

COMODO
Creating Trust Online®



Comodo Certificate Manager

Version 5.9

MRAO Administrator Guide

Guide Version 5.9.051517

Comodo CA Limited,
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom

Table of Contents

| | |
|---|-----------|
| 1 Introduction to Comodo Certificate Manager | 12 |
| 1.1 Guide Structure..... | 12 |
| 1.2 Definitions of Terms..... | 13 |
| 1.2.1 Organizations and Departments..... | 13 |
| 1.2.2 Certificate Types..... | 13 |
| 1.2.3 Administrative Roles..... | 14 |
| 1.2.4 Security Roles - Comparative Table..... | 29 |
| 1.2.5 Multiple Security Roles..... | 34 |
| 1.2.6 Organizations and Departments..... | 34 |
| 1.2.7 Reports..... | 35 |
| 1.3 Logging into Your Account..... | 36 |
| 1.4 The Main Interface - Summary of Areas..... | 36 |
| 1.5 Release Notes..... | 47 |
| 2 The Dashboard | 53 |
| 3 Certificates Management | 76 |
| 3.1 SSL Certificates Area..... | 77 |
| 3.1.1 Overview of the Interface..... | 77 |
| 3.1.1.1 Sorting and Filtering Options..... | 83 |
| 3.1.1.2 SSL Certificate 'Details' Dialog..... | 86 |
| 3.1.1.2.1 Uploading Private Key of a Certificate for Storage and Management by the Private Key Store..... | 92 |
| 3.1.1.2.2 Downloading private key of a certificate..... | 95 |
| 3.1.1.2.3 Resending Notification Email for Certs with 'Issued' State..... | 97 |
| 3.1.1.2.4 Viewing Installation Details of Certificates..... | 97 |
| 3.1.1.2.5 Restarting Apache after Auto-Installation of SSL Certificate..... | 98 |
| 3.1.1.3 Comodo SSL Certificates..... | 99 |
| 3.1.1.3.1 Definition of Terms..... | 99 |
| 3.1.2 Request and Issuance of SSL Certificates to Web Servers and Hosts..... | 100 |
| 3.1.2.1 Prerequisites..... | 101 |
| 3.1.2.2 Automatic Installation and Renewal..... | 102 |
| 3.1.2.2.1 Method 1 - Enterprise Controller Mode..... | 103 |
| 3.1.2.2.2 Method 2 - CCM Controller Mode..... | 118 |
| 3.1.2.3 Initiating SSL Enrollment using Application Forms..... | 130 |
| 3.1.2.3.1 Method 1 - Self Enrollment Form..... | 131 |
| 3.1.2.3.1.1 Initiating the Self Enrollment Process..... | 131 |
| 3.1.2.3.1.2 The Self Enrollment Form..... | 132 |
| 3.1.2.3.1.3 Form Parameters..... | 134 |
| 3.1.2.3.2 Method 2 - Built-in Enrollment Form - Manual CSR Generation..... | 137 |
| 3.1.2.3.2.1 Accessing the Built-in Application Form..... | 138 |
| 3.1.2.3.2.2 The Built-In Application Form..... | 138 |
| 3.1.2.3.2.3 Form Parameters..... | 139 |

| | |
|--|-----|
| 3.1.2.3.3 Method 3 - Built-in Enrollment Form - Auto CSR Generation..... | 143 |
| 3.1.2.3.3.1 The Built-In Application Form..... | 144 |
| 3.1.2.3.3.2 Form Parameters..... | 146 |
| 3.1.2.3.4 Certificate Collection..... | 149 |
| 3.1.2.3.4.1 Collection of SSL Certificate Through Email..... | 149 |
| 3.1.2.3.4.2 Collection of SSL certificate by Administrator..... | 150 |
| 3.1.2.3.5 Downloading and Importing SSL Certificates..... | 151 |
| 3.1.2.4 Certificate Requests - Approving, Declining, Viewing and Editing..... | 152 |
| 3.1.2.5 Certificate Renewal..... | 153 |
| 3.1.2.5.1 Certificate Renewal by Administrators..... | 154 |
| 3.1.2.5.2 Certificate Renewal by the End-User..... | 156 |
| 3.1.2.5.3 Scheduling Automatic Renewal and Installation..... | 157 |
| 3.1.2.6 Certificate Revocation, Replacement and Deletion..... | 159 |
| 3.2 The Client Certificates Area..... | 160 |
| 3.2.1 Overview..... | 160 |
| 3.2.1.1 Sorting and Filtering Options..... | 162 |
| 3.2.1.2 'Certs' Dialog..... | 163 |
| 3.2.2 Adding Cert End-Users..... | 166 |
| 3.2.2.1 Manually Adding End-Users..... | 166 |
| 3.2.2.1.1 'Add New Person' form - Table of Parameters..... | 167 |
| 3.2.2.2 Loading Multiple End-Users from a Comma Separated Values (.csv) File | 169 |
| 3.2.2.2.1 Procedure Overview..... | 169 |
| 3.2.2.2.2 Requirements for .csv file | 169 |
| 3.2.2.2.2.1 For Organizations with Principal Name Support Enabled..... | 170 |
| 3.2.2.2.2.2 For Organizations without Principal Name Support..... | 171 |
| 3.2.2.2.3 General Rules..... | 172 |
| 3.2.2.2.4 The Import Process..... | 173 |
| 3.2.2.2.5 Errors in .csv file..... | 175 |
| 3.2.2.3 Auto Creation of End-Users via Certificate Self Enrollment Form..... | 175 |
| 3.2.3 Editing End-Users | 175 |
| 3.2.4 Deleting an End-User..... | 177 |
| 3.2.5 Request and Issuance of Client Certificates to Employees and End-Users..... | 177 |
| 3.2.5.1 Self Enrollment by Access Code..... | 177 |
| 3.2.5.1.1 Prerequisites..... | 177 |
| 3.2.5.1.2 Procedure Overview..... | 178 |
| 3.2.5.1.3 Initiating the Enrollment Process..... | 179 |
| 3.2.5.1.3.1 The Access Code Based Self Enrollment Form..... | 180 |
| 3.2.5.1.3.2 Form Parameters..... | 180 |
| 3.2.5.1.4 Validation of the Application..... | 181 |
| 3.2.5.1.5 Certificate Collection..... | 184 |
| 3.2.5.2 Self Enrollment by Secret Identifier..... | 185 |
| 3.2.5.2.1 Prerequisites..... | 185 |

| | |
|--|-----|
| 3.2.5.2.2 Procedure Overview..... | 187 |
| 3.2.5.2.3 Initiating the Enrollment Process..... | 187 |
| 3.2.5.2.3.1 Secret Identifier Based Self Enrollment Form..... | 188 |
| 3.2.5.2.3.2 Form Parameters..... | 189 |
| 3.2.5.2.4 Certificate Collection..... | 190 |
| 3.2.5.3 Enrollment by Invitation..... | 190 |
| 3.2.5.3.1 Prerequisites..... | 190 |
| 3.2.5.3.2 Procedure Overview..... | 191 |
| 3.2.5.3.3 Initiating the Enrollment Process..... | 191 |
| 3.2.5.3.4 Validation of the Email Address..... | 193 |
| 3.2.5.3.5 Certificate Collection..... | 195 |
| 3.2.6 Revocation of Client Certificates..... | 196 |
| 3.2.6.1 Revocation of Client Certificates by End-Users..... | 196 |
| 3.2.6.1.1 Procedure Overview..... | 197 |
| 3.2.6.1.2 Revocation form..... | 197 |
| 3.2.6.1.3 Form Parameters..... | 197 |
| 3.2.7 Viewing End-User's Certificate..... | 197 |
| 3.3 The Code Sign Certificates Area..... | 200 |
| 3.3.1 Sorting and Filtering Options..... | 202 |
| 3.3.2 Code Sign Certificates View Dialog..... | 203 |
| 3.3.3 Adding Certificates to be Managed..... | 206 |
| 3.3.3.1 Manually Adding Certificates..... | 206 |
| 3.3.3.2 Loading Multiple Certificates from a Comma Separated Values (.csv) File..... | 207 |
| 3.3.3.2.1 Procedure Overview..... | 208 |
| 3.3.3.2.2 Requirements for .csv file..... | 208 |
| 3.3.3.2.3 Uploading .CSV File..... | 208 |
| 3.3.3.3 Auto Creation of End-Users by Initiating Self Enrollment..... | 210 |
| 3.3.4 Request and Issuance of Code Signing Certificates..... | 210 |
| 3.3.4.1 Prerequisites..... | 210 |
| 3.3.4.2 Procedure Overview..... | 211 |
| 3.3.4.3 Initiating the Enrollment Process..... | 211 |
| 3.3.4.4 Validation of Email address and Requisition..... | 213 |
| 3.3.4.5 Downloading and Installing the Certificate..... | 215 |
| 3.4 The Device Certificates Area..... | 215 |
| 3.4.1 Overview..... | 215 |
| 3.4.1.1 Sorting and Filtering Options..... | 219 |
| 3.4.1.2 Viewing Certificate Details..... | 220 |
| 3.4.2 Request and Issuance of Device Certificates..... | 222 |
| 3.4.2.1 Issuance of Device Certificates through Active Directory..... | 223 |
| 3.4.2.2 Issuance of Device Certificates through SCEP..... | 223 |
| 3.4.2.3 Issuance of Device Certificate through Self Enrollment..... | 226 |
| 3.4.2.3.1 Prerequisites..... | 226 |

| | |
|---|-----|
| 3.4.2.3.2 Procedure Overview..... | 226 |
| 3.4.2.3.3 Initiating the Enrollment Process | 226 |
| 3.4.2.3.4 The Self Enrollment Form..... | 226 |
| 3.4.2.4 Device Certificate Collection | 227 |
| 3.4.2.5 Resending Device Certificate Collection Email..... | 228 |
| 3.4.2.6 Device Certificate Revocation..... | 229 |
| 4 Code Signing on Demand..... | 230 |
| 4.1 Setting-up the CSD Controller..... | 232 |
| 4.1.1 Installing the Controller (Hosted Mode)..... | 232 |
| 4.2 Add Developers..... | 236 |
| 4.3 Obtain a code-signing certificate for CSD..... | 238 |
| 4.4 How to sign code using CSD..... | 242 |
| 4.5 Configure the CSD service..... | 249 |
| 4.5.1 In-House Hosted Mode..... | 249 |
| 4.5.2 Cloud Service Mode..... | 254 |
| 5 Admin Management..... | 255 |
| 5.1 Section Overview | 255 |
| 5.1.1 Sorting and Filtering Options..... | 258 |
| 5.2 Adding Administrators..... | 260 |
| 5.2.1 'Add New Client Admin' form - Table of Parameters..... | 261 |
| 5.2.2 Example: Adding a New Administrator with Multiple Roles..... | 264 |
| 5.2.2.1 The 'Certificate auth' Field..... | 265 |
| 5.3 Editing Administrators | 266 |
| 5.4 Deleting an Administrator..... | 267 |
| 6 Settings..... | 268 |
| 6.1 Overview..... | 268 |
| 6.2 Organizations..... | 269 |
| 6.2.1 Section Overview..... | 269 |
| 6.2.1.1 Example Scenarios..... | 270 |
| 6.2.2 Organization Management..... | 272 |
| 6.2.2.1 Organizations Area Overview..... | 272 |
| 6.2.2.2 Summary of Fields and Controls..... | 273 |
| 6.2.2.3 Sorting and Filtering Options..... | 274 |
| 6.2.2.4 Creating a New Organization | 275 |
| 6.2.2.4.1 General Settings..... | 277 |
| 6.2.2.4.2 General Settings - Table of Parameters..... | 278 |
| 6.2.2.4.3 EV Details Tab..... | 278 |
| 6.2.2.4.4 EV Details - Table of Parameters..... | 280 |
| 6.2.2.4.5 Client Cert Settings Tab..... | 280 |
| 6.2.2.4.6 Client Certificate tab - Table of Parameters..... | 281 |
| 6.2.2.4.6.1 Customize an Organization's Client Certificate Types..... | 283 |
| 6.2.2.4.7 SSL Certificates Settings Tab..... | 286 |

| | |
|--|-----|
| 6.2.2.4.8 SSL Certificate tab - Table of Parameters..... | 287 |
| 6.2.2.4.8.1 Customize an Organization's SSL Certificate Types..... | 290 |
| 6.2.2.4.8.2 Customize an Organization's Server Software Types..... | 292 |
| 6.2.2.4.9 'Code Signing Certificates' Settings tab..... | 294 |
| 6.2.2.4.10 Code signing Certificates - Table of Parameters..... | 294 |
| 6.2.2.4.11 Device Certificate Settings Tab..... | 294 |
| 6.2.2.4.12 Device Certificates - Table of Parameters..... | 295 |
| 6.2.2.5 Editing an Existing Organization..... | 295 |
| 6.2.2.5.1 Imposing Access Restrictions to CCM interface | 297 |
| 6.2.2.5.2 Customizing Notification Email Templates..... | 299 |
| 6.2.2.6 Validating an Organization..... | 302 |
| 6.2.2.7 Managing the Departments of an Organization..... | 304 |
| 6.2.2.7.1 Departments Dialog - Table of Parameters..... | 304 |
| 6.2.2.7.2 Sorting and Filtering Options..... | 305 |
| 6.2.2.7.3 Creating Departments..... | 306 |
| 6.2.2.7.4 Editing Departments belonging to an Organization..... | 309 |
| 6.2.2.7.5 Managing Domains Belonging to a Department..... | 310 |
| 6.2.2.7.6 Deleting an Existing Department..... | 310 |
| 6.2.2.8 Managing the Domains of an Organization..... | 310 |
| 6.2.2.9 Deleting an Existing Organization..... | 311 |
| 6.3 Departments..... | 311 |
| 6.4 Domains..... | 312 |
| 6.4.1 Section Overview..... | 312 |
| 6.4.1.1 Wildcard Domains..... | 314 |
| 6.4.2 Domain Management..... | 314 |
| 6.4.2.1 The Domains Area..... | 314 |
| 6.4.2.1.1 Domain Delegations..... | 315 |
| 6.4.2.1.1.1 Summary of Fields and Controls..... | 315 |
| 6.4.2.1.1.2 Sorting and Filtering Options..... | 316 |
| 6.4.2.1.1.3 Tool Tip..... | 319 |
| 6.4.2.1.2 DCV..... | 319 |
| 6.4.2.1.2.1 Summary of Fields and Controls..... | 320 |
| 6.4.2.1.2.2 Sorting and Filtering Options..... | 320 |
| 6.4.2.2 Creating a New Domain..... | 322 |
| 6.4.2.2.1 Create Domain - Table of Parameters..... | 323 |
| 6.4.2.2.2 Validating Domains..... | 324 |
| 6.4.2.2.2.1 Changing DCV method for Validation Pending Domains..... | 330 |
| 6.4.2.3 Delegating/Re-delegating an Existing Domain | 330 |
| 6.4.2.4 Viewing, Validating and Approving Newly Created Domains..... | 331 |
| 6.4.2.4.1 View Domain - Summary of Fields and Controls..... | 332 |
| 6.4.2.4.2 Approval of Creation and Delegation of Domains..... | 333 |
| 6.4.2.4.3 Viewing Requisition and Approval Details of a Domain..... | 334 |

