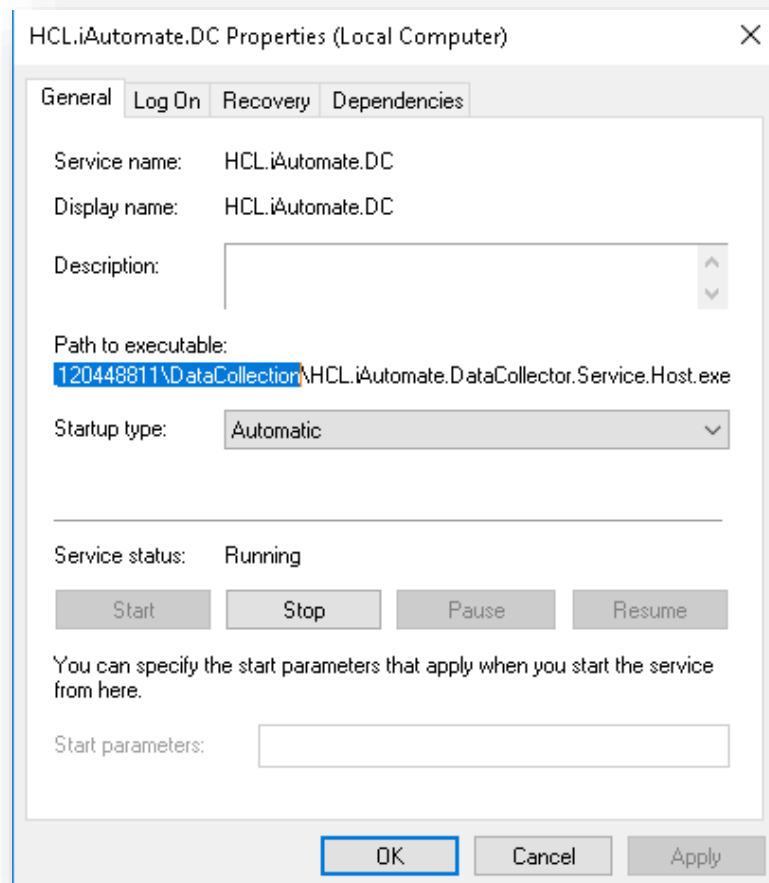


Figure 98 - Hosting Data Collector from HTTP to HTTPS (cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Search for HCL.iAutomate.DataCollector.Service.Host.exe config file and open it in a Notepad.

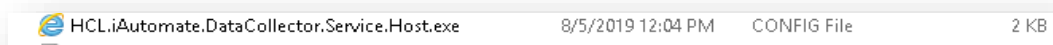


Figure 99 - Hosting Data Collector from HTTP to HTTPS (cont.)

8. Within the **HCL.iAutomate.DataCollector.Service.Host.exe** config file, find the key '**ServiceHostURL**' and change its value from HTTP to HTTPS.

```
<add key="ServiceHostURL" value="https://<ip>:<port>/DataCollector/" />
```

Figure 100 - Hosting Data Collector from HTTP to HTTPS (cont.)

9. Within the **HCL.iAutomate.DataCollector.Service.Host.exe** config file, find the key '**securityMode_Service**' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 101 - Hosting Data Collector from HTTP to HTTPS (cont.)

10. Within the **HCL.iAutomate.DataCollector.Service.Host.exe** config file, find the key '**IsSelfSigned_Service**' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 102 - Hosting Data Collector from HTTP to HTTPS (cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.

```
netsh http add sslcert ipport=<ip>:<port on which service is
running>appid={dcd67c7b-c67a-4956-b4cc-6545ace1d2e9}
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

13. Select **HCLiAutomate.DC** service and click **Restart** to restart the service.

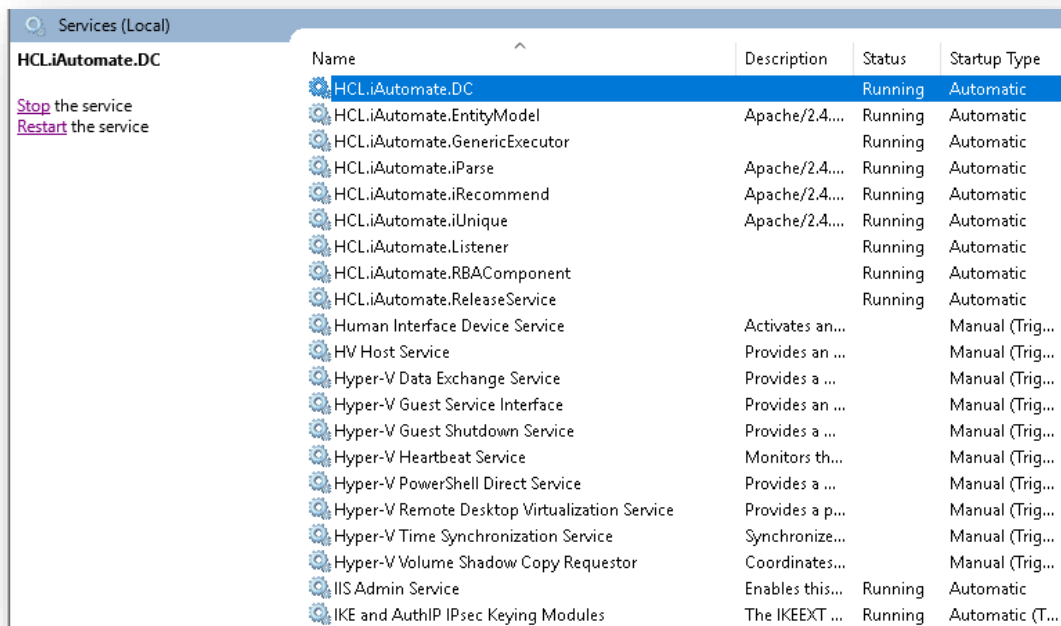


Figure 103 - Hosting Data Collector from HTTP to HTTPS (cont.)

3.6.1.2.3 Generic Service

To change the configuration of Generic Service from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

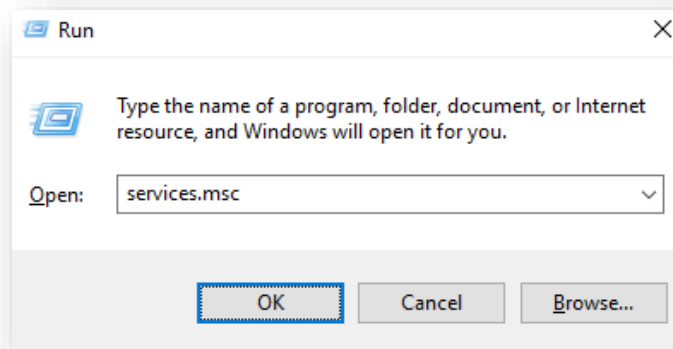


Figure 104 - Hosting Generic Service from HTTP to HTTPS

2. Click OK to open Windows Services.

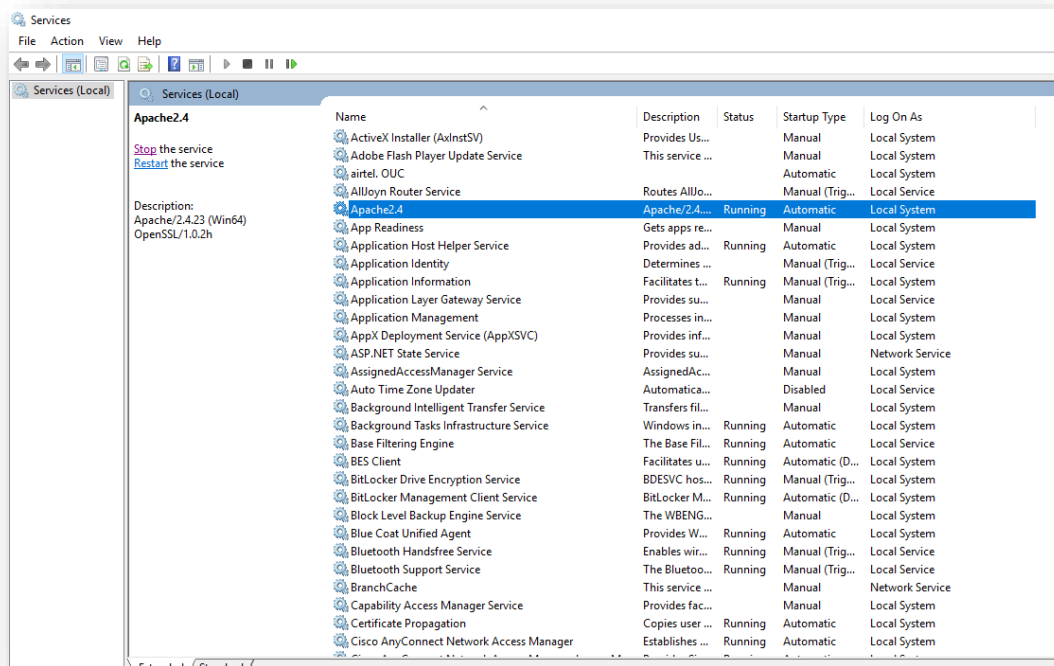


Figure 105 - Hosting Generic Service from HTTP to HTTPS (Cont.)

3. Search for HCLiAutomate.GenericExecutor service and right-click on it.
4. Click Properties.

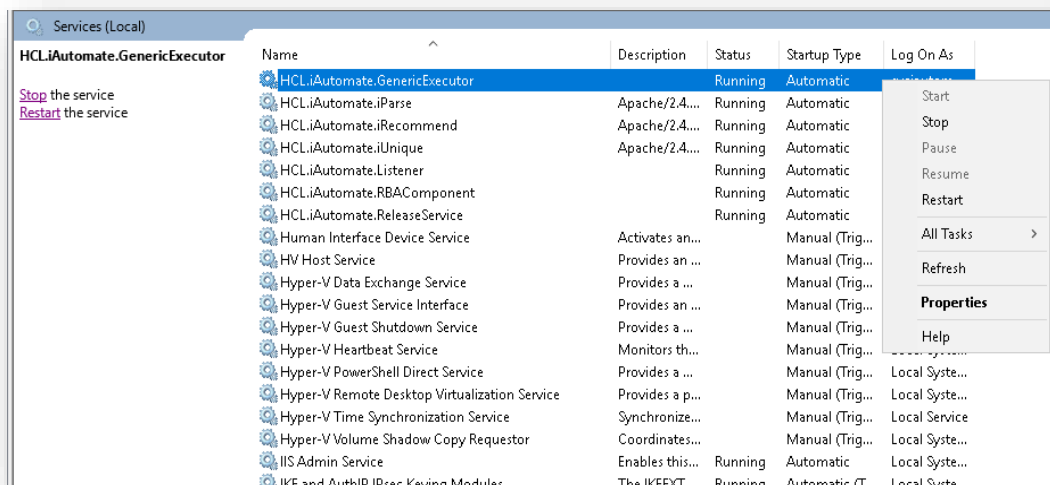


Figure 106 - Hosting Generic Service from HTTP to HTTPS (Cont.)

- Copy the value mentioned in **Path to executable** as shown in the image below.

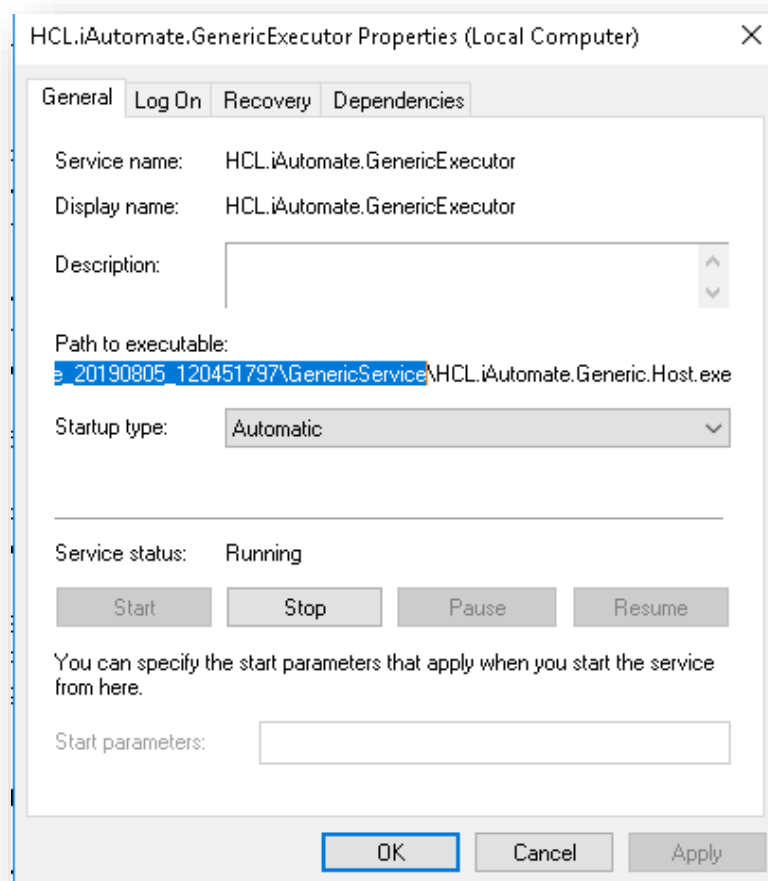


Figure 107 - Hosting Generic Service from HTTP to HTTPS (Cont.)

- Open **File Explorer** and then paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCLiAutomate.Generic.Host.exe** config file and open it in a Notepad.

Figure 108 - Hosting Generic Service from HTTP to HTTPS (Cont.)

8. Within the **HCLiAutomate.Generic.Host.exe** config file, find the key **'iAutomate.Generic.ServiceHostURL'** and change its value from HTTP to HTTPS.

```
<add key="iAutomate.Generic.ServiceHostURL" value="https://<ip>:<port>/GenericService" />
```

Figure 109-Hosting Generic Service from HTTP to HTTPS (Cont.)

9. Within the **HCLiAutomate.Generic.Host.exe** config file, find the key **'securityMode_Service'** and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 110 - Hosting Generic Service from HTTP to HTTPS (Cont.)

10. Within the **HCLiAutomate.Generic.Host.exe** config file, find the key **'IsSelfSigned_Service'** and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 111 - Hosting Generic Service from HTTP to HTTPS (Cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.

```
netsh http add sslcert iport=<ip>:<port on which service is running> appid={c60c3690-7b58-4c68-8590-e2fd061edd23}
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

13. Select **HCLiAutomate.GenericExecutor** service and click **Restart** to restart the service.

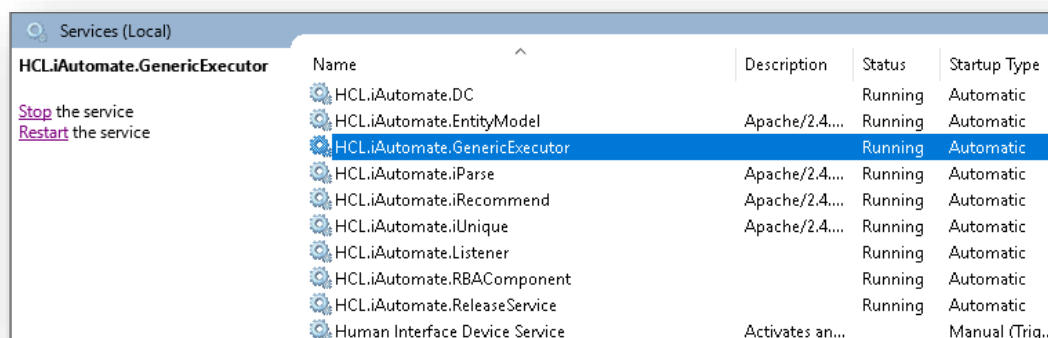


Figure 112 - Hosting Generic Service from HTTP to HTTPS (Cont.)

3.6.1.2.4 RBA Component

To change the configuration of RBA Component from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

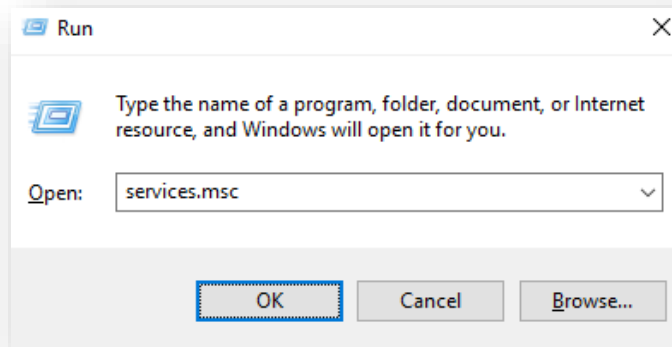


Figure 113 - Hosting RBA Component from HTTP to HTTPS

2. Click OK to open Windows Services.

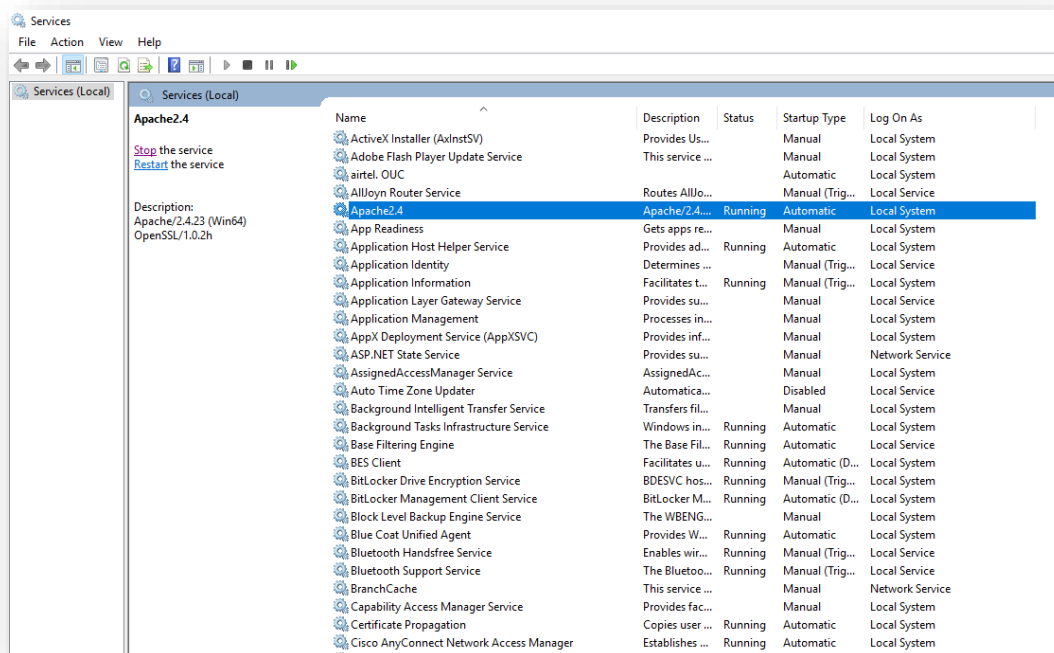


Figure 114 - Hosting RBA Component from HTTP to HTTPS

3. Search for **HCLiAutomate.RBAComponent** service and right-click on it.
4. Click **Properties**.

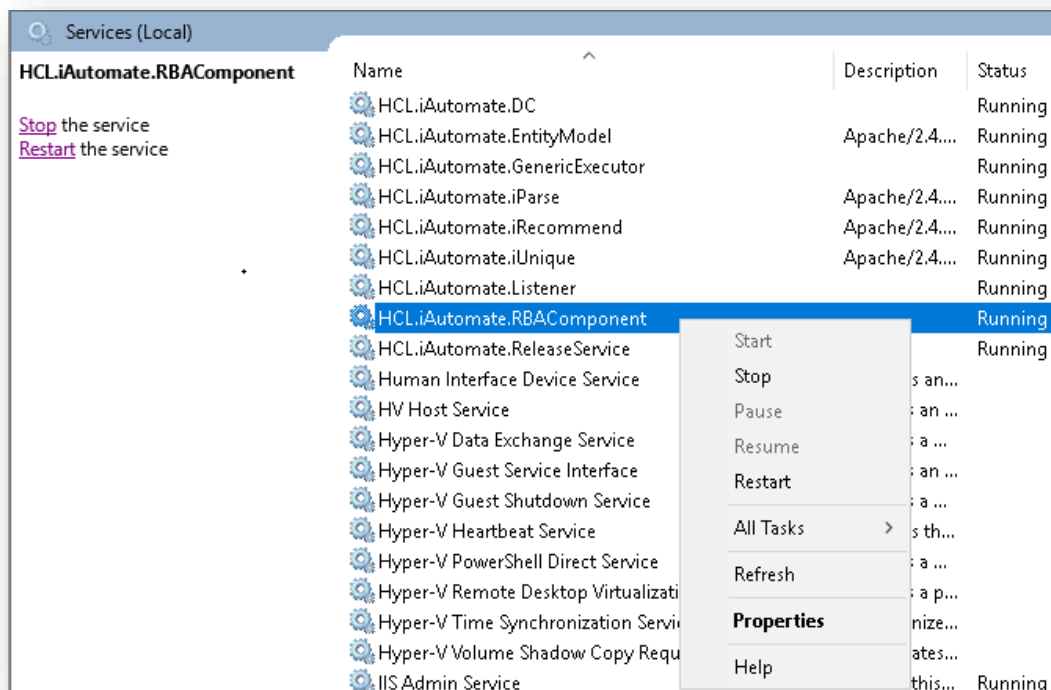


Figure 115 - Hosting RBA Component from HTTP to HTTPS (Cont.)

- Copy the value mentioned in **Path to executable** as shown in the image below.

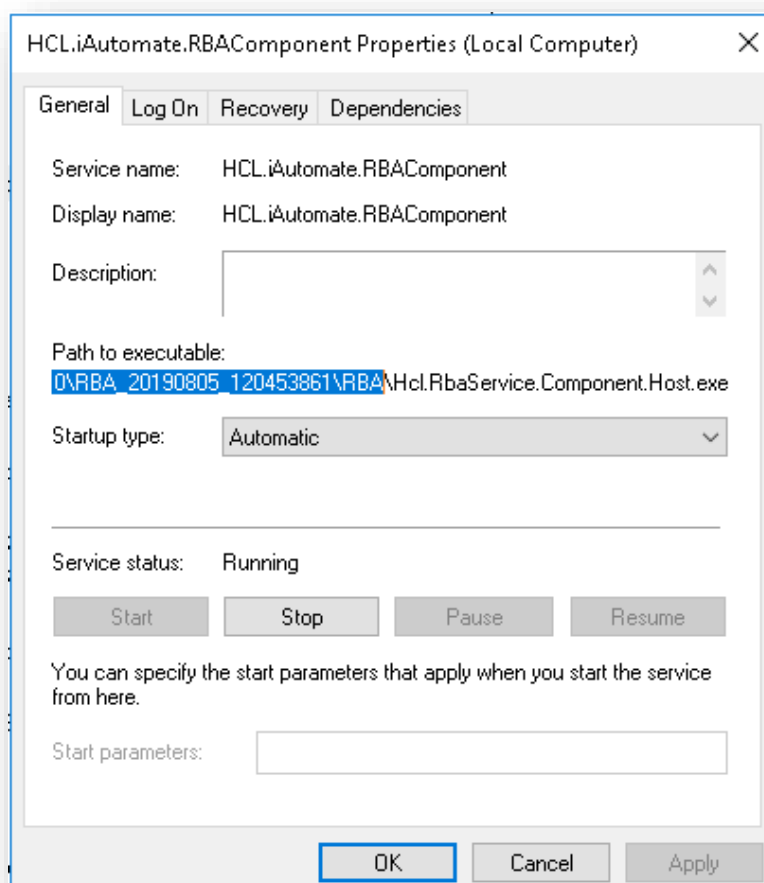


Figure 116 - Hosting RBA Component from HTTP to HTTPS (Cont.)

- Open **File Explorer** and then paste the **copied path** and press **Enter** to open the desired folder.

7. Search for **HCL.RbaService.Component.Host.exe** config file and open it in a Notepad.

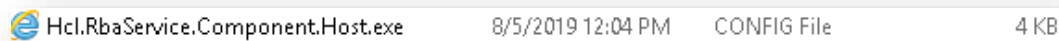


Figure 117 - Hosting RBA Component from HTTP to HTTPS (Cont.)

8. Within the **HCL.RbaService.Component.Host.exe** config file, find the key '**ServiceHostURL**' and change its value from HTTP to HTTPS.

```
<add key="ServiceHostURL" value="https://<ip>:<port>/RbaComponent/" />
```

Figure 118 - Hosting RBA Component from HTTP to HTTPS (Cont.)

9. Within the **HCL.RbaService.Component.Host.exe** config file, find the key '**securityMode_Service**' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 119 - Hosting RBA Component from HTTP to HTTPS (Cont.)

10. Within the **HCL.RbaService.Component.Host.exe** config file, find the key '**IsSelfSigned_Service**' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 120 - Hosting RBA Component from HTTP to HTTPS (Cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.

```
netsh http add sslcert ipport=<ip>:<port on which service is running> appid={11f43d84-3d5c-47cf-b29e-0dd38c0e8f85}
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

13. Select **HCL.iAutomate.RBAComponent** service and click **Restart** to restart the service.

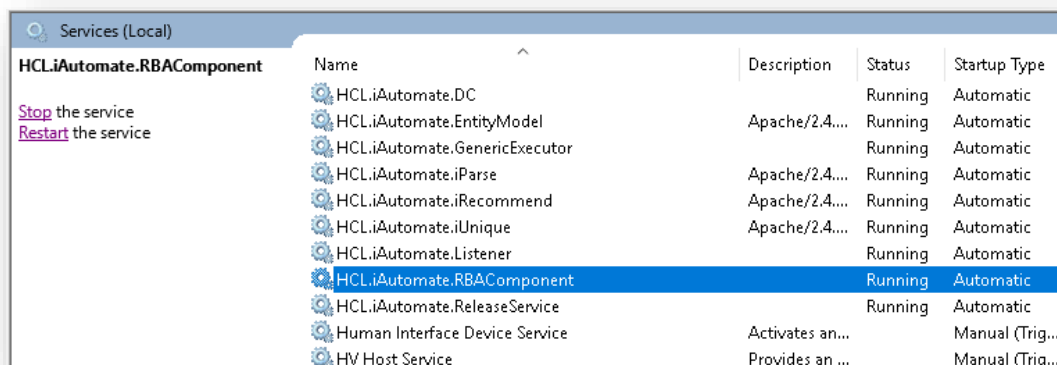


Figure 121 - Hosting RBA Component from HTTP to HTTPS (Cont.)

To change the configuration of Release Service from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

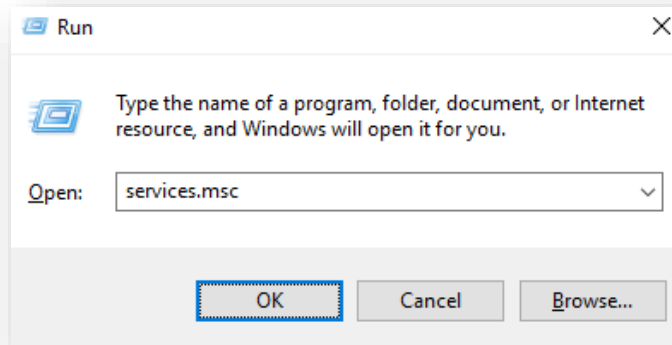


Figure 122 - Hosting Release Service from HTTP to HTTPS

2. Click **OK** to open **Windows Services**.

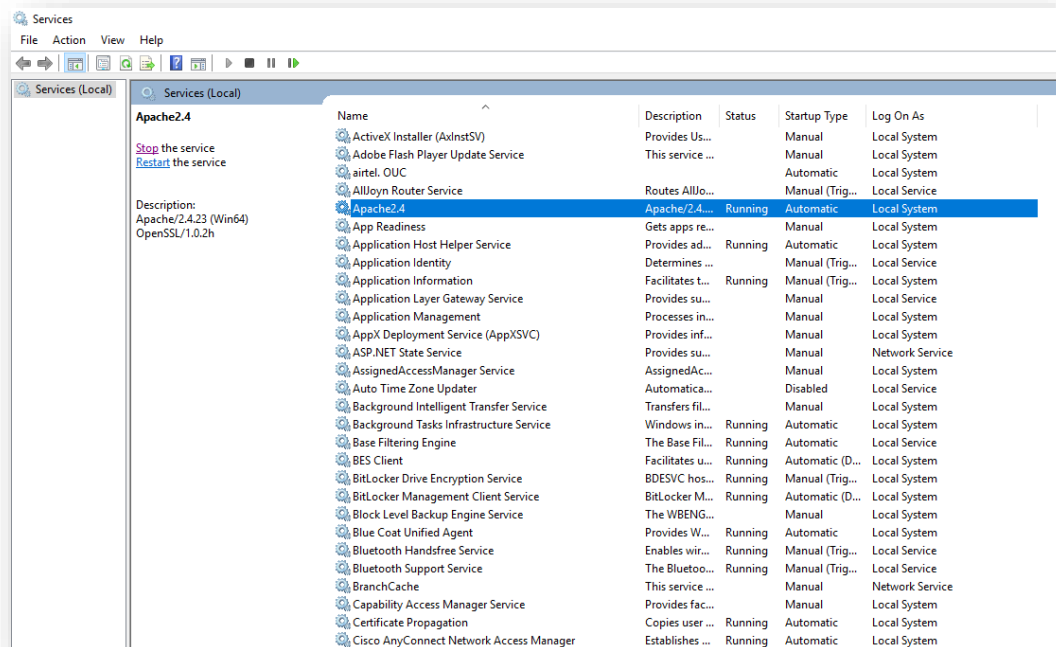


Figure 123 - Hosting Release Service from HTTP to HTTPS (Cont.)

3. Search for **HCL.iAutomate.ReleaseService** service and right-click on it.
4. Click on **Properties**.

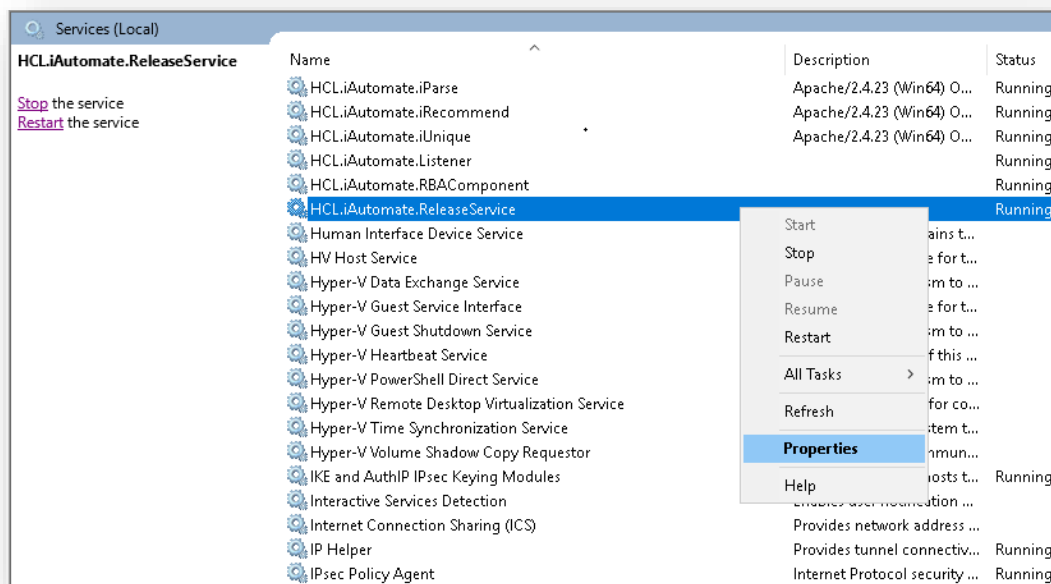


Figure 124 - Hosting Release Service from HTTP to HTTPS (Cont.)

- Copy the value mentioned in **Path to executable** as shown in the image below.

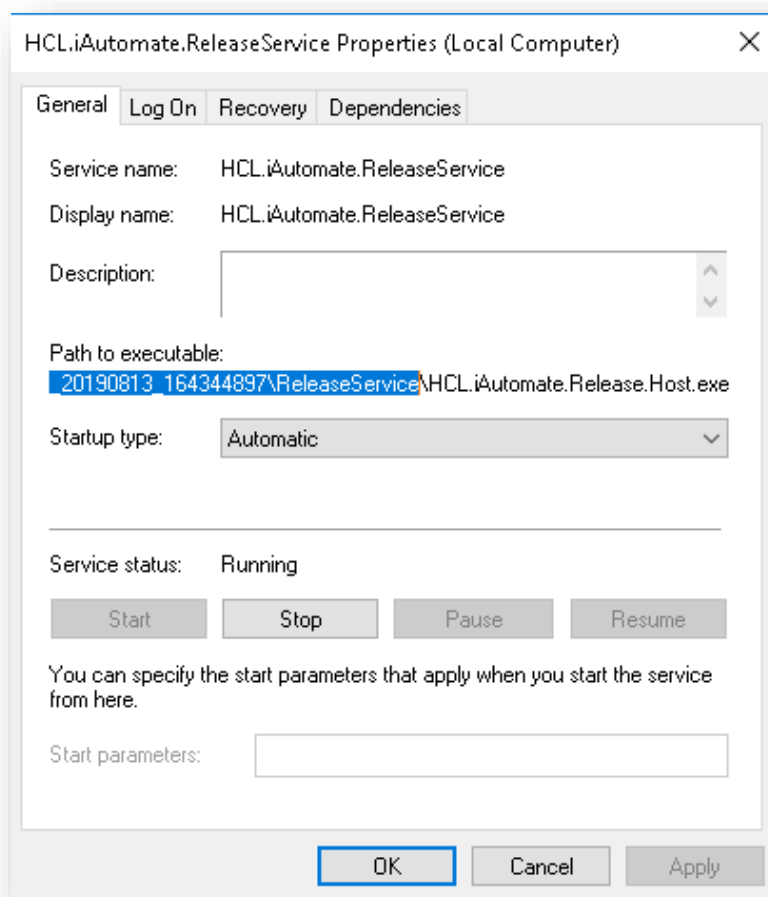


Figure 125 - Hosting Release Service from HTTP to HTTPS (Cont.)

- Open **File Explorer**, then paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCL.iAutomate.Release.Host.exe** config file and open it in a Notepad.

Figure 126 - Hosting Release Service from HTTP to HTTPS (Cont.)

8. Within the **HCL.iAutomate.Release.Host.exe** config file, find the key '**iAutomate.Release.ServiceHostURL**' and change its value from HTTP to HTTPS.

```
<add key="iAutomate.Release.ServiceHostURL" value="https://<ip>:<port>/ReleaseService" />
```

Figure 127 - Hosting Release Service from HTTP to HTTPS (Cont.)

9. Within the **HCL.iAutomate.Release.Host.exe** config file, find the key '**securityMode_Service**' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 128 - Hosting Release Service from HTTP to HTTPS (Cont.)

10. Within the **HCL.iAutomate.Release.Host.exe** config file, find the key '**IsSelfSigned_Service**' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 129 - Hosting Release Service from HTTP to HTTPS (Cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.