| | |
|---|-----|
| 6.4.2.4.4 Request Details - Table of Parameters..... | 335 |
| 6.5 Notifications..... | 336 |
| 6.5.1 Adding a Notification..... | 339 |
| 6.5.2 Notification Types..... | 343 |
| 6.5.2.1 'Client Certificate Expiration' Create Notification Form..... | 343 |
| 6.5.2.1.1 Table of Parameters..... | 344 |
| 6.5.2.2 'Client Certificate Revoked' Create Notification Form..... | 345 |
| 6.5.2.2.1 Table of Parameters..... | 346 |
| 6.5.2.3 'Code Signing Certificate Downloaded' Create Notification Form..... | 347 |
| 6.5.2.3.1 Table of Parameters..... | 347 |
| 6.5.2.4 'Code Signing Certificate Revoked' Create Notification Form..... | 348 |
| 6.5.2.4.1 Table of Parameters..... | 349 |
| 6.5.2.5 'Code Signing Certificate Expiration' Create Notification Form..... | 350 |
| 6.5.2.5.1 Table of Parameters..... | 351 |
| 6.5.2.6 'Code Signing Certificate Requested' Create Notification Form..... | 351 |
| 6.5.2.6.1 Table of Parameters..... | 352 |
| 6.5.2.7 'SSL Approved' Create Notification Form..... | 353 |
| 6.5.2.7.1 Table of Parameters..... | 354 |
| 6.5.2.8 'SSL Awaiting Approval' Create Notification Form..... | 354 |
| 6.5.2.8.1 Table of Parameters..... | 355 |
| 6.5.2.9 'SSL Declined' Create Notification Form..... | 356 |
| 6.5.2.9.1 Table of Parameters..... | 358 |
| 6.5.2.10 'SSL Expiration' Create Notification Form..... | 358 |
| 6.5.2.10.1 Table of Parameters..... | 360 |
| 6.5.2.11 'SSL Issuance Failed' Create Notification Form..... | 360 |
| 6.5.2.11.1 Table of Parameters..... | 361 |
| 6.5.2.12 'SSL Revoked' Create Notification Form..... | 362 |
| 6.5.2.12.1 Table of Parameters..... | 363 |
| 6.5.2.13 'Discovery Scan Summary' Create Notification Form..... | 364 |
| 6.5.2.13.1 Table of Parameters..... | 365 |
| 6.5.2.14 'Remote SSL Certificate Installed ' Create Notification Form..... | 366 |
| 6.5.2.14.1 Table of Parameters..... | 367 |
| 6.5.2.15 'Remote SSL Certificate Installation Failed' Create Notification Form..... | 368 |
| 6.5.2.15.1 Table of Parameters..... | 369 |
| 6.5.2.16 'Auto Installation/Renewal Failed' Create Notification Form..... | 370 |
| 6.5.2.16.1 Table of Parameters..... | 371 |
| 6.5.2.17 'Certificate Ready for Manual Installation' Create Notification Form..... | 373 |
| 6.5.2.17.1 Table of Parameters..... | 373 |
| 6.5.2.18 'Device Certificate Expiration' Create Notification Form | 375 |
| 6.5.2.18.1 Table of Parameters..... | 375 |
| 6.5.2.19 'Device Certificate Revoked' Create Notification Form..... | 376 |
| 6.5.2.19.1 Table of Parameters..... | 377 |

| | |
|---|-----|
| 6.5.2.20 'Device Certificate Awaiting Approval' Create Notification form..... | 378 |
| 6.5.2.20.1 Table of Parameters..... | 378 |
| 6.5.2.21 'Client Admin Creation' Create Notification Form..... | 379 |
| 6.5.2.21.1 Table of Parameters..... | 380 |
| 6.5.2.22 'Domain Awaiting Approval' Create Notification Form..... | 380 |
| 6.5.2.22.1 Table of Parameters..... | 382 |
| 6.5.2.23 'Domain Approved' Create Notification Form..... | 382 |
| 6.5.2.23.1 Table of Parameters..... | 384 |
| 6.5.2.24 'DCV Expiration' Create Notification Form..... | 384 |
| 6.5.2.24.1 Table of Parameters..... | 385 |
| 6.5.2.25 'DCV Validated' Create Notification Form..... | 386 |
| 6.5.2.25.1 Table of Parameters..... | 387 |
| 6.5.2.26 'DCV Needed-New Domain' Create Notification Form..... | 388 |
| 6.5.2.26.1 Table of Parameters..... | 389 |
| 6.5.2.27 'Code Sign Request Created' Create Notification Form..... | 389 |
| 6.5.2.27.1 Table of Parameters..... | 390 |
| 6.5.2.28 Code Signing CSoD Revoked Create Notification Form..... | 391 |
| 6.5.2.28.1 Table of Parameters..... | 391 |
| 6.6 Encryption and Key Escrow..... | 392 |
| 6.6.1 Introduction and Basic Concepts..... | 392 |
| 6.6.2 Setting up Key Escrow for an Organization..... | 392 |
| 6.6.3 Setting up Key Escrow for a Department..... | 394 |
| 6.6.4 Master Keys Required Prior to Client Cert Issuance..... | 395 |
| 6.6.5 Encryption..... | 397 |
| 6.6.5.1 Summary of Fields and Controls..... | 397 |
| 6.6.6 Encrypting the Private Keys..... | 398 |
| 6.6.7 Re-encryption..... | 399 |
| 6.6.8 Recovering a User's Private Key from Escrow..... | 402 |
| 6.7 Access Control..... | 403 |
| 6.7.1 Overview..... | 403 |
| 6.7.1.1 Access Control Options - Table of Parameters..... | 404 |
| 6.7.1.2 Filtering Options..... | 404 |
| 6.7.2 Adding a New IP Range..... | 405 |
| 6.7.2.1 Add IP Range - Table of Parameters..... | 406 |
| 6.7.3 Editing an IP Range..... | 407 |
| 6.8 Private Key Store..... | 407 |
| 6.8.1 Setting-up the Private Key Store..... | 408 |
| 6.8.2 Uploading Private Keys | 411 |
| 6.8.3 Downloading the Private Key of a Certificate..... | 414 |
| 6.8.4 Backup/Restore for the Private Key Store | 417 |
| 6.8.5 Removing Keys from Key Store..... | 418 |
| 6.8.6 Viewing Activities of the Controller..... | 419 |

| | |
|--|-----|
| 6.9 Certificates..... | 420 |
| 6.9.1 Section Overview..... | 420 |
| 6.9.2 SSL Types..... | 421 |
| 6.9.2.1 Customize SSL Certificate Types..... | 422 |
| 6.9.3 Client Cert Types..... | 424 |
| 6.9.3.1 Customize Client Certificate Types..... | 426 |
| 6.9.4 Device Cert Types..... | 427 |
| 6.9.4.1 Adding Device Cert Types..... | 429 |
| 6.9.4.2 Editing and Deleting a Device Cert Type..... | 430 |
| 6.9.5 Custom Fields..... | 432 |
| 6.9.5.1 Adding a new Custom Field..... | 433 |
| 6.9.5.2 Editing an Existing Custom Field..... | 435 |
| 6.9.5.3 Removing an Existing Custom Field..... | 436 |
| 6.10 Mapping MS AD Certificate Templates to CCM Certificate Types..... | 437 |
| 6.10.1 Configuring Custom MS AD Certificate Templates on AD server..... | 439 |
| 6.10.2 The 'MS AD Certificate Mapping' Area..... | 441 |
| 6.10.3 Adding MS AD Certificate Template Mapping..... | 444 |
| 6.10.4 Editing MS AD Certificate Template..... | 445 |
| 6.10.5 Deleting MS AD Certificate Template..... | 446 |
| 6.11 Email Templates..... | 446 |
| 6.11.1 Viewing and Editing the Email Templates..... | 447 |
| 6.12 MS Agents for AD server Integration..... | 449 |
| 6.13 Auto-Assignment Rules for Unmanaged Certificates..... | 456 |
| 7 Certificate Discovery and Agents..... | 461 |
| 7.1 Network Assets..... | 461 |
| 7.1.1 Network Discovery..... | 462 |
| 7.1.2 Web Servers..... | 470 |
| 7.1.3 Active Directory..... | 472 |
| 7.2 Discovery Tasks..... | 474 |
| 7.2.1 Sorting and Filtering Options..... | 476 |
| 7.2.2 Prerequisites..... | 477 |
| 7.2.3 Overview of Process..... | 477 |
| 7.2.4 Adding IP Range and Start Scanning..... | 477 |
| 7.2.5 Editing a Discovery Task..... | 484 |
| 7.2.6 Deleting a Discovery Task..... | 485 |
| 7.2.7 Viewing History of Discovery Tasks..... | 486 |
| 7.2.8 View Scan Results..... | 489 |
| 7.3 Agents..... | 492 |
| 7.3.1 Sorting and Filtering Options..... | 494 |
| 7.3.2 Configuring the Agent for Auto-Installation and Internal Scanning - Overview of the Process..... | 495 |
| 7.3.3 Prerequisites..... | 496 |
| 7.3.4 Configuring the Agent for Auto-Installation and Internal Scanning - Detailed Explanation of the | |

| | |
|---|-----|
| Process..... | 496 |
| 7.3.5 Configuring the Certificate Controller Agent through Web Interface..... | 505 |
| 7.3.5.1 Agent Configuration..... | 506 |
| 7.3.5.2 Server Management..... | 510 |
| 8 Reports..... | 514 |
| 8.1 Overview..... | 514 |
| 8.2 Reports - Security Roles Access Table..... | 517 |
| 8.3 Activity Log Report..... | 518 |
| 8.3.1 Report Type: Activity Log - Table of Parameters..... | 518 |
| 8.4 Client Certificates Reports..... | 519 |
| 8.4.1 Report Type: Client Certificates - Table of Parameters..... | 519 |
| 8.5 Discovery Scan Log Reports..... | 521 |
| 8.5.1 Discovery Scan Log Report: Summary type..... | 521 |
| 8.5.1.1 Report Type: Discovery Scan Log :Summary - Table of Parameters..... | 522 |
| 8.5.2 Discovery Scan Log Report: Detail type..... | 523 |
| 8.5.2.1 Report Type: Discovery Scan Log :Detail - Table of Parameters..... | 524 |
| 8.6 SSL Certificates Reports..... | 524 |
| 8.6.1 Report Type: SSL Certificates - Table of Parameters..... | 525 |
| 8.7 Code Signing Certificates Report..... | 526 |
| 8.7.1 Report Type: Code Signing Certificates - Table of Parameters..... | 527 |
| 8.8 Code Signing Requests Report..... | 528 |
| 8.8.1 Report Type: Code Signing Requests - Table of Parameters..... | 529 |
| 8.9 Admins Report..... | 530 |
| 8.10 XML Data Report..... | 530 |
| 8.11 DCV Report..... | 531 |
| 8.11.1 Report Type: DCV Report - Table of Parameters..... | 531 |
| 8.12 Agent Log Events Report..... | 533 |
| 8.13 Notification Log Statistics Report..... | 534 |
| 8.13.1 Notification Log Statistics - Email..... | 534 |
| 8.13.1.1 Report Type: Notification Log Statistics :Emails - Table of Parameters..... | 534 |
| 8.13.2 Notification Log Statistics - Notification Type..... | 535 |
| 8.13.2.1 Report Type: Notification Log Statistics :Notification Type - Table of Parameters..... | 535 |
| 8.13.3 Notification Log Statistics - Full Log..... | 535 |
| 8.13.3.1 Report Type: Notification Log Statistics :Full Log - Table of Parameters..... | 536 |
| 8.14 Private Key Controller Activity Log..... | 536 |
| 8.14.1 Report Type: Private Key Controller Activity Log - Table of Parameters..... | 537 |
| 8.15 Discovery Tasks Report..... | 537 |
| 8.16 Device Certificate Reports..... | 538 |
| 8.16.1 Report Type: Device Certificates - Table of Parameters..... | 538 |
| 9 Version and Feature Information..... | 540 |
| 10 My Profile..... | 540 |
| 11 Logging Out of Comodo Certificate Manager..... | 542 |

| | |
|--|-----|
| Appendix 1 - Your responsibilities when ordering SSL Certificates..... | 543 |
| Appendix 2 - Private Certificates for Internal Hosts..... | 544 |
| About Comodo..... | 545 |

1 Introduction to Comodo Certificate Manager

Comodo Certificate Manager (CCM) centralizes and streamlines the life-cycle management of web server, S/MIME, code signing and device authentication certificates through a unified interface. The system features full integration with Comodo Certificate Authority and enables nominated administrators to manage the lifespan, issuance, deployment, renewal and revocation of certificates on an Organization, Department and per-user basis. By consolidating and automating the often disparate processes involved in complex enterprise wide PKI deployments, CCM reduces the need for manual certificate management and thus creates a more efficient, productive and secure certification environment.

1.1 Guide Structure

This guide is intended to take you through the step-by-step process of Organization, configuration and use of Comodo **Certificate Manager** service.

- Section 1, **Introduction to Comodo Certificate Manager** - Contains a high level overview of the solution and serves as an introduction to the main themes and concepts that are discussed in more detail later in the guide - including security roles, Organizations, Reports and a summary of the main areas of the interface.
- Section 2, **The Dashboard** - Contains an overview of the dashboard that provides an at-a-glance graphical summary of key life-cycle information (such as certificates approaching expiry, certificates issued/requested and DCV status).
- Section 3, **Certificates Management** - Contains an overview of the area's main functionality and detailed explanations on how to request, collect and manage SSL certificates for web servers and hosts, client certificates for employees and corporate clients (end-users) and code signing certificates for digitally signing executables and scripts.
- Section 4, **Code Signing on Demand** - Contains an overview of the area's main functionality and detailed explanations on how to enroll developers, issue code signing certificates for them and code signing executables and script files without the need for developer downloading their certificate. The feature is available only if enabled for your account. Contact your Comodo Account manager if you wish to enable this feature for you.
- Section 5, **Admin Management** - Covers the creation and management of Certificate Manager Administrators and the assigning of privileges and responsibilities to those Administrators.
- Section 6, **Settings** - Contains overviews and tutorials pertaining to the functional areas housed under the 'Settings' tab, including guidance on how to create a **new Organization**, **manage Organizations**, **add domains** and associate them with an Organization or Department, limit which IP addresses can access the CCM interface in **Access Control**, set up **Notifications**, setting up a **Private Key Store**, customize overall and Organization based **SSL types** availability and manage **Encryption** settings. To view detailed information about each area, click on the links below:
 - **Organizations** (including full details on how to **Manage and Create Organizations**)
 - **Departments**
 - **Domains**
 - **Encryption and Key Escrow**
 - **Notifications**
 - **Access Control**
 - **Private Key Store**

- **Certificates**
- **Email Templates**
- **MS Agents for AD Server Integration**
- **Auto-Assignment Rules for Unmanaged Certificates**
- Section 7, **Certificate Discovery** - explains how to scan and monitor a network for all installed SSL certificates including certificates that may or may not have been issued using CCM, any third party vendor certificates and any self-signed certificates. This section also explains how to download and install agents that are used for automatic installation of certificates and for certificate scan.
- Section 8, **The Reports section** - Contains an overview of the area, descriptions of each report type and guidance on how to access the required report type.
- Section 9, **Version and Feature information** - explains how to view the version of CCM and the features enabled for the subscription.
- Section 10, **My Profile** - explains how to changes the time format and the password.
- Section 11, **Logging out of Comodo Certificate Manager** explains the process for logging out.
- Appendix 1 - **Your responsibilities when ordering SSL Certificate** contains a very short summary of certificate issuance guidelines.