```
netsh http add sslcert ipport=<ip>:<port on which service is running> appid={d32cb30c-7e1a-4549-a2e2-32bf01a1d345}
certhash="<Thumbprint of the certificate>"
```

Replace the **<Thumbprint of the certificate>** with the GUID identified earlier.

13. Select **HCL.iAutomate.ReleaseService** service and click **Restart** to restart the service.

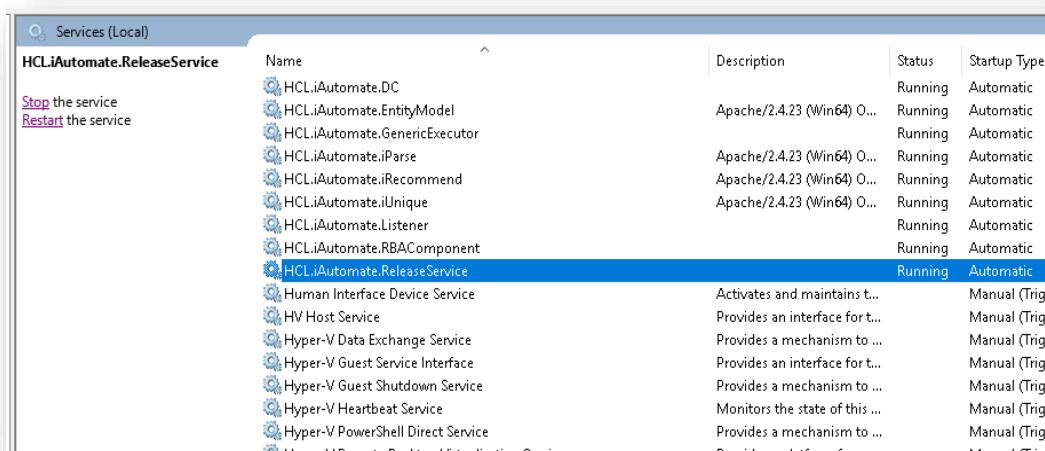


Figure 130 - Hosting Release Service from HTTP to HTTPS (Cont.)

To change the configuration of AD Sync from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

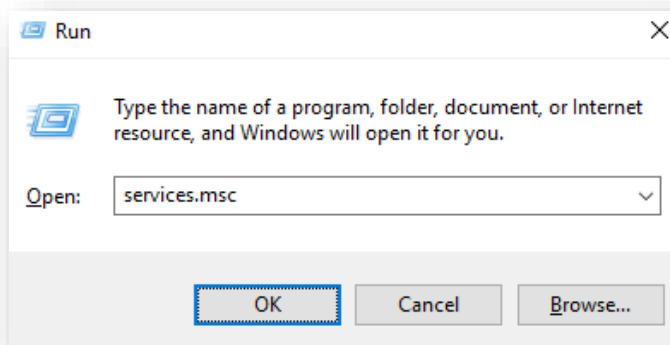


Figure 131 - Hosting AD Sync from HTTP to HTTPS

2. Click OK to open Windows Services.

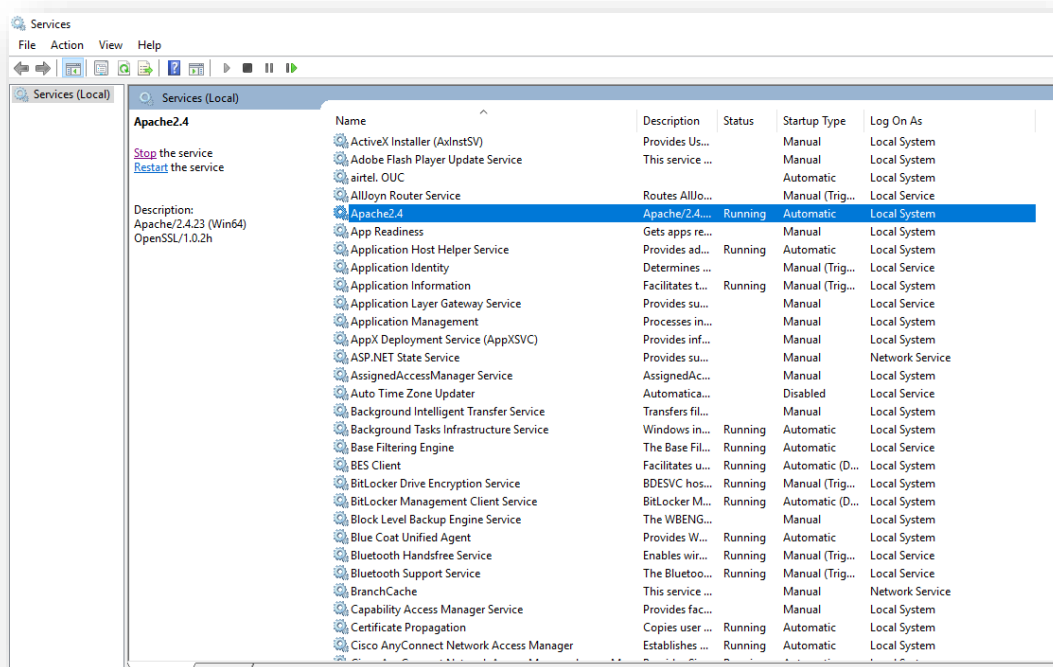


Figure 132 - Hosting AD Sync from HTTP to HTTPS (cont.)

3. Search for HCLiAutomate.ADSSyncService and right-click on it.
4. Click Properties.

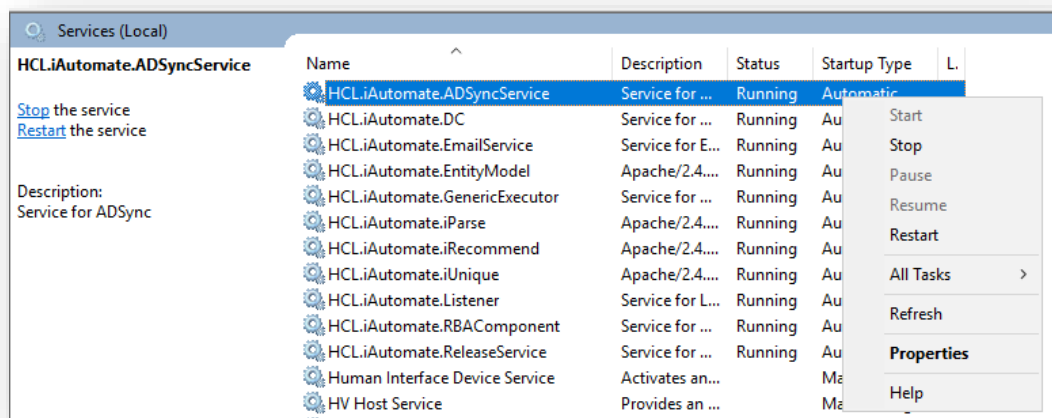


Figure 133 - Hosting AD Sync from HTTP to HTTPS (cont.)

- Copy the value mentioned in '**Path to executable**' as shown in the image below.

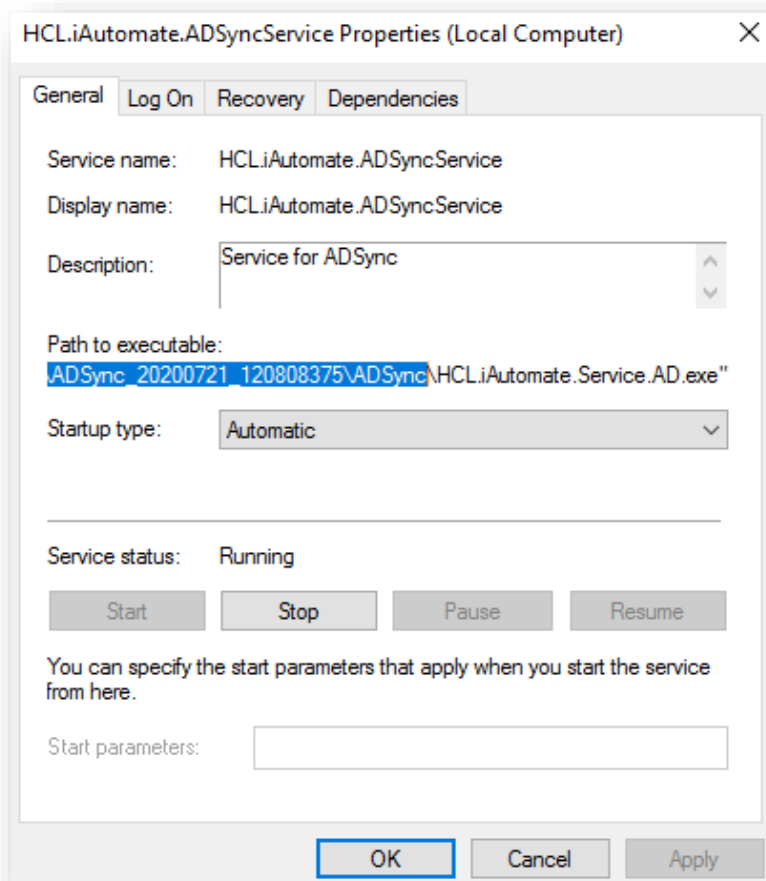


Figure 134 - Hosting AD Sync from HTTP to HTTPS (cont.)

- Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCLiAutomate.Service.AD.exe** config file and open it in a Notepad.

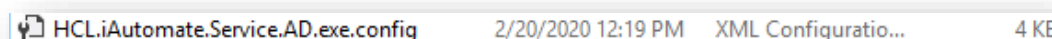


Figure 135 - Hosting AD Sync from HTTP to HTTPS (cont.)

8. Within the **HCL.iAutomate.Service.AD.exe** config file, find the key '**ServiceHostURL**' and change its value from HTTP to HTTPS.

```
<add key="ServiceHostURL" value="https://<IP>:<Port>/ADService" />
```

Figure 136 - Hosting AD Sync from HTTP to HTTPS (cont.)

9. Within the **HCL.iAutomate.Service.AD.exe** config file, find the key '**securityMode_Service**' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 137 - Hosting AD Sync from HTTP to HTTPS (cont.)

10. Within the **HCL.iAutomate.Service.AD.exe** config file, find the key '**IsSelfSigned_Service**' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 138 - Hosting AD Sync from HTTP to HTTPS (cont.)

11. Change the security mode="TransportWithMessageCredential" under <binding> tag

```
<system.serviceModel>
  <bindings>
    <wsHttpBinding>
      <binding name="Service_WSHttpBinding" maxBufferPoolSize="2147483647" maxReceivedMessageSize="2147483647">
        <readerQuotas maxDepth="2147483647" maxStringContentLength="2147483647" maxArrayLength="2147483647" maxBytesPerRead="2147483647" />
        <security mode="TransportWithMessageCredential">
          <message clientCredentialType="Certificate" establishSecurityContext="false" negotiateServiceCredential="false" />
        </security>
      </binding>
    </wsHttpBinding>
  </bindings>
```

Figure 137 - Hosting AD Sync from HTTP to HTTPS (cont.)

12. Save the file for changes to be reflected.
13. Open the command prompt as administrator and run the following command:

```
netsh http add sslcert ipport=<ip>:<port on which service is running> appid={8c00e29d-1a3e-439b-a449-7e26b64b9d27}
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

14. Select **HCL.iAutomate.ADSyncService** service and click **Restart** to restart the service.

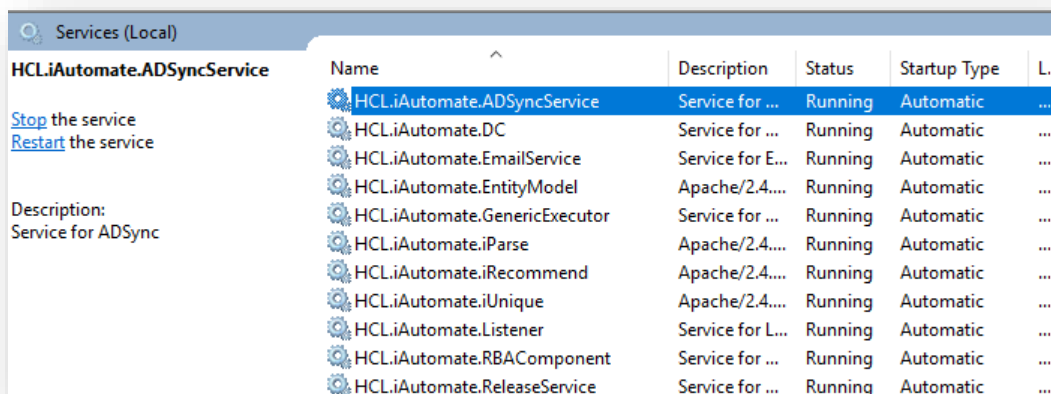


Figure 139 - Hosting AD Sync from HTTP to HTTPS (cont.)

3.6.1.2.7 Email Service

To change the configuration of Email Service from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

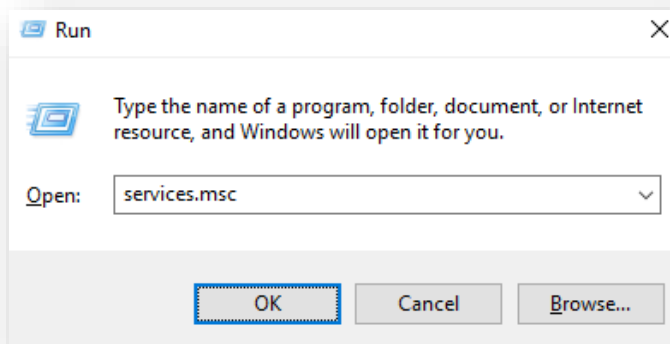


Figure 140 - Hosting Email Service from HTTP to HTTPS

2. Click OK to open Windows Services.

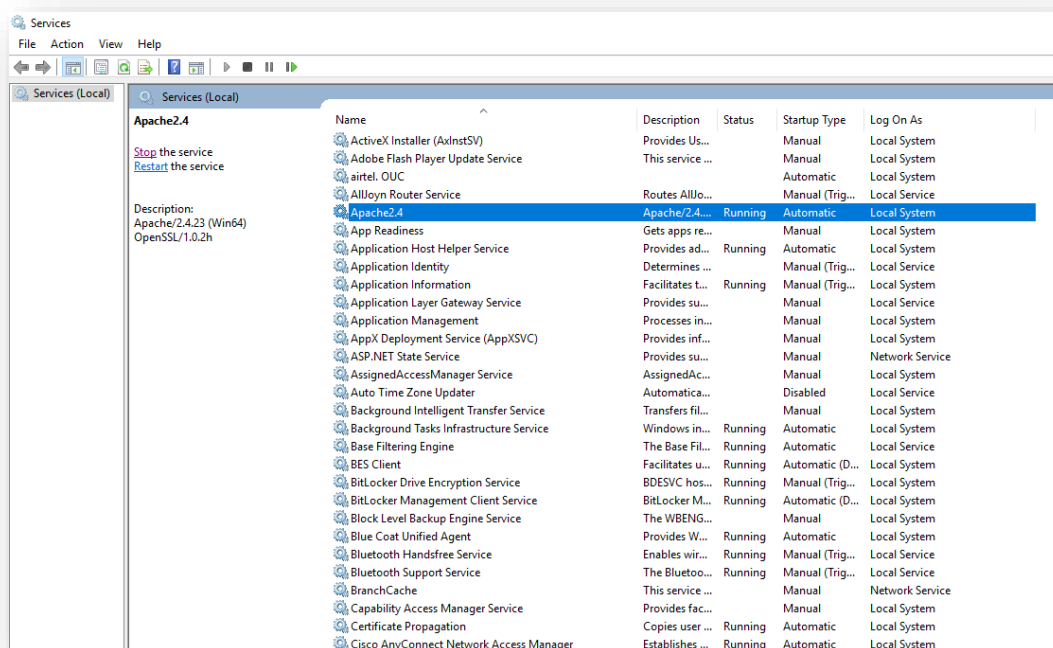


Figure 141 - Hosting Email Service from HTTP to HTTPS (cont.)

3. Search for **HCLiAutomate.EmailService** and right-click on it.
4. Click Properties.

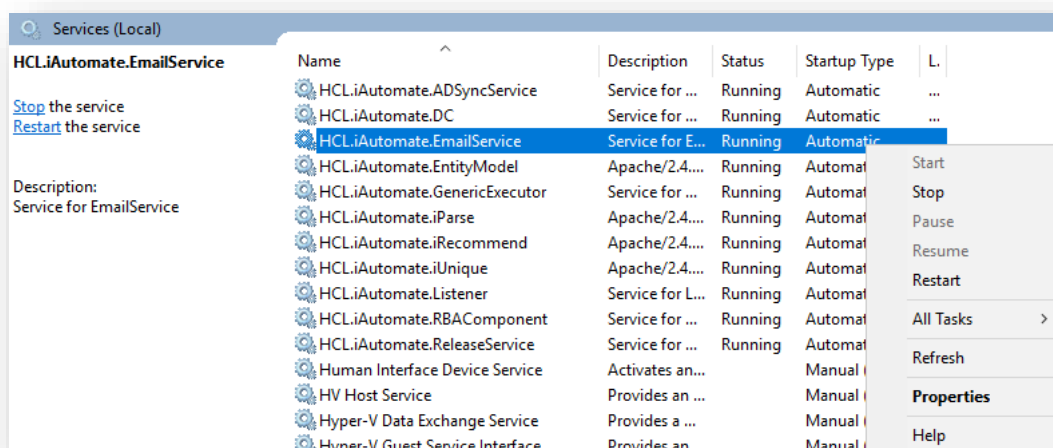


Figure 142 - Hosting Email Service from HTTP to HTTPS (cont.)

5. Copy the value mentioned in 'Path to executable' as shown in the image below.

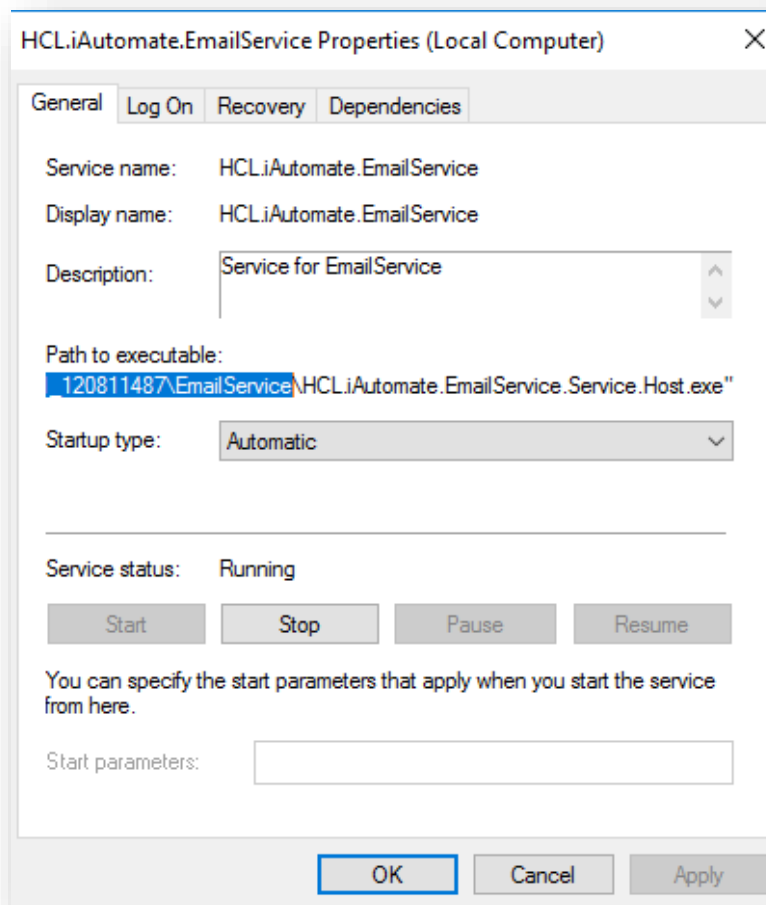


Figure 143 - Hosting Email Service from HTTP to HTTPS (cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Search for **HCL.iAutomate.EmailService.Service.Host.exe** config file and open it in a Notepad.

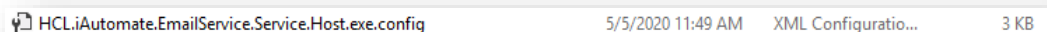


Figure 144 - Hosting Email Service from HTTP to HTTPS (cont.)

8. Within the **HCL.iAutomate.EmailService.Service.Host.exe** config file, find the key '**ServiceHostURL**' and change its value from HTTP to HTTPS.

```
<add key="ServiceHostURL" value="https://<IP>:<Port>/EmailService/" />
```

Figure 145 - Hosting Email Service from HTTP to HTTPS (cont.)

9. Within the **HCL.iAutomate.EmailService.Service.Host.exe** config file, find the key '**securityMode_Service**' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 146 - Hosting Email Service from HTTP to HTTPS (cont.)

10. Within the **HCL.iAutomate.EmailService.Service.Host.exe** config file, find the key '**IsSelfSigned_Service**' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 147 - Hosting Email Service from HTTP to HTTPS (cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.

```
netsh http add sslcert ipport=<ip>:<port on which service is running> appid={21fa9088-0c69-479e-8fdc-a81eb836e264}
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

13. Select HCLiAutomate.EmailService service and click Restart to restart the service.

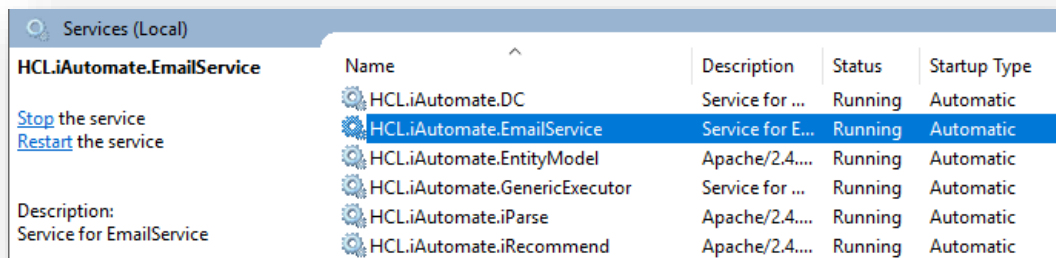


Figure 148 – Hosting Email Service from HTTP to HTTPS (cont.)

3.6.1.2.8 DAG Service

To change the configuration of DAG Service from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

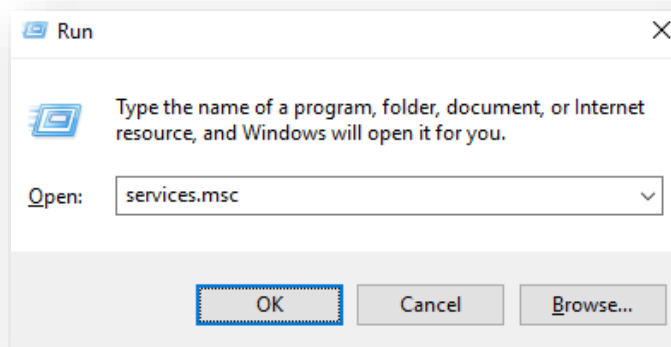


Figure 149 - Hosting DAG Service from HTTP to HTTPS

2. Click OK to open Windows Services.

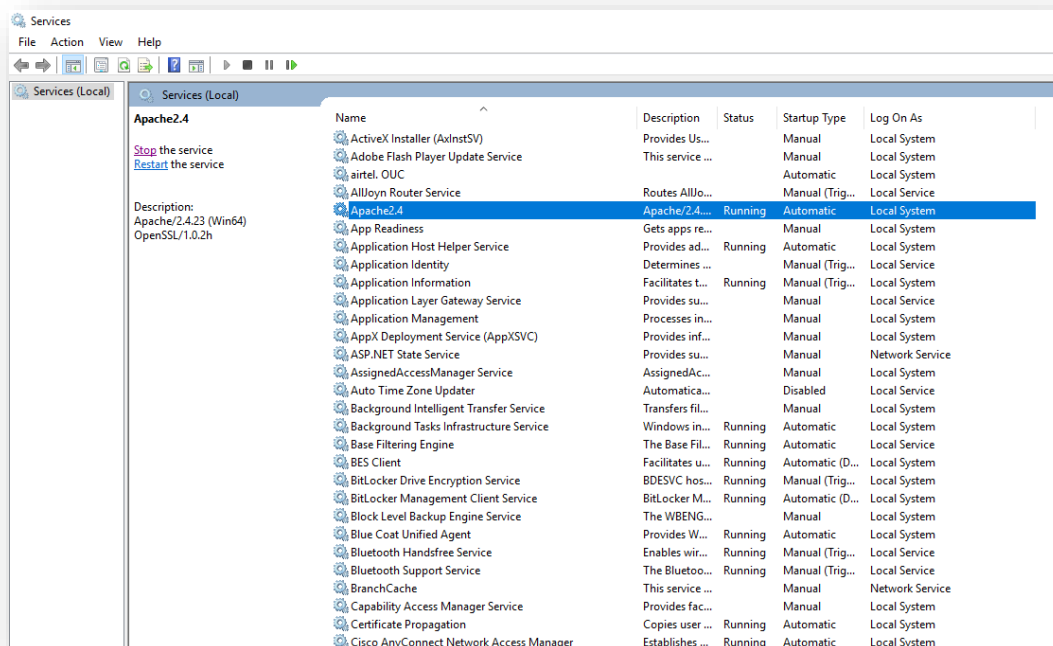


Figure 150 - Hosting DAG Service from HTTP to HTTPS (cont.)

3. Search for **HCL.iAutomat.DAGService** and right-click on it.
4. Click Properties.

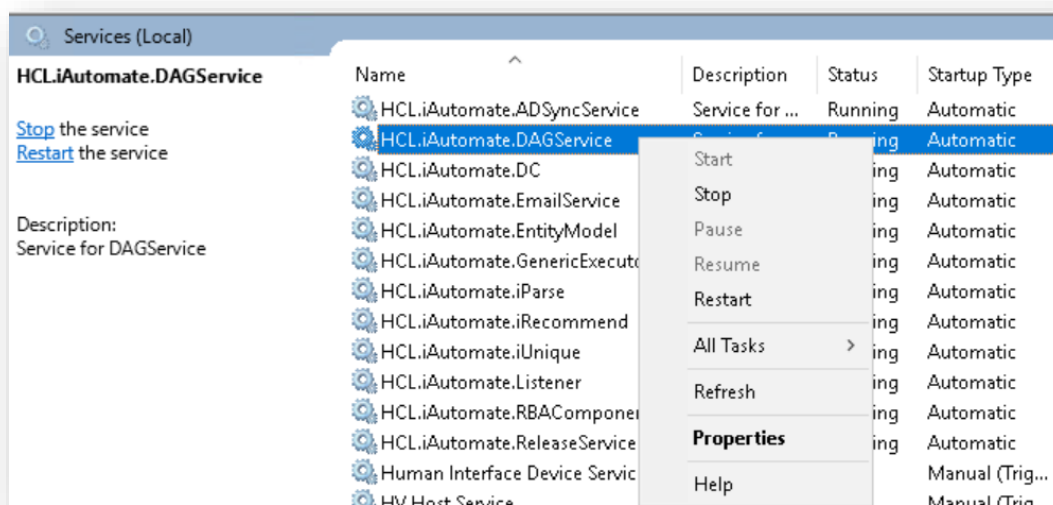


Figure 151 - Hosting DAG Service from HTTP to HTTPS (cont.)

5. Copy the value mentioned in '**Path to executable**' as shown in the image below.

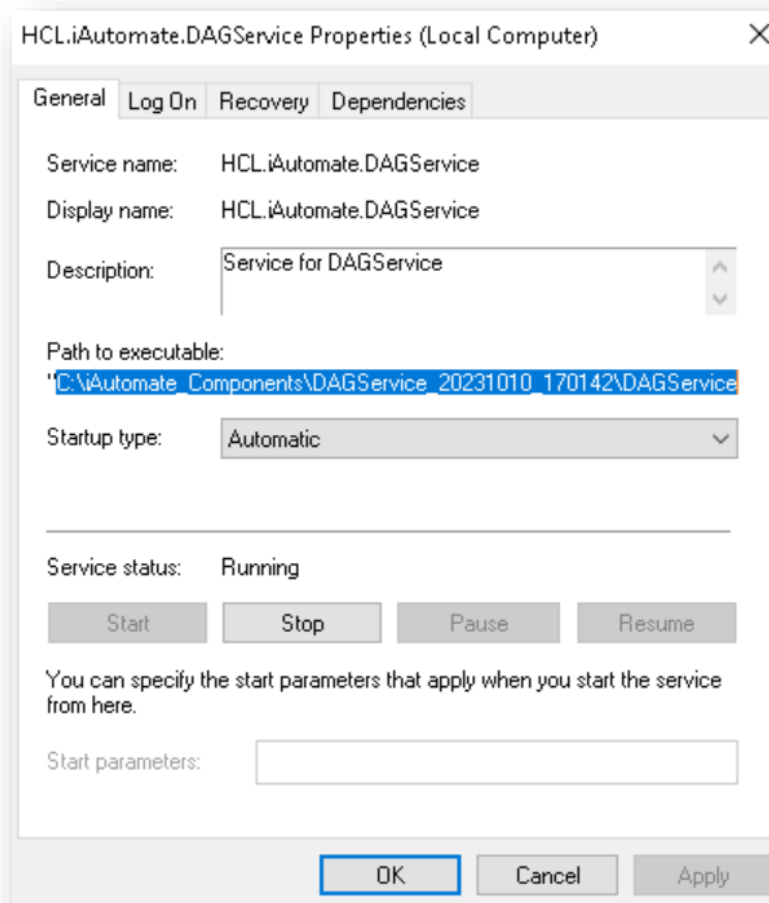


Figure 152 - Hosting DAG Service from HTTP to HTTPS (cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Search for **HCL.DagService.Component.Host.exe** config file and open it in a Notepad.

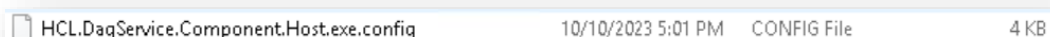


Figure 153 - Hosting DAG Service from HTTP to HTTPS (cont.)

8. Within the **HCL.DagService.Component.Host.exe** config file, find the key '**ServiceHostURL**' and change its value from HTTP to HTTPS.

```
<add key="ServiceHostURL" value="http://<IP>:<PORT>/DAGService/" />
```

Figure 154 - Hosting DAG Service from HTTP to HTTPS (cont.)

9. Within the **HCL.DagService.Component.Host.exe** config file, find the key '**securityMode_Service**' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 155 - Hosting DAG Service from HTTP to HTTPS (cont.)

10. Within the **HCL.DagService.Component.Host.exe** config file, find the key 'IsSelfSigned_Service' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 156 - Hosting DAG Service from HTTP to HTTPS (cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.

```
netsh http add sslcert ipport=<ip>:<port on which service is running> appid={21fa9088-0c69-479e-8fdc-a81eb836e264}  
certhash="<Thumbprint of the certificate>"
```

Replace the **< Thumbprint of the certificate>** with the GUID identified earlier.

13. Select **HCL.iAutomat.DAGService** service and click Restart to restart the service.

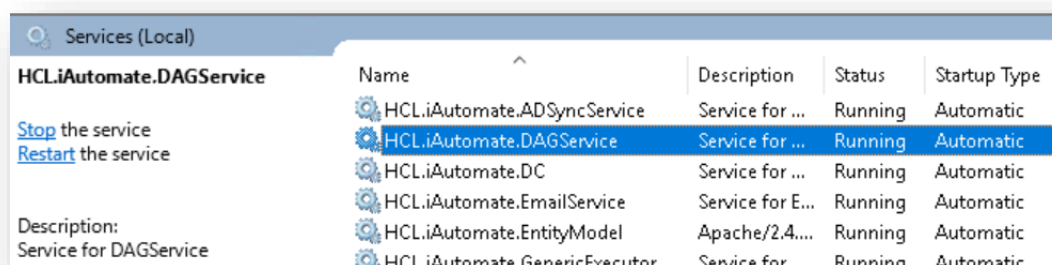


Figure 157 – Hosting DAG Service from HTTP to HTTPS (cont.)

3.6.1.2.9 Assignment Service

To change the configuration of Assignment Service from HTTP to HTTPS, please follow the following steps:

1. Press Win+R and type services.msc.

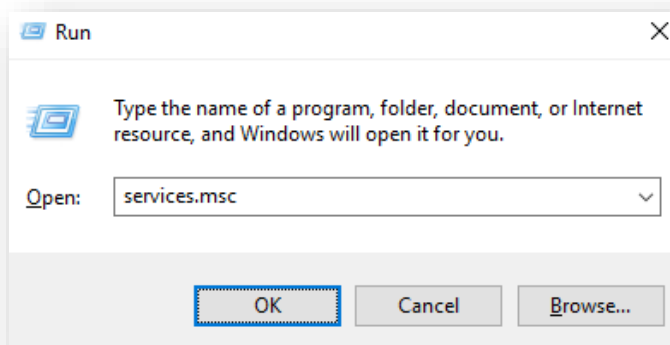


Figure 158 - Hosting Email Service from HTTP to HTTPS

2. Click OK to open Windows Services.

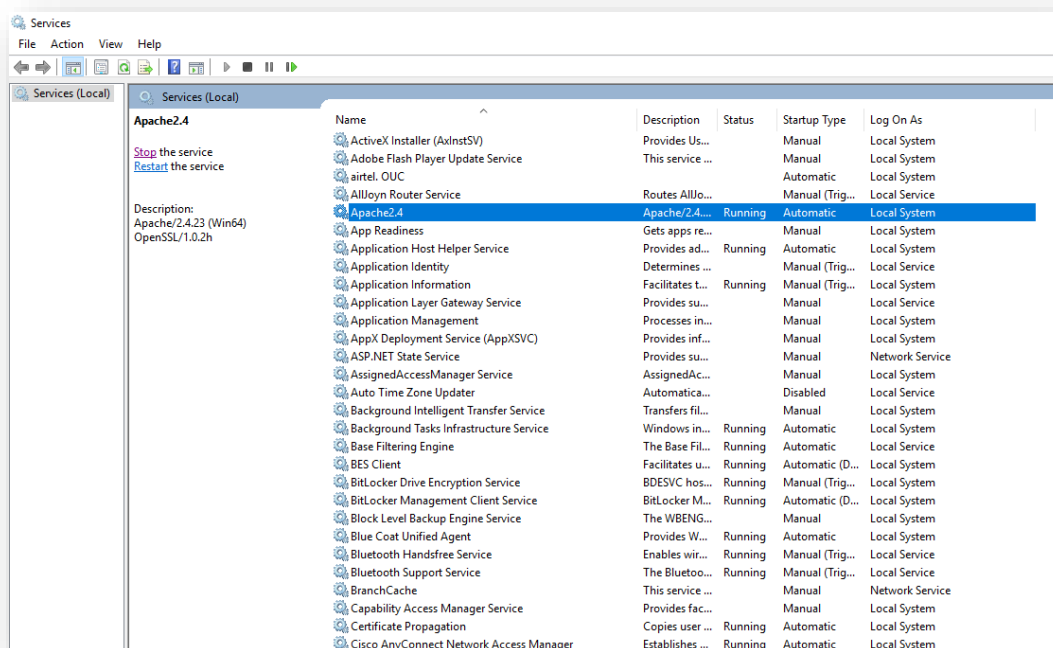


Figure 159 - Hosting Email Service from HTTP to HTTPS (cont.)

3. Search for HCLiAutomate.AssignmentService and right-click on it.
4. Click Properties.

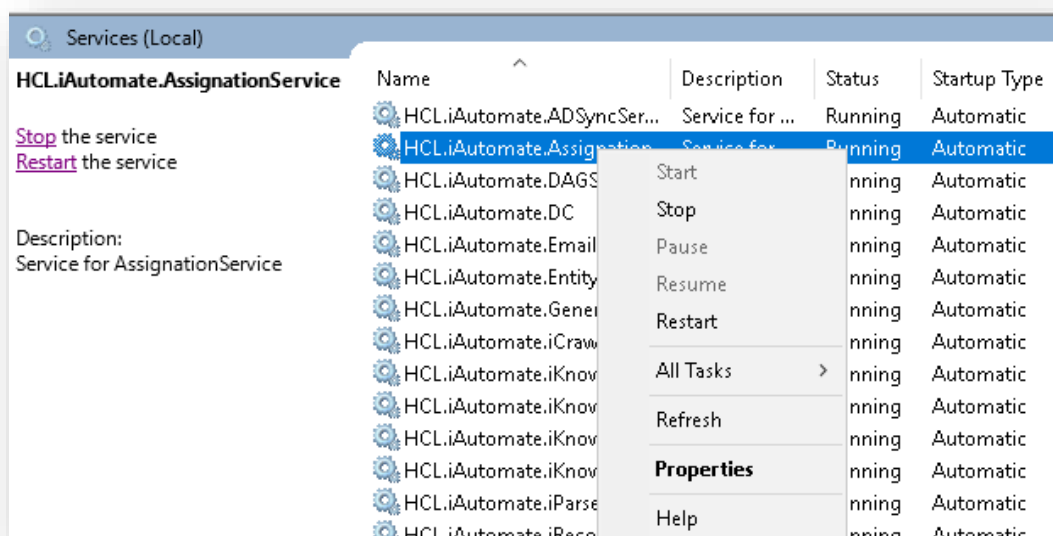


Figure 160 - Hosting Assignment Service from HTTP to HTTPS (cont.)

5. Copy the value mentioned in 'Path to executable' as shown in the image below.

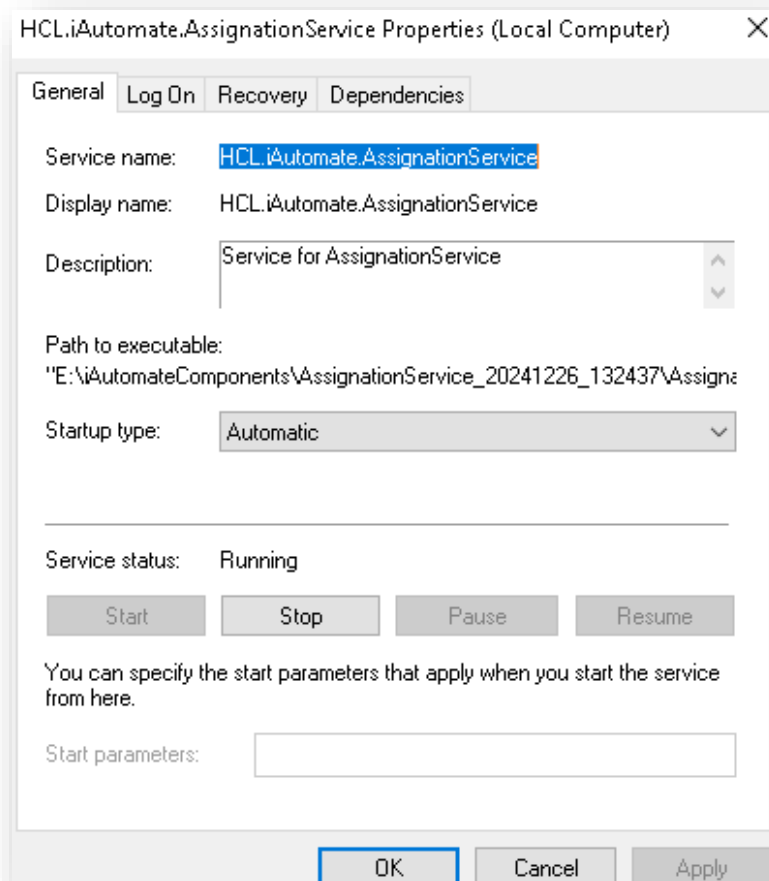


Figure 161 - Hosting Assignment Service from HTTP to HTTPS (cont.)

6. Open File Explorer and paste the copied path and press Enter to open the desired folder.
7. Search for Assignment.Service.Host.exe config file and open it in a Notepad.



Figure 162 - Hosting Service from HTTP to HTTPS (cont.)

8. Within the Assignment.Service.Host.exe config file, find the key 'ServiceHostURL' and change its value from HTTP to HTTPS.

```
<add key="ServiceHostURL" value="http://<IP>:<PORT>/AssignmentService/" />
```

Figure 163 - Hosting Service from HTTP to HTTPS (cont.)

9. Within the Assignment.Service.Host.exe config file, find the key 'securityMode_Service' and change its value from 2 to 3.

```
<add key="securityMode_Service" value="3"/>
```

Figure 164 - Hosting Service from HTTP to HTTPS (cont.)

10. Within the Assignment.Service.Host.exe config file, find the key 'IsSelfSigned_Service' and change its value from N to Y.

```
<add key="IsSelfSigned_Service" value="N"/>
```

Figure 165 - Hosting Service from HTTP to HTTPS (cont.)

11. Save the file for changes to be reflected.
12. Open the command prompt as administrator and run the following command.


```
netsh http add sslcert ipport=<ip>:<port on which service is running>appid={21fa9088-0c69-479e-8fdc-a81eb836e264}
certhash="<Thumbprint of the certificate>"
```
13. Replace the <Thumbprint of the certificate> with the GUID identified earlier.
14. Select HCL.iAutomat.AssignationService service and click Restart to restart the service.

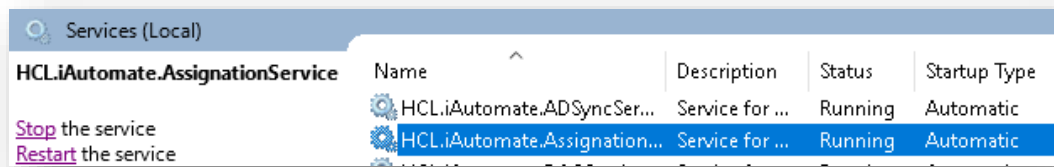


Figure 166 – Hosting Service from HTTP to HTTPS (cont.)

3.6.1.2.10 Configuration Changes via GUI

To change the configuration for various components via GUI from HTTP to HTTPS, please follow the below steps:

1. Login to **iAutomate** using the Super Admin credentials.
2. Roll-over to the Advance Configuration and click Load Balancer Configuration.
3. Select **Component Name** as **Web API**.
4. Change the **Load Balancer URL** from HTTP to HTTPS.

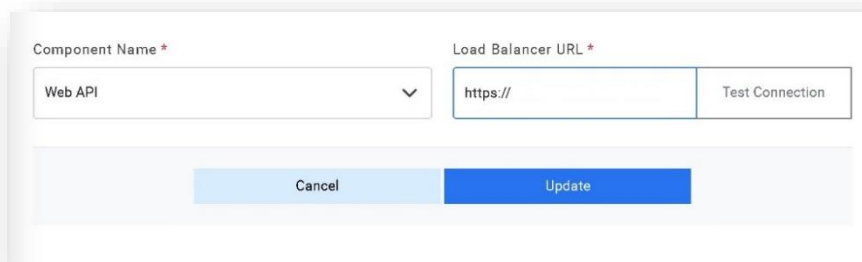


Figure 167 - Configuration Changes via GUI from HTTP to HTTPS

5. Click **Update** to save the changes.
6. Select Component Name as Data Collector.
7. Change the Load Balancer URL from HTTP to HTTPS.

Component Name *

Data Collector

Load Balancer URL *

https://[REDACTED]:8012

Test Connection

Cancel Update

Figure 168 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)

8. Click **Update** to save the changes.
9. Select **Component Name** as 'Generic Service'.
10. Change the **Load Balancer URL** from **HTTP** to **HTTPS**.

Component Name *

Generic Service

Load Balancer URL *

https://

Test Connection

Cancel Update

Figure 169 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)

11. Click **Update** to save the changes.
12. Select **Component Name** as 'Release Service'.
13. Change the Load Balancer URL from HTTP to HTTPS.

Component Name *

Release Service

Load Balancer URL *

https://

Test Connection

Cancel Update

Figure 170 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)

14. Click **Update** to save the changes.
15. Select **Component Name** as 'RBA Service'.
16. Change the Load Balancer URL from HTTP to HTTPS.

Component Name *

RBA Service

Load Balancer URL *

https://

Test Connection

Cancel Update

Figure 171 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)

17. Click **Update** to save the changes.
18. Select **Component Name** as 'Active Directory'.
19. Change the Load Balancer URL from HTTP to HTTPS.

Component Name *

Active Directory

Load Balancer URL *

[Redacted]

Test Connection

Cancel Update

Figure 172 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)

20. Click **Update** to save the changes.
21. Select **Component Name** as 'Email Service'.
22. Change the Load Balancer URL from HTTP to HTTPS.

Component Name *

Email Service

Load Balancer URL *

https://

Test Connection

Cancel Update

Figure 173 - Configuration Changes via GUI from HTTP to HTTPS (Cont.)

23. Click **Update** to save the changes.

3.6.2 Configuration Changes – Certificate Name Change (Type – PFX)

This section describes how to make the configurational changes if the SSL certificate name (Type - PFX) is other than 'HCL.iAutomate'.

Please install the certificate through the **Microsoft Management Console** in both **Personal** as well as **Trusted People** folder. Refer to the pre-requisites document for the detailed procedure for certificate installation at required locations.

3.6.2.1 Change name of Certificate used to connect KRS

3.6.2.1.1 Website

This section describes configuration changes required for the Website in case SSL certificate is other than **HCLiAutomate**. Following changes are required in the underlying components.

3.6.2.1.1.1 Key Rotation Service (KRS)

To make changes for the KRS, please follow the below steps:

1. Press **Win+R** and type **inetmgr**.
2. Click **OK** to open IIS.

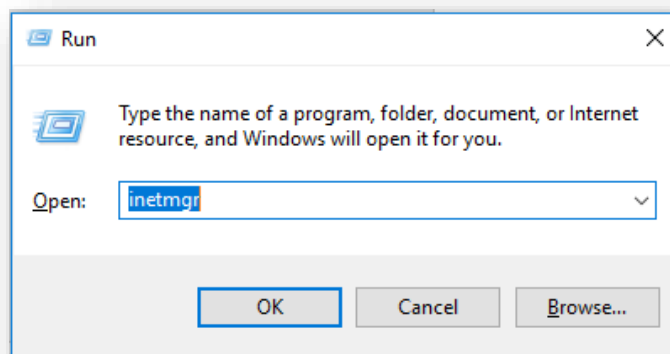


Figure 174 - Certificate Name Change – KRS

3. Expand Sites and click HCLiAutomateKRS.

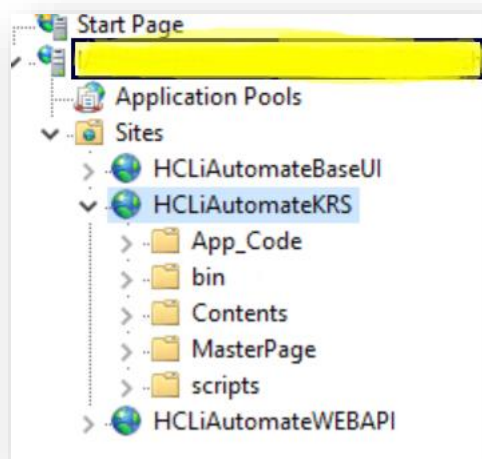


Figure 175 - Certificate Name Change – KRS (Cont.)

4. Right click HCLiAutomateKRS.
5. Click **Explore**.
6. Find **Web.config** file and open it in a Notepad.



Figure 176 - Certificate Name Change – KRS (Cont.)

7. Within the **Web.config** file, find the tag <serviceCertificate> and change the value of attribute 'findValue' with the updated **Certificate Name**.

```
<serviceCertificate findValue="HCLiAutomateBaseUI" />
```

Figure 177 - Certificate Name Change – KRS (Cont.)

8. If the certificate is self-signed, find the key '**IsSelfSigned**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned" value="Y"/>
```

Figure 178 - Certificate Name Change – KRS (Cont.)

9. Save the file for changes to be reflected.
10. Select the service and click **Restart** to restart the services.

3.6.2.1.1.2 Base User interface

To make changes for the BaseUI, please follow the below steps:

1. Press **Win+R** and type **inetmgr**.
2. Click **OK** to open **IIS**.

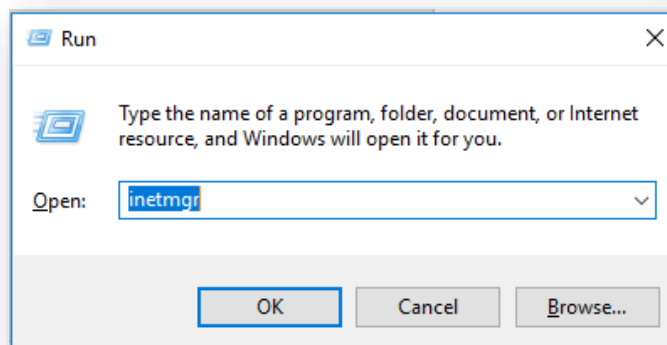


Figure 179 - Certificate Name Change – BaseUI

3. Expand **Sites** and click **HCLiAutomateBaseUI**.

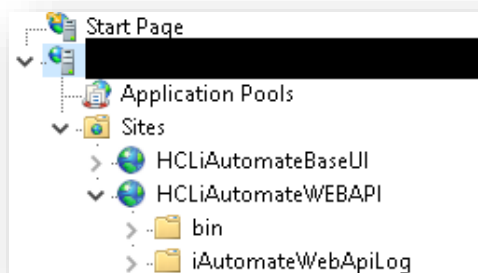


Figure 180 - Certificate Name Change – BaseUI (Cont.)

4. Right-click **HCLiAutomateBaseUI** and click **Explore**.
5. Find **Web.config** file and open it in a Notepad.



Figure 181 - Certificate Name Change – BaseUI (Cont.)

6. Within the **Web.config** file, find the key '**Certificate_Name_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 182 - Certificate Name Change – BaseUI (Cont.)

7. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 183 - Certificate Name Change – BaseUI (Cont.)

8. Save the file for changes to be reflected.
9. Select the service and click **Restart** to restart the services.

3.6.2.1.1.3 Web API

To make changes for the Web API, please follow the below steps:

1. Press **Win+R** and type **inetmgr**.
2. Click **OK** to open **IIS**.

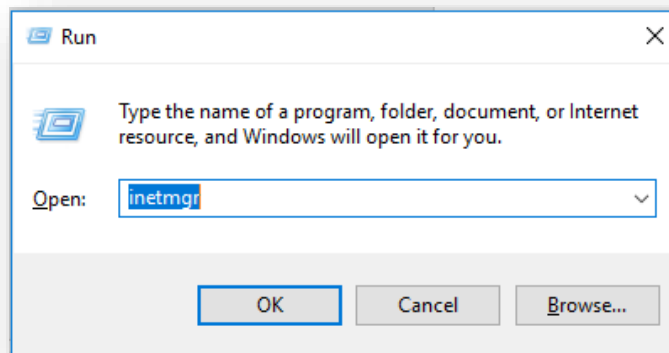


Figure 184 - Certificate Name Change – Web API

3. Expand **Sites** and right-click **HCLiAutomateWEBAPI**.
4. Click **Explore**.

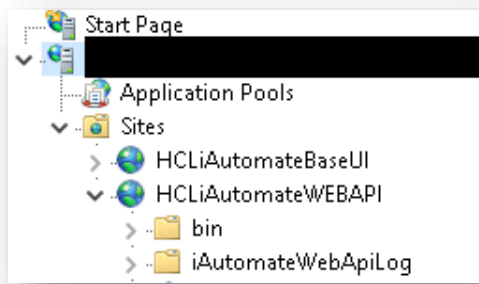


Figure 185 - Certificate Name Change – Web API (cont.)

5. Find **Web.config** file and open it in **Notepad**.

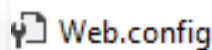


Figure 186 - Certificate Name Change – Web API (cont.)

6. Within the **Web.config** file, find the key '**Certificate_Name_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iAutomate.Web" />
```

Figure 187 - Certificate Name Change – Web API (cont.)

7. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 188 - Certificate Name Change – Web API (cont.)

8. Save the file for changes to be reflected.
9. Select the service and click **Restart** to restart the services.

3.6.2.1.2 Components

This section describes the configuration changes required for the Components in case the SSL Certificate name is other than **HclTech.iAutomate.Web**.

Following changes are required in the underlying components:

3.6.2.1.2.1 Listener

To make changes for the Listener, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

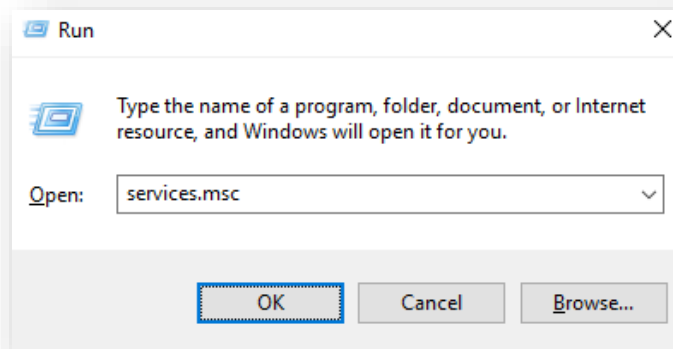


Figure 189 - Certificate Name Change – Listener

2. Click OK to open Windows Services.

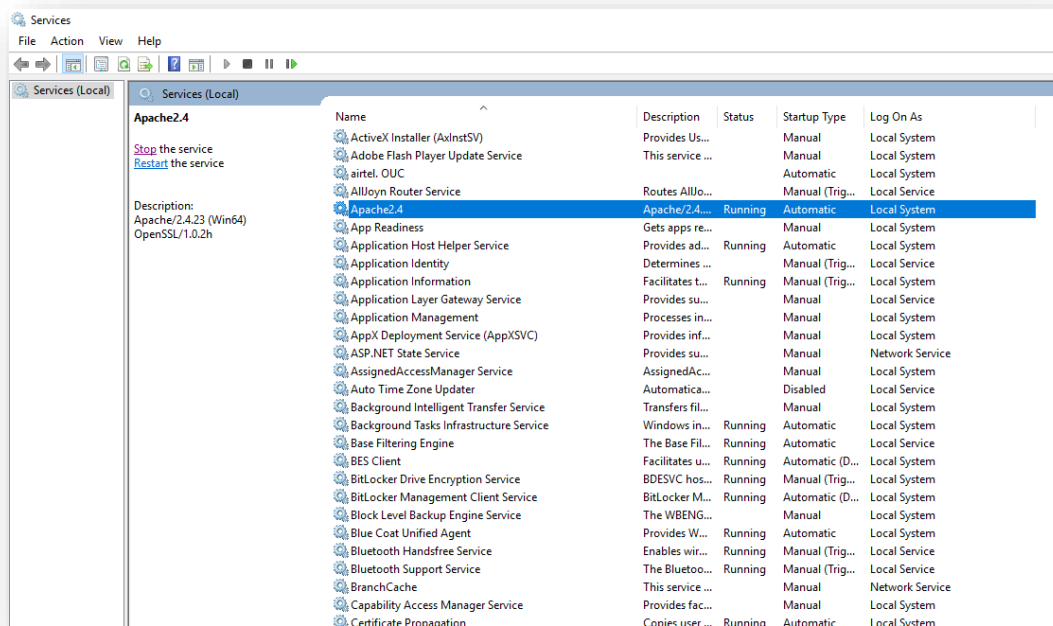


Figure 190 - Certificate Name Change – Listener (cont.)

3. Search for **HCL.iAutomate.Listener** service and right-click on it.
4. Click **Properties**.

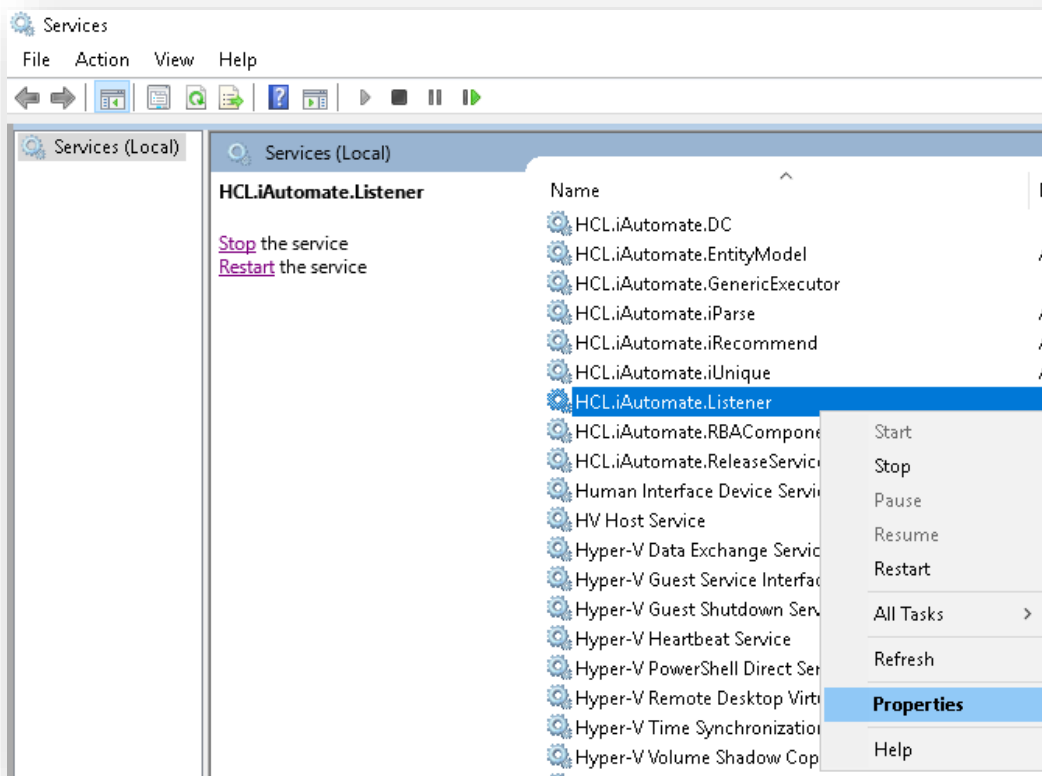


Figure 191 - Certificate Name Change – Listener (cont.)

5. Copy the value in **Path to executable** as shown in the image below.

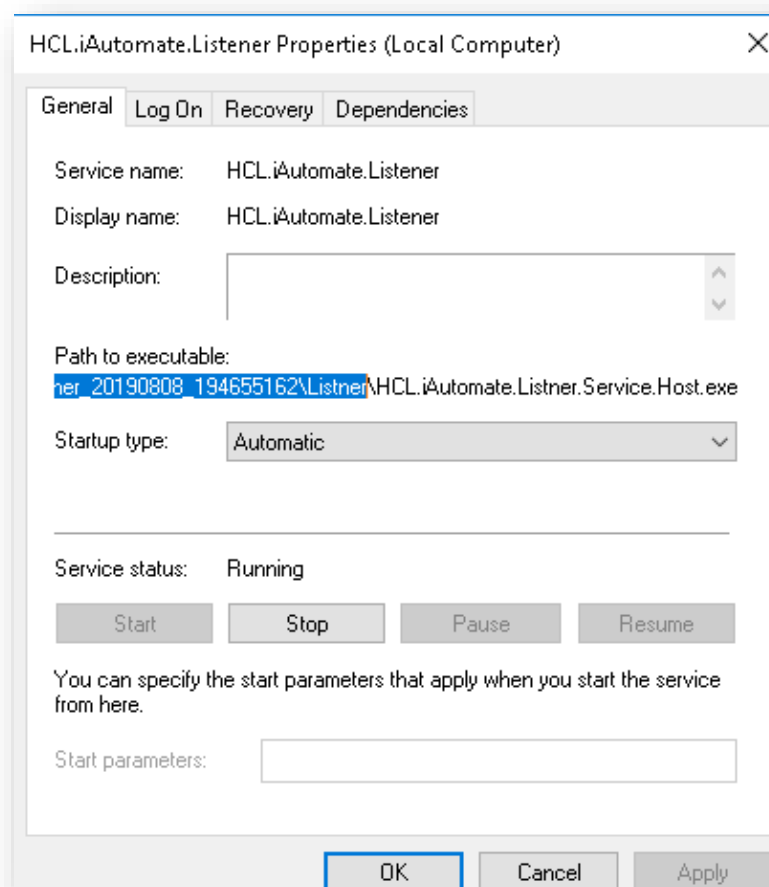


Figure 192 - Certificate Name Change – Listener (cont.)

6. Open **File Explorer** then paste the copied path and press Enter to open the desired folder.
7. Search for **HCLiAutomate.Listener.Service.Host** config file and open it in a Notepad.



Figure 193 - Certificate Name Change – Listener (cont.)

8. Within the **HCLiAutomate.Listener.Service.Host** config file, find the key '**CertificateName_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 194 - Certificate Name Change – Listener (cont.)

9. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 195- Certificate Name Change – Listener (cont.)

10. Save the file for changes to be reflected.
11. Select the service and click **Restart** to restart the services.

3.6.2.1.2.2 Data Collector

To make changes for the Data Collector, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

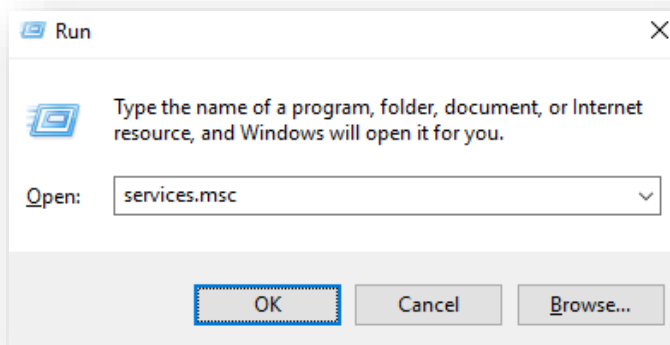


Figure 196 - Certificate Name Change – Data Collector

2. Click OK to open Windows Services.

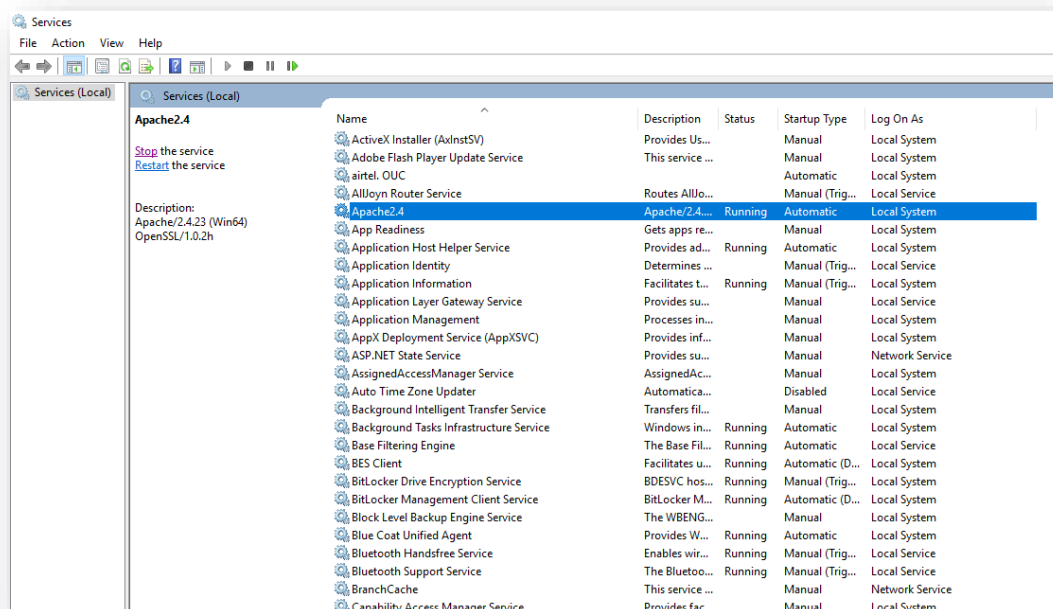


Figure 197 - Certificate Name Change – Data Collector (Cont.)

3. Search for **HCL.iAutomate.DC** service and right-click on it.
4. Click on **Properties**.

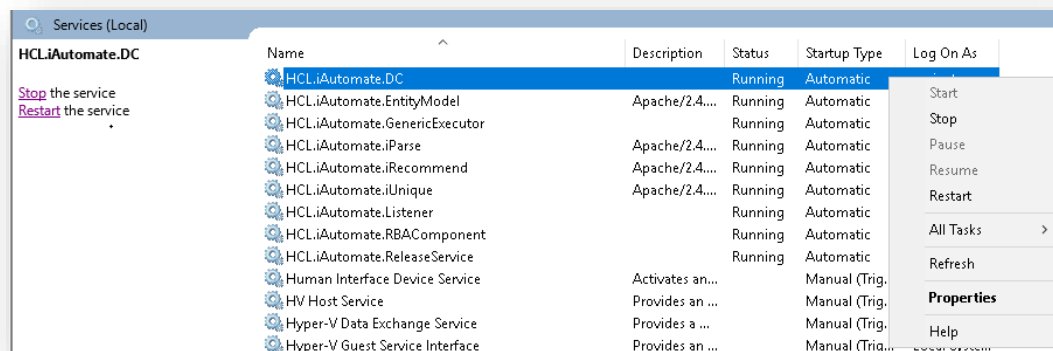


Figure 198 - Certificate Name Change – Data Collector (Cont.)

- Copy the value mentioned in **Path to executable** as shown in the image below.

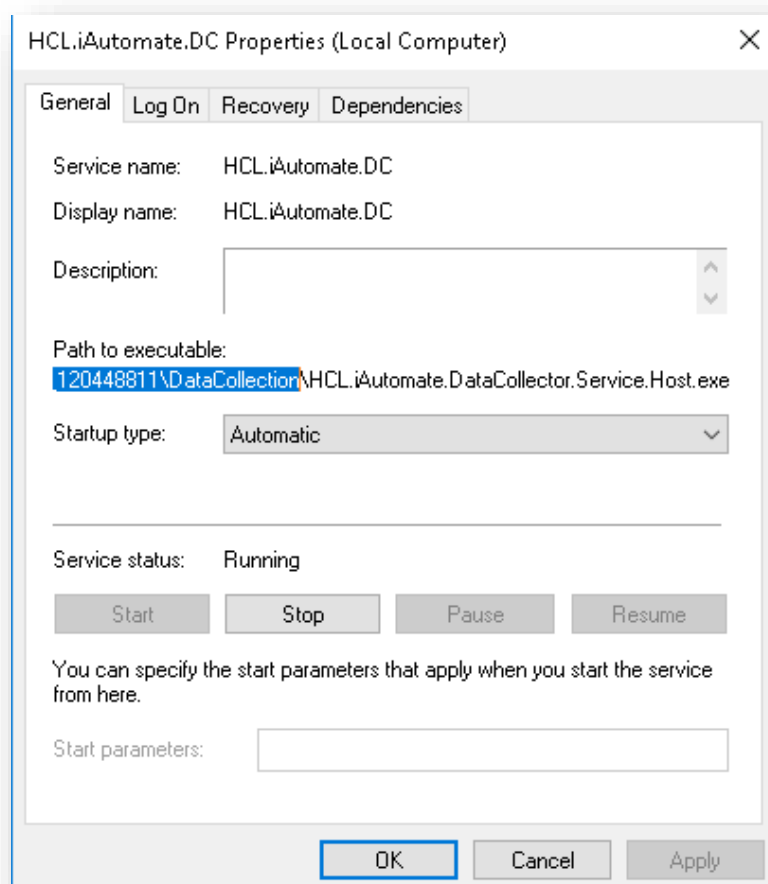


Figure 199 - Certificate Name Change – Data Collector (Cont.)

- Open **File Explorer**, then paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCLiAutomate.DataCollector.Service.Host.exe** config file and open it in a Notepad.



Figure 200 - Certificate Name Change – Data Collector (Cont.)

- Within the **HCLiAutomate.DataCollector.Service.Host.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new Certificate Name.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 201 - Certificate Name Change – Data Collector (Cont.)

9. If the certificate is self-signed, find the key 'IsSelfSigned_KRS' and change its value to 'Y'. Else the value will be 'N'..

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 202 - Certificate Name Change – Data Collector (Cont.)

10. Save the file for changes to be reflected.
11. Select **HCLiAutomate.DC** service and click **Restart** to restart the service.

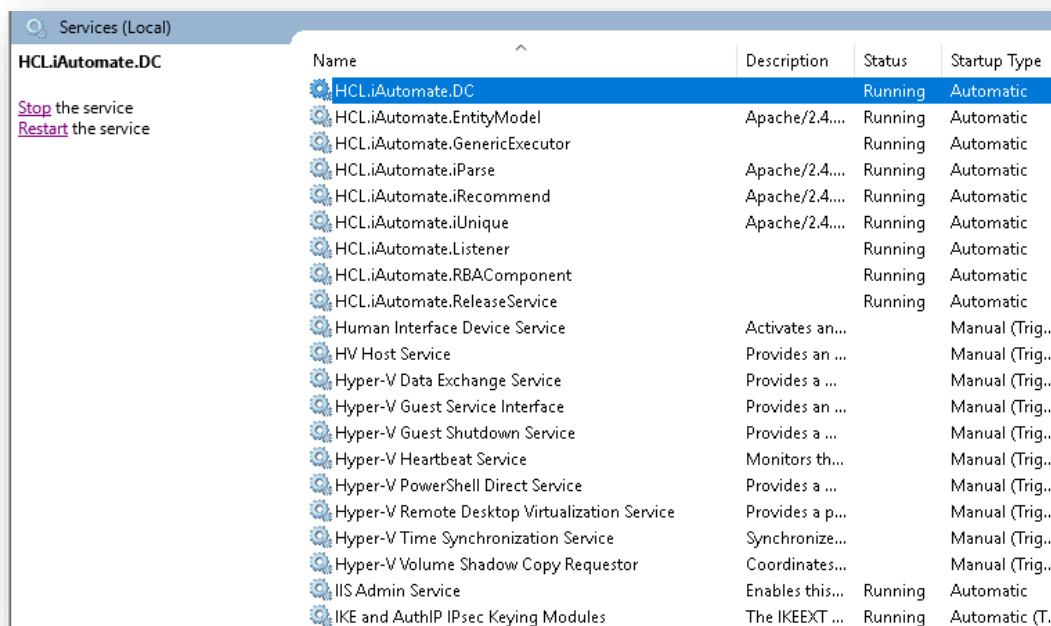


Figure 203 - Certificate Name Change – Data Collector (Cont.)

3.6.2.1.2.3 Generic Service

To make changes for the Generic Service, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

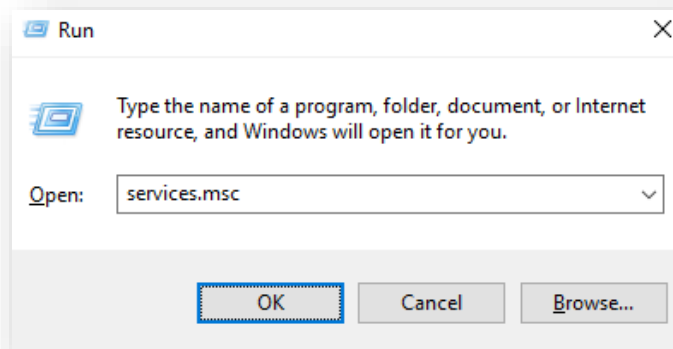


Figure 204 - Certificate Name Change – Generic Service

2. Click OK to open Windows Services.

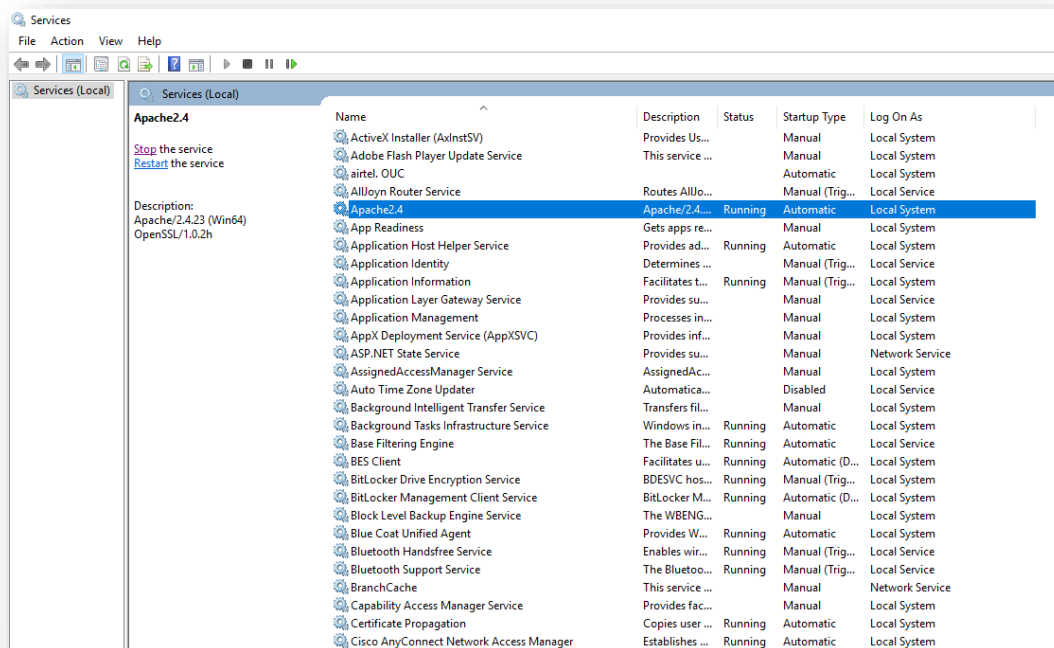


Figure 205 - Certificate Name Change – Generic Service (cont.)

3. Search for **HCL.iAutomate.GenericExecutor** service and right-click on it.
4. Click on **Properties**.

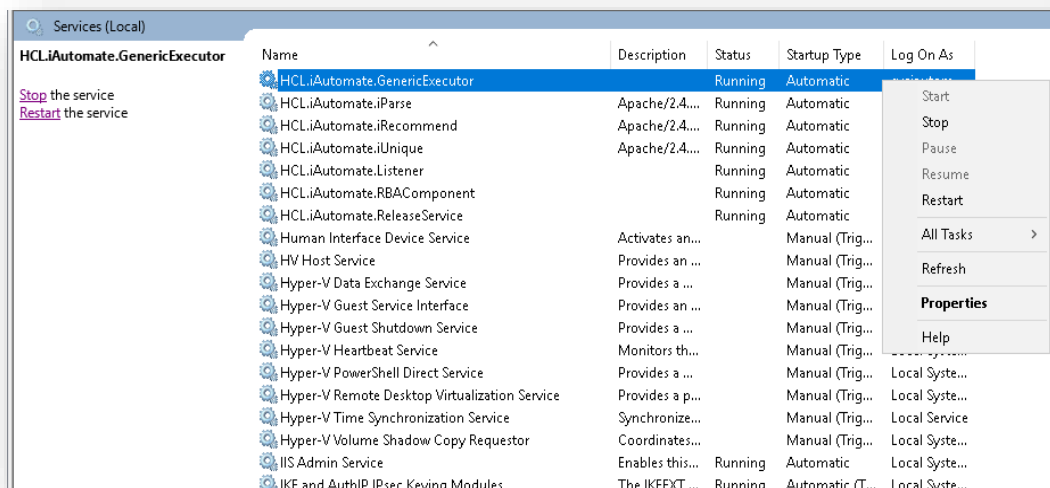


Figure 206 - Certificate Name Change – Generic Service (cont.)

- Copy the value in **Path to executable** as shown in the image below.

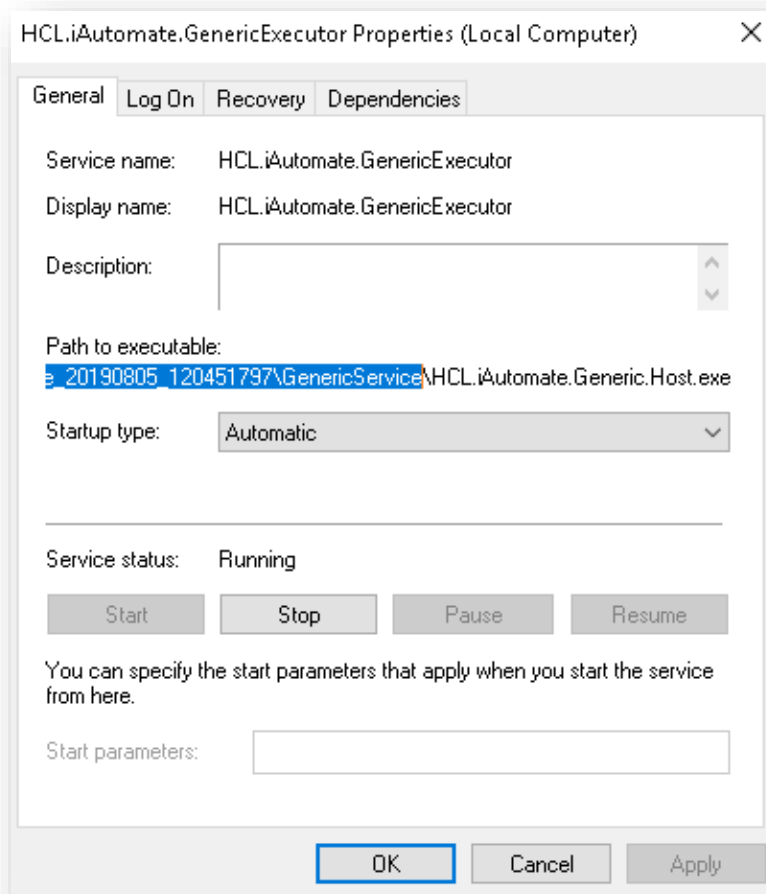


Figure 207 - Certificate Name Change – Generic Service (cont.)

- Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCLiAutomate.Generic.Host.exe** config file and open it in a Notepad.

Figure 208- Certificate Name Change – Generic Service (cont.)

8. Within the **HCLiAutomate.Generic.Host.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 209 - Certificate Name Change – Generic Service (cont.)

9. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 210 - Certificate Name Change – Generic Service (cont.)

10. Save the file for changes to be reflected.
11. Select **HCLiAutomate.GenericExecutor** service and click **Restart** to restart the service.

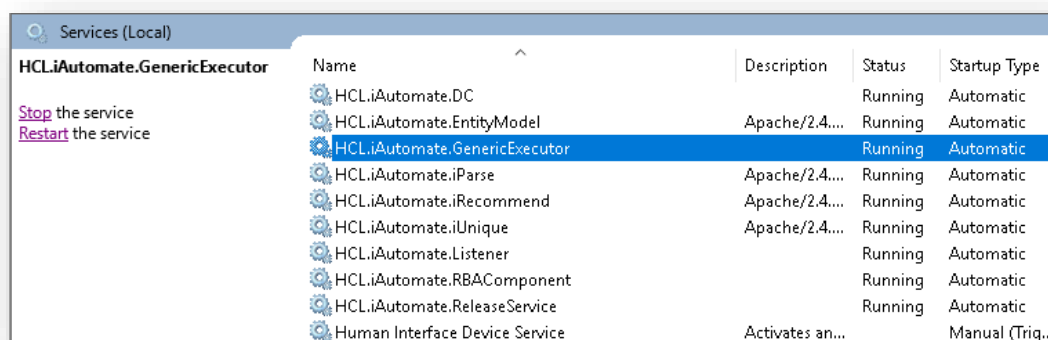


Figure 211- Certificate Name Change – Generic Service (cont.)

3.6.2.1.2.4 RBA Component

To make changes for the RBA component, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

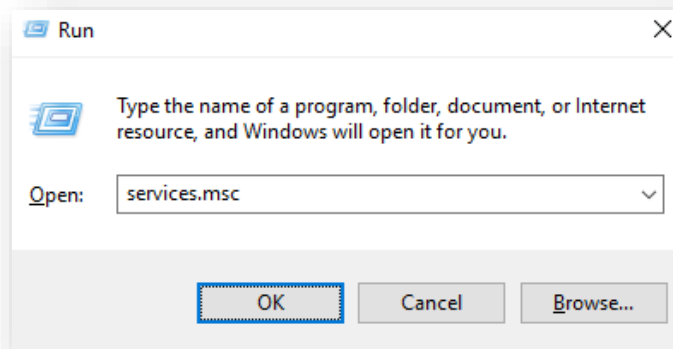


Figure 212 - Certificate Name Change – RBA Component

2. Click OK to open Windows Services.

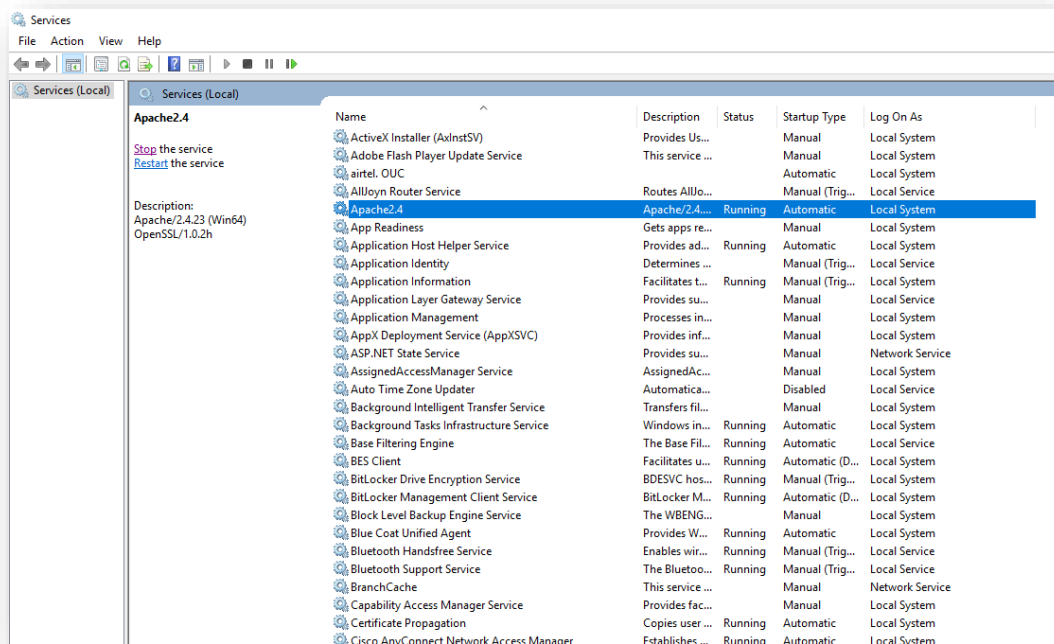


Figure 213 - Certificate Name Change – RBA Component (cont.)

3. Search for HCLiAutomate.RBAComponent service and right-click on it.
4. Click Properties.

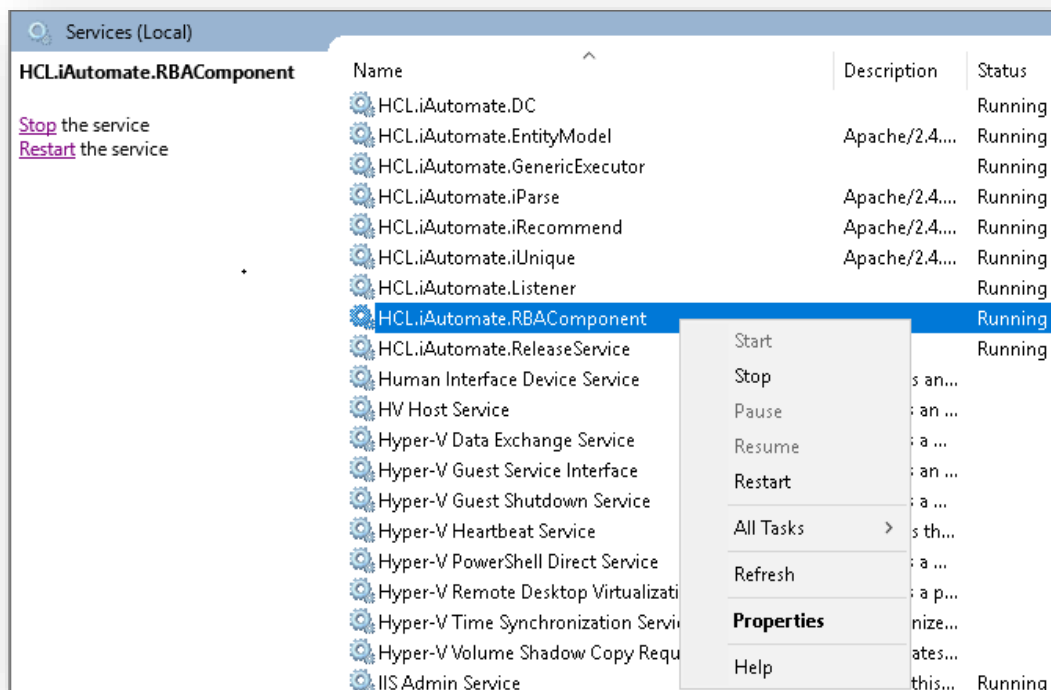


Figure 214 - Certificate Name Change – RBA Component (cont.)

- Copy the value mentioned in **Path to executable** as shown in the image below.

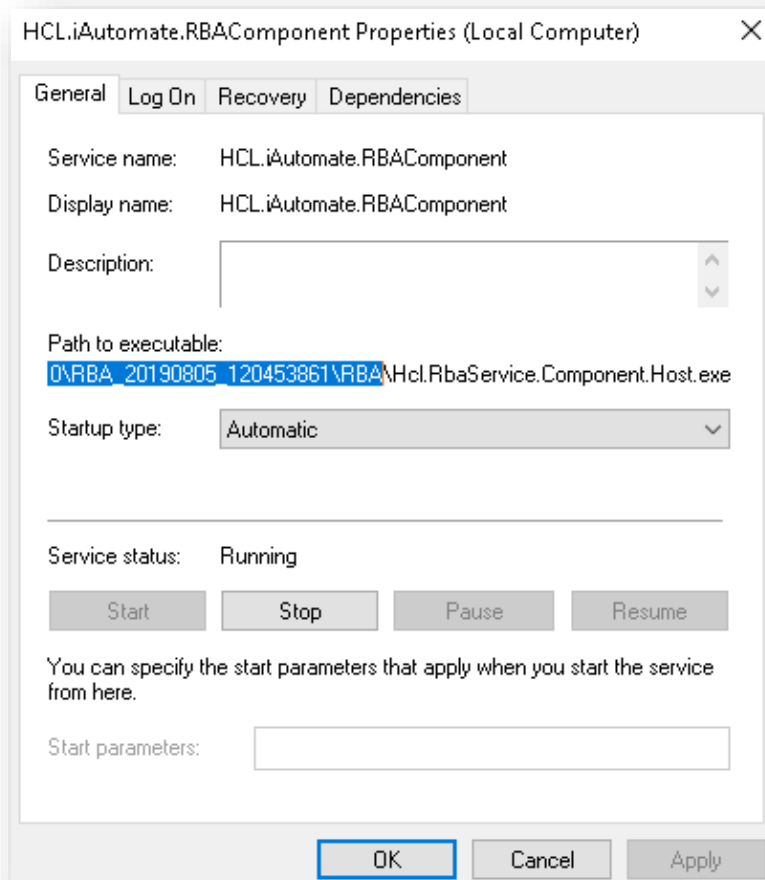


Figure 215 - Certificate Name Change – RBA Component (cont.)

- Open **File Explorer**, then paste the **copied path** and press **Enter** to open the desired folder.

7. Search for **HCL.RbaService.Component.Host.exe** config file and open it in a Notepad.

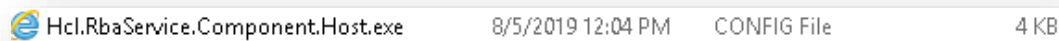


Figure 216 - Certificate Name Change – RBA Component (cont.)

8. Within the **HCL.RbaService.Component.Host.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iAutomate.Web" />
```