1.2 Definitions of Terms

1.2.1 Organizations and Departments

Organizations and Departments are created by administrators for the purposes of requesting, issuing and managing Comodo digital certificates. Each Organization can have multiple Departments.

Organizations are typically managed by a Registration Authority Officer (RAO) while Departments are typically managed by a Domain Registration Authority Officer (DRAO). A Master Registration Authority Officer (MRAO) can manage all Organizations and all Departments.

Once an Organization or Department has been created:

- Appropriately privileged officers can request and delegate domains to that Organization/Department
- Appropriately privileged officers can request, approve/decline requests and manage certificates on behalf of that Organization or Department.
- End-users can enroll into (or be assigned membership of) that Organization or Department and be provisioned with client certificates

1.2.2 Certificate Types

Comodo Certificate Manager can be used to request and manage the following types of digital certificate:

SSL Certificates - SSL Certificates are used to secure communications between a website, host or server and end-users that are connecting to that server. An SSL certificate will confirm the identity of the Organization that is operating the website; encrypt all information passed between the site and the visitor and will ensure the integrity of all transmitted data.

Client Certificates - Client certificates are issued to individuals and can be used to encrypt and digitally sign email messages; to digitally sign documents and files and to authenticate the identity of an individual prior to granting them access to secure online services.

Code Signing Certificates - Code Signing Certificates are used to digitally sign software executables and scripts. Doing so helps users to confirm that the software is 'genuine' by verifying content source (authentication of the publisher of the software) and content integrity that the software has not been modified, corrupted or hacked since

the time it was originally signed.

Device Certificates - Device authentication certificates are issued to desktop and mobile devices to authenticate those devices to networks and VPNs. Device certificates can be issued to devices that are enrolled to an AD server via NDES; by over-the-air enrollment through SCEP, by API integration or by self-enrollment form.

1.2.3 Administrative Roles

There are 3 classes of Administrator in Comodo Certificate Manager:

- **Master Registration Authority Officer (MRAO)** - The highest level of administrator in Comodo Certificate Manager (CCM) is the Master Registration Authority Officer (MRAO). An MRAO has access to all functional areas and may delegate control over the certificates, domains and notifications of any Organization or Department. An MRAO also has full rights over the creation and privileges of Registration Authority Officers (RAOs), Department Registration Authority Officers (DRAOs) and end-users of any Organization or Department.
- **Registration Authority Office (RAO)** - A Registration Authority Officer (RAO) is an administrative role created by an MRAO for the purposes of managing the certificates and end-users belonging to one or more CCM Organizations. They have control over the certificates that are ordered on behalf of their Organization(s); over Domains that have been delegated to their Organization/Dept by an MRAO; over any Departments of their Organization and over that Organization's end-user membership. RAOs can also create peer RAOs for their Organizations and edit or remove existing RAOs of their Organizations, if appropriate privileges are assigned by the MRAO.
- **Department Registration Authority Officer (DRAO)** - Department Registration Authority Officers are created by, and subordinate to, the RAO class of Administrator. They are assigned control over the certificates, users and domains belonging to a Department(s) of an Organization. DRAOs can also create peer DRAOs for their Departments and edit or remove existing RAOs of their Departments, if appropriate privileges are assigned by the MRAO or RAO.

The RAO and DRAO class of administrator are sub-divided into specific roles by certificate type:

- **RAO SSL administrators**
- **RAO S/MIME administrators**
- **RAO Code Signing administrators**
- **RAO Device Cert administrators**
- **DRAO SSL administrators**
- **DRAO S/MIME administrators**
- **DRAO Code Signing administrators**
- **DRAO Device Cert administrators**

Therefore, the privileges of any particular RAO or DRAO administrator are broadly defined by the elements described in sections **1.2.1**, **1.2.2** and **1.2.3**:

1. The Organization or Department that they are delegated to
2. The specific type of certificate that they are delegated responsibility for
3. Their specific administrative class (whether they are an RAO or a DRAO)

CCM also uses the following terms to identify personnel:

- **End-User**
- **Owner**
- **Requester**
- **Developer**

The following table contains detailed summaries of the privileges that apply to each type of administrator and also features descriptions of the 'end-user', 'owner', 'requester' and 'Developer' types of personnel.

MRAO Administrator

| Security Role / Type of Administrator | Definition |
|---|--|
| <p>MRAO (Master Registration Authority Officer)</p> | <p>The MRAO is the top level administrator and can access all areas and functionality of the Certificate Manager interface.</p> <ul style="list-style-type: none"> • MRAOs have full visibility of and control over the provisioning and life-cycle management of all certificate types • New MRAOs can only be created and managed by an existing MRAO. • MRAO level administrators are visible only to other MRAOs in the 'Admin Management' area of the CCM interface. • MRAO admins can create new Organizations and Departments and delegate them to RAO and DRAO class administrators respectively. • MRAO admins can initiate the process of validating Organizations for the purpose of requesting and issuance of OV SSL certificates to Organizations and Departments under them. • MRAOs are able to create and manage RAO and DRAO class administrators for any Organization or Department • MRAOs have full access and executive rights to add, modify and delegate Domains to any Organization or Department • MRAO can initiate Domain Control Validation (DCV) process on any domain added to any Organization or Department • MRAOs can view any type of Report for any Organization or Department • MRAOs can setup Certificate Controller Agents on a local network for any Department or Organization. Agents allows admins to scan internal hosts for installed SSL certificates which can then be tracked using the CCM admin console. Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat and IIS web servers. • MRAOs can setup a Private Key Store on their local network to store and manage the private keys of certificates managed by CCM. The Private Key Store requires a controller installed on a local server. Once installed, the controller is responsible for receiving commands for storing private keys and for generating CSRs for certificates created using the Auto CSR generation feature. • MRAOs can enable RAO S/MIME and DRAO S/MIME types of administrator with the ability to recover the private keys of client certificates for those Organizations / Departments that they administer. • If desired, it is possible for MRAO Administrators to recover |

| Security Role / Type of Administrator | Definition |
|---------------------------------------|--|
| | <p>from escrow the private keys of client certificates that belong to any Organization or Department with key recovery (escrow) enabled on them.</p> <ul style="list-style-type: none"> • MRAOs can view Activity Logs for all Organizations and Departments • MRAOs are the only individuals with sufficient privileges to manage 'SSL Types' and 'Client Cert Types'. • MRAOs have privileges to add custom fields in the Built-in Application and Self-Enrollment Forms for SSL and Client certificates requisition. • MRAOs can request their account manager for different types of client certificates with different capabilities to be added to their account. For example, 'Signing Only', 'Encryption Only', 'Dual Use' (Signing + Encryption), 'Smart Card Logon and Authentication' and more. It is also possible to create custom client certificate types with combinations of capabilities. MRAOs can restrict issuance of types of client certificates to end-users on per-organization basis. • MRAOs can setup/configure the Code Signing on Demand (CSD) service / controller, can create developers and approve code signing requests generated by developers for all the Organizations and Departments. (Applicable only if CSD service is enabled for your account) • MRAOs can integrate AD servers belonging to any Organization or Department by installing an MS Agent. • MRAOs can view network assets such as certificates installed on various endpoints as identified by manual or scheduled discovery scans. • MRAOs can view AD objects and certificates installed on them which were identified by scans run by the MS agent. • MRAOs can map MS AD certificate templates from an AD server to private CA Certificate types in CCM, enabling CCM to issue private certificates with custom parameters. Custom parameters include key usage, extended key usages, key sizes, validity period and so on. • MRAOs can assign unmanaged certificates identified by discovery/AD server scans to Organizations and Departments and so bring them under CCM management. • MRAOs can approve device certificate requests from MS Agents (installed on AD servers with AD CS/NDES role) or requested directly from Devices via SCEP • MRAOs can enable Organizations / Departments for enrollment of device certificates via SCEP |

RAO Administrators

| Security Role / Type of Administrator | Definition |
|---|--|
| <p>RAO SSL (Registration Authority Officer - SSL Certificates)</p> | <p>Administrators with the security role 'RAO SSL' have privileges to request and manage SSL certificates for domains that have been delegated to their Organization</p> <ul style="list-style-type: none"> • RAO SSL admins have visibility and control over SSL certificates that belong to their delegated Organization. They can approve or decline requests for SSL certificates made using the Self-Enrollment form for their Organization(s) and sub-ordinate Department(s). • They have no access to manage SSL certificates belonging to Organizations for which they have not been granted permissions. • RAO SSL admins can only manage SSL Certificates and have no privileges to manage other certificate types (such as client certificates, code signing certificates and device certificates) - including those that belong to the Organization that he or she is the SSL Administrator of. • RAO SSL admins will see only those Organizations that have been delegated to them in the 'Organizations' area. • RAO SSL admins can upload private keys of SSL certificates belonging to their organizations and their sub-ordinate departments for management by Private Key Store, configured in the local network. They can also download the private keys of the certificates. • It is possible for a MRAO to make the same individual as an 'RAO S/MIME ' an 'RAO SSL' AND an RAO Code Signing for an single Organization during the Administrator creation or editing process (for more details, see section Admin Management). • RAO SSL admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those Organizations of which they are SSL Certificate administrator. • RAO SSL administrators can create Departments only within Organizations that have been delegated to them • RAO SSL admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow RAO SSL admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them • Request and approve the creation of DRAO SSL admins • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them • Cannot request or approve creation of |

| Security Role / Type of Administrator | Definition |
|---|--|
| | <p>administrators of any other certificate type - even for those Organizations that have been delegated to them</p> <ul style="list-style-type: none"> • RAO SSL admins can delegate Domains to sub-ordinate Departments of Organizations that they administrate. • RAO SSL admins can initiate DCV process for the Domains delegated to sub-ordinate Departments of Organizations that they administrate if they were given 'Allow DCV' privileges. RAO SSL with 'Allow DCV' privileges can be created only by the MRAO. • RAO SSL Admins can setup Certificate Controller Agents in a local network for scanning internal hosts with internally facing IP addresses for installed SSL certificates for the Organization(s) that are delegated to them and any sub-ordinate Departments there of. Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat and IIS web servers. • RAO SSL Admins can view the network assets like certificates installed on various servers and endpoints and web servers with websites/domains hosted on them, as identified by manual or scheduled discovery scans configured for the networks belonging to their Organizations (and their sub-ordinate Departments). • RAO SSL Admins can assign unmanaged SSL certificates identified by discovery scans and AD server scans to their Organizations and Departments, in order to bring them under management through CCM. • RAO SSL admins can view the SSL certificates Reports and Certificate Discovery Reports for the Organization that they were assigned rights to. • RAO SSL admins cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with the 'RAO SMIME' role. • RAO SSL admins can only view Activity Logs for their Organization(s). • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| <p>RAO S/MIME (Registration Authority Officer - S/MIME Certificates)</p> | <p>Administrators with the security role 'RAO S/MIME' have privileges to access, manage, request and approve the requests of Client Certificates for domains that have been delegated to their Organization</p> <ul style="list-style-type: none"> • RAO S/MIME admins have visibility and control over the client certificates belonging to End-Users of the Organizations for which they have been assigned rights. They have no access to manage the Client Certificates of End-Users that belong to Organizations which they have not |

| Security Role / Type of Administrator | Definition |
|---------------------------------------|--|
| | <p>been granted permissions.</p> <ul style="list-style-type: none"> • RAO S/MIME admins can only manage S/MIME certificates and have no privileges to manage other certificate types (such as SSL Certificates, Code Signing Certificates and Device certificates) - including those that belong to the Organization of which they are S/MIME Administrator. • It is possible for a MRAO to make the same individual an 'RAO S/MIME ' an 'RAO SSL' an RAO Code Signing AND an RAO Device Cert for a single Organization during the Administrator creation or editing process (for more details, see section Admin Management). • RAO S/MIME admins will see only those Organizations that have been delegated to them in the 'Organizations' area. • RAO S/MIME admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those Organizations of which they are S/MIME administrator. • RAOs can request MRAO or their Account Manager for different types of client certificates with different capabilities to be added to their Organization. For example, 'Signing Only', 'Encryption Only', 'Dual Use' (Signing + Encryption), 'Smart Card Logon and Authentication' and more. It is also possible to create custom client certificate types with combinations of capabilities. RAOs can also restrict issuance of types of client certificates to end-users belonging to their organization. • RAO S/MIME administrators can create Departments only within Organizations that have been delegated to them • RAO S/MIME admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow RAO S/MIME admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them • Request and approve the creation of DRAO S/MIME admins • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them • Cannot request or approve creation of administrators of any other certificate type - even for those Organizations that have been delegated to them • RAO S/MIME admins can delegate Domains to sub-ordinate Departments of Organizations that they administrate. • When creating a new Department, an RAO S/MIME admin |

| Security Role / Type of Administrator | Definition |
|---|--|
| | <p>can:</p> <ul style="list-style-type: none"> • Enable or disable the ability of MRAOs to recover the private keys of client certificates that belong to this Department • Enable or disable the ability of RAO S/MIME admins (themselves) to recover the private keys of client certificates that belong to this Department • Enable or disable the ability of DRAO S/MIME admins to recover the private keys of client certificates that belong to this Department • All or any combination of the above • RAO S/MIME admins can only view Activity Logs for their Organization. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| <p>RAO Code Signing (Registration Authority Officer - Code Signing Certificates)</p> | <p>Administrators with the security role 'RAO Code Signing' have privileges to access, manage, request and approve the requests of Code Signing Certificates for domains that have been delegated to their Organization</p> <ul style="list-style-type: none"> • RAO Code Signing Administrators have visibility and control over the code signing certificates belonging to End-Users of the Organization for which they have been assigned rights. They have no access to manage the Code Signing Certificates of End-Users that belong to Organizations of which they have not been granted permissions. • RAO Code Signing admins can only manage Code Signing Certificates. They have no privileges to manage other types such as SSL, S/MIME or Device certificates - including those SSL/S/MIME/Device certificates belonging to the Organization of which they are Code Signing Certificate Administrator. • It is possible for a MRAO to make the same individual an 'RAO S/MIME' an 'RAO SSL' an RAO Code Signing AND an RAO Device Cert for a single Organization during the Administrator creation or editing process (for more details, see section Admin Management). • RAO Code Signing admins will see only those Organizations that have been delegated to them in the 'Organizations' area. • RAO Code Signing admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those Organizations of which they are Code Signing Certificate administrator. • RAO Code Signing administrators can create Departments only within Organizations that have been delegated to them |

| Security Role / Type of Administrator | Definition |
|---|---|
| | <ul style="list-style-type: none"> • RAO Code Signing admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow RAO Code Signing admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them • Request and approve the creation of DRAO Code Signing admins • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them • Cannot request or approve creation of administrators of any other certificate type - even for those Organizations that have been delegated to them • RAO Code Signing admins can delegate Domains to sub-ordinate Departments of Organizations that they administrate. • RAO Code Signing admins can create developers for Code Signing on Demand (CSD) service and approve code signing requests generated by developers only for the Organization(s) (and their sub-ordinate Departments) that are delegated to them. (Applicable only if CSD service is enabled for your account) • RAO Code Signing admins can only view Activity Logs for their Organization. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| <p>RAO Device Cert (Registration Authority Officer - Device Certificates)</p> | <p>Administrators with the security role 'RAO Device Cert' have privileges to access, manage, request and approve the requests of Device Certificates for devices enrolled to the Active Directory servers or networks belonging to the Organization(and their sub-ordinate Departments) delegated to them.</p> <ul style="list-style-type: none"> • RAO Device Cert admins have visibility and control over the device certificates issued to the devices belonging to the Organization for which they have been assigned rights. They have no access to manage the device certificates that belong to Organizations of which they have not been granted permissions. • RAO Device Cert admins can only manage device certs. They have no privileges to manage other types such as SSL S/MIME or code signing certificates - including those SSL/S/MIME/code signing certificates belonging to the Organization of which they are Device Certificate Administrator. |

| Security Role / Type of Administrator | Definition |
|---------------------------------------|---|
| | <ul style="list-style-type: none"> • It is possible for a MRAO to make the same individual an 'RAO S/MIME' an 'RAO SSL' an RAO Code Signing AND RAO Device Cert for a single Organization during the Administrator creation or editing process (for more details, see section Admin Management). • RAO Device Cert admins will see only those Organizations that have been delegated to them in the 'Organizations' area. • RAO Device Cert admins cannot create new Organizations. Neither can they edit the General settings of any Organization - even those Organizations of which they are Device Certificate administrator. • RAO Device Cert administrators can create Departments only within Organizations that have been delegated to them • RAO Code Signing admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow RAO Device Cert admins only for Organizations that have been delegated to them if MRAO has enabled this feature for them • Request and approve the creation of DRAO Device Cert admins • Cannot request or approve the creation of any type of administrator for Organizations that have not been delegated to them • Cannot request or approve creation of administrators of any other certificate type - even for those Organizations that have been delegated to them • RAO Device Cert Admins can delegate Domains to subordinate Departments of Organizations that they administrate. • RAO Device Cert admins can approve requests for device certificates from MS Agents (installed on AD servers with AD CS/NDES role) or directly from the Devices through SCEP for request and issuance of Device Certificates. • RAO Device Cert admins can enable their Organizations / Departments for enrollment of device certificates via SCEP • RAO Device Cert admins can only view Activity Logs for their Organization. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |

DRAO Administrators

| Security Role / Type of Administrator | Definition |
|---|--|
| <p>DRAO SSL (Department Registration Authority Officer - SSL Certificates)</p> | <p>Administrators with the security role 'DRAO SSL' have privileges to access, manage and request SSL certificates for domains that have been delegated to their Department by an RAO or MRAO</p> <ul style="list-style-type: none"> • DRAO SSL admins have visibility and control over SSL certificates that belong to their delegated Department(s). A DRAO SSL admin can only request SSL certificates for domains that have been delegated to their Department. They can approve or decline requests for SSL certificates made using the Self-Enrollment form for their Department(s). • They have no access to manage SSL certificates belonging to Departments for which they have not been granted permissions. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs. • DRAO SSL admins have no visibility of and cannot request certificates of any other type - including those other certificate types that belong to the Department of which they are DRAO SSL . • DRAO SSL admins can upload private keys of SSL certificates belonging to their departments for management by Private Key Store, configured in the local network. They can also download the private keys of the certificates. • It is possible for an RAO to make the same individual a 'DRAO S/MIME' , 'DRAO SSL', 'DRAO Code Signing' AND/OR DRAO Device Cert for a single Department during the Admin creation or editing process (for more details, see section Admin Management). • DRAO SSL admins cannot request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow DRAO SSL admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them • Cannot request the creation of any type of administrator for Departments that have not been delegated to them • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them • DRAO SSL admins can request the addition of new Domains only for to Departments that have been delegated to them. • DRAO SSL admins can initiate DCV process for the Domains delegated to their Department(s) they administrate if they were given 'Allow DCV' privileges. DRAO SSL admin with such privileges can be created only by MRAO or RAO |

| Security Role / Type of Administrator | Definition |
|---|--|
| | <p>SSL having the same privilege.</p> <ul style="list-style-type: none"> • DRAO SSL Admins can setup Certificate Controller Agents in a local network for scanning internal hosts with internally facing IP addresses for installed SSL certificates for the Department(s) that are delegated to them. Agents also facilitate the automatic installation of SSL certificates on Apache, Apache Tomcat and IIS web servers. • DRAO SSL Admins can view the network assets like certificates installed on various servers and endpoints and web servers with websites/domains hosted from them, as identified by manual or scheduled discovery scans run on networks belonging to their department. • DRAO SSL Admins can assign unmanaged SSL certificates identified from discovery scans to their Department, to bring them under management through CCM. • DRAO SSL admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them. • DRAO SSL admins cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with 'DRAO S/MIME' role. • DRAO SSL admins cannot view Activity Logs. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| <p>DRAO S/MIME (Department Registration Authority Officer - S/MIME Certificates)</p> | <p>Administrators with the security role 'DRAO S/MIME' have privileges to access, manage and request Client Certificates for domains that have been delegated to their Department by an RAO or MRAO</p> <ul style="list-style-type: none"> • DRAO S/MIME admins have visibility over the client certificates belonging to end-users of the Department(s) which have been delegated to them. They have no access to manage the Client Certificates of end-users that belong to Departments which they have not been delegated. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs. • A DRAO S/MIME admin can only request S/MIME certificates for domains that have been delegated to their Department. • DRAO S/MIME admins have no visibility of and cannot request certificates of any other type - including those other certificate types that belong to the Department of which they are DRAO S/MIME. • It is possible for an RAO to make the same individual a 'DRAO S/MIME' , 'DRAO SSL', 'DRAO Code Signing' AND/OR DRAO Device Cert for a single Department during the Admin creation or editing process (for more details, see |

| Security Role / Type of Administrator | Definition |
|---|--|
| | <p>section Admin Management).</p> <ul style="list-style-type: none"> • DRAO S/MIME admins cannot request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow DRAO S/MIME admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them • Cannot request the creation of any type of administrator for Departments that have not been delegated to them • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them • DRAO S/MIME admins can request the addition of new Domains only for to Departments that have been delegated to them. • If enabled for their Department, a DRAO S/MIME admin can recover the private keys of client certificates belonging to their Department • DRAO S/MIME admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them. • DRAO S/MIME admins cannot view Activity Logs. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| <p>DRAO Code Signing (Department Registration Authority Officer - Code Signing Certificates)</p> | <p>Administrators with the security role 'DRAO Code Signing' have privileges to access, manage and request Code Signing certificates for Departments of an Organization that have been delegated to them by an RAO or MRAO.</p> <ul style="list-style-type: none"> • DRAO Code Signing admins have visibility of and can request Code Signing certificates for the Department(s) that have been delegated to them. They have no access to manage Code Signing certificates belonging to Departments for which have not been delegated to them. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs. • A DRAO Code Signing admin can only request Code Signing certificates for domains that have been delegated to their Department. • DRAO Code Signing admins have no visibility of and cannot request certificates of any other type - including those other types of certificate that belong to the Department of which they are DRAO Code Signing. • It is possible for an RAO to make the same individual a 'DRAO S/MIME' , 'DRAO SSL' , 'DRAO Code Signing' |

| Security Role / Type of Administrator | Definition |
|--|--|
| | <p>AND/OR DRAO Device Cert for a single Department during the Admin creation or editing process (for more details, see section Admin Management).</p> <ul style="list-style-type: none"> • DRAO Code Signing admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow DRAO Code Signing admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them • Cannot request the creation of any type of administrator for Departments that have not been delegated to them • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them • DRAO Code Signing admins can request the creation of new Domains only for Departments that have been delegated to them. • DRAO Code Signing admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them. • DRAO Code Signing Administrators cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with DRAO S/MIME role. • DRAO Code Signing admins can create developers for Code Signing on Demand (CSD) service and approve code signing requests generated by developers only for the Department(s) that are delegated to them. (Applicable only if CSD service is enabled for your account) • DRAO Code Signing Administrators cannot view Activity Logs. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| <p>DRAO Device Cert (Department Registration Authority Officer - Device Certificates)</p> | <p>Administrators with the security role 'DRAO Device Cert' have privileges to access, manage and request Device certificates for Departments of an Organization that have been delegated to them by an RAO or MRAO.</p> <ul style="list-style-type: none"> • DRAO Device Cert admins have visibility of and can approve device certificate requests for the Department(s) that have been delegated to them. They have no access to manage device certificates belonging to Departments for which have not been delegated to them. They will only see their own Departments(s) listed in the 'Departments' area. The 'Organizations' area is not visible to DRAOs. |

| Security Role / Type of Administrator | Definition |
|---------------------------------------|--|
| | <ul style="list-style-type: none"> • DRAO Device Cert admins have no visibility of and cannot request certificates of any other type - including those other types of certificate that belong to the Department of which they are DRAO Device Cert. • It is possible for an RAO to make the same individual a 'DRAO S/MIME', 'DRAO SSL', 'DRAO Code Signing' AND/OR DRAO Device Cert for a single Department during the Admin creation or editing process (for more details, see section Admin Management). • DRAO Device Cert admins cannot approve or request the creation of administrators that have more privileges than themselves. They can: <ul style="list-style-type: none"> • Request the creation of fellow DRAO Device Cert admins only for Departments that have been delegated to them if the RAO administrator has enabled this feature for them • Cannot request the creation of any type of administrator for Departments that have not been delegated to them • Cannot request creation of administrators of any other certificate type - even for those Departments that have been delegated to them • DRAO Device Cert Admins can request the creation of new Domains only for Departments that have been delegated to them. • DRAO Device Cert admins can view Reports, edit Access Control Lists and modify Email Templates for the Department that has been delegated to them. • DRAO Device Cert Administrators cannot access or manage 'Settings' > 'Encryption' as this can only be managed by those with DRAO S/MIME role. • DRAO Device Cert Admins cannot view Activity Logs. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |

End-User, Owner, Requester and Developer

| Security Role / Type of Administrator | Definition |
|---------------------------------------|--|
| <p>End-User</p> | <p>An End-User in CCM is a person that has been issued with or requested a Client Certificate or has made an application for an SSL certificate using the Self Enrollment form.</p> <ul style="list-style-type: none"> • 'End-Users' have no access rights whatsoever to the CCM interface. They exist in CCM only as a function of their |

| Security Role / Type of Administrator | Definition |
|---------------------------------------|---|
| | <p>request for or ownership of a client certificate.</p> <ul style="list-style-type: none"> • A new end-user and the Client Certificate for that end-user can be created in CCM via: <ul style="list-style-type: none"> • Manual creation by a Administrator in the 'Client Certificate' area; • The End-User ordering a Client Certificate using the Self Enrollment Form; • End-User is imported into CCM from .csv file. • A new end-user will also be added via SSL certificate applications made through the self enrollment form. If the applicant does not already exist as an end-user then Comodo Certificate Manager will automatically add this applicant when the form is submitted. End- Users that are auto-created in this way will not (yet) have a Client Certificate. • All end-users and Client Certificates owned or requested by that end-user are listed in the 'Client Cert' sub-tab of the 'Certificates' section of CCM interface. • An 'at-a-glance' summary of Administrator security roles and access rights is available here. |
| Owner | <p>The Owner of the certificate is the Administrator that first approved the request for the certificate. The privileges of the 'Owner' therefore depend on that Administrator's administrative role. (See the definitions above).</p> |
| Requester | <p>The Requester of the certificate is the person that created and successfully submitted the initial application for the certificate.</p> <ul style="list-style-type: none"> • The 'Requester' can be any class of Administrator or End-User. • SSL certificates and Client certificates can be requested by people that do not yet 'exist' in CCM as either End-Users or Administrators if they applied using use the self-enrollment/external application forms. |
| Developer | <p>Applicable only if 'Code Signing on Demand' feature is enabled for your account.</p> <p>A developer is the person that can use the Code Signing on Demand service to sign the executables and script files. CCM can store the code-signing certificate issued to them and use it for signing code files uploaded by the developer. The developer can then download the signed file from CCM.</p> <ul style="list-style-type: none"> • A new user can be added as a developer as a new user or an existing end-user can be assigned the Developer role |

1.2.4 Security Roles - Comparative Table

| Organization and Department Management | | | | | | |
|---|---------------------------------------|---|---|---|-------------------|---|
| Action | Controls | MRAO | RAO | DRAO | | |
| Configure other Administrators | Add, View Delete, Edit | Any MRAO Any RAO of Any Certificate Type Any DRAO of Any Certificate Type | Create DRAOs of Subordinate Departments who are responsible for same Certificate Type Creation of RAOs of Delegated Organization who are responsible for same Certificate Type | Creation of DRAOs of Delegated Department who are responsible for the same certificate type if enabled by a RAO administrator or a MRAO | | |
| Approve/Reject Administrator Creation Requests | Approve, Reject | Any RAO of Any Certificate Type Any DRAO of Any Certificate Type | DRAOs of Subordinate Departments who are responsible for same Certificate Type | ✘ | | |
| Activate/Deactivate Administrators | Checkbox | Any MRAO Any RAO of Any Certificate Type Any DRAO of Any Certificate Type | RAOs of Delegated Organization who are responsible for same Certificate Type DRAOs of Subordinate Departments who are responsible for same Certificate Type | ✘ | | |
| Certificate Management | | | | | | |
| Action | Controls | MRAO | RAO | DRAO | | |
| Directly submit Certificate Requests to the issuing Certificate Authority for Auto-Installation by CCM (IIS , Apache and Apache Tomcat only) | Add, Renew, Approve, Decline, Install | Any Organization Any Department | Delegated Organizations Subordinate Departments | Delegated Departments | | |
| | | | RAO SSL | ✔ | DRAO SSL | ✔ |
| | | | RAO S/MIME | ✘ | DRAO S/MIME | ✘ |
| | | | RAO Code Signing | ✘ | DRAO Code Signing | ✘ |