Figure 217 - Certificate Name Change – RBA Component (cont.)

9. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 218 - Certificate Name Change – RBA Component (cont.)

10. Save the file for changes to be reflected.
11. Select **HCL.iAutomate.RBAComponent** service and click **Restart** to restart the service.

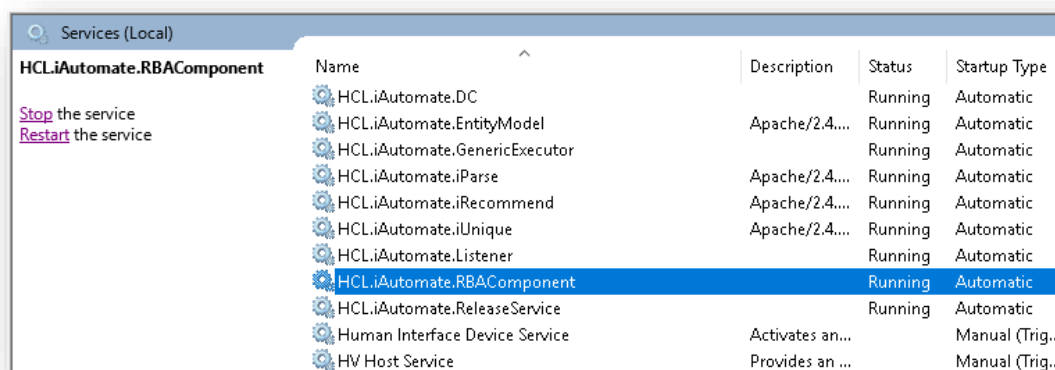


Figure 219 - Certificate Name Change – RBA Component (cont.)

3.6.2.1.2.5 Release Service

To make changes for the Release Service, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

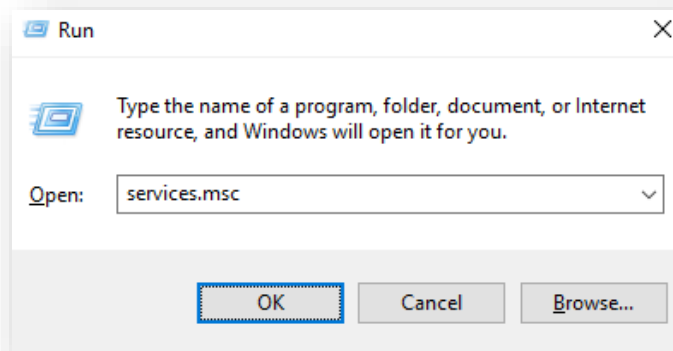


Figure 220 - Certificate Name Change – Release Service

2. Click OK to open Windows Services.

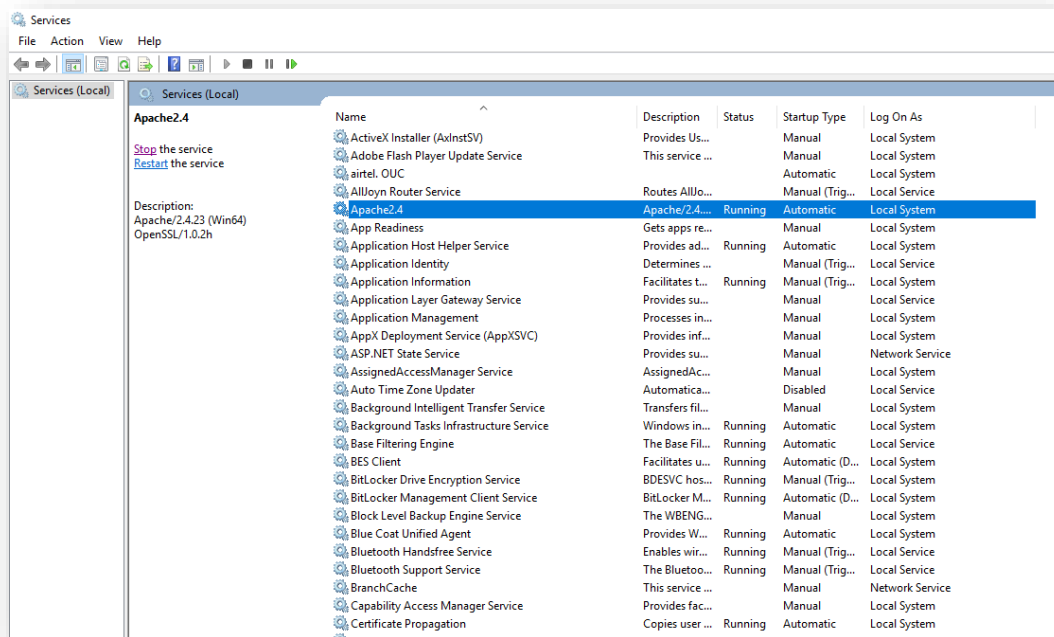


Figure 221 - Certificate Name Change – Release Service (cont.)

3. Search for HCL.iAutomate.ReleaseService and right-click on it.
4. Click Properties.

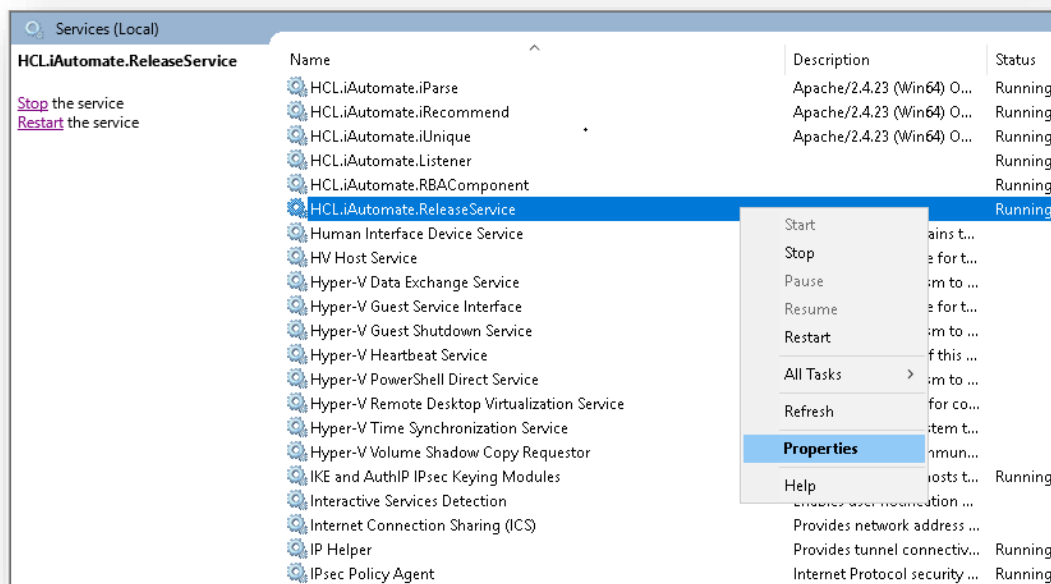


Figure 222 - Certificate Name Change – Release Service (cont.)

- Copy the value mentioned in **Path to executable** as shown in the image below.

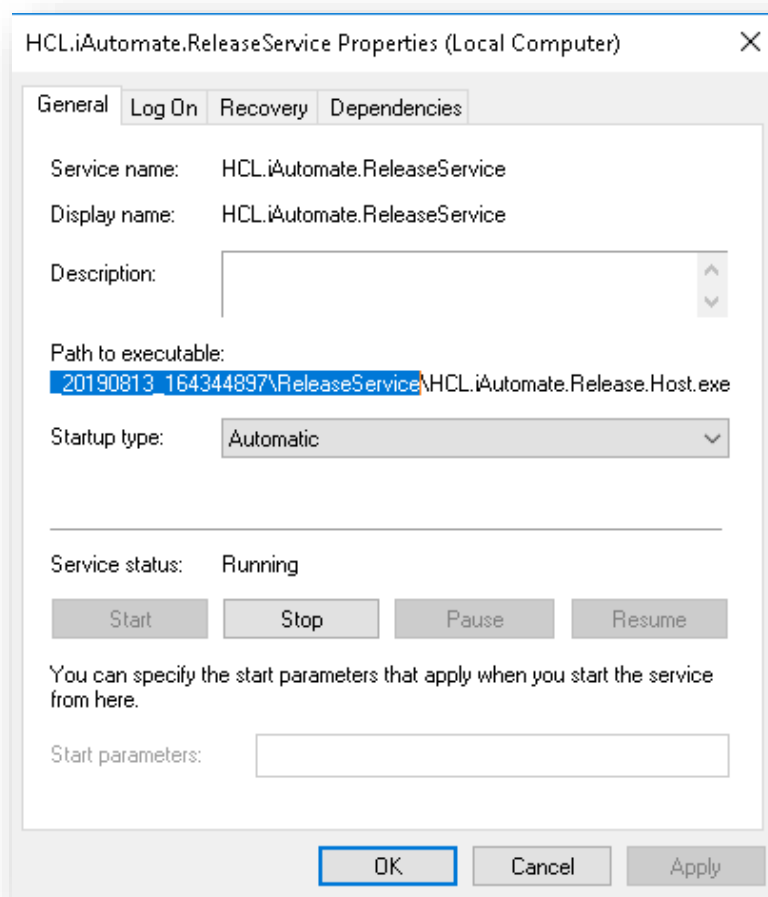


Figure 223 - Certificate Name Change – Release Service (cont.)

- Open **File Explorer**, then paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCL.iAutomate.Release.Host.exe** config file and open it in a Notepad.

Figure 224 - Certificate Name Change – Release Service (cont.)

8. Within the **HCL.iAutomate.Release.Host.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 225 - Certificate Name Change – Release Service (cont.)

9. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 226 - Certificate Name Change – Release Service (cont.)

10. Save the file for changes to be reflected.
11. Select **HCL.iAutomate.ReleaseService** service and click **Restart** to restart the service.

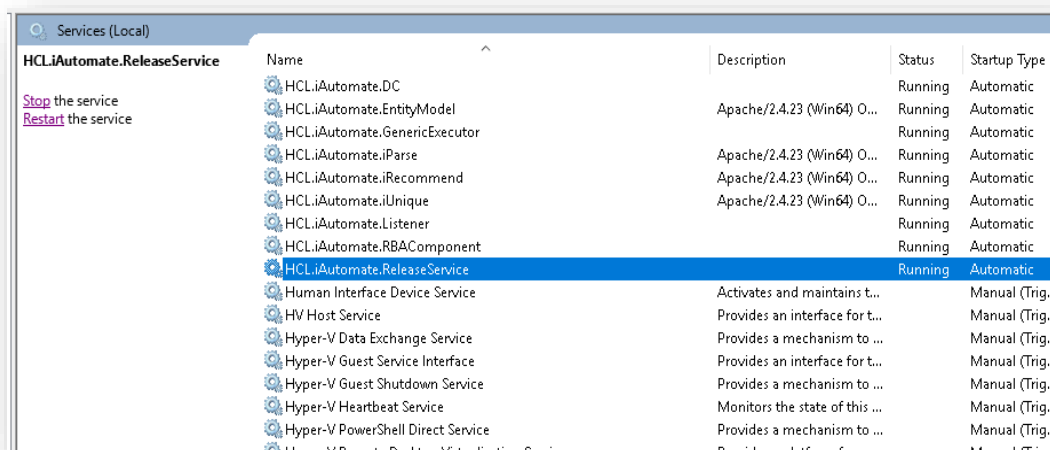


Figure 227 - Certificate Name Change – Release Service (cont.)

3.6.2.1.2.6 AD Sync

To change the configuration of AD Sync from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

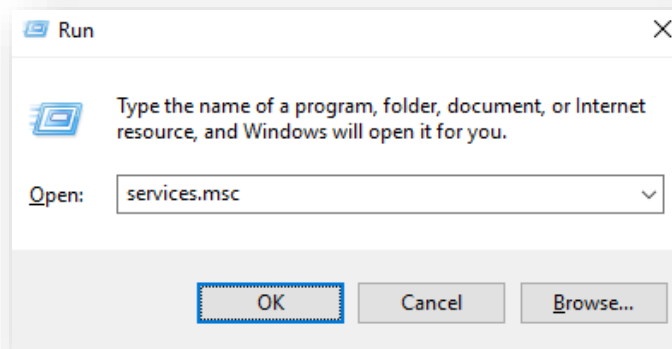


Figure 228 - Certificate Name Change – AD Sync Service

2. Click OK to open Windows Services.

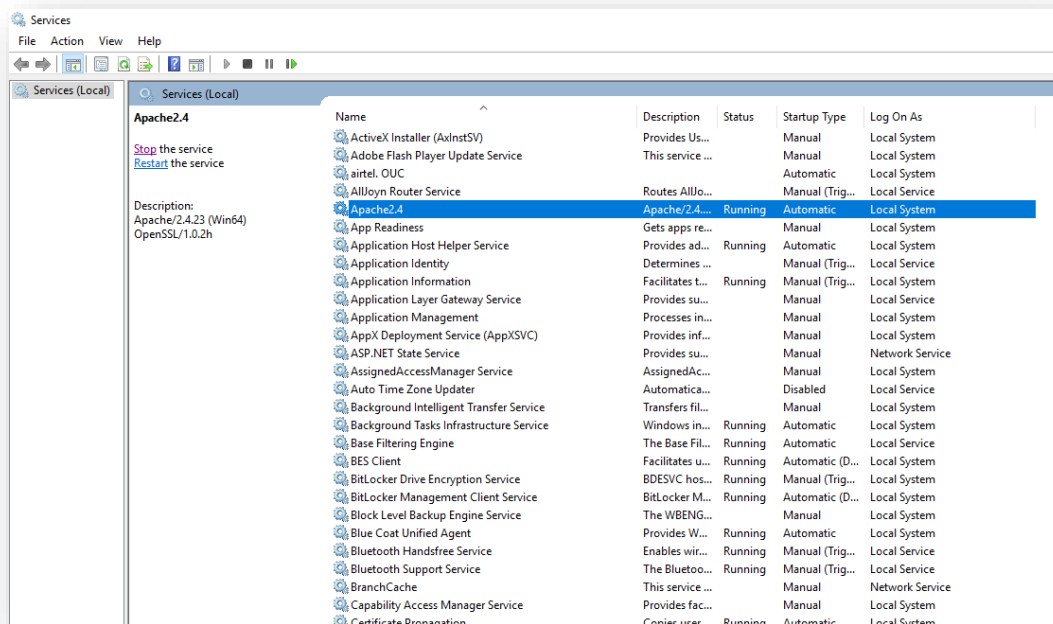


Figure 229 - Certificate Name Change – AD Sync Service (cont.)

3. Search for HCLiAutomate.ADSyncService and right-click on it.
4. Click **Properties**.

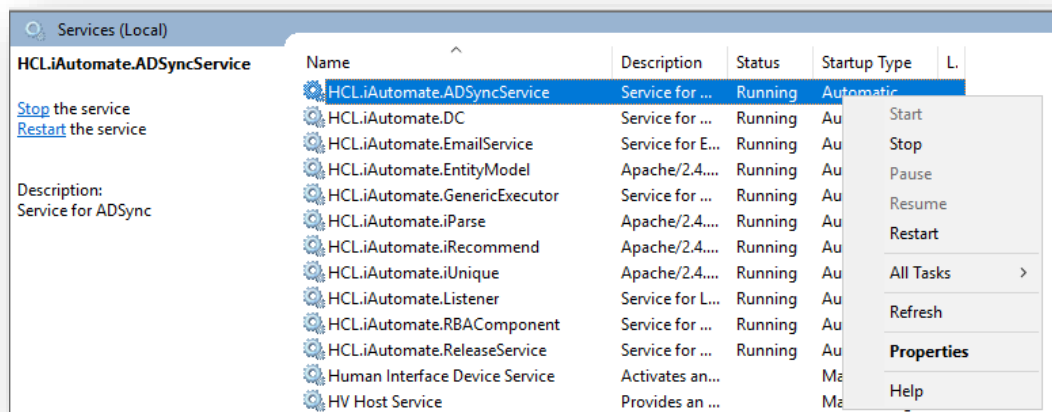


Figure 230 - Certificate Name Change – AD Sync Service (cont.)

- Copy the value mentioned in '**Path to executable**' as shown in the image below.

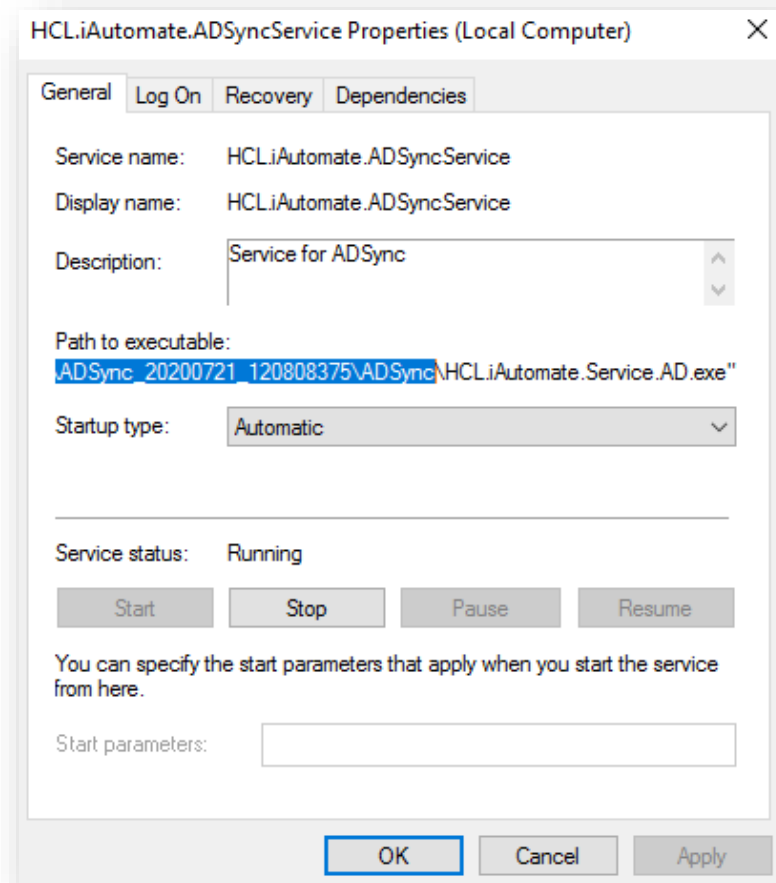


Figure 231 - Certificate Name Change – AD Sync Service (cont.)

- Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCLiAutomate.Service.AD.exe** config file and open it in a Notepad.

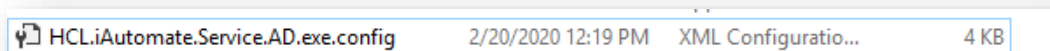


Figure 232 - Certificate Name Change – AD Sync Service (cont.)

- Within the **HCLiAutomate.Service.AD.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new **Certificate Name**.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 233 - Certificate Name Change – AD Sync Service (cont.)

- If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 234 - Certificate Name Change – AD Sync Service (cont.)

- Save the file for changes to be reflected.
- Select **HCLiAutomate.ADSyncService** service and click **Restart** to restart the service.

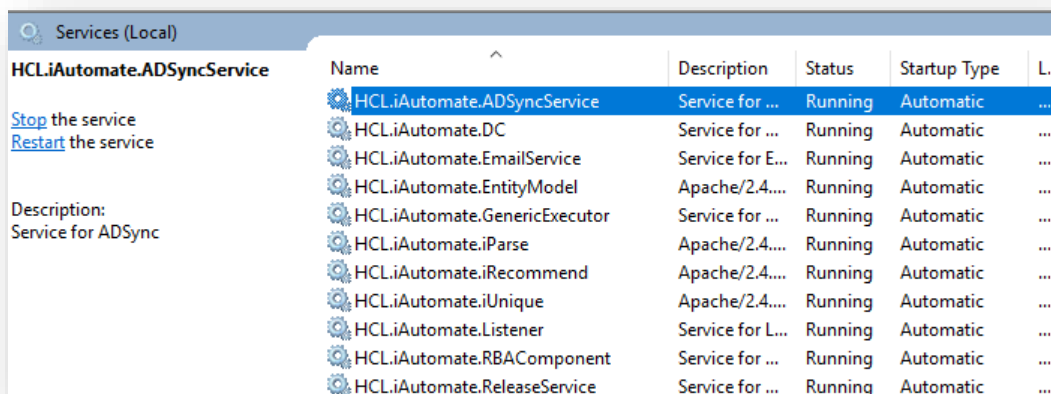


Figure 235 - Certificate Name Change – AD Sync Service (cont.)

3.6.2.1.2.7 Email Service

To change the configuration of Email Service from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

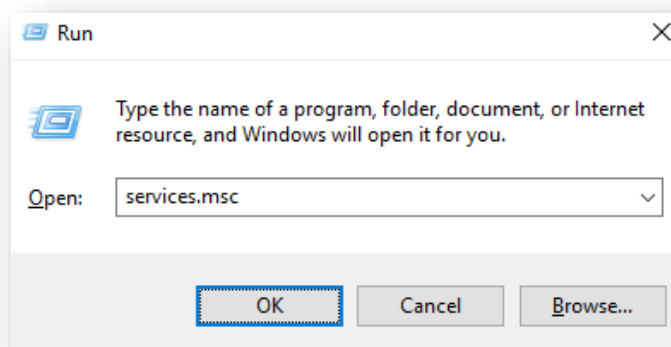


Figure 236 - Certificate Name Change – Email Service

2. Click OK to open Windows Services.

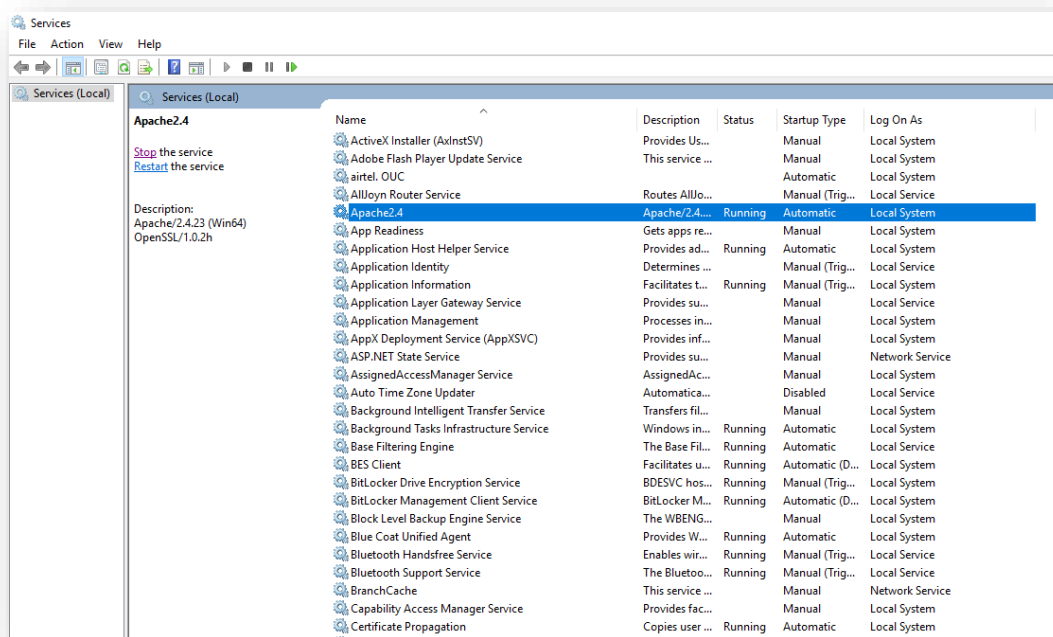


Figure 237 - Certificate Name Change – Email Service (cont.)

3. Search for **HCLiAutomate.EmailService** and right-click on it.
4. Click Properties.

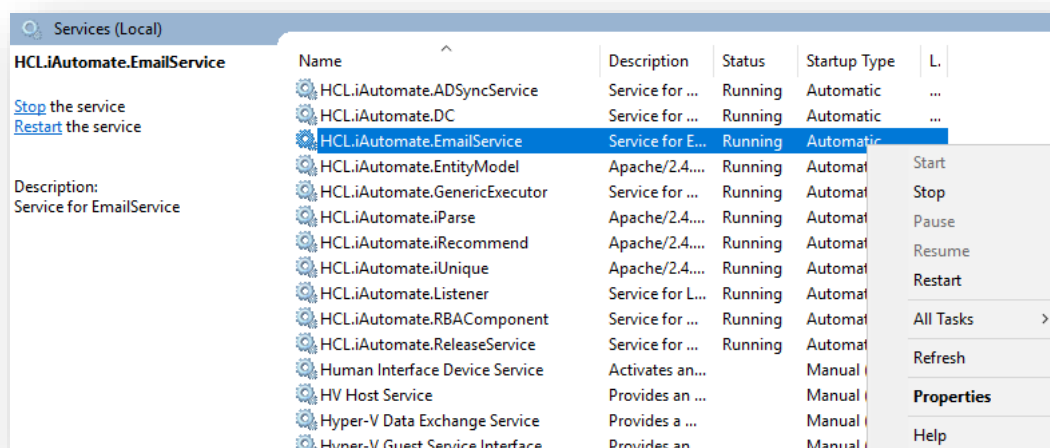


Figure 238 - Certificate Name Change – Email Service (cont.)