| | | | | | | |
|--|---------------------|---|---|---|-------------------|---|
| Directly submit Certificate Requests using the built-in application form | Add, Renew, Replace | Any Organization Any Department Any Certificate Type | Delegated Organizations Subordinate Departments Only those Certificate Types for which RAO is responsible | Delegated Departments Only those Certificate Types for which DRAO is responsible | | |
| Approve/Decline Certificate Requests that have been made using the Self-Enrollment form | Approve, Decline | Any Organization Any Department Of any Certificate Type | Delegated Organizations Subordinate Departments Only those Certificate Types for which RAO is responsible | Delegated Departments Only those Certificate Types for which DRAO is responsible | | |
| Manage Certificates | View, Edit, Revoke | Any Organization Any Department Of any Certificate Type | Delegated Organizations Subordinate Departments Only those Certificate Types for which RAO is responsible | Delegated Departments Only those Certificate Types for which DRAO is responsible | | |
| Setup and manage Private Key Controller Agent | | ✓ | ✗ | ✗ | | |
| Download the Private Key of an SSL certificate Upload the Private Key of an SSL certificate | | Any Organization Any Department ✓ | Delegated Organizations Subordinate Departments | Delegated Departments | | |
| | | | RAO SSL | ✓ | DRAO SSL | ✓ |
| | | | RAO S/MIME | ✗ | DRAO S/MIME | ✗ |
| | | | RAO Code Signing | ✗ | DRAO Code Signing | ✗ |
| Certificate | Add CIDR, | ✓ | RAO SSL | ✓ | DRAO SSL | ✓ |

| | | | | | | |
|---|---|------------------------------------|---|---|-----------------------|--|
| Discovery | Delete CIDR, Setup Certificate controller agent for internal scanning | | RAO S/MIME | ✘ | DRAO S/MIME | ✘ |
| | | | RAO Code Signing | ✘ | DRAO Code Signing | ✘ |
| Request Domains for... | Add | Any Organization Any Department | Delegated Organizations Subordinate Departments | | Delegated Departments | |
| Approve / Reject Domain Requests for... | Approve, Reject | Any Organization Any Department | Subordinate Departments | | ✘ | |
| Delegate Domains to... | Delegate | Any Organization Any Department | Subordinate Departments RAOs can only delegate domains to the Departments belonging to the Organization that have been delegated to them but cannot re-delegate to remove a domain's delegation. | | ✘ | |
| Activate/Deactivate Domains for... | Checkbox | Any Organization Any Department | | ✘ | | ✘ |
| Initiate DCV | Select method of DCV as applicable to the domain | Any Organization Any Department | RAO SSL | On Domains added to Delegated Organizations and Subordinate Departments | DRAO SSL | On Domains added to Delegated Department |
| | | | RAO S/MIME | ✘ | DRAO S/MIME | ✘ |
| | | | | ✘ | DRAO | ✘ |

| | | | RAO Code Signing | Code Signing | |
|---|-------------------------------------|--|--|-------------------------|--|
| Organization and Department Management | | | | | |
| Action | Controls | MRAO Administrator | RAO | DRAO | |
| Create and Manage Organizations | Add, Delete, Edit | ✓ | ✗ | ✗ | |
| Approve/Reject Organization Creation | Approve | ✓ | ✗ | ✗ | |
| Create and Manage Departments | Add, Delete, Edit | ✓ | Subordinate Departments of Delegated Organization | ✗ | |
| Approve Department Creation | Approve | ✓ | Subordinate Departments of Delegated Organization | ✗ | |
| Key Escrow | | | | | |
| Action | Controls | MRAO | RAO S/MIME | DRAO S/MIME | |
| Manage Encryption of client certificates | Initialize, Re-encrypt | Any delegated RAO Any delegated DRAO | Delegated Organizations Subordinate Departments | Delegated Organizations | |
| Recover private keys from escrow | Decrypt | Any Enabled Organization * Any Enabled Department * | Delegated Organizations Subordinate Departments | Delegated Organizations | |
| Can permit Administrators other than themselves to recover keys for a particular Organization or Department | Allow key recovery by... (Checkbox) | MRAO admins RAO S/MIME admins | MRAO Admins RAO S/MIME Admins DRAO S/MIME Admins | ✗ | |

* Escrow privileges are configured at the point of Organization / Department creation.

When setting up an Organization, the MRAO can specify any, all or none of the following:

1. Whether or not the MRAO (themselves) should have the ability to recover the private keys of client certificates of that Organization
2. Whether or not the RAO S/MIME admin of the Organization should have the ability to recover private keys of client certificates of that Organization

If granted escrow privileges above, the RAO S/MIME admin will be subsequently be able to specify any, all or none of the following for any Departments they create:

1. Whether or not the MRAO should have the ability to recover the private keys of client certificates of that Department
2. Whether or not the RAO S/MIME admin (themselves) should have the ability to recover the private keys of client certificates of that belonging to that Department
3. Whether or not the DRAO S/MIME admin should have the ability to recover the private keys of client certificates belonging to that Department

See '[Encryption and Key Escrow](#)' for more details.

| Notifications, Reports and Miscellaneous | | | | |
|--|---|------------------------------------|--|----------------------|
| Action | Controls | MRAO Administrator | RAO Administrator | DRAO Administrator |
| Configure access control settings | Add, Delete, Edit CIDR | ✓ | ✓ | ✓ |
| View Notifications for... | Add, Delete, Edit | Any Organization Any Department | Delegated Organizations Subordinate Departments | Delegated Department |
| Create Notifications for... | Add, Delete, Edit | Any Organization Any Department | Delegated Organizations Subordinate Departments | Delegated Department |
| View Reports for... | See ' Reports - Security Role Access Table ' section for details. | Any Organization Any Department | Delegated Organizations Subordinate Departments | Delegated DRAO |
| Manage SSL Type Availability | Type, Term | ✓ | ✗ | ✗ |
| Modify Email Templates for... | Edit | Any Organization | Delegated Organizations | Delegated Department |

| | | | | |
|--|--|----------------|-------------------------|--|
| | | Any Department | Subordinate Departments | |
|--|--|----------------|-------------------------|--|

1.2.5 Multiple Security Roles

Multiple security roles may be selected for any particular administrator. An MRAO can assign SSL, S/MIME and Code Signing administrative privileges to the same RAO for a particular Organization. An RAO that has been granted administrative rights over multiple certificate types can assign similar, multi-role, privileges to a sub-ordinate DRAO administrator for a particular Department.

1.2.6 Organizations and Departments

The creation of an Organization and the delegation of a domain to that Organization is an important step towards the issuance and effective management of SSL, code signing or client certificates via the Certificate Manager interface.

Organizations and Departments are created by administrators for the purposes of requesting, issuing and managing certificates for domains and employees. Organizations can be sub-divided into Departments for the purposes of certificate and end-user management. (See section [Creating a New Organization](#) for more details).

Each Organization can have multiple Departments. Organizations are typically managed by a Registration Authority Officer (RAO). Departments are typically managed by a Department Registration Authority Officer (DRAO). A Master RAO (MRAO) can manage all Organizations and all Departments.

Once an Organization has been created:

- MRAOs can create (or assign existing) RAOs to manage that Organization
- MRAOs can initiate the process of validating Organizations for the purpose of requesting and issuance of OV SSL certificates to Organizations and Departments under them.
- MRAOs and RAOs can create multiple Departments within that Organization (See '[Organizations / Section Overview](#)' for more details).
- MRAOs can create (or assign existing) RAOs to manage individual Departments
- MRAOs can delegate domain(s) to the Organization or Department
- RAO and DRAO class administrators can directly request that certificates be issued to domains that have been delegated to their Organization(s) and/or Department(s). They can also approve/decline certificate requests from individuals using the external application form.
- End-users can be assigned membership of an Organization or Department and provisioned with client certificates for the domain that is associated with that Organization/Department.
- Administrators can manage the client certificates of end-users belonging to an Organization or Department via the 'Certificates Management - Client Certificates' interface and can manage SSL certificates for the Organization via the '[Certificate Managements - SSL Certificates](#)' area. Code Signing Certificates are managed from the 'Code Signing' area
- A wide range of Organization and Department specific email notifications can be set up to alert personnel to changes in certificate status, changes to domain status, Discovery Scan Summaries, Admin creation and more.
- MRAOs, RAOs and DRAOs can utilize the [Certificate Discovery](#) feature to audit then monitor all existing certificates on the network by assigning them to either an Organization or one of its Departments.
- Certificate reports and activity logs can be viewed and exported for that Organization and/or specific Department.

1.2.7 Reports

Certificate reports and activity logs can be viewed and exported for an Organization and/or Department via the **Reports** section. Administrators can view reports which are appropriate for their security role. The following types of reports are available:

| Type of Report | Description |
|--|--|
| Activity Log | Enables the MRAO to view all actions that have occurred within the interface within specific time periods. |
| SSL Certificates | Enables the MRAO and RAO/DRAO SSL administrators to monitor all statistics related to SSL certificates including usage, ownership, issuance, provisioning and status. |
| Discovery Scan Log | Enables the MRAO and RAO/DRAO SSL administrators to view the Discovery Scan Log. A Discovery Scan is an audit of all SSL certificates installed on your network. |
| Client Certificates | Enables the MRAO and RAO/DRAO S/MIME administrators to monitor all statistics, related to client certificates including usage, ownership, issuance, provisioning and status. |
| Code Signing Certificates | Enables the MRAO and RAO/DRAO Code Signing administrators to monitor all statistics, related to code signing certificates including usage, ownership, issuance, provisioning and status. |
| Admin | Enables the MRAO to generate and view reports providing the details of the enrolled Administrators of all privilege levels. |
| XML Data | Enables the MRAO to generate a report containing complete details of all the Organizations, Departments, their administrators and the all the certificates in XML format. |
| DCV Report | Enables the MRAO and RAO/DRAO SSL administrators to generate a report containing details on all of their registered domains, with their DCV status and expiration dates. |
| Notification Log Statistics Report | Enables the MRAO administrator to generate reports containing complete details of the notifications emails sent to RAO and DRAO administrators for various CCM events. |
| Private Key Controller Activity Log | Enables the MRAO administrator to generate reports containing the actions executed by the private key controller installed on the local network. |
| Discovery Tasks | Enables MRAO Administrators and RAO/DRAO Administrators to generate and view reports on Discovery Tasks, configured for their Organization(s) and Department(s). |
| Device Certificates | Enables the MRAO and RAO/DRAO Device Cert administrators to monitor all statistics related to device certificates, including key usage, ownership, issuance, |

| Type of Report | Description |
|----------------|--------------------------|
| | provisioning and status. |

For more detailed information see the section **'Reports'** of the guide.

1.3 Logging into Your Account

Once your Organization has subscribed for a Comodo account, your Comodo account manager will provide you with a username, password and login URL for the Certificate Manager interface. By default, the format of this URL is: [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/](https://cert-manager.com/customer/[REAL CUSTOMER URI]/)

If you have not been supplied with your login details, please contact your Comodo account manager.

If you are not able to login with your login details, you can raise a support ticket at the Comodo Support portal by clicking 'Support link'. You can create an account for free and submit your ticket to get your login problems resolved.

Depending on the Access Control Settings specified by the administrator, you will be prompted to change your password after logging in for the first time. You may also change your password at any time via the **'My Profile'** area.

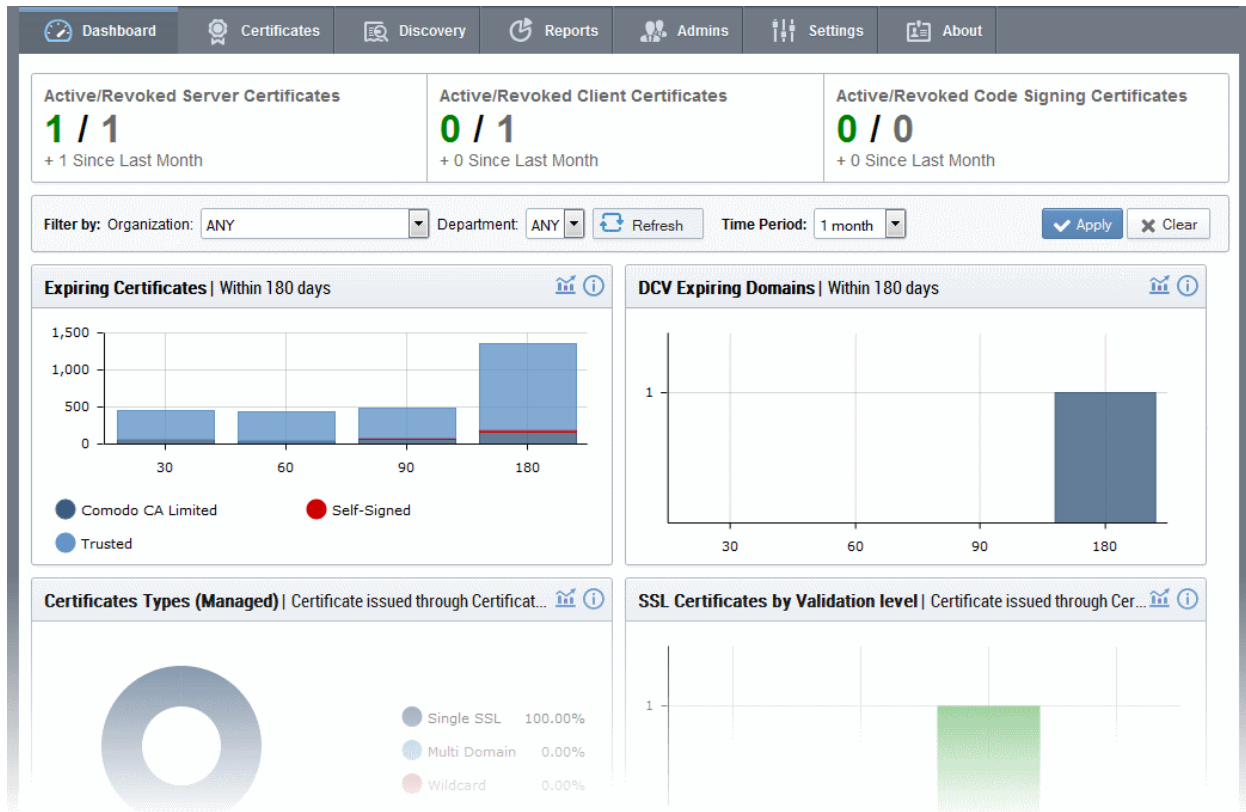
1.4 The Main Interface - Summary of Areas

Comodo Certificate Manager interface has a tab structure that facilitates access to all major settings.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|------------------|--------------|------------|---------|------------|---------------|---------------|
| c2.loca[53] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| c3.loca[54] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| c3.loca[55] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| c4.ccmqa.com[56] | org2 | | Invalid | | Not scheduled | Not scheduled |
| ccmqa.com[87] | org1 | | Invalid | | Not scheduled | Not scheduled |

- There are (a maximum of) seven tabs that cover each of the main functional areas of the application. These are 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', 'Admins', 'Settings' and 'About'.
- The 'Certificates' tab contains sub-sections for managing the certificate types that have been enabled for your company. There is therefore a maximum of four sub-sections - 'SSL Certificates', 'Client Certificates', 'Code Signing Certificates' and 'Device Certificates'.
- The 'Discovery' tab contains sub-sections for scanning the network for installed certificates and for managing Certificate Discovery (CD) agents. The sub-sections are 'Network Assets', 'Discovery Tasks' and 'Agents'.
- The 'Code Signing on Demand' tab is displayed only if the Code Signing on Demand (CSD) feature is enabled for your account. The tab contains sub-sections for configuring the CSD service for your account, adding and managing developers and handling code signing requests from the developers. The sub-sections are 'Configuration', 'Requests' and 'Developers'.
- The 'Settings' tab contains sub-sections for 'Organizations', 'Organizations', 'Domains', 'Notifications', 'Encryption', 'Access Control', 'Private Key Store', 'Certificates', 'Email Templates', 'MS Agents' and 'Assignment Rules'.
- The 'Reports' tab contains sub sections for generating reports for 'Activity Log', 'Client Certificates', 'Discovery Scan Log', 'SSL Certificates', 'Code Signing Certificates', 'Code Signing Requests', 'Admins', 'XML Data', 'DCV Report', 'Agent Log Events', 'Notification Log Statistics', 'Private Key Controller', 'Discovery Tasks' and 'Device Certificates'.
- The remainder of this introduction contains an introduction to each tabbed area and the Security Role requirements for access to that area. Full details of the actual usage and functionality of the tabbed areas listed above are in sections 2. The Dashboard, 3. Certificates Management, 4. Code Signing on Demand, 5. Admin Management, 6. Settings, 7. Certificate Discovery and Agents, 8. Reports, 9. Version and Feature Information, 10. My Profile and 10. Logging out of Comodo Certificate Manager.