5. Copy the value mentioned in 'Path to executable' as shown in the image below.

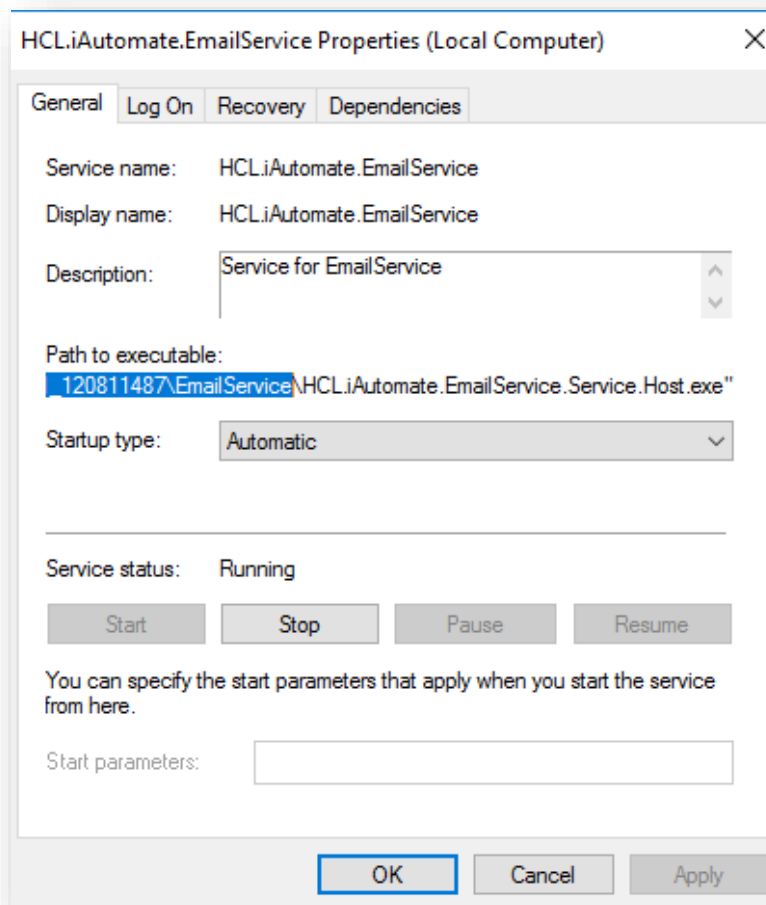


Figure 239 - Certificate Name Change – Email Service (cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Search for **HCL.iAutomate.EmailService.Service.Host.exe** config file and open it in a Notepad.



Figure 240 - Certificate Name Change – Email Service (cont.)

8. Within the **HCL.iAutomate.EmailService.Service.Host.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new Certificate Name.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 241 - Certificate Name Change – AD Sync Service (cont.)

9. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 242 - Certificate Name Change – Email Service (cont.)

10. Save the file for changes to be reflected.
11. Select **HCL.iAutomate.EmailService** service and click Restart to restart the service.

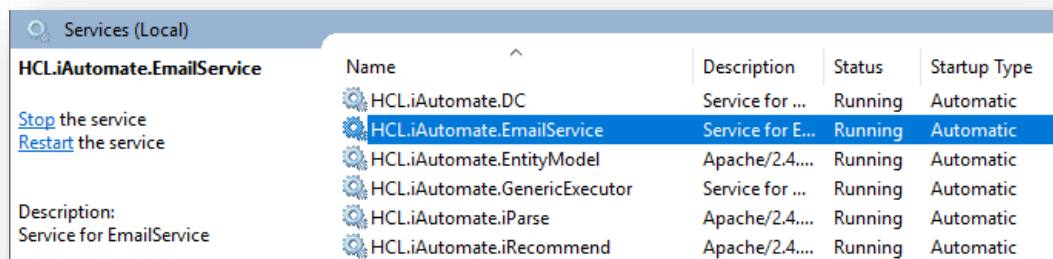


Figure 243 – Certificate Name Change – Email Service (cont.)

3.6.2.1.2.8 DAG Service

To change the configuration of DAG Service from HTTP to HTTPS, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

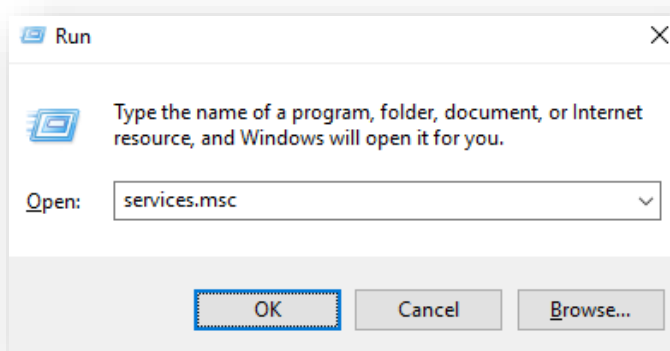


Figure 244 - Certificate Name Change – DAG Service

2. Click OK to open Windows Services.

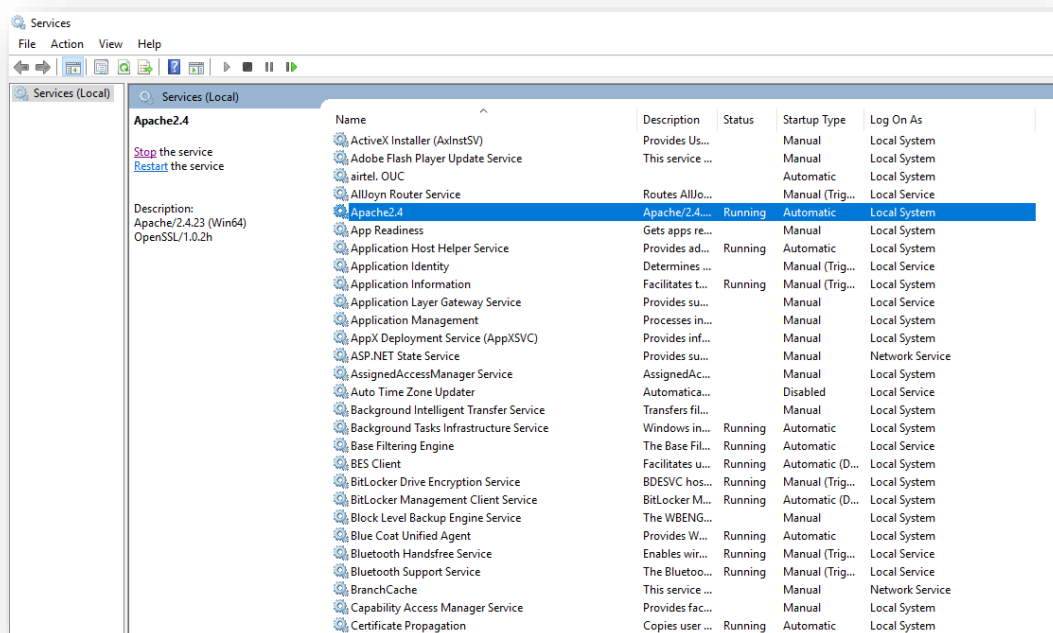


Figure 245 - Certificate Name Change – DAG Service (cont.)

3. Search for **HCLiAutomate.DAGService** and right-click on it.

- Click Properties.

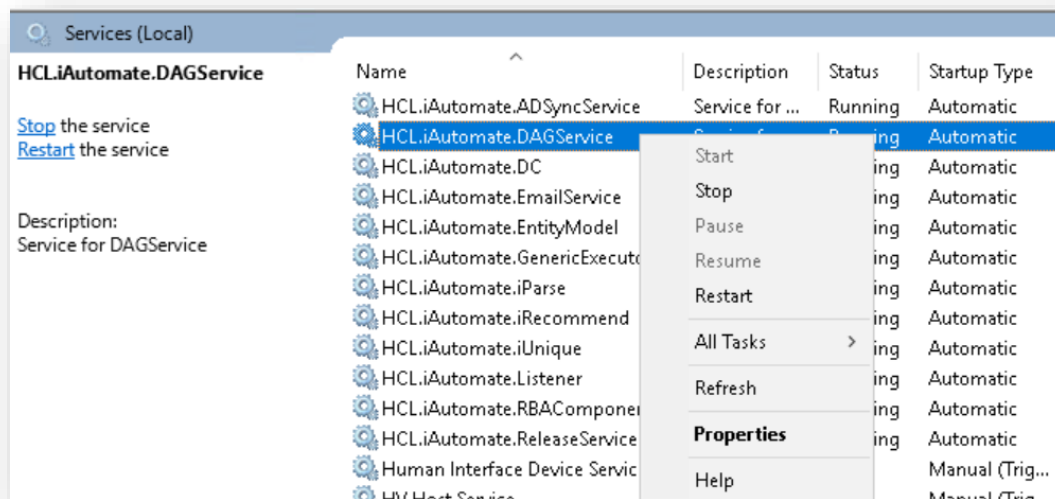


Figure 246 - Certificate Name Change – DAG Service (cont.)

- Copy the value mentioned in 'Path to executable' as shown in the image below.

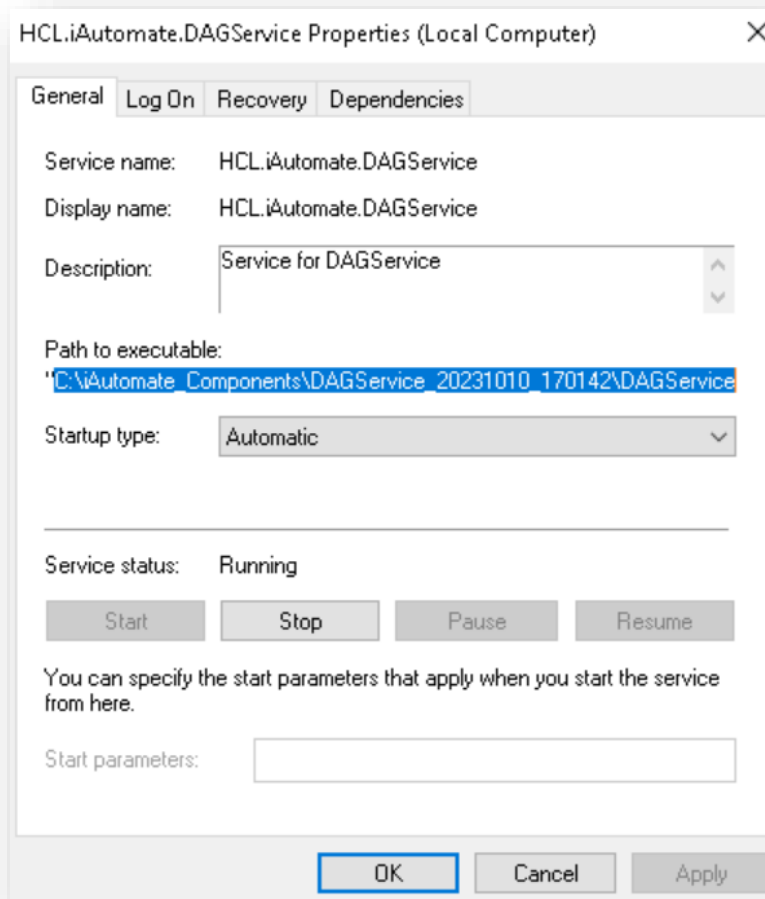


Figure 247 - Certificate Name Change – DAG Service (cont.)

- Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
- Search for **HCL.DagService.Component.Host.exe** config file and open it in a Notepad.

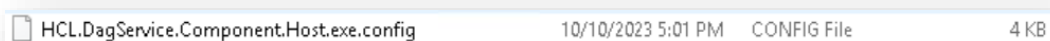


Figure 248 - Certificate Name Change – DAG Service (cont.)

8. Within the **HCL.DagService.Component.Host.exe** config file, find the key '**CertificateName_KRS**' and change its value with the new Certificate Name.

```
<add key="CertificateName_KRS" value="HclTech.iautomate.Web" />
```

Figure 249 - Certificate Name Change – DAG Service (cont.)

9. If the certificate is self-signed, find the key '**IsSelfSigned_KRS**' and change its value to '**Y**'. Else the value will be '**N**'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 250 - Certificate Name Change – DAG Service (cont.)

10. Save the file for changes to be reflected.
11. Select **HCL.iAutomate.DAGService** service and click Restart to restart the service.

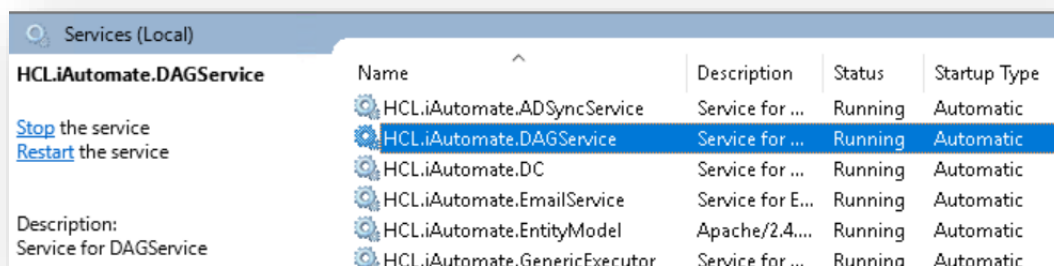


Figure 251 – Certificate Name Change – DAG Service (cont.)

3.6.2.1.2.9 Assignment Service

To change the configuration of Assignment Service from HTTP to HTTPS, please follow the following steps:

1. Press Win+R and type services.msc.

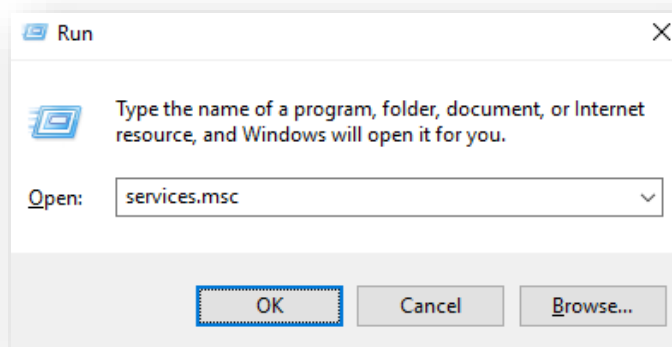


Figure 252 - Certificate Name Change – Assignment Service

2. Click OK to open Windows Services.

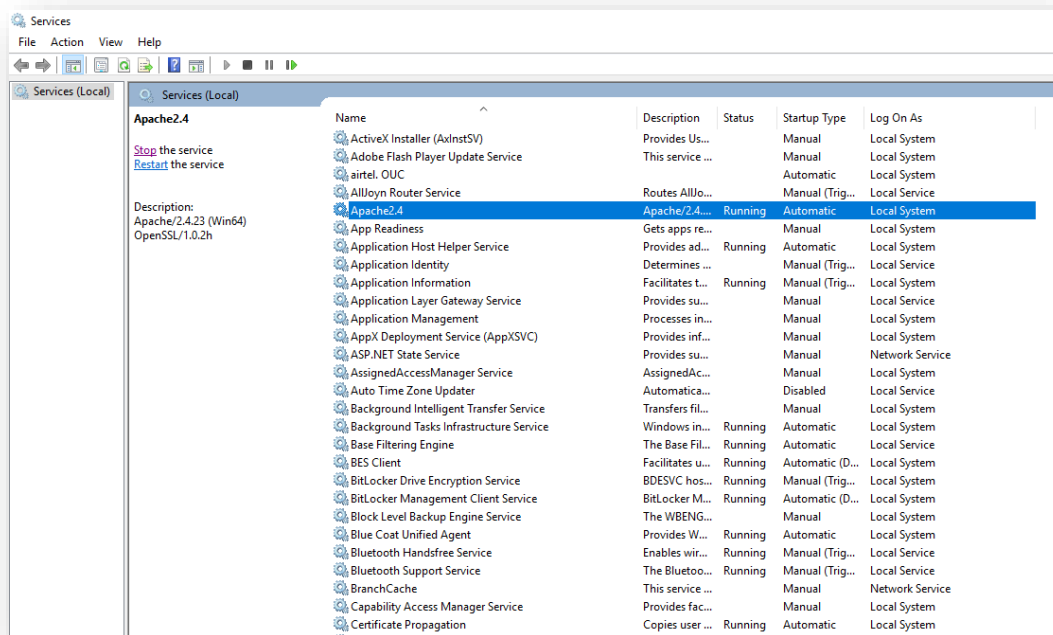


Figure 253 - Certificate Name Change – Assignment Service (cont.)

3. Search for HCL.iAutomate.AssignmentService and right-click on it.
4. Click Properties.

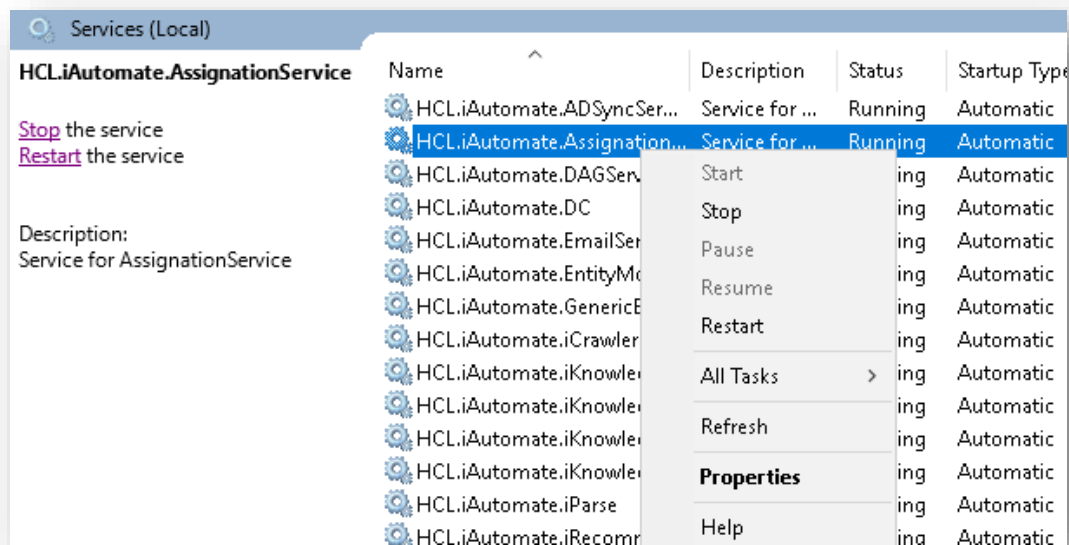


Figure 254 - Certificate Name Change – Assignment Service (cont.)

5. Copy the value mentioned in 'Path to executable' as shown in the image below.

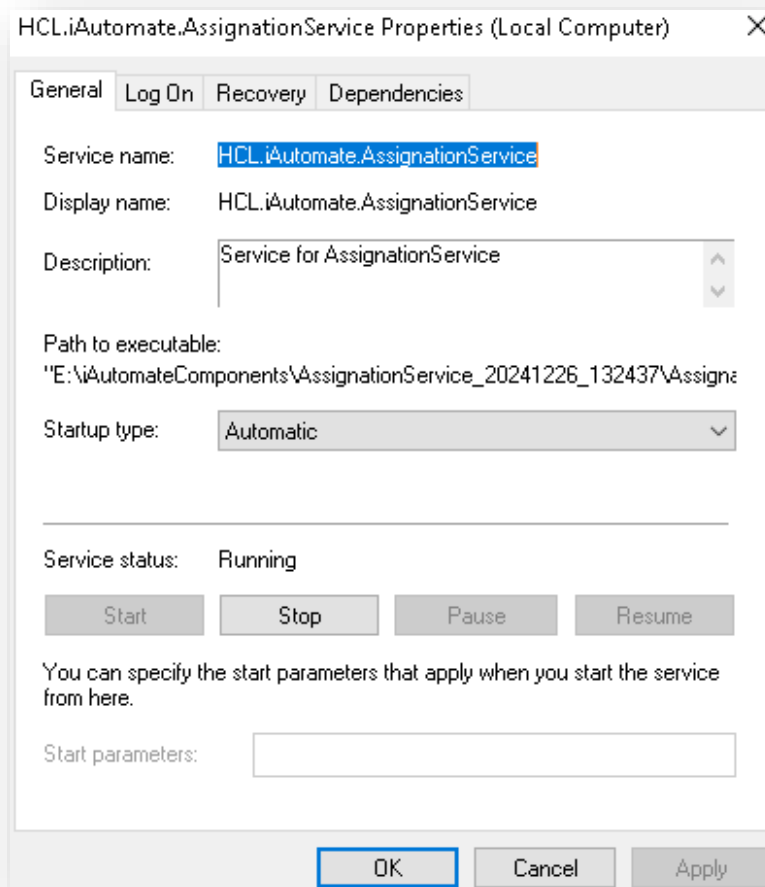


Figure 255 - Certificate Name Change – Assignment Service (cont.)

6. Open File Explorer and paste the copied path and press Enter to open the desired folder.
7. Search for Assignment.Service.Host.exe config file and open it in a Notepad.

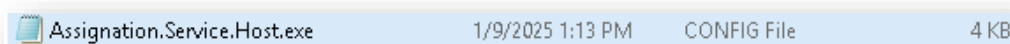


Figure 256 - Certificate Name Change – Assignment Service (cont.)

8. Within the Assignment.Service.Host.exe config file, find the key 'CertificateName_KRS' and change its value with the new Certificate Name.

```
<add key="CertificateName_KRS" value="HclTech.iAutomate.Web" />
```

Figure 257 - Certificate Name Change – Assignment Service (cont.)

9. If the certificate is self-signed, find the key 'IsSelfSigned_KRS' and change its value to 'Y'. Else the value will be 'N'.

```
<add key="IsSelfSigned_KRS" value="N" />
```

Figure 258 - Certificate Name Change – Assignment Service (cont.)

10. Save the file for changes to be reflected.
11. Select HCL.iAutomate.AssignmentService service and click Restart to restart the service.

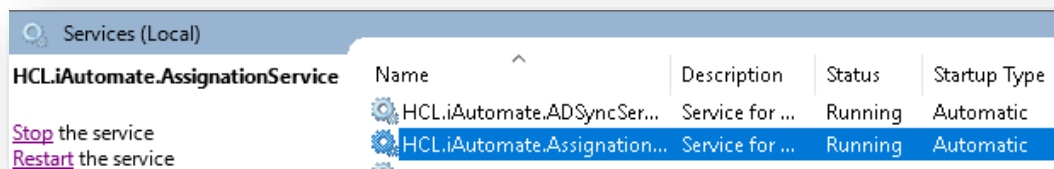


Figure 259 – Certificate Name Change – Assignment Service (cont.)

3.6.2.1.2.10 iRecommend

To make changes for iRecommend service, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

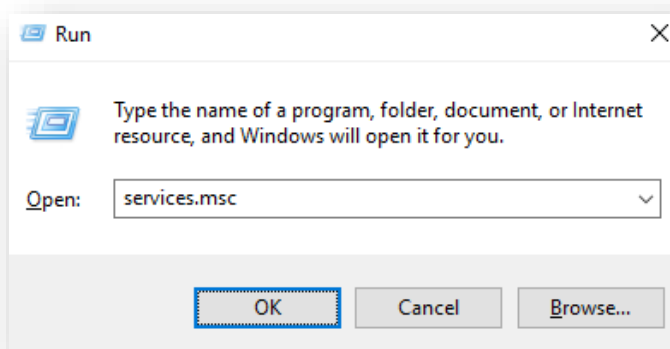


Figure 260 - Certificate Name Change – iRecommend

2. Click OK to open Windows Services.

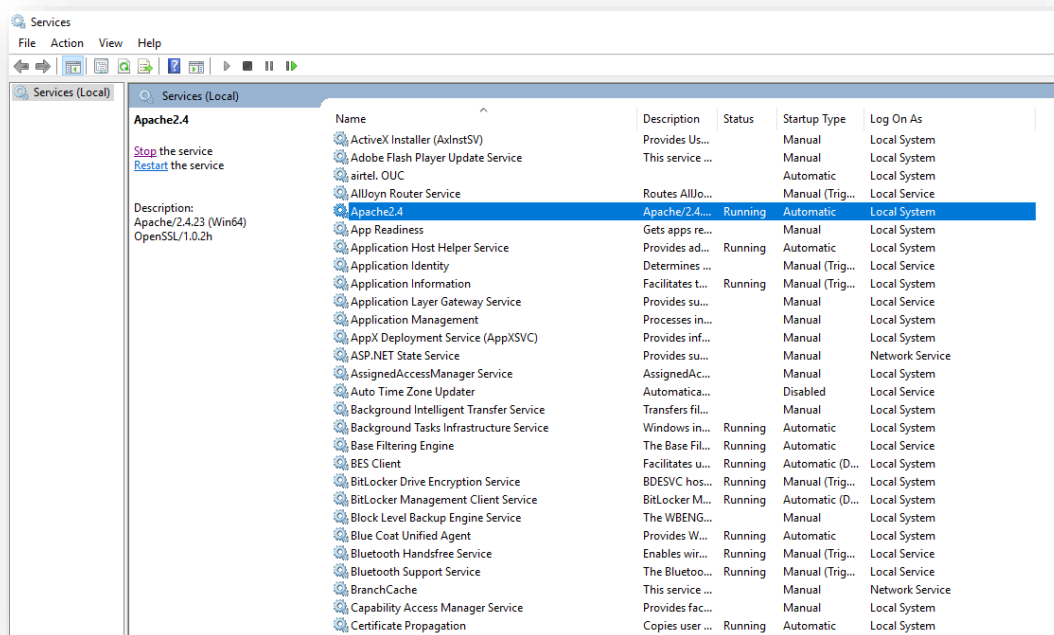


Figure 261 - Certificate Name Change – iRecommend (Cont.)

3. Search for **HCLiAutomate.Listener** service and right-click on it.
4. Click on **Properties**.

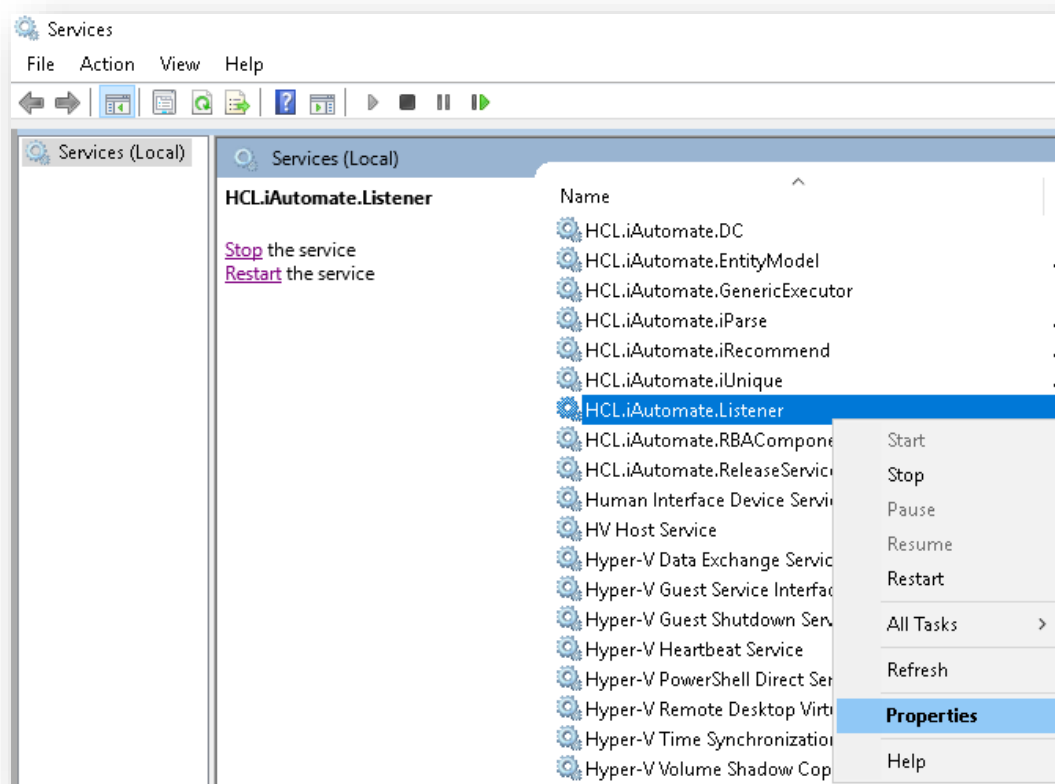


Figure 262 - Certificate Name Change – iRecommend (Cont.)

5. Copy the value mentioned in **Path to executable** as shown in the image below.

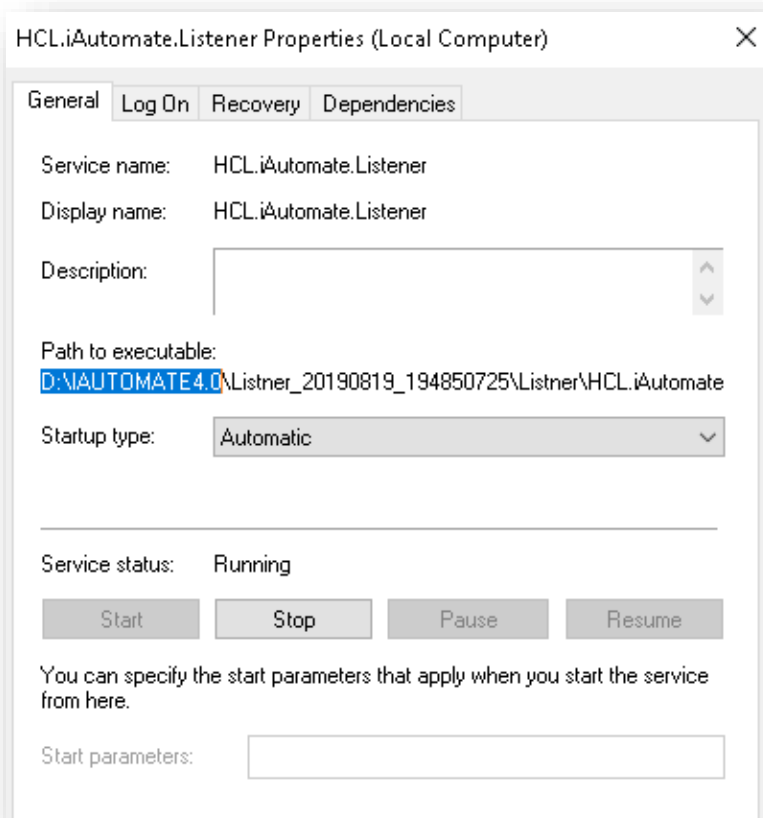


Figure 263 - Certificate Name Change – iRecommend (Cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Go to **iRecommend** folder. Locate **irecommend.config** file.
8. Open **irecommend.config** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 264 - Certificate Name Change – iRecommend (Cont.)

9. Change **Certificate_Name** and the value from **HclTech.iautomate.Web** to the new Certificate name.
10. Save the file to implement the changes.
11. Go to **iRecommend** → **config** folder.
12. Locate **entity.config** file.
13. Open **entity.config** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 265 - Certificate Name Change – iRecommend (Cont.)

14. Change **Certificate_Name** and the value from **HclTech.iautomate.Web** to the new Certificate name.
15. Save the file for changes to get reflected.

3.6.2.1.2.11 iParse

To make changes for iParse service, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

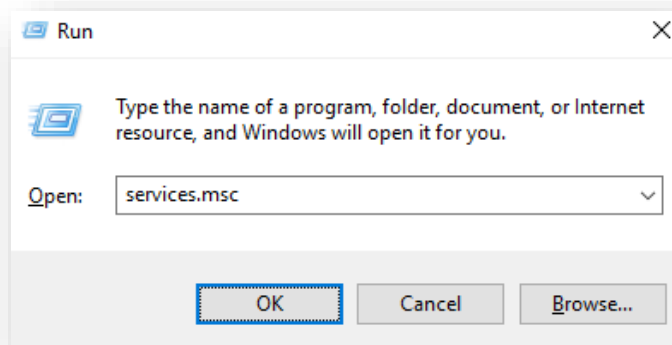


Figure 266 - Certificate Name Change – iParse

2. Click OK to open Windows Services.

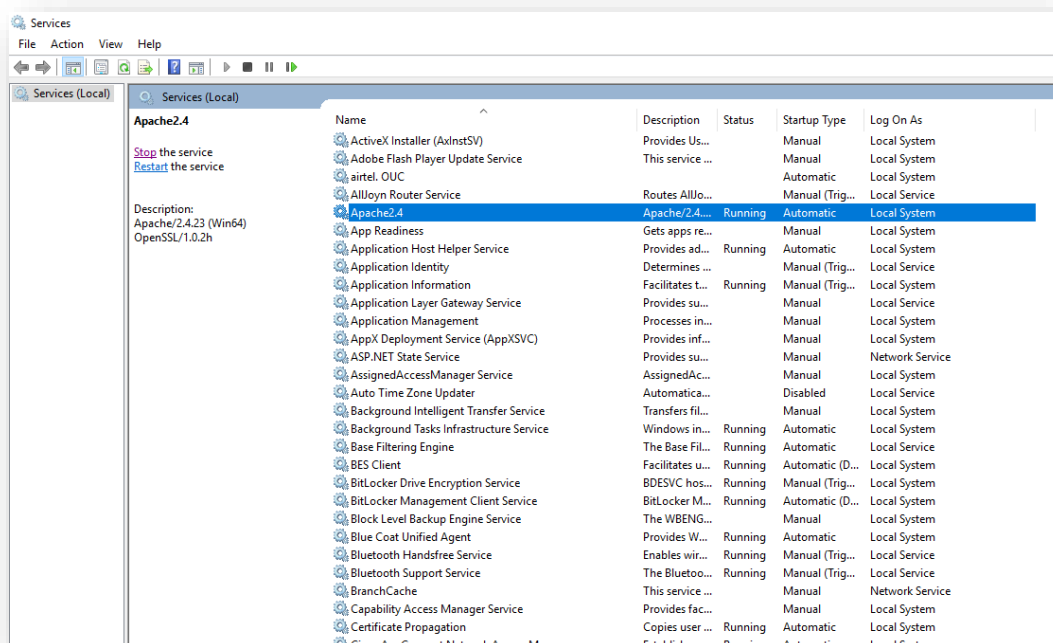


Figure 267 - Certificate Name Change – iParse (Cont.)

3. Search for **HCL.iAutomate.Listener** service and right-click on it.
4. Click on **Properties**.

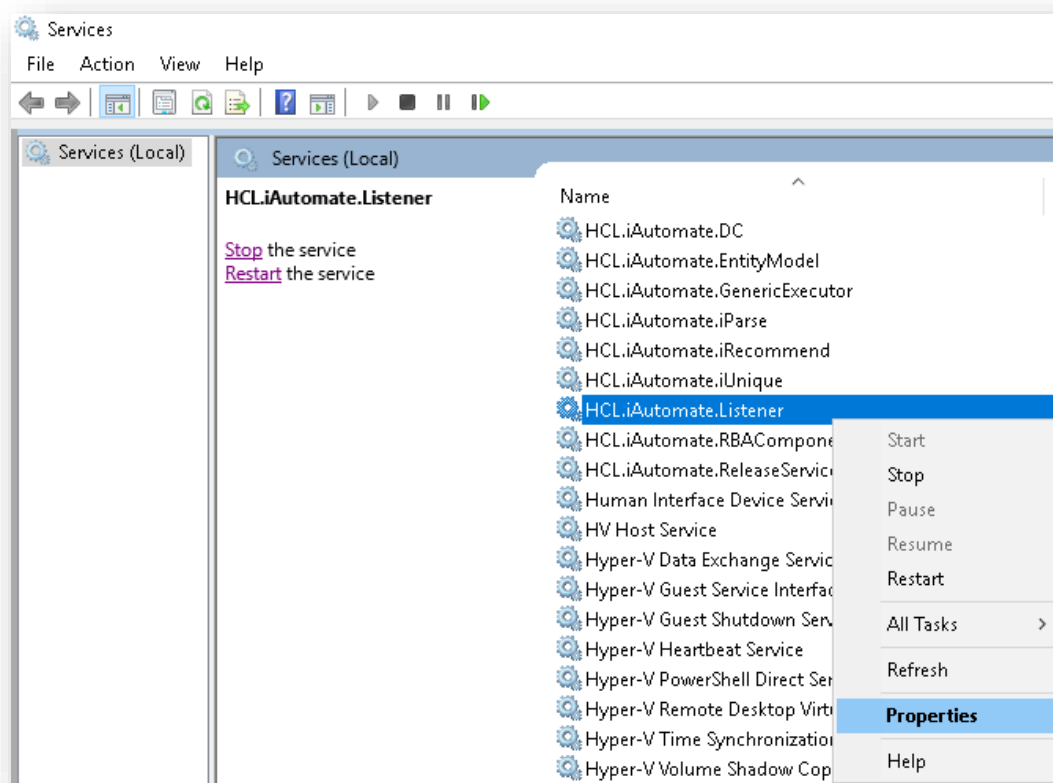


Figure 268 - Certificate Name Change – iParse (Cont.)

5. Copy the value mentioned in **Path to executable** as shown in the image below.

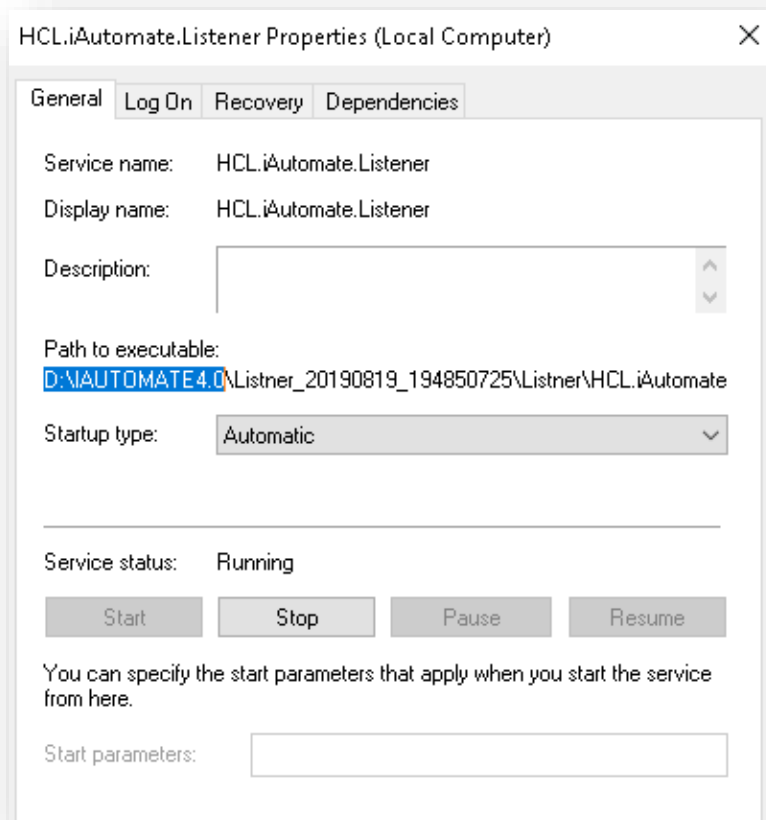


Figure 269 - Certificate Name Change – iParse (Cont.)

6. Open **File Explorer** and paste the **copied path** and press **Enter** to open the desired folder.
7. Go to **\iParse\IParse\iparse\config** folder.
8. Locate **parse_config.config** file.
9. Open **parse_config.config** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 270 - Certificate Name Change – iParse (Cont.)

10. Change **Certificate_Name** and the value from **HclTech.iautomate.Web** to the new Certificate name.
11. Save the file to implement the changes.

3.6.2.1.2.12 iScrape

To make changes for iScrape service, please follow the below steps:

1. Go to the folder where user has installed knowledge components.
2. Go to **\iScript\iScript\iScript\config** folder.
3. Locate **iScrape.cfg** file.
4. Open **iScrape.cfg** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 271 - Certificate Name Change – iScrape

5. Change **Certificate_Name** and **value** from **HclTech.iautomate.Web** to the new Certificate name.
6. Save the file to implement the changes.

3.6.2.1.2.13 iUnique

To make changes for iUnique service, please follow the below steps:

1. Press **Win+R** and type **services.msc**.

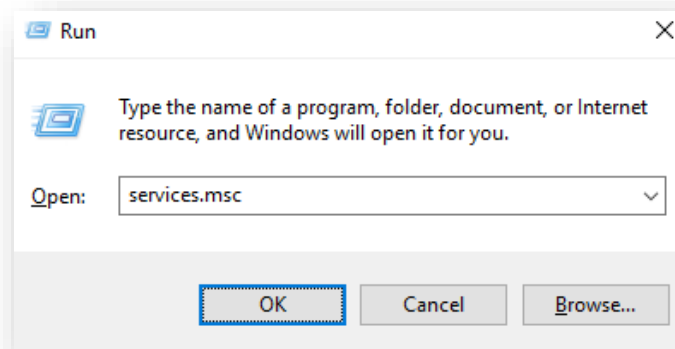


Figure 272 - Certificate Name Change – iUnique

2. Click OK to open Windows Services.

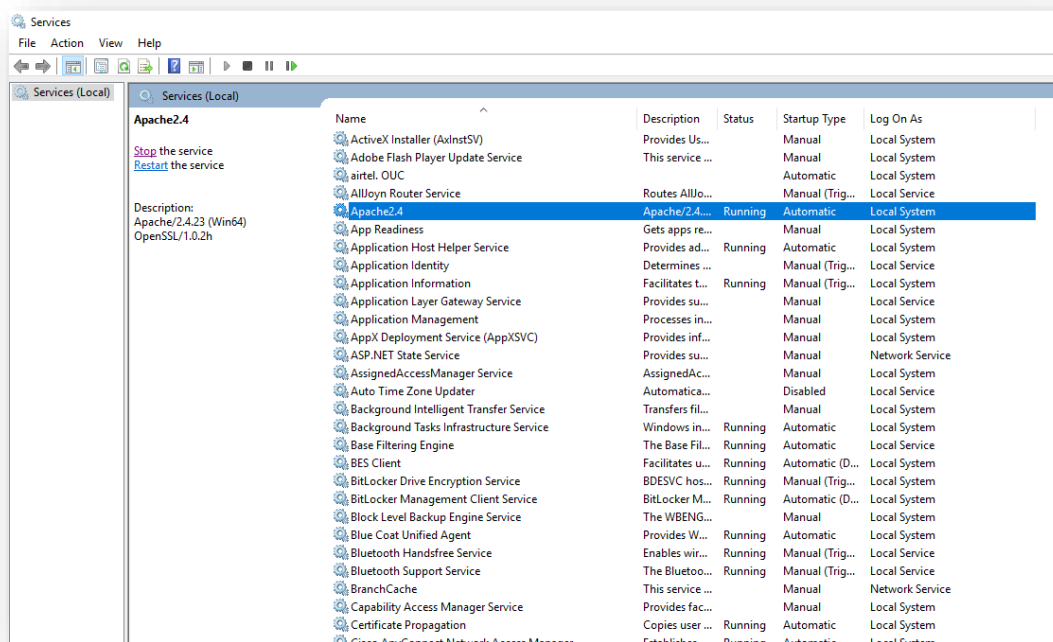


Figure 273 - Certificate Name Change – iUnique

3. Search for **HCLiAutomate.Listener** service and right-click on it.
4. Click on **Properties**.

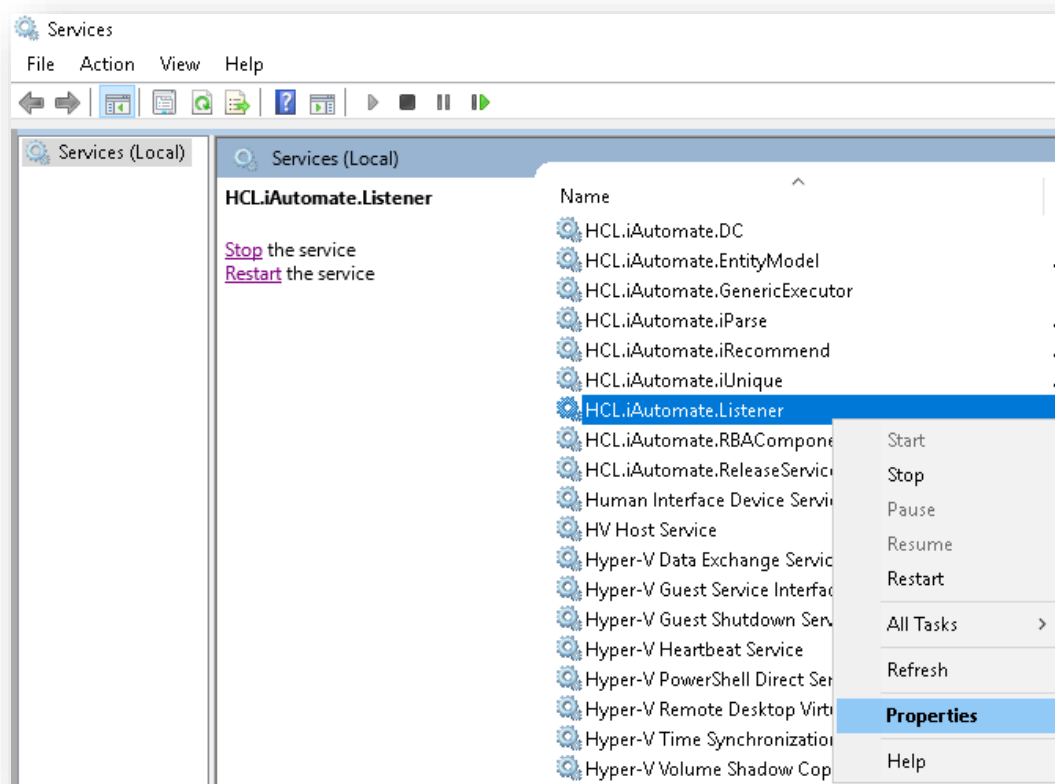


Figure 274 - Certificate Name Change – iUnique

5. Copy the value in '**Path to executable**' as shown in the image below.

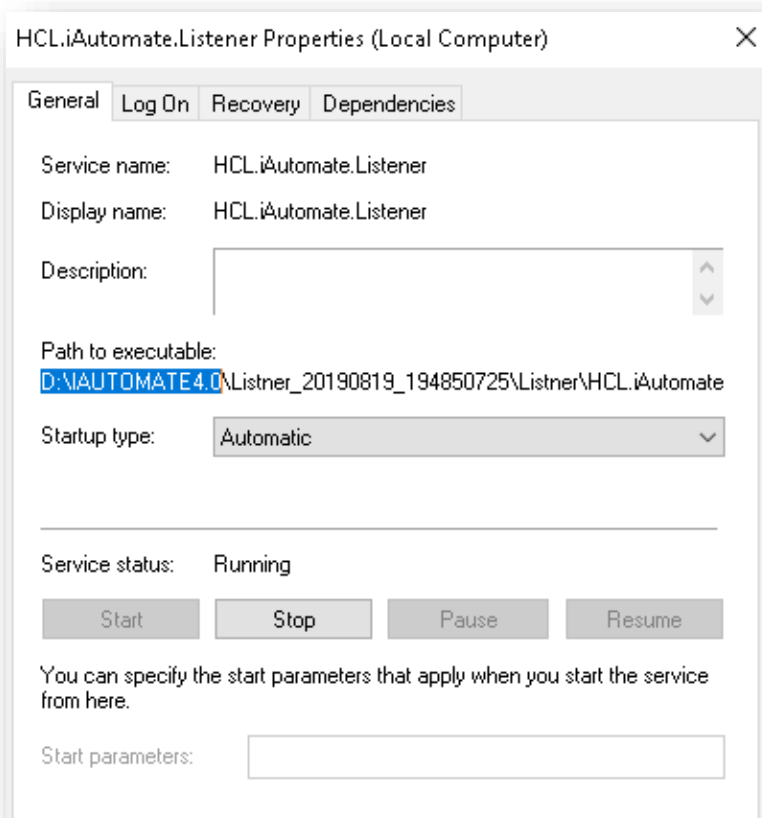


Figure 275 - Certificate Name Change – iUnique

6. Open **File Explorer**, then paste the copied path and press Enter to open the desired folder.
7. Go to \iUnique\iUnique\iUnique_final\config folder.
8. Locate iUnique.cfg file.
9. Open **iUnique.cfg** in Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 276 - Certificate Name Change – iUnique

10. Change Certificate_Name and the value from HclTech.iAutomate.Web to the new Certificate Name.
11. **Save** the file to implement the changes.

3.6.2.1.2.14 Knowledge

To make changes for Knowledge service, please follow the below steps:

1. Go to the folder where user has installed knowledge components.
2. Go to \KnowledgeRating\KnowledgeRating\iKnowledge_Rating folder.
3. Locate **rating.cfg** file.
4. Open **rating.cfg** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 277 - Certificate Name Change – Knowledge

5. Change **Certificate_Name** and the value from HclTech.iautoate.web to the new Certificate name.
6. **Save** the file for changes to get reflected.
7. Go to the folder where user has installed knowledge components.
8. Go to \AdvanceKnowledge\Crawler\crawler_v5\config folder. Locate icrawler.cfg file.
9. Open **indexer.cfg** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 278 - Certificate Name Change – Knowledge (Cont.)

10. Change Certificate_Name and their value from HclTech.iautomate.web to the new Certificate name.
11. **Save** the file for changes to get reflected.
12. Go to the folder where user has installed knowledge components.
13. Go to \AdvanceKnowledge\iKnowledge_Indexer folder. Locate indexer.cfg file.
14. Open **indexer.cfg** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 279 - Certificate Name Change – Knowledge (Cont.)

15. Change Certificate_Name and their value from HclTech.iautomate.Web to the new Certificate name.
16. **Save** the file for changes to get reflected.
17. Go to the folder where user has installed knowledge components.
18. Go to AdvanceKnowledge\iKnowledge_Screen folder.
19. Locate iKnowledge_Screen.cfg file.
20. Open **iKnowledge_Screen.cfg** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 280 - Certificate Name Change – Knowledge (Cont.)

21. Change **Certificate_Name** and the value from HclTech.iautomate.Web to the new Certificate name.
22. **Save** the file for changes to get reflected.
23. Go to the folder where user has installed knowledge components.
24. Go to \AdvanceKnowledge\iKnowledge_Search folder.
25. Locate iKnowledge_Search file.
26. Open **iKnowledge_Search** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 281 - Certificate Name Change – Knowledge (Cont.)

27. Change **Certificate_Name** and the value from HclTech.iautomate.Web to the new Certificate name.
28. Save the file for changes to get reflected.
29. Go to the folder where user has installed knowledge components.
30. Go to iKnowledge\iKnowledge\knowledge_v4 folder.
31. Locate iKnowledge.cfg file.
32. Open **iKnowledge.cfg** in a Notepad and search for below line.

```
Certificate_Name = HclTech.iautomate.Web
```

Figure 282 - Certificate Name Change – Knowledge (Cont.)

33. Change **Certificate_Name** and the value from HclTech.iautomate.Web to the new Certificate name.
34. **Save** the file to implement the changes.

3.6.2.2 CHANGE NAME OF CERTIFICATE USED TO CONNECT SERVICES

This section describes configuration changes required for the components in case ssl certificate is other than **HclTech.iautomate.App**.

Follow all steps mentioned in section “change name of certificate used to connect KRS” with below changes:

Search for key “CertificateName_Service” instead ‘CertificateName_KRS’.

Search for key ‘IsSelfSigned_Service’ instead ‘IsSelfSigned_KRS’.

For below components:

Base User Interface, Listener, Data Collector, Generic Service, RBA Component, Release Service, Email Service, Ad Sync

For BASEUI and Listener follow below steps:

Search for “<dns value=“HclTech.iautomate.App” />” in web.config and change with New Certificate.

3.6.3 Configuration Changes – Certificate Name Change for PEM/CRT/KEY Certificates

If the Certificate that is used for connecting the REST API hosted by Apache gets changed (PEM/CRT/KEY), user needs to change some parameters (params) in the **httpd.conf** file in apache directory: **/Apache24/conf/httpd.conf**.

The parameters define the path of the certificates that are used along with certificate names.

For instance, suppose the certificate changes from **server.crt** to **server1.crt** then, by default, they are set to default location as "**C:/Program Files/certificate/server.crt**", which needs to be changed to new file name of certificates as "**C:/Program Files/certificate/server1.crt**".

```
SSLCertificateFile "C:/Program Files/certificate/server.crt"
SSLCertificateKeyFile "C:/Program Files/certificate/server.key"
SSLCACertificateFile "C:/Program Files/certificate/ca.pem"
SSLVerifyClient require
SSLVerifyDepth 10
```

Figure 283 - Certificate Name Change (PEM / CRT / Key Certificate)

3.6.4 Load Balancer Configuration

This section describes the steps for making the required configurational changes if, iAutomate is installed in *High Availability* mode.

To make the configuration changes, please follow the below steps:

1. Press **Win+R** and type **services.msc**.
2. Click **OK** to open IIS.

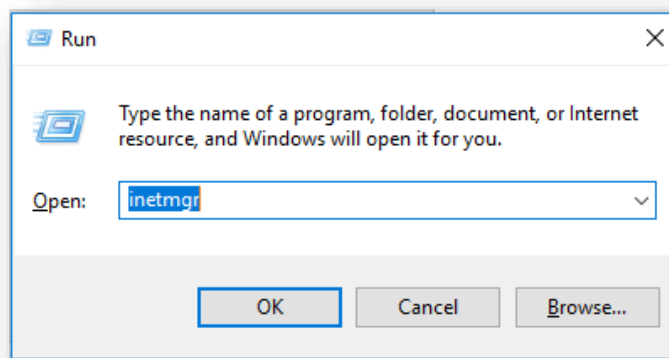


Figure 284 - Load Balancer Configuration

3. Expand Sites under Connections and click HCLiAutomateBaseUI.

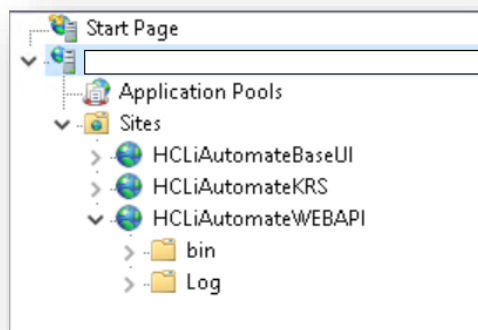


Figure 285 - Load Balancer Configuration (cont.)

4. Click on **Bindings** in the **Edit Site** section.

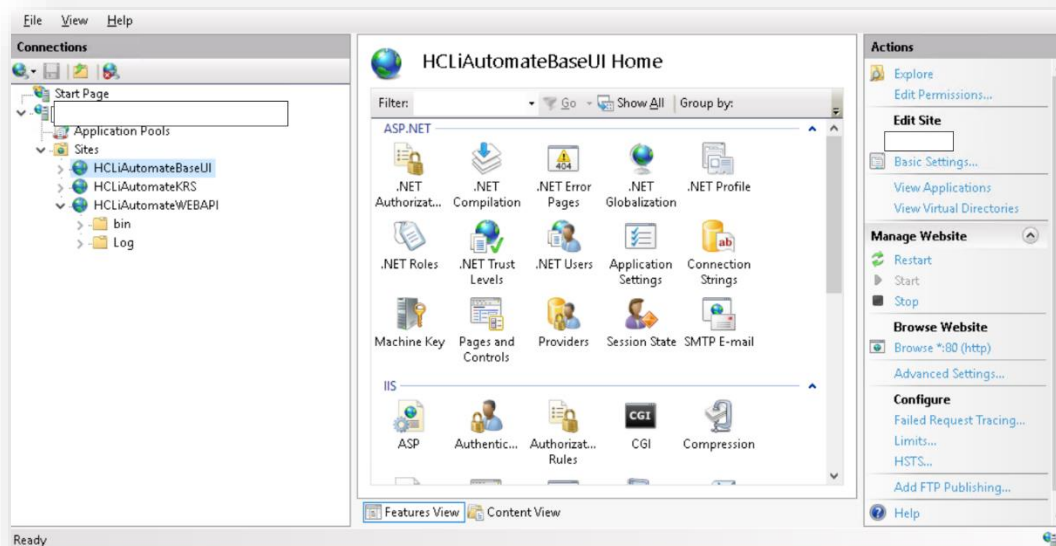


Figure 286 - Load Balancer Configuration (cont.)

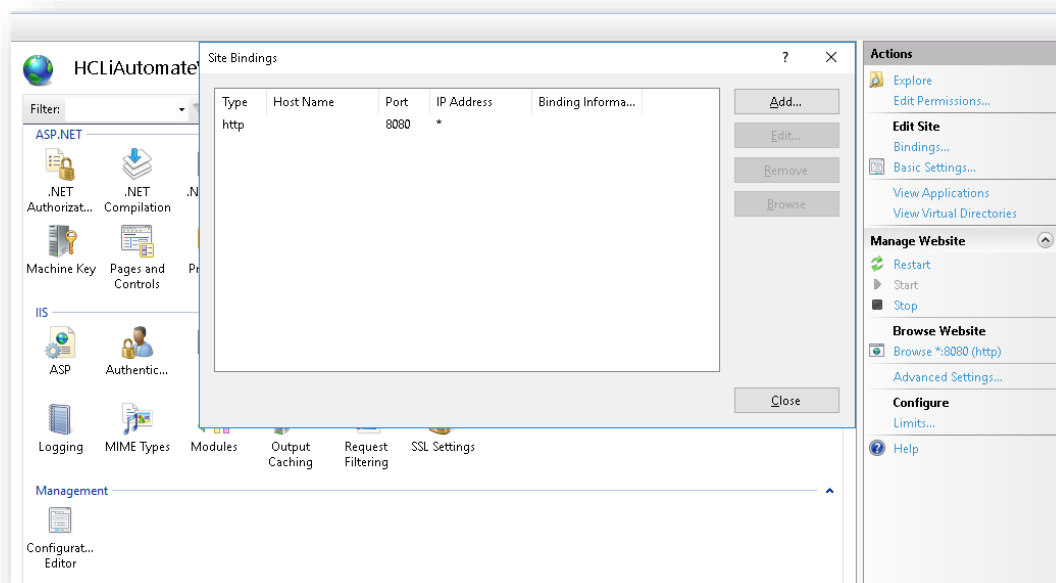


Figure 287 - Load Balancer Configuration (cont.)

5. Ensure that the value of **Port** mentioned is same as configured in Load Balancer. If that is not the case, click **Edit** to change the **Port** value.
6. Right-click on **HCLiAutomateBaseUI** and click **Explore**.
7. Find **Web.config** file and open it in a Notepad.



Figure 288 - Load Balancer Configuration (cont.)

8. Within the **Web.config** file, search for the key '**URL**' and replace the '**<ip>:<portnumber>**' with the *Load balancer IP* and *Web API Port*.

```
<add key="URL" value="http://. /KeyManagement.svc" />
```

Figure 289 - Load Balancer Configuration (cont.)

9. Save the file to implement the changes.
10. Select the service and click **Restart** to restart the services.
11. Expand Sites in Connections section and click HCLiAutomateWEBAPI.

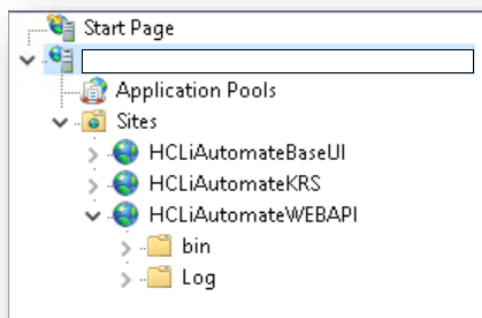


Figure 290 - Load Balancer Configuration (cont.)

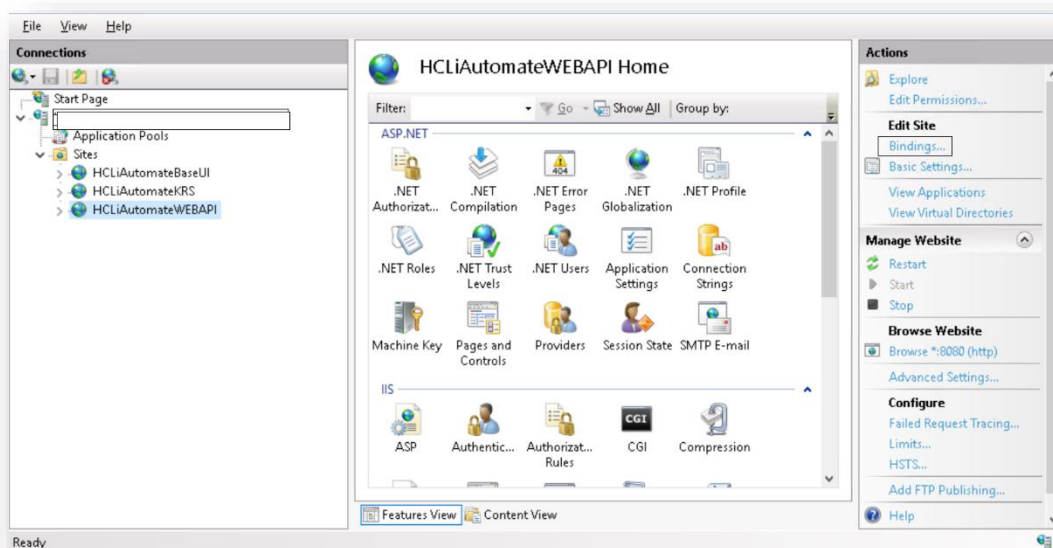


Figure 291 - Load Balancer Configuration (cont.)

12. Right-click on **HCLiAutomateWEBAPI** and click **Explore**.
13. Find **Web.config** file and open it in a Notepad.



Figure 292 - Load Balancer Configuration (cont.)

14. Within the **Web.config** file, search for the key 'URL' and replace the '<ip>:<portnumber>' with the *Load balancer IP* and *Web API Port*.

```
<add key="URL" value="http://. /KeyManagement.svc" />
```

Figure 293 - Load Balancer Configuration (cont.)

15. Save the file to implement the changes.
16. Select the service and click **Restart** to restart the services.
17. Press **Win+R** and type **services.msc**.

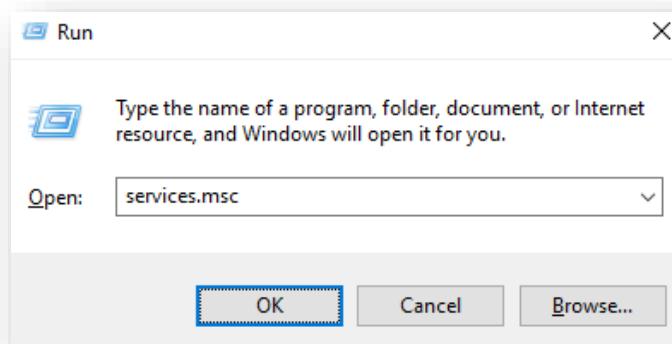


Figure 294 - Load Balancer Configuration (cont.)

18. Click OK to open Windows Services.

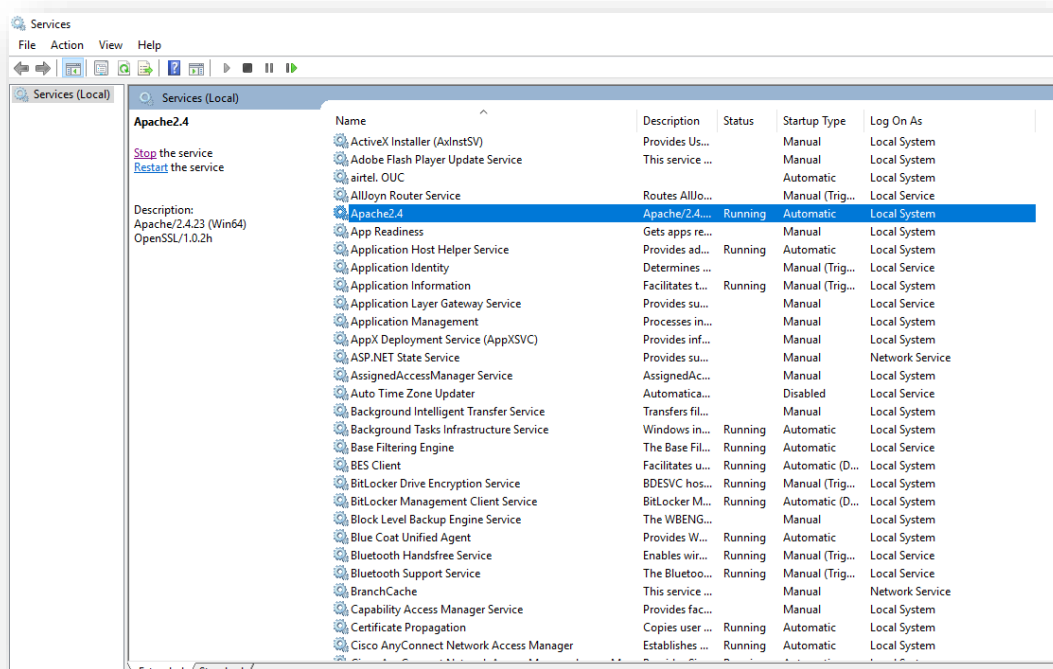


Figure 295 - Load Balancer Configuration (cont.)

19. Search for **HCLiAutomate.Listener** service and right-click on it.
20. Click Properties.

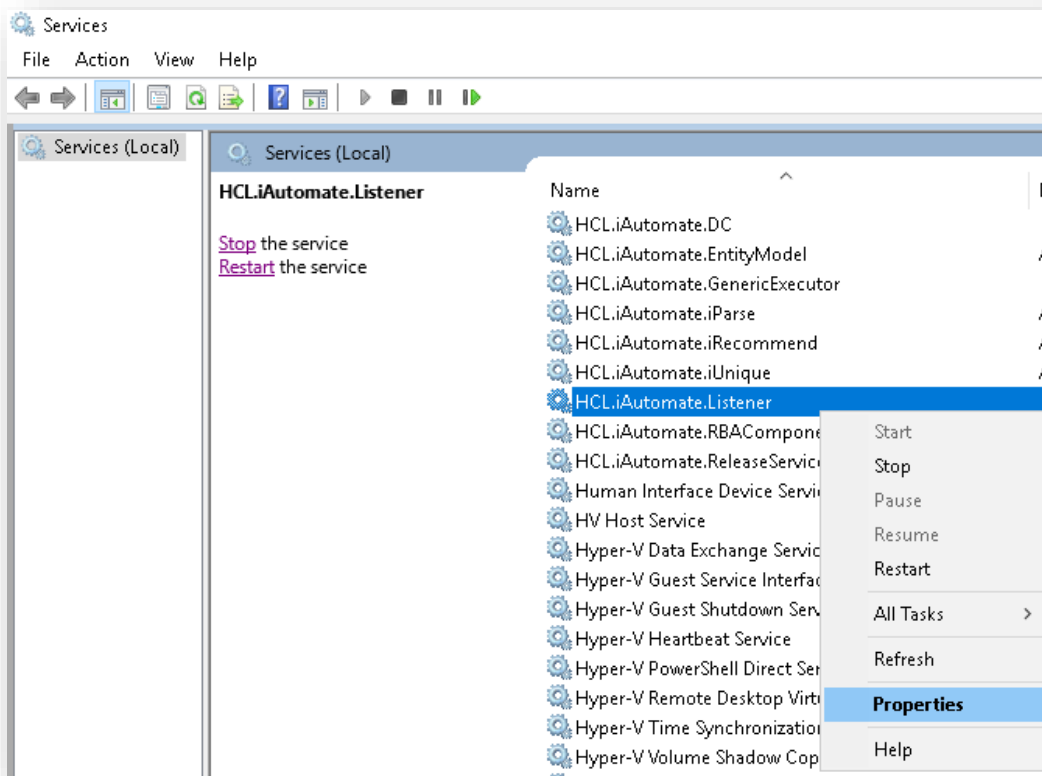


Figure 296 - Load Balancer Configuration (cont.)

21. Copy the value mentioned in **Path to executable** as shown in the image below.

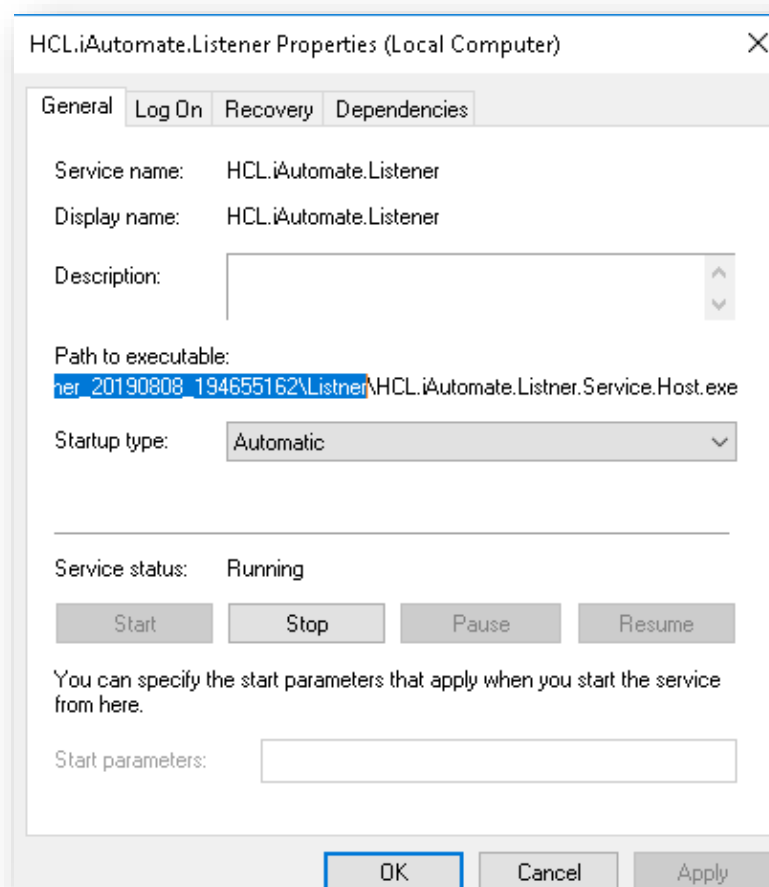


Figure 297 - Load Balancer Configuration (cont.)

22. Open **File Explorer**, then paste the copied path and press Enter to open the desired folder.
23. Search for HCL.iAutomate.Listener.Service.Host config file and open it in a Notepad.



Figure 298 - Load Balancer Configuration (cont.)

24. Within the **HCL.iAutomate.Listener.Service.Host** config file, search for the key '**URL**' and replace the '**<ip>:<portnumber>**' with the *Load balancer IP* and *Web API Port*.

```
<add key="URL" value="http://. " />
```

Figure 299 - Load Balancer Configuration (cont.)

25. Save the file to implement the changes.
26. Select the service and click **Restart** to restart the services.

Repeat the steps mentioned above on all the load balanced servers.

27. Login to iAutomate using the **Super Admin** credentials.
28. Roll-over Environment and click **iAutomate Configuration**.
29. Select **Component Name** as '**Web API**'. Change the **Load Balancer URL** to the Load Balancer IP.

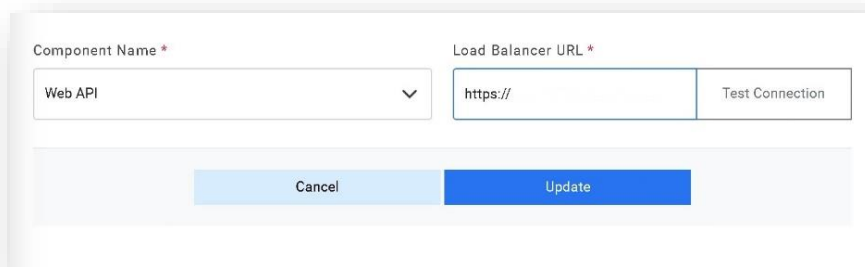


Figure 300 shows a configuration window for a component. It has two main sections at the top: 'Component Name *' and 'Load Balancer URL *'. The 'Component Name' dropdown is set to 'Web API'. The 'Load Balancer URL' text box contains 'https://'. To the right of the URL is a 'Test Connection' button. At the bottom of the window are two buttons: 'Cancel' and 'Update'.

Figure 300 - Load Balancer Configuration (cont.)

30. Click **Update** to save the changes.
31. Above step must be repeated for all the components. Additionally, for the **Component Name 'iRecommend'**, provide the path of the shared drive location in the **'iRecommend Model Location'** field.

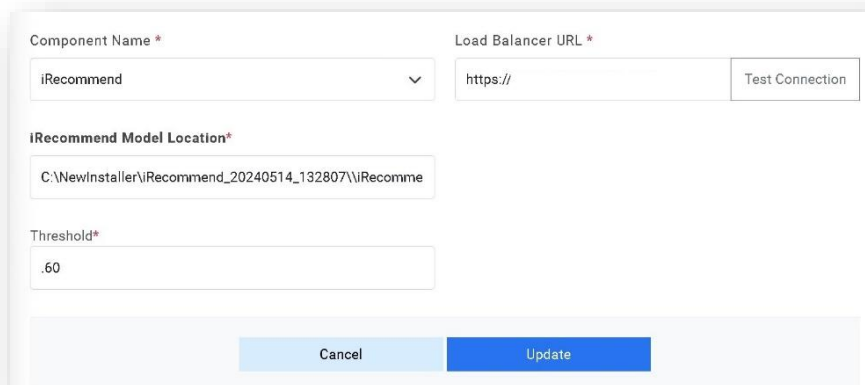


Figure 301 shows the configuration window for the 'iRecommend' component. The 'Component Name' dropdown is set to 'iRecommend'. The 'Load Balancer URL' text box contains 'https://'. Below these fields is a new section labeled 'iRecommend Model Location*'. It contains a text box with the path 'C:\NewInstaller\iRecommend_20240514_132807\iRecommen'. Below this is a 'Threshold*' text box containing '.60'. At the bottom are 'Cancel' and 'Update' buttons.

Figure 301 - Load Balancer Configuration (cont.)

32. Click **Update** to save the changes.
33. Additionally, for the **Component Name Entity Model**, provide the path of the shared drive location in the **EntityModel Model Location** field.

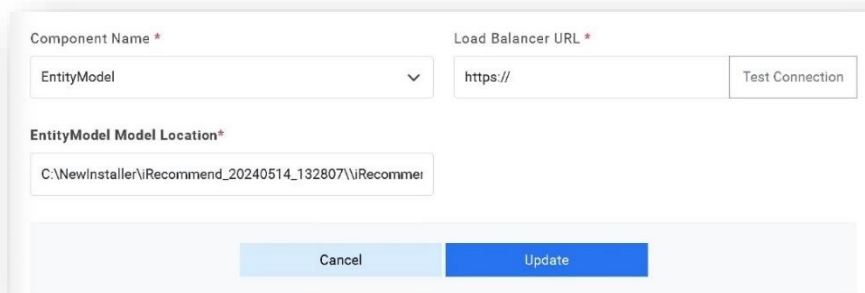


Figure 302 shows the configuration window for the 'EntityModel' component. The 'Component Name' dropdown is set to 'EntityModel'. The 'Load Balancer URL' text box contains 'https://'. Below these fields is a section labeled 'EntityModel Model Location*'. It contains a text box with the path 'C:\NewInstaller\iRecommend_20240514_132807\iRecommen'. At the bottom are 'Cancel' and 'Update' buttons.

Figure 302 - Load Balancer Configuration (cont.)

34. Click **Update** to save the changes.
35. Additionally, for the **Component Name** given as **Crawler**, provide the path of the shared drive location in the **Data Directory Location** field.