Dashboard: Contains graphs and charts that display snap-shot summaries of certificate key life-cycle information such as certificates approaching expiry, certificates issued/requested, DCV status, breakdown of certificates by types, issuers, and more.



[Click here for more information about the Dashboard.](#)

Certificates Management: Contains up to three sub-sections for the management of SSL, Client and Code Signing certificates.

The Certificates Management section displays a table of SSL certificates with the following data:

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|------------------|--------------|------------|---------|------------|---------------|---------------|
| c2.loca[53] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| c3.loca[54] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| c3.loca[55] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| c4.comqa.com[56] | org2 | | Invalid | | Not scheduled | Not scheduled |
| comqa.com[87] | org1 | | Invalid | | Not scheduled | Not scheduled |

These sub-tabs are accessible according administrator security role privileges:

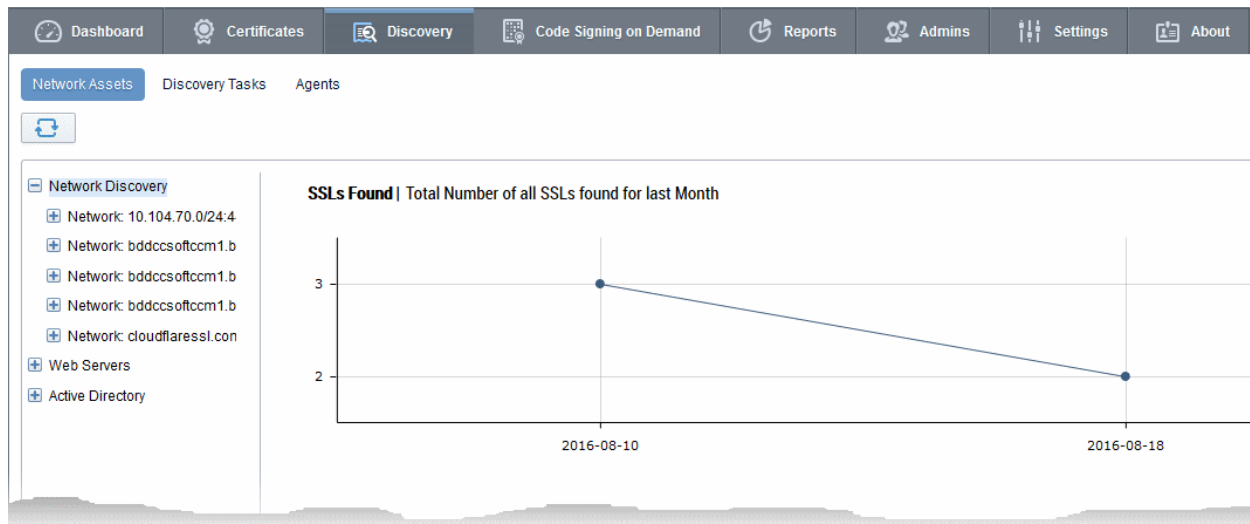
| Security Role / Type of Administrator | Available Action |
|---------------------------------------|---|
| MRAO | Can access all areas and functionality of the section: has full visibility and control over all types of certificates. |
| RAO SSL | Can access all areas and functionality of the SSL Certificates section; has visibility and control over SSL Certificates belonging to their |

| Security Role / Type of Administrator | Available Action |
|---------------------------------------|--|
| | delegated Organization(s). |
| RAO S/MIME | Can access all areas and functionality of the Client Certificates section; has visibility and control over client certificates and end-users belonging to their delegated Organization(s). |
| RAO Code Signing | Can access all areas and functionality of the Code Signing Certificates section; has visibility and control over Code Signing Certificates issued to end-users belonging to their delegated Organization(s). |
| RAO Device Cert | Can access all areas and functionality of the Device Certificates section; has visibility and control over Device Certificates issued to devices and endpoints belonging to their delegated Organization(s). |
| DRAO SSL | Can access all areas and functionality of the SSL Certificates section; has visibility and control only over SSL Certificates belonging to belonging to their delegated Department(s). |
| DRAO S/MIME | Can access all areas and functionality of the Client Certificates section; has visibility and control over client certificates and end-users belonging to their delegated Department(s). |
| DRAO Code Signing | Can access all areas and functionality of the Code Signing Certificates section; has visibility and control over Code Signing Certificates issued to end-users belonging to their delegated Department(s). |
| DRAO Device Cert | Can access all areas and functionality of the Device Certificates section; has visibility and control over Device Certificates issued to devices and endpoints belonging to their delegated Department(s). |

[Click here for more information about the Certificates Management section.](#)

Certificate Discovery and Agents: Certificate Discovery requires the installation of the Certificate Controller agent, a small piece of software that identifies certificates installed in the network. The agent is also required for automatic request and installation of SSL certificates on remote servers. The Discovery area enables administrators to configure certificate controller agents for the network and to commence certificate discovery tasks.

Discovery scan results are displayed in the 'Network Assets' area under the 'Discovery' tab. The results include 'Managed' certificates (those issued through CCM) and 'Unmanaged' certificates (those acquired from other CAs, Comodo certs not obtained through CCM and self-signed certificates). Administrators can assign unmanaged certificates to an Organization or Department to bring them under CCM management. The Network Assets area also displays web-servers and domains found on scanned networks. If AD servers are integrated to CCM, the Network Assets area displays all certificates found by scans run on the AD servers.



The 'Discovery' area is accessible only by MRAO, RAO SSL and DRAO SSL administrators.

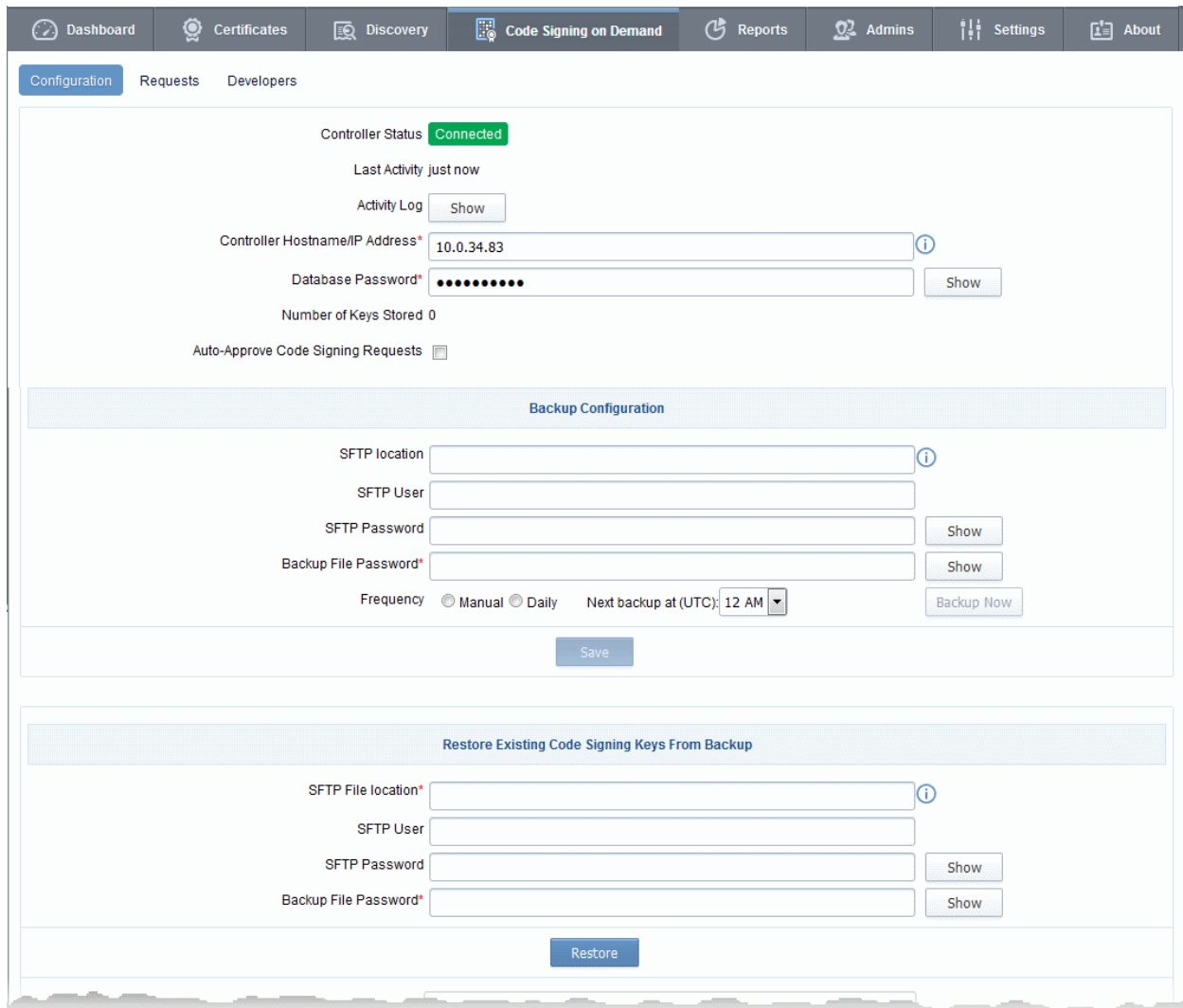
| Security Role / Type of Administrator | Available Action |
|---------------------------------------|--|
| MRAO | Can set up agents for any Organization and Department and can scan for certificates requested, issued, expired, revoked and replaced for any Organization or Department. |
| RAO SSL | Can set up agents for and can scan for certificates requested, issued, expired, revoked and replaced for Organizations (and any sub-ordinate Departments) that have been delegated to them. |
| DRAO SSL | Can set up agents for and can scan for certificates requested, issued, expired, revoked and replaced only for the Department(s) that have been delegated to them. |

[Click here for more information about the Discovery section.](#)

Code Signing on Demand - The 'Code Signing on Demand' tab is visible only if the feature is enabled for your account. If you wish to enable this feature, contact your Comodo Account Manager.

The CSD service is available in two modes:

- In-House Hosted mode** - The CSD controller installed and configured at the local network generates Code Signing certificate requests for 'Developers' added to CCM, forwards the request to CCM. Once the certificate is issued, the controller downloads it and stores it local database. A developer can generate a code signing request by uploading the files to be signed by logging-in to the CSD service portal created by the agent. The controller signs the files using the certificate belonging to the user, upon approval from the respective administrator CCM sends a notification mail to the developer to download the signed files.
- Cloud Service Mode** - The code signing process is performed within Comodo's highly secure cloud servers. After enrolling for a code signing certificate for a developer, the service generates the certificate request for the developer, submits the request to CCM, tracks the order and collects the certificate once issued. Developers can then upload files to the cloud portal for signing. Upon approval by the administrator, the service will sign the code and notify the developer to download the signed files.



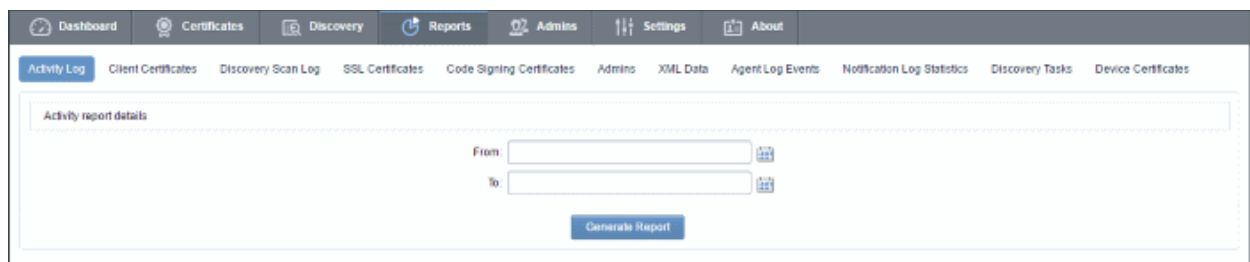
The 'Code Signing on Demand' area is accessible only by MRAO, RAO Code Signing and DRAO Code Signing administrators.

| Security Role / Type of Administrator | Available Action |
|---------------------------------------|---|
| MRAO | <p>For In-House Hosted mode</p> <ul style="list-style-type: none"> • Can setup and configure the CSD controller in the local network • Can add and manage developers for any Organization/Department • Can approve code signing requests from developers pertaining to any Organization/Department <p>For Cloud Service Mode</p> <ul style="list-style-type: none"> • Can setup and configure the CSD controller in the local network • Can add and manage developers for any Organization/Department • Can approve code signing requests from developers pertaining to any Organization/Department |

| Security Role / Type of Administrator | Available Action |
|---------------------------------------|--|
| RAO Code Signing | <ul style="list-style-type: none"> • Can add and manage developers for any Organizations (and any sub-ordinate Departments) that have been delegated to them. • Can approve code signing requests from developers pertaining to Organizations (and any sub-ordinate Departments) that have been delegated to them. |
| DRAO Code Signing | <ul style="list-style-type: none"> • Can add and manage developers only for the Department(s) that have been delegated to them. • Can approve code signing requests only from developers pertaining to Department(s) that have been delegated to them. |

The 'Code Signing on Demand' area is fully explained in the section '[Code Signing on Demand](#)'.

Report: Enables administrators to view a range of reports depending on their privilege level. The 'Reports' interface is fully explained in the Section '[Reports](#)'.