Figure 303 shows a configuration dialog box. It has two main sections. The top section contains a 'Component Name' dropdown menu with 'Crawler' selected, and a 'Load Balancer URL' text field with the placeholder 'https://<ip>:<port>'. To the right of the URL field is a 'Test Connection' button. The bottom section is titled 'Data Directory Location*' and contains a text field with the path 'C:\Apache24\Knowledge_Default'. At the very bottom are 'Cancel' and 'Save' buttons.

Figure 303 - Load Balancer Configuration (cont.)

36. Click **Update** to save the changes.

3.6.5 Configuration Changes – Access iAutomate without Certificate (Type – PFX)

This section describes the steps for making the required configurational changes to enable access to iAutomate when PFX certificate is not available.

To make the configuration changes, please follow the below steps:

3.6.5.1 Without Certificate used to connect KRS

3.6.5.1.1 WCF Services:

1. When no certificate is present in **Personal** and **Trusted** folder, following error will occur while loading the KRS wsdl (<IP address:port>/KRS/KeyManagement.svc)

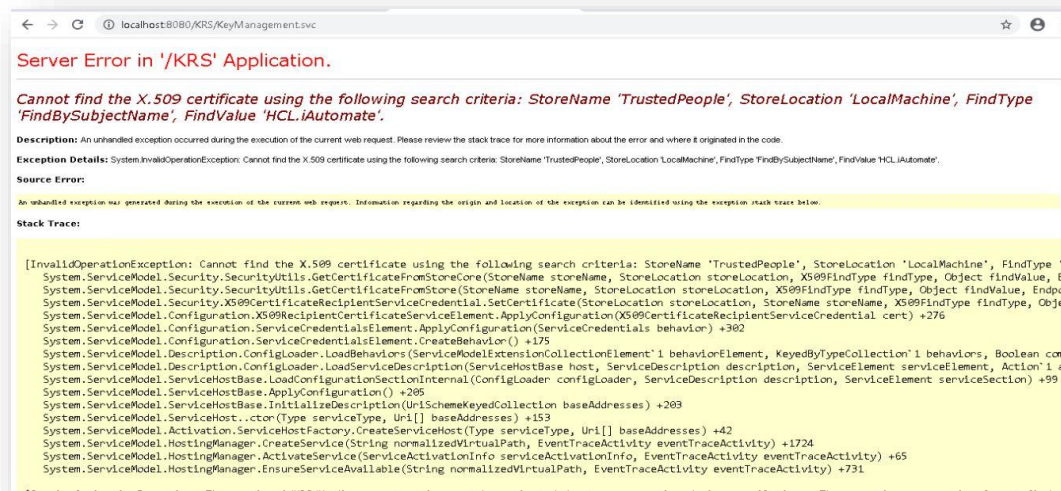


Figure 304 - Configuration Changes – Access iAutomate without Certificate (Type – PFX)

2. Go to <iAutomate Installer path>.

Name	Date modified	Type	Size
ADSync_20230410_213331	4/10/2023 9:33 PM	File folder	
AdvanceKnowledge_20230410_213323	4/10/2023 9:36 PM	File folder	
BaseUI_20230410_213308	6/1/2023 10:26 AM	File folder	
DataCollection_20230410_213316	4/10/2023 9:33 PM	File folder	
EmailService_20230410_213333	4/10/2023 9:33 PM	File folder	
GenericService_20230410_213319	4/10/2023 9:33 PM	File folder	
iKnowledge_20230410_213310	4/10/2023 9:33 PM	File folder	
iParse_20230410_213304	4/10/2023 9:33 PM	File folder	
iRecommend_20230410_213304	4/11/2023 3:53 PM	File folder	
iScript_20230410_213304	4/10/2023 9:33 PM	File folder	
iUnique_20230410_213304	4/10/2023 9:33 PM	File folder	
KnowledgeRating_20230410_213304	4/10/2023 9:33 PM	File folder	
KRS_20230410_213304	4/10/2023 9:33 PM	File folder	
Listner_20230410_213329	4/10/2023 9:33 PM	File folder	
Log_Baseui	4/28/2023 3:53 PM	File folder	
RBA_20230410_213325	4/10/2023 9:33 PM	File folder	
ReleaseService_20230410_213328	4/10/2023 9:33 PM	File folder	
WebAPI_20230410_213306	4/13/2023 2:59 PM	File folder	

Figure 305 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

3. Go to Path <iAutomate Installer path>\KRS.
4. Open **Web.config** file.
5. Add mode="None" in <security> tag
6. Change **clientCredentialType="None"** in <serviceCredentials> tag.
7. Comment the <serviceCertificate> tag in <serviceCredentials>.

```

31      </endpoint>
32    </service>
33  </services>
34  <bindings>
35    <wsHttpBinding>
36      <binding name="wsHttpEndpointBinding">
37        <security mode="None">
38          <message clientCredentialType="None" />
39        </security>
40      </binding>
41    </wsHttpBinding>
42  </bindings>
43  <behaviors>
44    <serviceBehaviors>
45      <behavior>
46        <!-- To avoid disclosing metadata information, set the values below to false before deployment -->
47        <serviceMetadata httpGetEnabled="true" httpsGetEnabled="true" />
48        <!-- To receive exception details in faults for debugging purposes, set the value below to true. Set to false before deployment -->
49        <serviceDebug includeExceptionDetailInFaults="false" />
50      </behavior>
51    </serviceBehaviors>
52  </behaviors>
53  <add binding="basicHttpsBinding" scheme="https" />
54  </protocolMapping>
55  <serviceHostingEnvironment aspNetCompatibilityEnabled="true" multipleSiteBindingsEnabled="true" />
56  </system.serviceModel>

```

Figure 306 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

8. Go to Path <iAutomate Installer path>\ WebAPI
9. Open **Web.config** file.
10. Set key "enableCertificate_KRS" value to "N".

```
<add key="enableCertificate_KRS" value="N" />
```

Figure 307 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

11. Go to Path <iAutomate Installer path>\Listener...\Listener
12. Open HCL.iAutomate.Listener.Service.Host.exe config file.
13. Set “enableCertificate_KRS” key to “N”

```
<add key="enableCertificate_KRS" value="N" />
```

Figure 308 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

14. Go to Path <iAutomate Installer path>\BaseUI...\BaseUI
15. Open **Web.config** file.
16. Set “enableCertificate_KRS” key to “N”.

```
<add key="enableCertificate_KRS" value="N" />
```

Figure 309 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

17. Go to Path <iAutomate Installer path>\DataCollection...\DataCollection folder location
18. Open HCL.iAutomate.DataCollector.Service.Host.exe config file.
19. Set “enableCertificate_KRS” key to “N”.

```
<add key="enableCertificate_KRS" value="N" />
```

Figure 310 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

20. Follow the last 3 mentioned steps to make the configurational changes required for **AD Sync, Email Service, Generic Service, RBA Service, DAG Service, Asssignation Service and Release Service**

3.6.5.1.2 AI Services:

1. Go to Path <iAutomate Installer path>\iRecommend...\
2. Open IRECOMMEND.CFG file.
3. Replace value of “**enableCertificate**” with “**N**”.

```

24 RANKING_MODEL_VERSION=1
25 RANKING_VOTES_TYPE=Average
26
27 [PROPERTIES]
28 SCORE_BOOSTING_THRESHOLD=0.5
29 RETRY_COUNT=5
30 SALT = 560A18CD-6346-4CF0-A2E8-671F9B6B9EA9
31 IsSelfSigned=Y
32 enableCertificate=N
33 Certificate_Name=HCL.iAutomate
34 DetailLogging=True
35 PROPERTY_LOCATION=DB
36 RECOMMENDATION_MODEL_VERSION=1
37 ENTITY_MODEL_VERSION=1
38 ENTITY_MODEL_LOCATION=D:/Entity/Location
39

```

Figure 311 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX)

4. Open **entity.cfg** file in **entity** folder in same location and replace value of “**enableCertificate**” with “**N**”

```

5 DB_NAME = iAutomateDB
6 CONNECTION_TYPE = Windows
7
8 [MISC]
9 KEY=150
10 loggerState=1
11 SUCCESS_STATUS=0
12 FAIL_STATUS=1
13 KEY_SALT=560A18CD-6346-4CF0-A2E8-671F9B6B9EA9
14 Certificate_Name=HCL.iAutomate
15 IsSelfSigned=Y
16 enableCertificate=N
17 IsJobupdateError=Y
18

```

Figure 312 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX)

5. Go to Path <iAutomate Installer path>\iParse...\iParse\iparse\config
6. Open Parse_data.cfg file.
7. Replace value of “**enableCertificate**” with “**N**”

```

5 DB_NAME = iAutomateDB
6 CONNECTION_TYPE = Windows
7
8 [MISC]
9 KEY=150
10 loggerState=1
11 SUCCESS_STATUS=0
12 FAIL_STATUS=1
13 KEY_SALT=560A18CD-6346-4CF0-A2E8-671F9B6B9EA9
14 Certificate_Name=HCL.iAutomate
15 IsSelfSigned=Y
16 enableCertificate=N
17 IsJobupdateError=Y
18

```

Figure 313 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

8. Go to Path <iAutomate Installer path>\iUnique...\iUnique\iUnique_final\config
9. Open **iUnique.cfg** file.
10. Replace “**enableCertificate**” with “**N**”

```

21
22 [DATA_FROM_DB]
23 VALUE=True
24
25 [SIMILARITY]
26 S_VALUE=0.70
27
28 [MISC]
29 KEY=150
30 loggerState=1
31 KEY_SALT=560A18CD-6346-4CF0-A2E8-671F9B6B9EA9
32 Certificate_Name=HCL.iAutomate
33 IsSelfSigned=Y
34 enableCertificate=N
35

```

Figure 314 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)

11. Go to <iAutomate Installer path>\iScript...\iScript\iScript\config
12. Open **iScrape.cfg** file.
13. Replace “**enableCertificate**” with “**N**”

```

1  [DATABASE]
2  DB_HOST = 52.62.30.61
3  DB_USER = sa
4  DB_PASSWORD = Welcome@123
5  DB_NAME = iAutomateDB
6  DOWNLOAD_PATH = C:/Apache24/htdocs/Scripts/Scripts
7
8  [logging]
9  filename = action.log
10
11 [urls]
12 docsExtensions = .pdf,.doc,.txt,.xlsx,.xslm,.docx,.sql
13 scriptExtensions = .ps1,.rar,.psml
14
15 [MISC]
16 loggerState=0
17 KEY_SALT=560A18CD-6346-4CF0-A2E8-671F9B6B9EA9
18 Certificate_Name=HCL.iAutomate
19 IsSelfSigned=Y
20 enableCertificate=N
21

```

Figure 315 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)

14. Go to <iAutomate Installer path>\AdvanceKnowledge\Crawler\crawler_v5\config
15. Open **iCrawler.cfg** file.
16. Replace “**enableCertificate**” with “**N**”
17. Go to <iAutomate Installer path>\ AdvanceKnowledge\ iKnowledge_Indexer
18. Open **INDEXER.cfg** file.
19. Replace “**enableCertificate**” with “**N**”
20. Go to <iAutomate Installer path>\ AdvanceKnowledge\ iKnowledge_Screen
21. Open **IKNOWLEDGE_SCREEN.cfg** file.
22. Replace “**enableCertificate**” with “**N**”
23. Go to <iAutomate Installer path>\ AdvanceKnowledge\ iKnowledge_Search
24. Open **IKNOWLEDGE_SEARCH.cfg** file.
25. Replace “**enableCertificate**” with “**N**”
26. Go to <iAutomate Installer path>\ KnowledgeRating ...\ iKnowledge_Rating
27. Open **rating.cfg** file.
28. Replace “**enableCertificate**” with “**N**”

29. Go to <iAutomate Installer path>\iKnowledge \ iKnowledge \ knowledge_v4
30. Open iknowledge.cfg file.
31. Replace “enableCertificate” with “N”

3.6.5.2 Without Certificate used to connect Services

3.6.5.2.1 WCF Services:

1. Go to <iAutomate Installer path>.

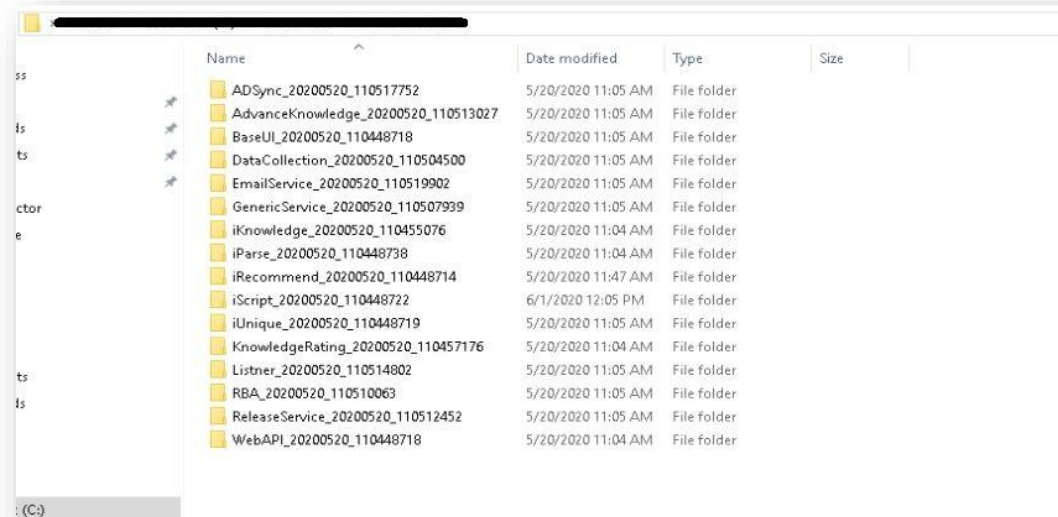


Figure 316 – Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)

2. Go to Path <iAutomate Installer path>\BaseUI...\BaseUI
3. Open **Web.config** file.
4. Replace value of “enableCertificate_Service” key to “N”.

```
<add key="enableCertificate_Service" value="N" />
```

```
<security mode="None">
  <message clientCredentialType="None" establishSecurityContext="false" negotiateServiceCredential="false" />
</security>
```

Figure 317 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)

5. Change mode="None" and clientCertificateType="None".
6. Go to Path <iAutomate Installer path>\Listener...\Listener
7. Open HCL.iAutomate.Listener.Service.Host.exe config file.
8. Replace value of “enableCertificate_Service” key to “N”.

```
<add key="enableCertificate_Service" value="N" />
```

```
<security mode="None">  
  <message clientCredentialType="None" establishSecurityContext="false" negotiateServiceCredential="false" />  
</security>
```

Figure 318 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

9. Change mode="None" and clientCertificateType="None".
10. Go to Path <iAutomate Installer path>\DataCollection...\DataCollection folder location
11. Open HCL.iAutomate.DataCollector.Service.Host.exe config file.
12. Replace value of "enableCertificate_Service" key to "N".

```
<add key="enableCertificate_Service" value="N" />
```

Figure 319 - Configuration Changes – Access iAutomate without Certificate
(Type – PFX) (cont.)

13. Follow the last 3 mentioned steps to make the configurational changes required for **AD Sync, Email Service, Generic Service, RBA Service, DAG Service, Assignment Service and Release Service**

3.6.6 Configuration Changes – Access iAutomate with Certificate (Type – PFX)

This section describes the steps for making the required configurational changes to enable access to iAutomate when PFX certificate is available. By default, iAutomate will install with Certificate.

To make the configuration changes, please follow the below steps:

3.6.6.1 With Certificate used to connect KRS

3.6.6.1.1 WCF Services:

1. Go to <iAutomate Installed path>.

Name	Date modified	Type	Size
ADSync_20230410_213331	4/10/2023 9:33 PM	File folder	
AdvanceKnowledge_20230410_213323	4/10/2023 9:36 PM	File folder	
BaseUI_20230410_213308	6/1/2023 10:26 AM	File folder	
DataCollection_20230410_213316	4/10/2023 9:33 PM	File folder	
EmailService_20230410_213333	4/10/2023 9:33 PM	File folder	
GenericService_20230410_213319	4/10/2023 9:33 PM	File folder	
iKnowledge_20230410_213310	4/10/2023 9:33 PM	File folder	
iParse_20230410_213304	4/10/2023 9:33 PM	File folder	
iRecommend_20230410_213304	4/11/2023 3:53 PM	File folder	
iScript_20230410_213304	4/10/2023 9:33 PM	File folder	
iUnique_20230410_213304	4/10/2023 9:33 PM	File folder	
KnowledgeRating_20230410_213304	4/10/2023 9:33 PM	File folder	
KRS_20230410_213304	4/10/2023 9:33 PM	File folder	
Listner_20230410_213329	4/10/2023 9:33 PM	File folder	
Log_Baseui	4/28/2023 3:53 PM	File folder	
RBA_20230410_213325	4/10/2023 9:33 PM	File folder	
ReleaseService_20230410_213328	4/10/2023 9:33 PM	File folder	
WebAPI_20230410_213306	4/13/2023 2:59 PM	File folder	

Figure 320 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

- Go to Path <iAutomate Installer path>\KRS.
- Open **Web.config** file.
- Add mode=" Message" in <security> tag.
- Change clientCredentialType="Certificate" in <message> tag.

```
<binding name="wsHttpEndpointBinding">
  <security>
    <message clientCredentialType="Certificate" establishSecurityContext="false" negotiateServiceCredential="false"/>
  </security>
</binding>
```

Figure 321 Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

- Change certificateValidationMode="PeerTrust" in <serviceCredentials> tag.

```
<serviceCredentials>
  <clientCertificate>
    <authentication certificateValidationMode="PeerTrust"/>
  </clientCertificate>
  <serviceCertificate findValue="HCL.iAutomate" storeLocation="LocalMachine" storeName="TrustedPeople" x509FindType="FindBySubjectName"/>
</serviceCredentials>
```

Figure 322 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

- Uncomment the <serviceCertificate > tag, if commented.
- Go to Path <iAutomate Installer path>\ WebAPI
- Open **Web.config** file.
- Set key "enableCertificate_KRS" value to "Y".

```
<add key="enableCertificate_KRS" value="Y" />
```

Figure 323 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

- Go to Path <iAutomate Installer path>\Listener...\Listener
- Open HCL.iAutomate.Listener.Service.Host.exe config file.
- Set "enableCertificate_KRS" key to "Y".

```
<add key="enableCertificate_KRS" value="Y" />
```

Figure 324 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

14. Go to Path <iAutomate Installer path>\BaseUI...\BaseUI
15. Open **Web.config** file.
16. Set "enableCertificate_KRS" key to "Y".

```
<add key="enableCertificate_KRS" value="Y" />
```

Figure 325 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

17. Go to Path <iAutomate Installer path>\DataCollection...\DataCollection folder location
18. Open HCL.iAutomate.DataCollector.Service.Host.exe config file.
19. Replace value of "enableCertificate_KRS" key to "Y".

```
<add key="enableCertificate_KRS" value="Y" />
```

Figure 326 - Configuration Changes – Access iAutomate without Certificate (Type – PFX) (cont.)

20. Follow the last 3 mentioned steps to make the configurational changes required for **AD Sync, Email Service, Generic Service, RBA Service, DAG Service, Assignment Service and Release Service**

3.6.6.1.2 AI Services

1. Go to Path <iAutomate Installer path>\iRecommend...\
2. Open IRECOMMEND.CFG file.
3. Replace value of "enableCertificate" with "Y".
4. Open **entity.cfg** file in **entity** folder in same location and replace value of "enableCertificate" with "Y"
5. Go to Path <iAutomate Installer path>\iParse...\iParse\iparse\config
6. Open Parse_data.cfg file.
7. Replace value of "enableCertificate" with "Y".
8. Go to Path <iAutomate Installer path>\iUnique...\iUnique\iUnique_final\config
9. Open **iUnique.cfg** file.
10. Replace "enableCertificate" with "Y".
11. Go to <iAutomate Installer path>\iScript...\iScript\iScript\config
12. Open **iScrape.cfg** file.
13. Replace "enableCertificate" with "Y".
14. Go to <iAutomate Installer path>\AdvanceKnowledge\Crawler\crawler_v5\config
15. Open **iCrawler.cfg** file.
16. Replace "enableCertificate" with "Y".
17. Go to <iAutomate Installer path>\ AdvanceKnowledge\ iKnowledge_Indexer
18. Open **INDEXER.cfg** file.
19. Replace "enableCertificate" with "Y".
20. Go to <iAutomate Installer path>\ AdvanceKnowledge\ iKnowledge_Screen
21. Open **IKNOWLEDGE_SCREEN.cfg** file.
22. Replace "enableCertificate" with "Y".

23. Go to <iAutomate Installer path>\AdvanceKnowledge\iKnowledge_Search
24. Open IKNOWLEDGE_SEARCH.cfg file.
25. Replace “enableCertificate” with “Y”.
26. Go to <iAutomate Installer path>\KnowledgeRating ...\iKnowledge_Rating
27. Open rating.cfg file.
28. Replace “enableCertificate” with “Y”.
29. Go to <iAutomate Installer path>\iKnowledge \iKnowledge \ knowledge_v4.
30. Open iknowledge.cfg file.
31. Replace “enableCertificate” with “Y”.

3.6.6.2 With Certificate used to connect Services

3.6.6.2.1 WCF Services:

1. Go to <iAutomate Installed path>.

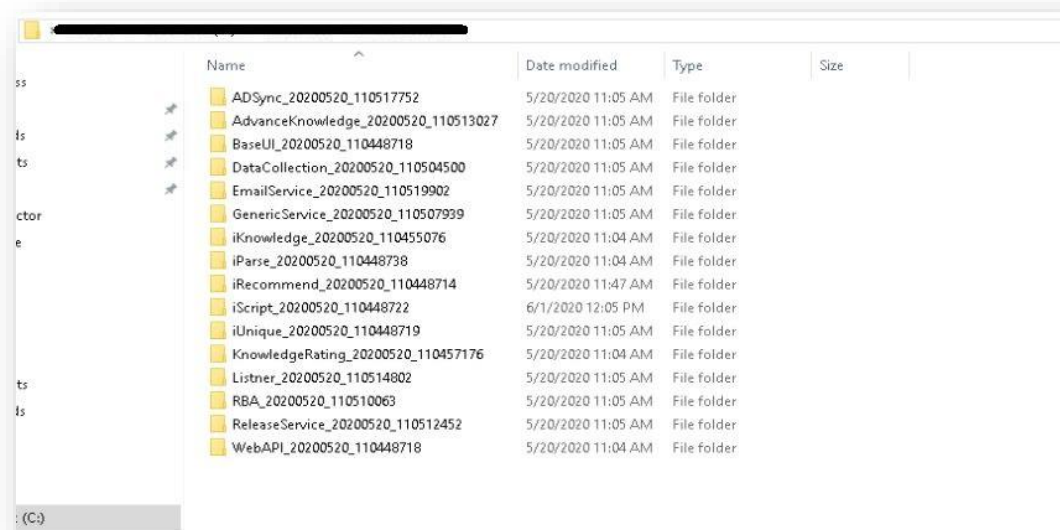


Figure 327 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

2. Go to Path <iAutomate Installer path>\BaseUI...\BaseUI
3. Open **Web.config** file.
4. Replace value of “enableCertificate_Service” key to “Y”.

```
<add key="enableCertificate_Service" value="Y" />
```

Figure 328- Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

5. Go to Path <iAutomate Installer path>\Listener...\Listener.
6. Open HCL.iAutomate.Listener.Service.Host.exe config file.
7. Replace value of “enableCertificate_Service” key to “Y”.

```
<add key="enableCertificate_Service" value="Y" />
```

Figure 329 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

8. Go to Path <iAutomate Installer path>\DataCollection...\DataCollection folder location
9. Open HCL.iAutomate.DataCollector.Service.Host.exe config file.
10. Replace value of “enableCertificate_Service” key to “Y”.

```
<add key="enableCertificate_Service" value="Y" />
```

Figure 330 - Configuration Changes – Access iAutomate with Certificate (Type – PFX) (cont.)

11. Follow the last 3 mentioned steps to make the configurational changes required for **AD Sync, Email Service, Generic Service, RBA Service, DAG Service, Assignment Service and Release Service**

3.6.7 Configuration Changes - Access iAutomate without Certificate (Type – PEM)

This section describes the steps for making the required configurational changes to enable access to iAutomate when PEM certificate is not available.

To make the configuration changes, please follow the below steps:

3.6.7.1 AI Services:

1. Go to Path <iAutomate Installer path>\Listener...\Listener
2. Open HCL.iAutomate.Listener.Service.Host.exe config file.
3. Replace value of “enablePEMCertificate” key with “N”.

```
69 <add key="PythonCertiPath" value="C:\Program Files\Certificate\server.pem" />
70 <!--Check PFX Certificate required or not-->
71 <add key="enableCertificate" value="N" />
72 <!--Check Pem (Python)Certificate required or not-->
73 <add key="enablePEMCertificate" value="N" />
74 <add key="IsSelfSigned" value="N" />
75 <!--Error log folder Path-->
76 <add key="Errorlog" value="C:\Logs" />
```

Figure 331 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

4. Go to Path <iAutomate Installer path>\BaseUI...\BaseUI
5. Open **Web.config** file.
6. Replace value of “enablePEMCertificate” key to “N”.
7. Got to Path C:/Apache24/conf and open **iRecommend.cfg** file. Comment the following lines:
 - a. SSLEngine on
 - b. SSLCertificateFile "C:/Program Files/certificate/server.crt"
 - c. SSLCertificateKeyFile "C:/Program Files/certificate/server.key"
 - d. SSLCACertificateFile "C:/Program Files/certificate/ca.pem"
 - e. SSLVerifyClient require
 - f. SSLVerifyDepth 10
 - g. LoadModule ssl_module modules/mod_ssl.so.

```

162 #LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
163 #LoadModule socache_dbm_module modules/mod_socache_dbm.so
164 #LoadModule socache_memcache_module modules/mod_socache_memcache.so
165 LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
166 #LoadModule spelling_module modules/mod_spelling.so
167 #LoadModule ssl_module modules/mod_ssl.so
168 #LoadModule status_module modules/mod_status.so
169 #LoadModule substitute_module modules/mod_substitute.so
170 #LoadModule unique_id_module modules/mod_unique_id.so
171 #LoadModule userdir_module modules/mod_userdir.so
172 #LoadModule usertrack_module modules/mod_usertrack.so

```

Figure 332 - Configuration Changes – Access iAutomate without Certificate
(Type – PEM)

```

530
531 #SSLEngine on
532
533 #SSLCertificateFile "C:/Program Files/certificate/server.crt"
534 #SSLCertificateKeyFile "C:/Program Files/certificate/server.key"
535 #SSLCACertificateFile "C:/Program Files/certificate/ca.pem"
536
537
538
539
540 <VirtualHost *>
541
542     WSGIScriptAlias /iAutomate C:/iAutomate/iAutomate5.1/iKnowledge_20200
543
544     #SSLVerifyClient require
545
546     #SSLVerifyDepth 10
547

```

Figure 333 - Configuration Changes – Access iAutomate without Certificate
(Type – PEM)

8. To make the changes to the **Endpoint URL**, go to the iAutomate website.
9. Click Advance Configuration → Load Balancer Configuration.

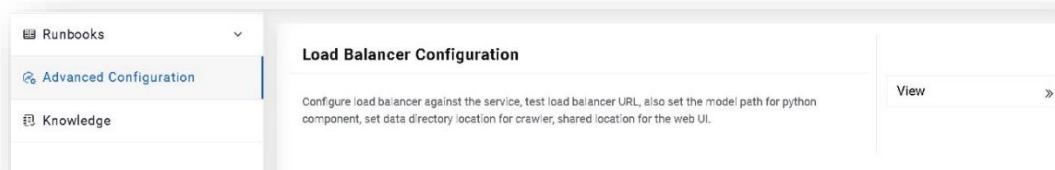


Figure 334 - Configuration Changes – Access iAutomate without Certificate
(Type – PEM)

10. Select **Component Name** as 'iRecommend'.
11. Change the **Load Balancer URL** from 'https' to 'http'.
12. Click **Update**.

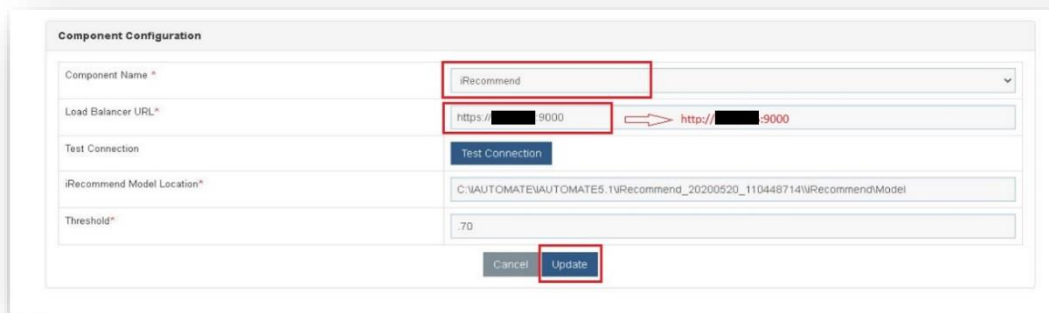


Figure 335 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

13. Repeat Steps 7 & 8 for each of the AI components mentioned below –

- Entity
- iKnowledge
- iKnowledgeCrawler
- iKnowledgeIndexer
- iKnowledgeScreen
- iKnowledgeSearch
- iParse
- iRecommend
- iScript
- iUnique
- ratingMongo

3.6.7.2 IIS Configuration:

1. Press **Win + R** and type **inetmgr**.
2. Click **OK** to open **IIS**.

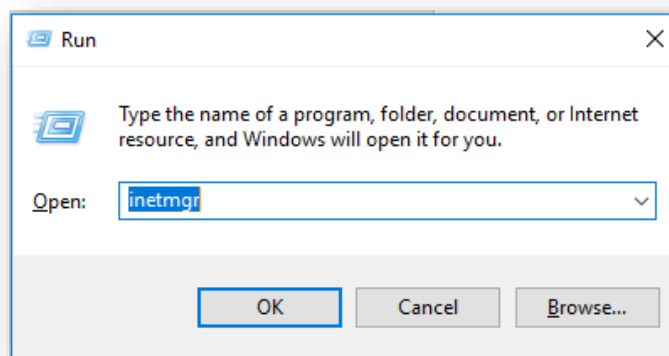


Figure 336 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

3. Expand **Sites**.

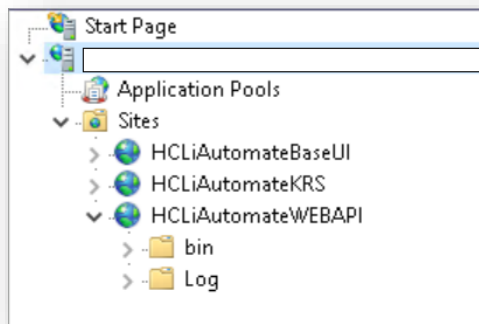


Figure 337 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

4. Go to **Application Pools**. Click on your specific application pool. Click **Recycle** or **Stop** and then click **Start**

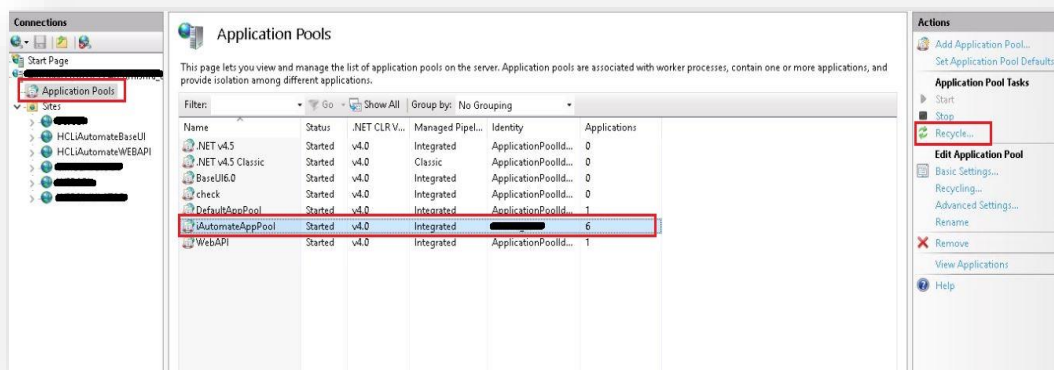


Figure 338 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

5. Go to **Sites**. Click the site having name **BaseUI**. Click on **Restart**.

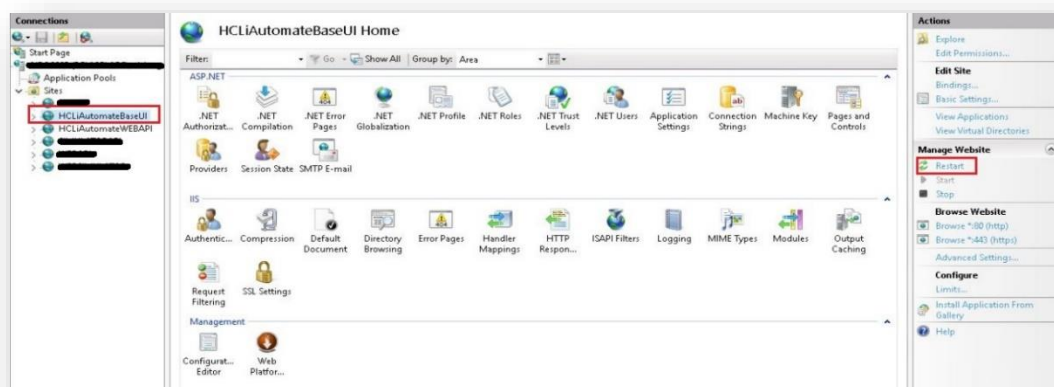


Figure 339 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

6. Go to **Sites**. Click the site having name **WEBAPI**. Click on **Restart**.

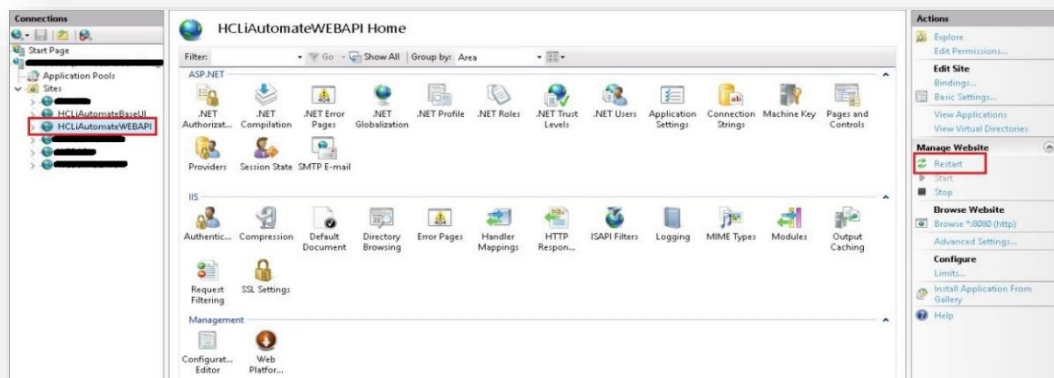


Figure 340 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

3.6.7.3 Restart Services

1. Press **Win+R** and type services.msc.

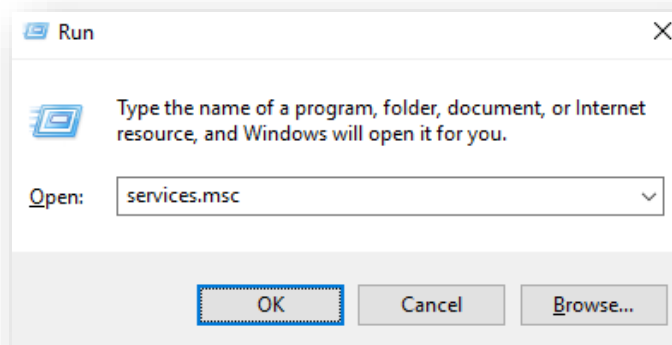


Figure 341 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

2. Click OK to open Windows Services.

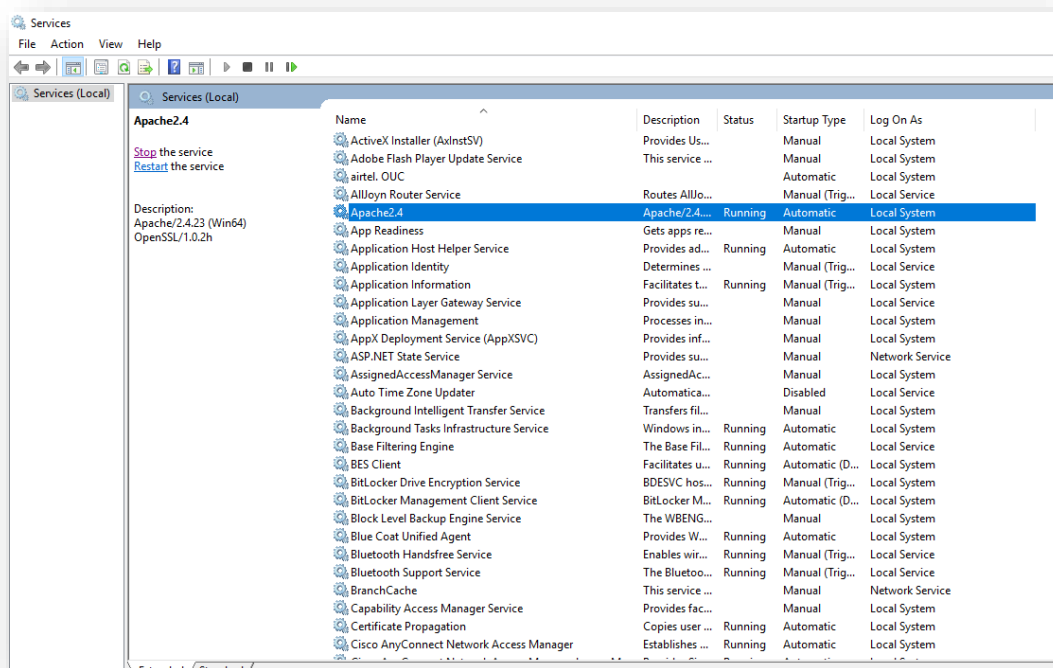


Figure 342 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

3. Search for iAutomate Services.
4. Restart **Apache24** service.
5. Restart all **HCL.iAutomate** services.

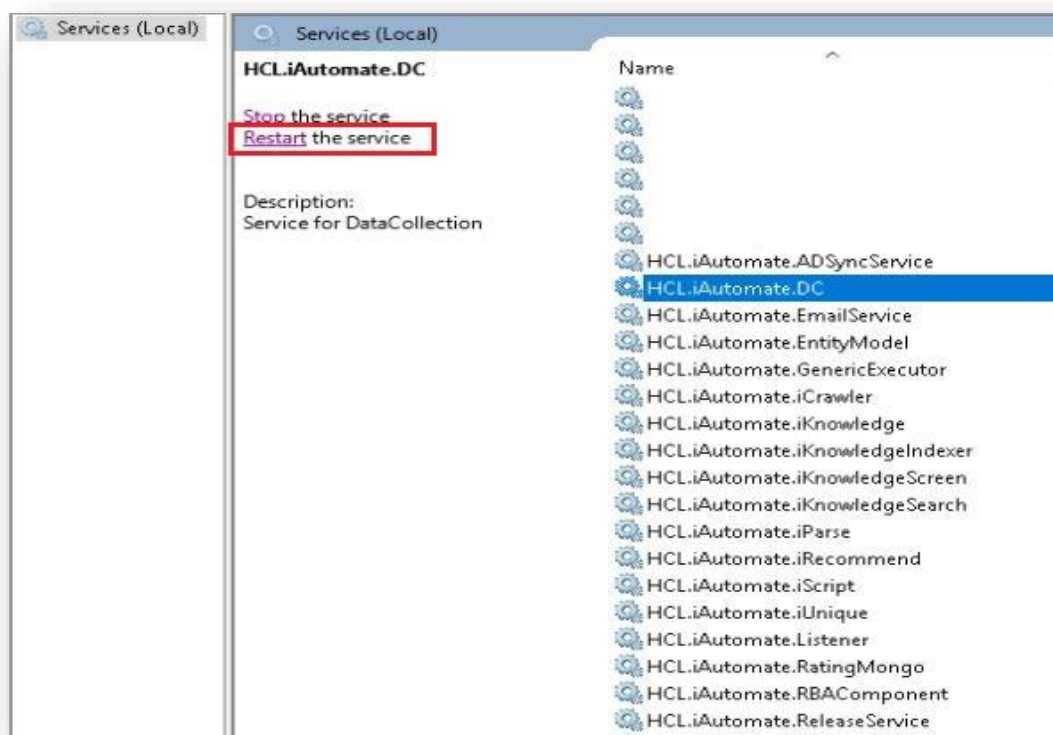


Figure 343 - Configuration Changes – Access iAutomate without Certificate (Type – PEM)

3.6.8 Configuration Changes – SaaS based Ticket Analysis

This section describes the steps for making the required configurational changes to enable access to SaaS based Ticket Analysis module.