Available reports are 'Activity Log', 'Client Certificates', 'Discovery Scan Logs', 'SSL Certificates', 'Code Signing Certificates', 'Code Signing Requests', 'Admins', XML Data, DCV Report', 'Agent Log Events', 'Notification Log Statistics', 'Private Key Controller Activity Log', 'Discovery Tasks' and 'Device Certificates'. The types of report available to a particular administrator is dependent on their security role:

| Security Role / Type of Administrator | Available Action |
|---------------------------------------|---|
| MRAO | <p>Can view all types of report for all Organizations and Departments</p> <ul style="list-style-type: none"> • 'Activity' reports for any Organization and Department • 'Certificate Discovery' reports for any Organization and Department • Can view 'SSL', 'Client Certificates' and 'Code Signing Certificates' reports for any Organization and Department • 'Admin' reports for any Organization and Department • XML Data report for all the Organizations and Departments • 'DCV' report for any Organization and Department • 'Agent Log Events' for any Organization and Department • Private Key Controller Activity Log report • 'Device Certificates' reports for any Organization and Department |

| Security Role / Type of Administrator | Available Action |
|--|--|
| <p>RAO SSL RAO S/MIME RAO Code Signing RAO Device Cert</p> | <p>Can view:</p> <ul style="list-style-type: none"> • 'Certificate Discovery' reports on scans that have been run on behalf of their delegated Organization(s) and Department(s) (Only RAO SSL Admins) • 'SSL / S/MIME / Code Signing Certificate' reports appropriate to their administrative type and for their Organization(s) and Department(s) only • 'DCV' report and 'Discovery Tasks' reports for their delegated Organization(s) and Department(s) (Only RAO SSL Admins) • 'Code Signing Requests' reports for their delegated Organization(s) and Department(s) (Only RAO Code Signing Admins) • 'Device Certificates' reports for their delegated Organization(s) and Department(s) (Only RAO Device Certificate Admins) |
| <p>DRAO SSL DRAO S/MIME DRAO Code Signing DRAO Device Cert</p> | <p>Can view:</p> <ul style="list-style-type: none"> • 'Certificate Discovery' reports on scans that have been run on behalf of their delegated Department(s) (Only DRAO SSL Admins) • 'SSL / S/MIME / Code Signing Certificate' report that is appropriate to their administrative type and for their Organization(s) and Department(s) only • 'DCV' report and 'Discovery Tasks' report of their Department(s) (Only RAO SSL Admins) • Code Signing Requests reports of their Department(s) (Only DRAO Code Signing Admins) • 'Device Certificates' reports for their Department(s) (Only DRAO Device Cert Admins) |

Admin Management: Enables the currently logged-in administrator to view a list of administrative personnel. The 'Admin Management' interface is fully explained in Section [Admin Management](#).

| NAME | EMAIL | LOGIN | TYPE | ROLE | ACTIVE |
|------------|-----------------------|-----------|----------|--|-------------------------------------|
| John Smith | john@company.com | john_mrao | Standard | MRAO Admin | <input checked="" type="checkbox"/> |
| admin 1 | staticadmin@ccmqa.com | admin | Standard | MRAO Admin | <input checked="" type="checkbox"/> |
| drao1 | drao1@ccmqa.com | drao1 | Standard | DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> |
| drao10 | drao10@ccmqa.com | drao10 | Standard | DRAO Admin - SSL | <input checked="" type="checkbox"/> |
| drao11 | drao11@ccmqa.com | drao11 | Standard | DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> |

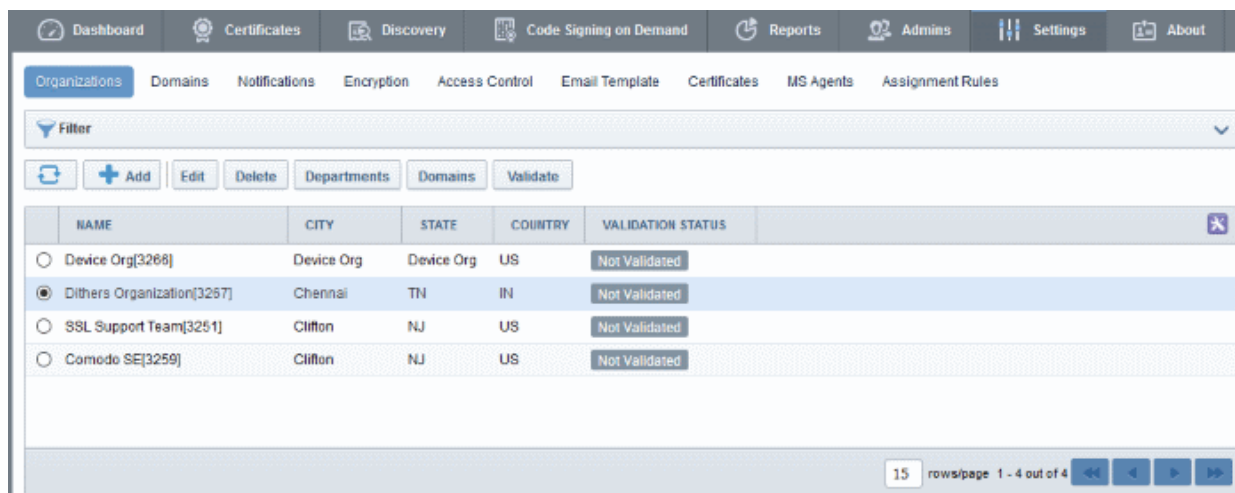
The visibility of other administrators and the availability of controls in this area is dependent on which type of administrator is currently logged in:

| Security Role / Type of Administrator | Available Action |
|--|---|
| MRAO | <p>Full visibility of all administrators across every Organization and Department.</p> <p>Can perform the following actions on administrators of any class or type:</p> <ul style="list-style-type: none"> • View • Add/Delete • Edit • Approve/Reject • Activate/Deactivate |
| RAO SSL RAO S/MIME RAO Code Signing RAO Device Cert | <ul style="list-style-type: none"> • View/Edit RAOs and DRAOs of their delegated Organization(s) and any subordinate Department(s) who are responsible for the same certificate type(s) as themselves • Request the creation of fellow RAOs who are responsible for the same certificate type(s) as themselves • Approve/Reject the creation of DRAOs who are responsible for the same certificate type(s) as themselves from. |
| DRAO SSL DRAO S/MIME DRAO Code Signing DRAO Device Cert | <ul style="list-style-type: none"> • View DRAOs of their delegated Department(s) who are responsible for the same certificate type(s) as themselves • Request the creation of fellow DRAOs who are responsible for the same certificate type(s) as themselves • Edit their own details |

[Click here for more information about Admin Management section.](#)

Settings: The 'Settings' area contains several tabs relating to the overall configuration of CCM. The number of tabs

that are visible to a particular administrator is dependent on their security role (MRAO, RAO or DRAO).



- (1) **Organizations:** Visible only to MRAO and RAO class administrators. RAOs can view, edit, request new domains and add Departments to Organizations that have been delegated to them. MRAOs can view, edit, request new domains, create new Departments and delete any Organization or Department. MRAOs can initiate the process of validating Organizations for the purpose of requesting and issuance of OV SSL certificates to Organizations and Departments under them.
- (2) **Departments:** Visible only to DRAO class administrators (DRAO's see a 'Departments' tab instead of the 'Organizations' tab). Allows DRAOs to view all Departments that have been delegated to them and to request new domains for those Departments.
- (3) **Domains:** MRAOs can view all domains that have been requested or created; submit domain requests for validation, select the validation method, activate, deactivate, edit domains and delegate, a domain to any Organization or Department, delete a domain. RAOs can view domains for Organization that they control, can delegate domains to subordinate Departments and can request new domains for their Organization. DRAOs can view existing domains and request the addition of new ones.
- (4) **Notifications:** Allows administrators to set up and manage email notifications to various personnel - including notifications triggered by SSL certificate status, notifications triggered by Client Certificate status and Discovery Scan Summaries.
- (5) **Encryption:** Allows administrators to initialize a new master key pair or to re-encrypt the private keys of client certificates held in escrow.
- (6) **Access Control:** Allows the MRAO to grant access access to the CCM login page only for specified IP range.
- (7) **Private Key Store:** Allows the MRAO to configure backup of the private keys of SSL certificates.
- (8) **Certificates** - Allows MRAOs to customize the types and term lengths of SSL and Client certificates available through the Built-in application form and the Self Enrollment form. In addition to the standard fields that appear in the Built-in application form and the Self Enrollment form, MRAO admins can also configure to add additional custom fields in these forms.
- (9) **Email Templates:** Enables MRAO and RAO administrators to customize the content of templates for event-based email notifications. DRAO administrators can edit templates for their Department via the 'Edit Department' dialog (Settings > Departments > Edit)
- (10) **MS Agents** - Enables MRAO to add AD servers to CCM by installing the MS Agents on them. The MS Agent acts as CA proxy to issue Device Certs to the devices enrolled to the AD Server through NDES and periodically scans the AD server for installed certificates for reporting to CCM. The results are displayed under the 'Active Directory' category in the 'Discovery' > 'Network Assets' area.
- (11) **Assignment Rules** - Enables MRAO and RAO administrators to define assignment rules for automatically assigning unmanaged certificates identified by discovery scans to required Organizations and Departments and apply the rules while configuring Discovery Scans.


[Click here for more information about the 'Settings' area](#)

About - Enables currently logged-in administrator to view the version of CCM and the features that are enabled and disabled for the account.

| STATE | | CLIENT CERTS | |
|--------------------------------------|----------|---|----------|
| Version | 5.8 | Allow Client Certs | Enabled |
| Extra Agent Version | 2.2 | Web API | Enabled |
| Private Key Agent Version | 1.1 | Allow principal name in certificates | Enabled |
| Code Signing on Demand Agent Version | 2.3 | Allow customization of principal name SAN field | Enabled |
| Active Directory Agent Version | 2.0 | Web Enrollment Type | |
| Balance (tokens) | 0 | Invitation | Enabled |
| | | AccessCode | Enabled |
| | | Secret ID | Disabled |
| | | Auto Revoke | Enabled |
| | | Allow Empty PIN | Disabled |
| | | Allow send notification upon upload from csv | Disabled |
| DOMAIN | | | |
| Domain Dual Approval by MRAO | Disabled | | |
| SSL CERTS | | | |
| Allow SSL | Enabled | | |
| Web API | Enabled | | |
| DCV Validation | Enabled | | |
| CODE SIGNING CERTS | | | |
| Allow Code Signing Certificates | Enabled | | |
| MaxTerm | 1 | | |


© 2007-2017. All rights reserved.

My Profile - Enables currently logged-in administrator to view/edit address details, change the interface language, time format and change password.


Support - Clicking the help icon  takes you to Comodo's support page at <https://support.comodo.com/>, the

Comodo support web page, an online knowledge-base and support ticketing system. The fastest way to get further assistance in case you find any problem using CCM management console.



Notification - The notification icon  at the top indicates the number of message that are yet be read. Click on the icon to view the messages. The types of messages displayed are related to validation, controller, agent and so on.

✕
Notifications


Mark All As Read


| | MESSAGE | CREATE DATE |
|-----------------------|---|---------------------|
| <input type="radio"/> | MS Controller is connected now. | 08/25/2016 15:47:25 |
| <input type="radio"/> | Extra Controller is connected now. | 08/25/2016 15:47:25 |
| <input type="radio"/> | Extra Controller is not active a long time. | 08/25/2016 15:46:06 |
| <input type="radio"/> | Extra Controller is not active a long time. | 08/25/2016 15:46:05 |
| <input type="radio"/> | Extra Controller is not active a long time. | 08/25/2016 14:48:41 |
| <input type="radio"/> | Extra Controller is not active a long time. | 08/25/2016 14:48:41 |
| <input type="radio"/> | MS Controller is connected now. | 08/25/2016 13:48:20 |
| <input type="radio"/> | Extra Controller is connected now. | 08/25/2016 13:48:20 |
| <input type="radio"/> | Extra Controller is not active a long time. | 08/25/2016 13:41:01 |
| <input type="radio"/> | MS Controller is connected now. | 08/22/2016 16:15:59 |
| <input type="radio"/> | MS Controller is connected now. | 08/22/2016 16:04:33 |
| <input type="radio"/> | MS Controller is connected now. | 08/22/2016 16:02:10 |
| <input type="radio"/> | MS Controller is connected now. | 08/22/2016 04:35:49 |
| <input type="radio"/> | Extra Controller is connected now. | 08/22/2016 04:35:48 |
| <input type="radio"/> | Extra Controller is not active a long time. | 08/22/2016 04:22:01 |

<
15
rows/page
1 - 15 out of 846
⏪
⏩
⏴
⏵

Close

Unread messages will be in bold. To view a full message, select it and click the 'Details' button at the top. To remove a message from the list, select and click the 'Delete' button.

Logout:

- Click the  icon to log out of Comodo Certificate Manager.

1.5 Release Notes

| Version History | |
|-----------------|-----------------|
| Version Number | List of Changes |

| | |
|---------------------------|--|
| <p><u>Version 5.8</u></p> | <ul style="list-style-type: none"> • Support for RESTful APIs for Code Signing on Demand service • Added client certificate authentication support for SOAP APIs • Improved device cert reports with addition of status information • Added ability to edit device certificate collection email template • Added ability to resend device certificate collection emails • Improvements to SCEP configuration of device certificates |
| <p><u>Version 5.7</u></p> | <ul style="list-style-type: none"> • Added ability to integrate CCM with a Hardware Security Module (HSM) to generate and store keys and code signing certificates enrolled for Code Signing on Demand (CSoD) • Added ability to enroll device certificates through Simple Certificate Enrollment Protocol (SCEP) |
| <p><u>Version 5.6</u></p> | <ul style="list-style-type: none"> • Improvements in auto-installation including scheduled auto-renew and enhanced scheduling abilities. • Added ability to map MS AD Certificate Templates to CCM certificate types • Added ability to for issuance of device certificates from Private Certificate Authorities using CCM certificate types • Added ability for self-enrollment of device certificates by applicants |
| <p><u>Version 5.5</u></p> | <ul style="list-style-type: none"> • Added the ability to issue Device Certificates for authentication of devices and endpoints, including BYOD devices connected to the networks. • Added ability to integrate AD servers by installing MS agents, for running discovery scans on the servers and issue device certificates to devices enrolled to them. • Added ability to define assignment rules for automatically assigning unmanaged certificates identified by discovery scans to required Organizations and Departments for bringing them under management. • Added Network Assets view to display the SSL certificates installed on various nodes, servers and endpoints, as identified by discovery scans, web-servers with details on websites/domains hosted on them and Active Directory objects with certificates installed on them as discovered by AD server scans. • Added new API for integration to Mobile Device Management (MDM) solutions, for issuance of Device Certificates. • Various Bug fixes. |
| <p><u>Version 5.4</u></p> | <ul style="list-style-type: none"> • Maintenance update addressing bug fixes and various back-end improvements • 'Code Signing on The Fly' feature renamed as 'Code Signing on Demand' • Added Identity Providers (IdP) feature, which allows admins to log |