It is a three-step process –

- **Manage SMTP** – required to enable mail-based notifications to the users and administrators
- **Build Model** – required to build the Entity and Recommendation models used for ticket analysis
- **Change hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis** – enable users to access the SaaS Ticket Analysis UI

3.6.8.1 Manage SMTP

To make the configuration changes, please follow the below steps:

1. Login into iAutomate console with **Super Admin** credentials.
2. On the main menu bar, click **Configuration** and then click **Manage SMTP**. The **Manage SMTP** page appears.

The screenshot shows the 'Manage SMTP' configuration page. It has a header 'SMTP Information' and a sub-header 'Manage SMTP configurations for your organization.' The form contains the following fields and controls:

- SMTP Server ***: Text input field.
- SMTP Port ***: Text input field.
- User Name ***: Text input field.
- Password ***: Text input field with an 'Add Password' button.
- Mailto Cc ***: Text input field.
- Mailto Bcc**: Text input field.
- From Email ***: Text input field.
- Timeout ***: Text input field with the value '10909889'.
- SMTP Type ***: Dropdown menu with '-Select-' selected.
- SSL**: Toggle switch.
- Submit**: Blue button at the bottom.

Figure 344- Manage Proxy

3. In the **SMTP Server** field, type the SMTP Server.
4. In the **SMTP Port** field, type the SMTP port.
5. In the **SMTP UserName** and **SMTP Password** fields, type the username and password to access the SMTP server.

For password, click on icon next to it. If the password is available in plaintext, then select Input type as Input Text and enter the password in Value field. Else if it is available in any Key Vault such as CyberArk then select Input Type as CyberArk and then select any of the configured details from the value field. Else if it is available in Internal Secret Manager then select Input Type as Internal Secret Manager and then select any of the configured details from the value field.

Secret Selector [X]

Input Type

Value

☐ Show Password

Cancel Save

Figure 345 - Password in plaintext

Secret Selector [X]

Input Type

Value

Cancel Save

Figure 346 - Password from Key Vault (CyberArk)

Secret Selector [X]

Input Type

Value

Cancel Save

Figure 347 - Password from Internal Secret Manager

6. In the **Mail to Cc** field, type the email of CC User.
7. In the **Mail to Bcc** field, type the email of BCC User.

8. Select SMTP Type.
9. In the **From Email** field, type the email of user whose id is used to send email.
10. Click **Save**.

3.6.8.2 Build Models

To make the configuration changes, please follow the below steps:

1. Login into iAutomate console with **Super Admin** credentials.
2. On the main menu bar, click **Configurations**. Click **Build Models**. The **Build Models** page appears and lists the available build models with their status, the associated organization, module, and the Runbook tool in a tabular view.

Organization	Module	Runbook Tool	Runbook Tool Type	Status	Last Build	Model Type	Remarks	Latest Version	Published Vers...	Action
NA	NA	NA	NA	Queued		Entity Model		V0	V0	
NA	NA	NA	TPAM	Queued		Recommend Model		V0	V0	
NA	NA	NA	ANSIBLE TOWER/AWX	Queued		Recommend Model		V0	V0	
NA	NA	NA	BigFix	Queued		Recommend Model		V0	V0	
NA	NA	NA	TPAM	Queued		Feedback Model		V0	V0	
NA	NA	NA	ANSIBLE TOWER/AWX	Queued		Feedback Model		V0	V0	
NA	NA	NA	BigFix	Queued		Feedback Model		V0	V0	

Figure 348- Build Models

3. On the Build Models page, click next to the **Inventory** → **Entity Model** to build the model. A message confirming the initiation of model build appears.

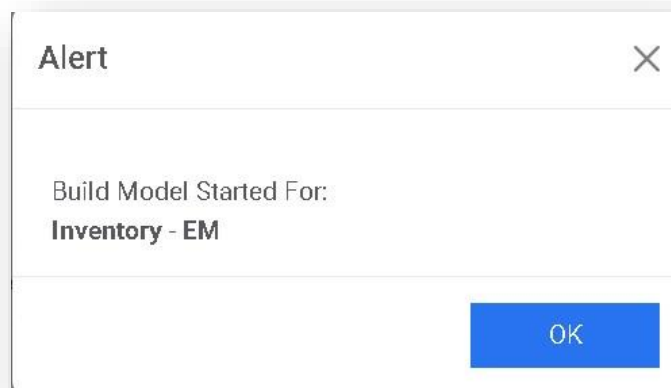


Figure 349- Build Models (cont.)

The status of the build changes from **Queued** to **Initiate**.

Organization	Module	Runbook Tool	Runbook Tool Type	Status	Last Build	Model Type	Remarks
Inventory	NA	NA	NA	Initiate	15-05-2024 07:32:41	Entity Model	

Figure 350- Build Models (cont.)

4. Once the build is successfully created, the status changes from **Initiate** to **Successful** and the **Remarks** column is updated.

Organization ▼	Module	Runbook Tool	Runbook Tool Type ▼	Status	Last Build	Model Type ▼	Remarks	Latest Version	Published Ver...
Inventory	NA	NA	NA	Successful	15-05-2024 07:33:21	Entity Model	Model Creation Successful	V1	V1

Figure 351- Build Models (cont.)

- On the **Build Models** page, click  next to the **Inventory** → **Recommend Model** to build the model.
- A message confirming the initiation of model build appears.

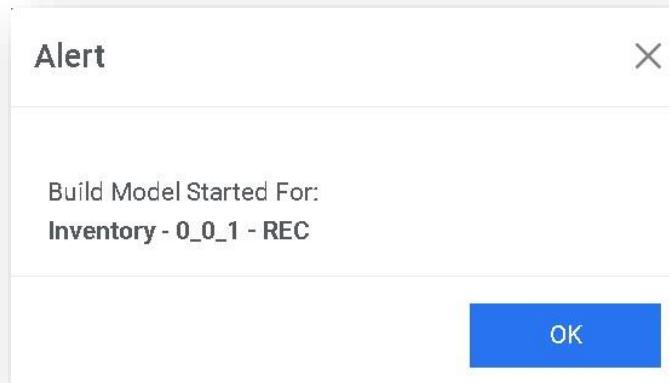


Figure 352- Build Models (cont.)

- The status of the build changes from **Queued** to **Initiate**.

Organization ▼	Module	Runbook Tool	Runbook Tool Type ↓	Status ▼	Last Build	Model Type ▼	Remarks
Inventory	NA	NA	BigFix	Initiate	16-05-2024 02:55:21	Recommend Model	

Figure 353- Build Models (cont.)

- Once the build is successfully created, the status changes from **Initiate** to **Successful** and the **Remarks** column is updated.

Organization ▼	Module	Runbook Tool	Runbook Tool Type ▼	Status ↓	Last Build	Model Type ▼	Remarks
Inventory	NA	NA	BigFix	Successful	16-05-2024 02:11:01	Recommend Model	Model Creation Successful.

Figure 354- Build Models (cont.)

- Logout from the portal and proceed further.

3.6.8.3 Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis

To make the configuration changes, please follow the below steps:

- Press **Win+R** and type **inetmgr**.
- Click **OK** to open **IIS**.

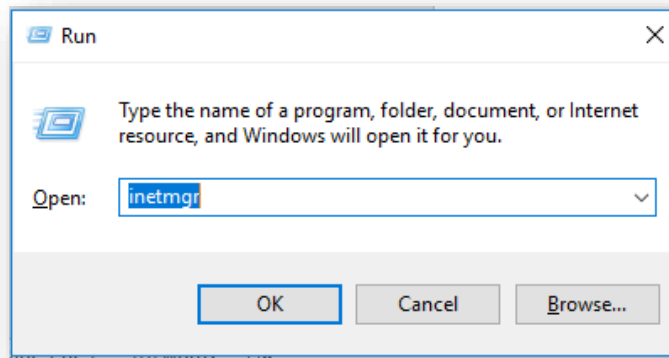


Figure 355- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis

3. Expand Sites and click on HCLiAutomateBaseUI.

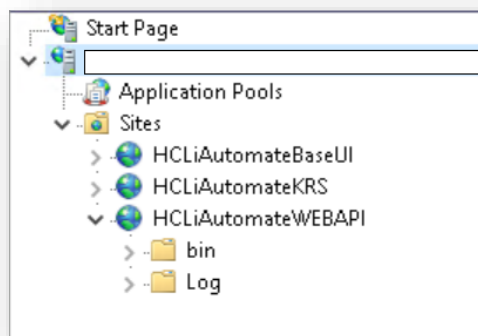


Figure 356- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.)

4. Click on **Default Document** under **IIS** section as shown in below image.

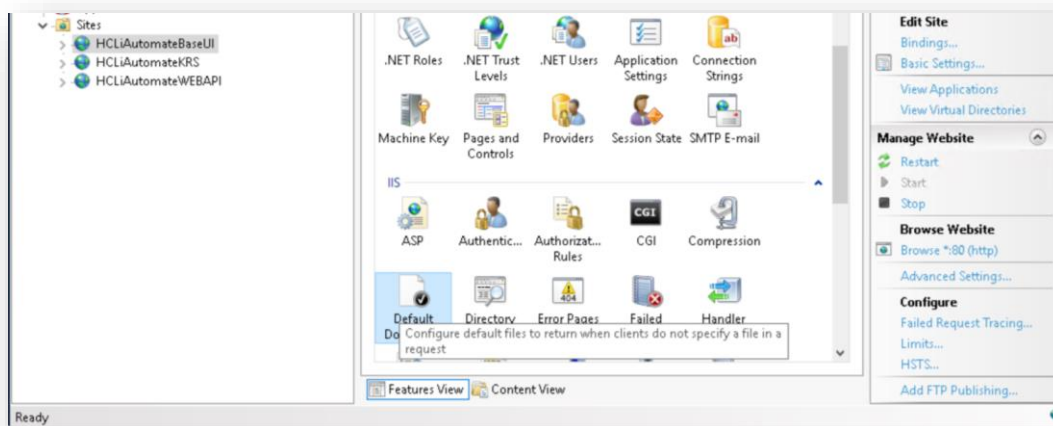


Figure 357- Change Hosting of iAutomate from Base Web Portal to SaaS Ticket Analysis (cont.)

5. Click on **Add** under **Actions** Section.

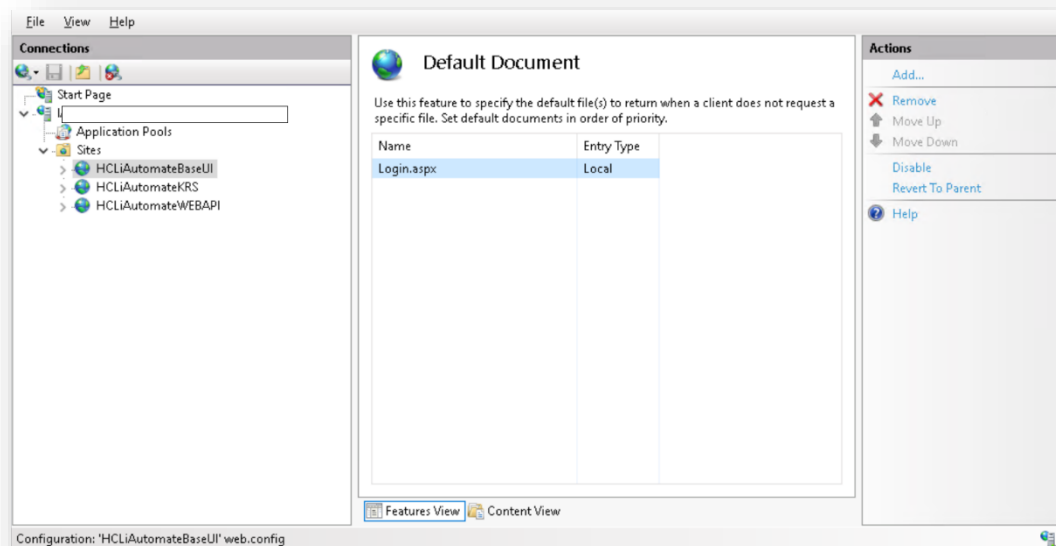


Figure 358- Change Hosting of iAutomate from Base Web Portal to SaaS
Ticket Analysis (cont.)

6. Type in **SignIn.aspx** in the dialog box and click **OK**.

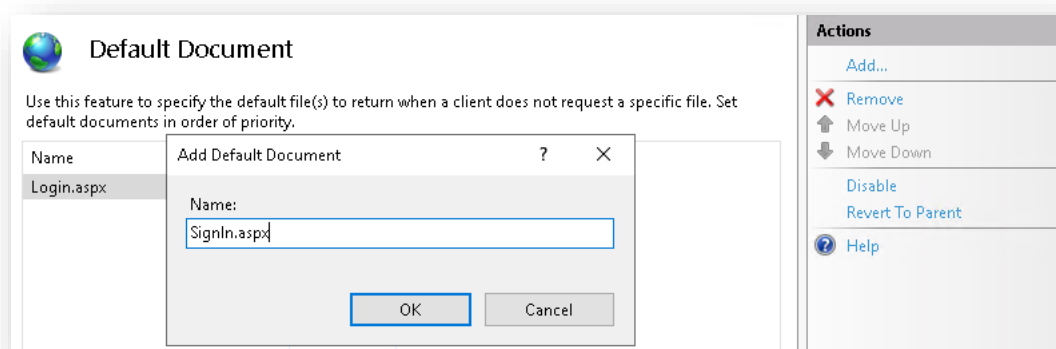


Figure 359- Change Hosting of iAutomate from Base Web Portal to SaaS
Ticket Analysis (cont.)

7. Select **Login.aspx** in Default Document section and click on **Remove** under **Actions** section.

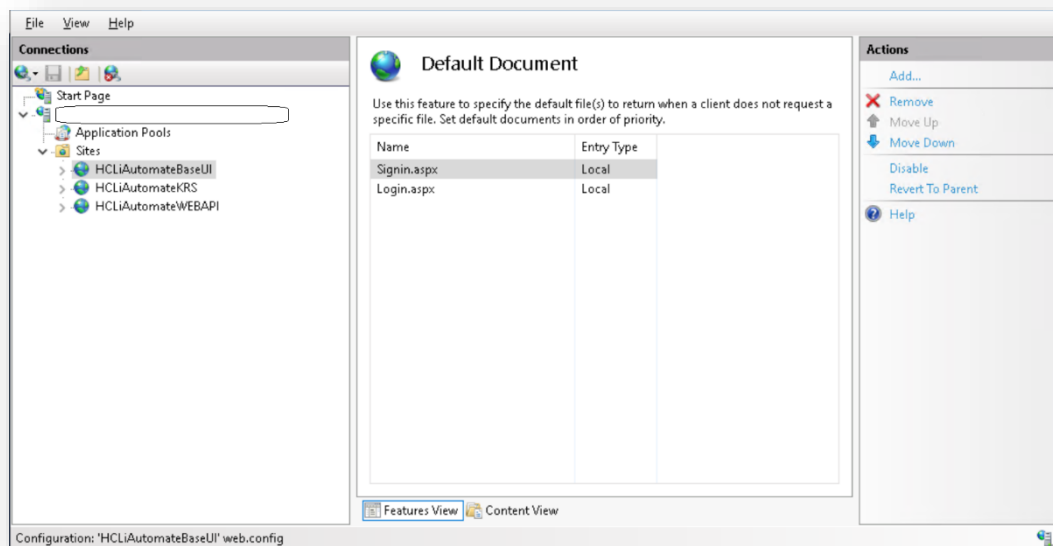


Figure 360- Change Hosting of iAutomate from Base Web Portal to SaaS
Ticket Analysis (cont.)

8. Right Click on HCLiAutomateBaseUI.
9. Click **Explore**.
10. Find **Web.config** file and open it in a **Notepad**.



Figure 361- Change Hosting of iAutomate from Base Web Portal to SaaS
Ticket Analysis (cont.)

11. Within the Web.config file, find the tag `<LogoutRedirectPage>` and change it to `<add key="LogoutRedirectPage" value="~/SignIn.aspx" />`
12. Find the tag `<resetRedirectPage>` and change it to `<add key="resetRedirectPage" value="SignIn.aspx" />`
13. Find the tag `<redirectPage>` and change it to `<add key="redirectPage" value="~/SignIn.aspx" />`
14. Find the tag `<welcomePageURL>` and change it to `<add key="welcomePageURL" value="TicketAnalysis/AnalysisGridPage.aspx"/>`
15. Save the file for changes to be reflected.
16. Select **HCLiAutomateBaseUI** and click **Restart** to restart the Application.

3.6.9 Configuration Changes - Run BASEUI and WEBAPI on Same Port

This section describes the steps for making the required configurational changes to enable BASEUI and WEBAPI on Same Port.

1. Press Win+R and type `inetmgr`.

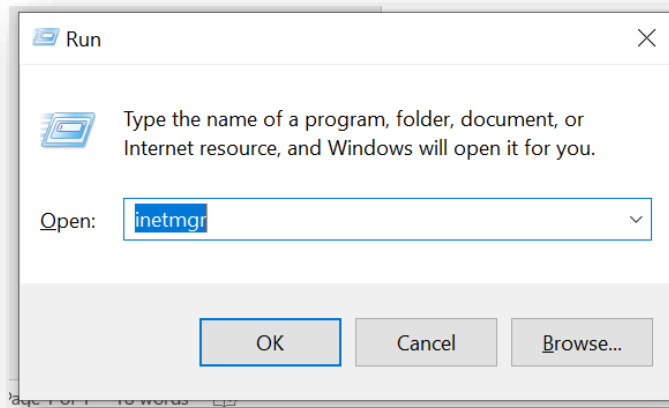


Figure 362 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

2. IIS will be opened. Expand the server's name and then the sites.

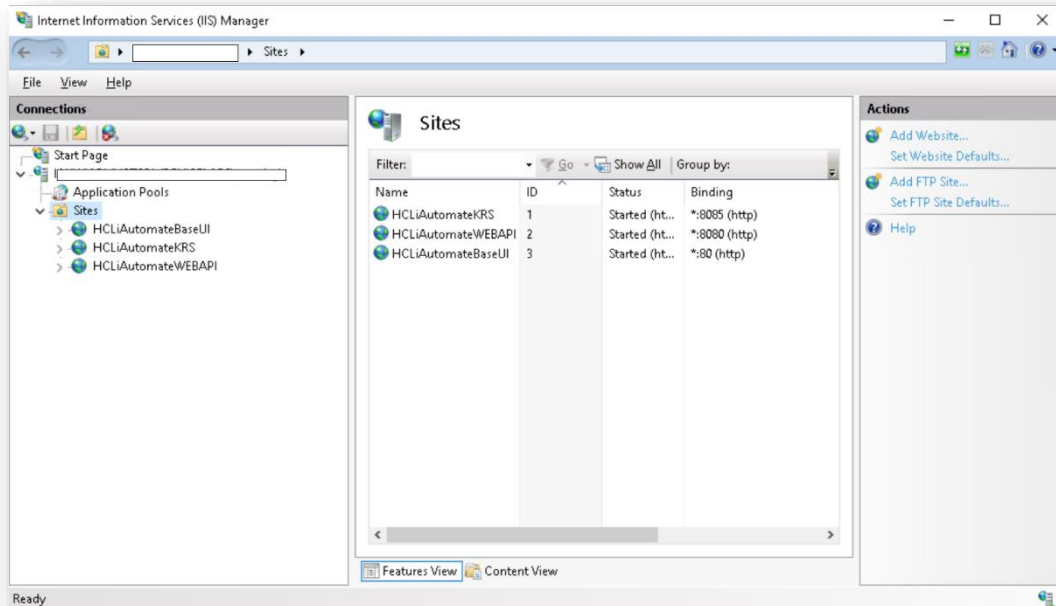


Figure 363 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

3. Right click on **HCLiAutomateBaseUI** and click on add application.

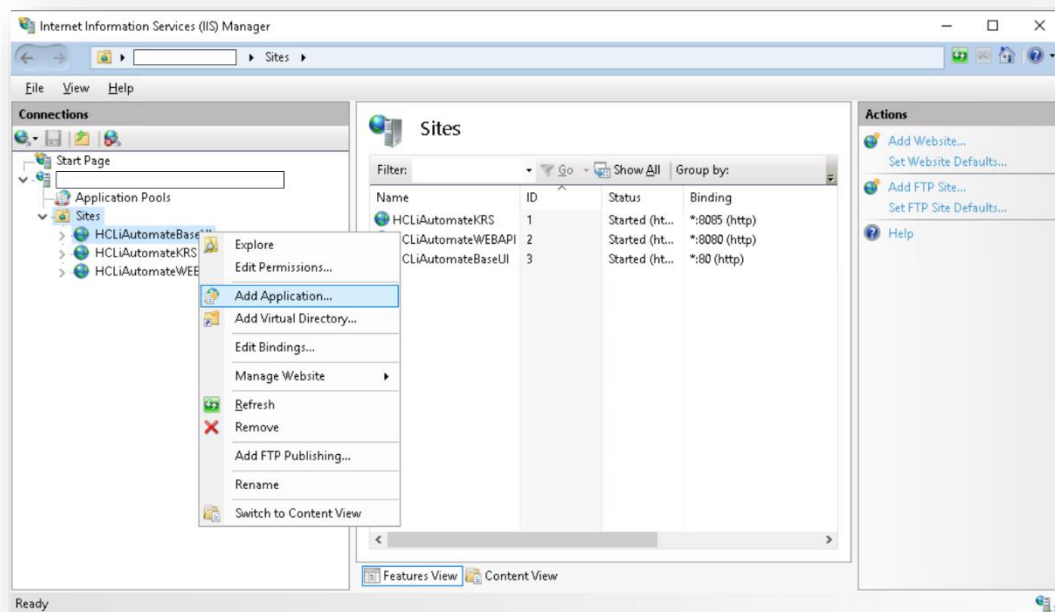


Figure 364 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

4. On the popup opened, enter Alias as '**WebAPI**', Application pool as 'iAutomateAppPool' and enter the path till **WebAPI** folder in Physical Path. Click Ok.

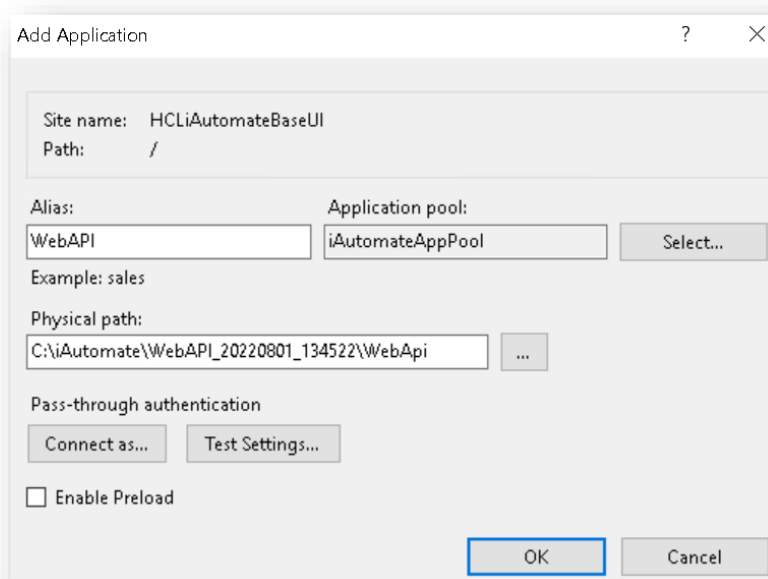


Figure 365 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

5. The WebAPI application will now appear under HCLiAutomateBaseUI.

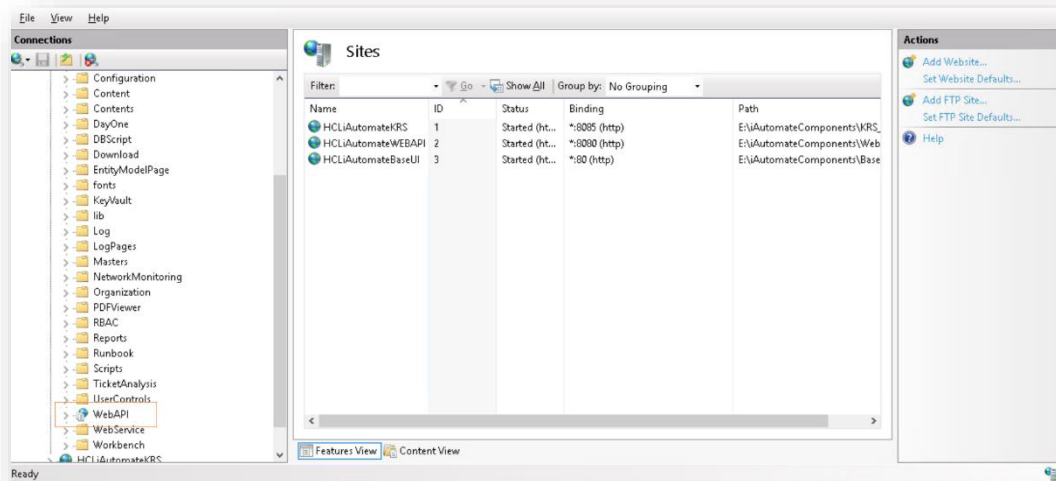


Figure 366 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

6. To test whether API and BaseUI is working on same port, if BaseUI is accessible as <https://localhost:443> then type below URL and see if WebAPI is also accessible with below URL:
WebAPI URL: <BaseUI URL>/<Alias Name of Folder>/iAutomateAPI/Request/Getheartbeat
Eg: [https:// <BaseUI URL>/WebAPI/iAutomateAPI/Request/Getheartbeat](https://<BaseUI URL>/WebAPI/iAutomateAPI/Request/Getheartbeat)
7. Go to web.config file of BaseUI. For that, go to IIS, expand server name and sites, and right click on HCLiAutomateBaseUI and click on explore. Search the web.config file in the opened folder and open the file.
8. In the web.config file, search for 'sessionState mode= "SQLServer"'. Comment this line and uncomment the line with sessionState mode= "InProc" like given below:

```
<!--<sessionState mode="SQLServer" allowCustomSqlDatabase="true" partitionResolverType="iAutomateWeb.App_Code.ConnectionStringResolver"
regenerateExpiredSessionId="true" compressionEnabled="true" useHostingIdentity="true" timeout="20" />-->
<sessionState mode="InProc" cookieless="false" timeout="3600" />
```

Figure 367 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

9. Save the web.config and restart the HCLiAutomateBaseUI in IIS. Now enter the WEBAPI URL (mentioned in Step 6) in browser. Now it should successfully give the below output:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<string xmlns="http://schemas.xmlsoap.org/soap/envelope/">ok</string>
```

Figure 368 - Configuration Changes - Run BASEUI and WEBAPI on Same Port

3.6.10 Configuration Changes in Apache – For Python Components

1. Go to **Run (Windows + R)** and type **services.msc** and search and stop the python services.

Name	Description	Status	Startup Type	Log On As
HCL.iAutomate.DC	Service for ...	Running	Automatic	spandan_...
HCL.iAutomate.EmailService	Service for E...	Running	Automatic	spandan_...
HCL.iAutomate.EntityModel	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.GenericExecutor	Service for ...	Running	Automatic	spandan_...
HCL.iAutomate.iCrawler	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledge	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledgeIndexer	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledgeScreen	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledgeSearch	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iParse	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iRecommend	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iScript	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iUnique	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.Listener	Service for L...	Running	Automatic	spandan_...
HCL.iAutomate.RatingMongo	Apache/2.4...	Running	Automatic	spandan_...

Figure 369 -Apache Upgradation

- Apache2.4
 - HCL.iAutomate.Entitymodel
 - HCL.iAutomate.iCrawler
 - HCL.iAutomate.iknowledge
 - HCL.iAutomate.iKnowledgeIndexer
 - HCL.iAutomate.iKnowledgeScreen
 - HCL.iAutomate.iKnowledgeSearch
 - HCL.iAutomate.iRecommend
 - HCL.iAutomate.iParse
 - HCL.iAutomate.iScript
 - HCL.iAutomate.iUnique
 - HCL.iAutomate.RatingMongo
 - HCL.iAutomate.AssignationService
2. Open below path in explorer: C:\Apache24\conf
 3. Navigate to the above path mentioned, need to update in .conf file of all python components as mentioned in the below screenshot:

Disk (C:) > Apache24 > conf

Name	Date modified	Type	Size
extra	3/3/2023 11:25 AM	File folder	
original	3/3/2023 11:25 AM	File folder	
ssl	4/28/2023 5:47 PM	File folder	
charset.conv	8/25/2022 5:06 PM	CONF File	2 KB
☒ Entity.conf	4/10/2023 9:37 PM	CONF File	21 KB
☒ httpd.conf	9/19/2022 8:11 PM	CONF File	21 KB
☒ iKnowledge.conf	4/10/2023 9:36 PM	CONF File	21 KB
☒ iKnowledgeCrawler.conf	4/10/2023 9:38 PM	CONF File	21 KB
☒ iKnowledgeIndexer.conf	4/10/2023 9:36 PM	CONF File	21 KB
☒ iKnowledgeScreen.conf	4/10/2023 9:36 PM	CONF File	21 KB
☒ iKnowledgeSearch.conf	4/10/2023 9:36 PM	CONF File	21 KB
☒ iParse.conf	4/10/2023 9:35 PM	CONF File	21 KB
☒ iRecommend.conf	4/10/2023 9:35 PM	CONF File	21 KB
☒ iScript.conf	4/10/2023 9:36 PM	CONF File	21 KB
☒ iUnique.conf	4/10/2023 9:35 PM	CONF File	21 KB
magic	8/25/2022 5:06 PM	File	14 KB
mime.types	8/25/2022 5:06 PM	TYPES File	62 KB
openssl.cnf	8/25/2022 5:06 PM	CNF File	11 KB
☒ ratingMongo.conf	4/10/2023 9:35 PM	CONF File	21 KB

Figure 370 - Apache Upgradation (cont.)

4. Open the conf files one by one in notepad++/notepad, locate the word **"Define SRVROOT "/Apache24"**.
5. If it is present you can skip this step and proceed with Step 6, if not add the following 3 lines by searching for the word **"ServerRoot "c:/Apache24"**
6. Replace **"ServerRoot "c:/Apache24"** line in the file with below 3 lines
 - Define SRVROOT "/Apache24"
 - ServerRoot "\${SRVROOT}"
 - PidFile "\${SRVROOT}/httpd.pid"

By default, TLS version, 1.3 has been enabled in this Apache configuration. If you want to enable any other TLS version for a specific window build you need to follow below mentioned steps else continue with step 9.

7. Then find the line **"SSLEngine on"** in the same document.
8. Based on the TLS requirement, check the TLS version that needs to be enabled and copy the lines mentioned below for respective TLS version and paste it after **"SSLEngine on"** line in conf file by removing/uncomment **"#"** from the beginning and save the file.
9. If the required TLS line is already uncommented, skip, and proceed with Step No 9, if it's not present perform below steps.

Table 15 - TLS versions -Apache

- #To enable SSL protocol TLS1.1 uncomment the below line
- #SSLProtocol -all +TLSv1.1
- #To enable SSL protocol TLS1.2 uncomment the below line
- #SSLProtocol -all +TLSv1.2
- #To enable SSL protocol TLS1.3 uncomment the below line
- #SSLProtocol -all +TLSv1.3
- #To enable and integrate SSL protocol TLS1.2 and TLS1.3 uncomment the below line
- #SSLProtocol -all +TLSv1.2 +TLSv1.3
- #To enable SSL protocol till TLS1.2 uncomment the below line
- #SSLProtocol +SSLv2 +SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2

For example:

```
SSLEngine on
# To enable SSL protocol TLS1.1 uncomment the below line
#SSLProtocol -all +TLSv1.1
# To enable SSL protocol TLS1.2 uncomment the below line
SSLProtocol -all +TLSv1.2
# To enable SSL protocol TLS1.3 uncomment the below line
#SSLProtocol -all +TLSv1.3
# To enable and integrate SSL protocol TLS1.2 and TLS1.3 uncomment the below line
#SSLProtocol -all +TLSv1.2 +TLSv1.3
# To enable SSL protocol till TLS1.2 uncomment the below line
#SSLProtocol +SSLv2 +SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2
```

Figure 371 - Apache Upgradation (cont.)

10. If need to go with TLS version 1.2: Removed “#” in the below screenshot and save the file.
11. Changes needs to be done for all Python Components that are selected in the figure above.
12. Verify the changes done in all python components.
13. Go to **Run (Windows + R)** and type **services.msc** and start the python services, which are in stop state.

Name	Description	Status	Startup Type	Log On As
HCL.iAutomate.DC	Service for ...	Running	Automatic	spandan_...
HCL.iAutomate.EmailService	Service for E...	Running	Automatic	spandan_...
HCL.iAutomate.EntityModel	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.GenericExecutor	Service for ...	Running	Automatic	spandan_...
HCL.iAutomate.iCrawler	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledge	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledgeIndexer	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledgeScreen	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iKnowledgeSearch	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iParse	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iRecommend	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iScript	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.iUnique	Apache/2.4...	Running	Automatic	spandan_...
HCL.iAutomate.Listener	Service for L...	Running	Automatic	spandan_...
HCL.iAutomate.RatingMongo	Apache/2.4...	Running	Automatic	spandan_...

Figure 372 - Screenshot of the Apache Python Services

4 Appendix

4.1 List of Abbreviations

Table 16 - List of Abbreviations

Abbreviation	Expansion
AD	Active Directory
AI	Artificial Intelligence
ITOPS	IT Operations
ITSMS	IT Service Management System
KEDB	Known Error Database
SNOW	ServiceNow

5 Support

To get support for this product, go to <https://support.hcl-software.com/csm>

For any additional queries, please reach out to us at aiops-pmg-team@hcl-software.com.

HCLSoftware

hcltechsw.com