| | |
|---------------------------|---|
| | <p>into CCM using credentials of his/her IdP. New admins can also be enrolled using the IdP method.</p> |
| <u>Version 5.3</u> | <ul style="list-style-type: none"> Added 'Code Signing On-The-Fly' feature that offers developers a faster, more intuitive and highly secure way to digitally sign their software. The service is available in both hosted and cloud versions. Added Bulk DCV feature that enables validate multiple domains at once as long as all domains share a common email listed on the Whois record. |
| <u>Version 5.1</u> | <ul style="list-style-type: none"> Added Private Key Store feature that enables storage and management of private keys of managed SSL certificates at customers network. Certificates whose private keys are managed at the private key store can be imported in .p12 format for directly imported to any server(s) for installation. |
| <u>Version 5.0</u> | <ul style="list-style-type: none"> Redesigned User Interface. Support for issuance of certs to private domain names. Improved Dashboard with drill-down statistical reports. |
| <u>Version 4.6</u> | <ul style="list-style-type: none"> Added the new Dashboard feature with graphs and charts that allow the administrator to quickly gain an overview of all SSL, S/MIME and code-signing certificates on the network. |
| <u>Version 4.5</u> | <ul style="list-style-type: none"> Added a new report type 'Notification log Statistics' to enable MRAO administrators to generate and view logs of automated notification emails sent to other administrators during various events Added ability to external applicants to renew their SSL certificates through self-renewal form, by entering their certificate ID and Pass Phrase. Various bug fixes and UI improvements |
| <u>Version 4.4</u> | <ul style="list-style-type: none"> Added new process of validating Organizations for the issuance of OV SSL certificates Improved the process of validating Organizations for the quick issuance of EV SSL certificates. Added ability to create domains without delegating them to Organizations or Departments. Various bug fixes |
| <u>Version 4.3</u> | <ul style="list-style-type: none"> Streamlined the DCV process for a faster validation. Added ability to sort items in various interfaces by clicking the column headers Added ability to search and filter certificates based on requester in |

| | |
|---------------------|--|
| | <p>SSL Certificates interface</p> <ul style="list-style-type: none"> • Custom field data included for a certificate will continue on the renewal certificates too • Various bug fixes and several optimizations to improve the performance of the database and application server for improved stability |
| <u>Version 4.2</u> | <ul style="list-style-type: none"> • Added ability for MRAO administrators to add custom fields in the Built-in Application Form and Self-Enrollment Form for SSL and Client certificates requisition. • Various bug fixes |
| <u>Version 4.1</u> | <ul style="list-style-type: none"> • Introduced HTTPS method introduced in addition to HTTP. • Updated and improved SCEP support of iOS. • Enhanced the self-enrollment form, optimized to be used on iPhones. When a user wants to enroll and install a client certificate with the self-enrollment form, CCM presents an optimized page. After the enrollment process completes, the user can automatically install the certificate onto the iOS device. • Several UI improvements, including saving search filters. The filters configured for various interfaces will be saved and automatically applied when the same interface is opened again • Enabled auto installation feature for Apache Tomcat server. Version 4.1 supports auto-installation / auto-renewal for following platforms: <ul style="list-style-type: none"> • Apache Web Server (Linux 32/64bit) • IIS 7/7.5/8 (Windows 32/64) • Apache Tomcat (Windows 32/64bit, Linux 32/64bit) • Various Bug Fixes |
| <u>Version 4.0</u> | <ul style="list-style-type: none"> • User Interface changes • Multiple certificate discovery tasks can be run at the same time • Agents will automatically check for newer versions and update itself |
| <u>Version 2.11</u> | <ul style="list-style-type: none"> • Added automatic installation and renewal of SSL certificates. This feature is enabled for accounts on a per-case basis. There are two available modes: <ul style="list-style-type: none"> • Enterprise Controller Mode - Software installed on a local host will communicate directly with the CA issuance infrastructure to automatically apply for and install certificates on designated web-servers. • Certificate Manager Controller mode - An agent is installed on each webserver which will communicate with CCM for certificate requests. If a request exists, the agent will generate a CSR and present it to the administrator for approval in the CCM interface. |

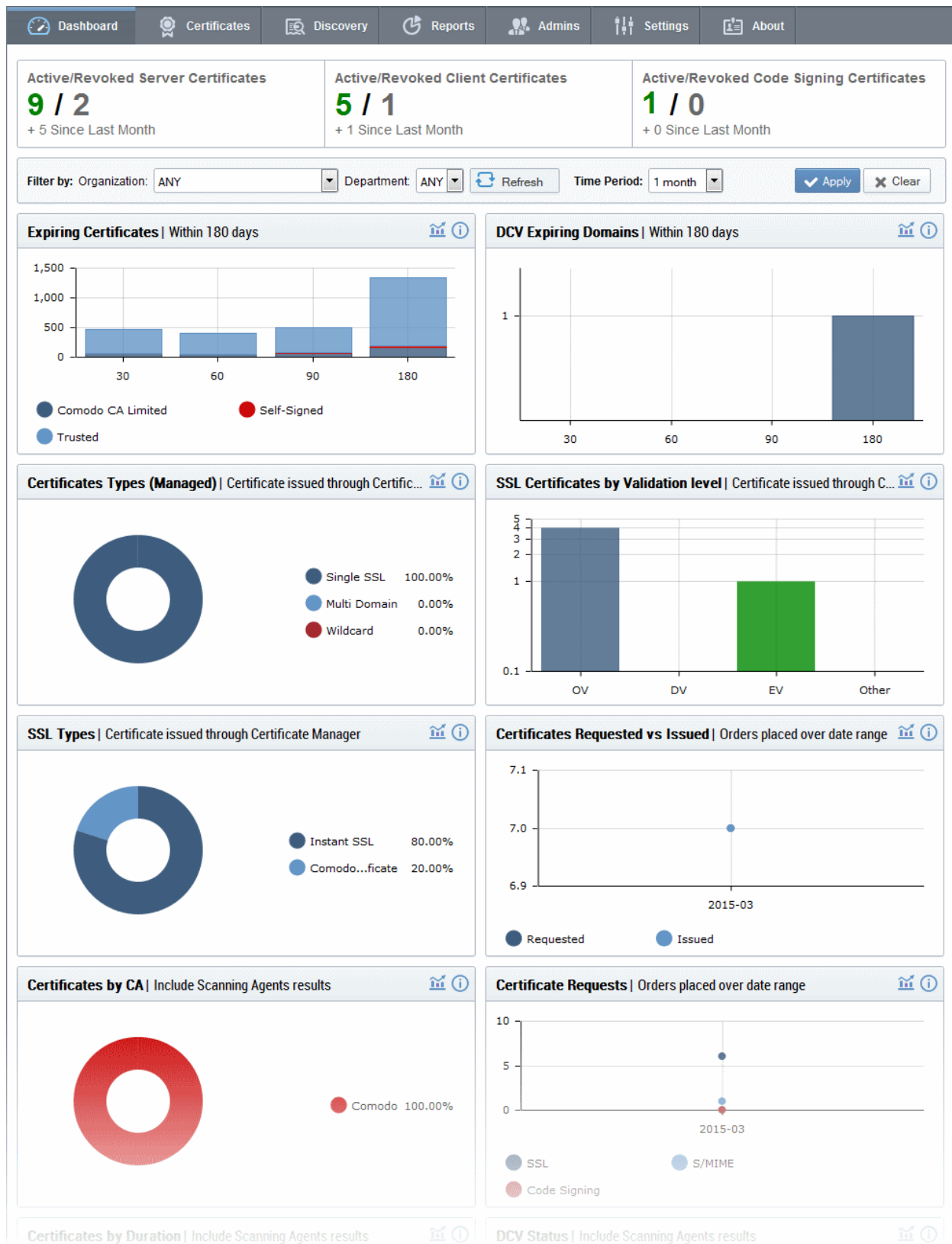
| | |
|-------------------------|--|
| | <ul style="list-style-type: none"> • Various Bug fixes |
| <u>Version 2.10</u> | <ul style="list-style-type: none"> • Added Auto-installation and Auto-renewal features for automatic SSL application, CSR generation, and certificate installation on IIS and Apache. • Various Bug fixes |
| <u>Version 2.8.26</u> | <ul style="list-style-type: none"> • Added functionality for scanning internal servers for installed certificates using Certificate Discovery (CD) Agent, installed in a local computer. • Various Bug Fixes |
| <u>Version 2.8.25</u> | <ul style="list-style-type: none"> • Added three methods EMAIL, HTTP file and DNS CNAME for Domain Control Validation (DCV) functionality to validate new and existing domains |
| <u>Version 2.8.23</u> | <ul style="list-style-type: none"> • Enhanced logging for system resources/usage statistics • Improved error handling/logging • Added a column 'External Requester' to SSL report • Improvements to the notifications system • Bug Fixes: <ul style="list-style-type: none"> • Fixed bug whereby MRAO is sent 'Discovery Scan Summary' notification even though the Notify Master Admin(s) checkbox is not selected • Fixed bug related to issue of SSL through Self-Enrollment Links for local hostnames • Fixed bug whereby an administrator was not able to edit Organization under certain circumstances • RAO administrators can see only the client cert types that are allowed for them • Fixed logo bug in IE 9.0 window • Fixed bug related to invalid CSR common name • Fixed issue related to mismatch of available notifications during Notification creation • RAOs can set up a notification which notifies MRAOs • Fixed bug related to incorrect timing of 'Your session has expired' messages • Fixed bug whereby Domains are in a 'Suspended' state after an entry by RAO |
| <u>Version 2.8.21.8</u> | <ul style="list-style-type: none"> • The functionality Settings > Email Templates for editing templates of email messages corresponding to various events is restricted only to MRAO level Administrators • Domain creation/delegation requests approved by MRAO |

| | |
|------------------------------|--|
| | <p>Administrators with privilege 'Allowing domain validation without Dual Approval' are activated immediately without requiring approval by a second MRAO.</p> <ul style="list-style-type: none"> • Domains created by DRAO Administrators are to be approved by RAO of the Organization to which the Department belongs prior to approval by MRAOs. • Added option to specify default Client Certificate Type(s) for all Organizations • Add 'Apply' button to Client Cert customization interfaces • Bug Fixes: <ul style="list-style-type: none"> • All the server types are now available in the self-enrollment form for applying for SSL certificate. • Administrators can now enroll for EV SSL Certificate manually • Fixed issues related to Firefox version 4 Browser. • Only the default Client Cert types customized for an Organization are made visible in the self-enrollment forms. • RAO and DRAO can send invitations for Client Certificates only for Certificate types allowed for their Organization • SCEP Logs are improved |
| <p><u>Version 2.8.21</u></p> | <ul style="list-style-type: none"> • Added Key Usage Template (KUT) support to determine capabilities of Client Certificates of end-users belonging to an Organization. • Implemented Simple Certificate Enrollment Protocol (SCEP) support to Client Certificates in addition to SSL Certificates. • Subscriber's Agreements are made specific to the Certificate type selected while requesting for SSL Certificate and Code Signing Certificates. • Bug Fixes: <ul style="list-style-type: none"> • Fixed bug whereby user can now enroll for Code Signing Certificates through Internet Explorer. • Fixed bug whereby DRAO Administrators can request for SSL certificates from the management interface. • Correct Subscriber Agreements are displayed on both built in application form and Self enrollment form according to Certificate type selected. • Fixed bug to accept CSR of size less than 2048 bits for SSL Certificate replacement |
| <p><u>Version 2.8.20</u></p> | <ul style="list-style-type: none"> • 'Person upload' notification messages are now customizable; • 'Active' checkbox in 'Settings/Domains' is now, by default, always enabled for MRAO; • Bug Fixes: <ul style="list-style-type: none"> • Fixed bug whereby an MRAO could bypass 'dual domain |

| | |
|--|---|
| | <p>auto approval' by using 'domain edit';</p> <ul style="list-style-type: none">• Fixed bug that sometimes allowed domains created by an MRAO to be automatically sent forward for validation without requiring approval from second MRAO;• Fixed bug where some notifications did not correspond to the modified E-mail Template;• Fixed bug that caused domain delegation requests to be displayed incorrectly;• Fixed occasional bug whereby an MRAO could modify their own privileges and/or those of a fellow MRAO;• Fixed occasional internal error that occurred when editing a deleted Administrator;• Fixed bug whereby an incorrect error would be displayed while importing from CSV;• Fixed Internal error that occurred when an RAO Admin tried to approve a Domain that had not yet been delegated by DRAO Admin;• Fixed bug that allowed Administrators to add and activate a domain for an Organization that has already been added to a Department;• Fixed bug whereby incorrect data was displayed in the domain details window;• Fixed bug whereby Client Certificate Administrators that were created in a certain manner were not made to follow password policy rules;• Fixed bug whereby variables could not be added via the 'Insert Variables' button while editing an email template in Internet Explorer;• Fixed bug whereby only active MRAO by changing admin role of another MRAO. |
|--|---|

2 The Dashboard

The CCM Dashboard will be displayed by default when an administrator first logs into the CCM interface. The dashboard provides a heads-up-display which allows you to quickly gain an overview of all SSL, S/MIME and code-signing certificates on the network.



The charts and graphs in the dashboard provide an essential combination of key life-cycle information (such as certificates approaching expiry, certificates issued/requested and DCV status) as well as important technical insights like how many servers have support for perfect forward secrecy, renegotiation and RC4 suites.

Chart data is updated in real-time, so any modifications should be reflected in the dashboard near-instantly.

Security Roles:

- MRAO - can view charts for all certificate types, domains and web servers pertaining to all Organizations

and Departments.

- RAO SSL, RAO S/MIME and RAO Code Signing - can view charts relevant to the certificate types, domains and web servers of the Organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO SSL, DRAO S/MIME and DRAO Code Signing - can view the charts relevant to the certificate types, domains and web servers of the Departments that have been delegated to them.

The area at the top of the dashboard displays a real-time summary of Active/Revoked certificates:

| | | |
|---|---|---|
| Active/Revoked Server Certificates 9 / 2 + 5 Since Last Month | Active/Revoked Client Certificates 5 / 1 + 1 Since Last Month | Active/Revoked Code Signing Certificates 1 / 0 + 0 Since Last Month |
|---|---|---|

Filtering Options:

The statistics displayed in the dashboard can be filtered based on the time period and by Organization/Department:

Filter by: Organization: Department: Time Period:

- To add a filter
 - Choose an Organization / Department from the respective drop-downs
 - Select the time period for which you wish to view statistics from the 'Time Period' drop-down
 - Click 'Apply'
- To reset the filters, click 'Clear'

Charts available in first release. Click any link to view more details:

- **Expiring Certificates by Issuer** - Comodo, self-signed and 'Other Trusted' certificates expiring within 180 days
- **DCV Expiring Domains** - Domains for which Domain Control Validation will expire within 180 days
- **Certificates Types (Managed)** - Single Domain, Wildcard, Multi-Domain, UCC etc.
- **Certificates by Validation Level** - EV, DV, OV.
- **SSL Certificate Types** - Certificates issued through CCM and broken down by brand names like Instant SSL, Premium SSL, EV SSL etc.
- **Certificate Requests versus Certificates Issued**
- **Certificates by CA** - Comodo, VeriSign, GoDaddy, Thawte, self-signed etc.
- **Certificate Requests by Category of Certificate** - SSL requests, S/MIME requests, Code signing requests
- **Certificates By Duration** - How many of your certificates are 1 year, 2 year, 3 year etc
- **DCV Status** - The current stage in the Domain Control Validation process held by your certificate-hosting domains
- **Certificates by Organization** - Certificates broken down by the Organizations they are issued to.
- **Certificates by Key Strength** - Certificates by the strength of key with which they were signed (1024 bit, 2048 bit etc)
- **Certificates by Signing Algorithm** - Certificates by hashing and signing algorithms (e.g. SHA1withRSA)
- **Certificates by Public Key Algorithm** - Certificates broken down by encryption algorithm (RSA, DSA etc)

Charts which are coming soon. Click any link to view more details:

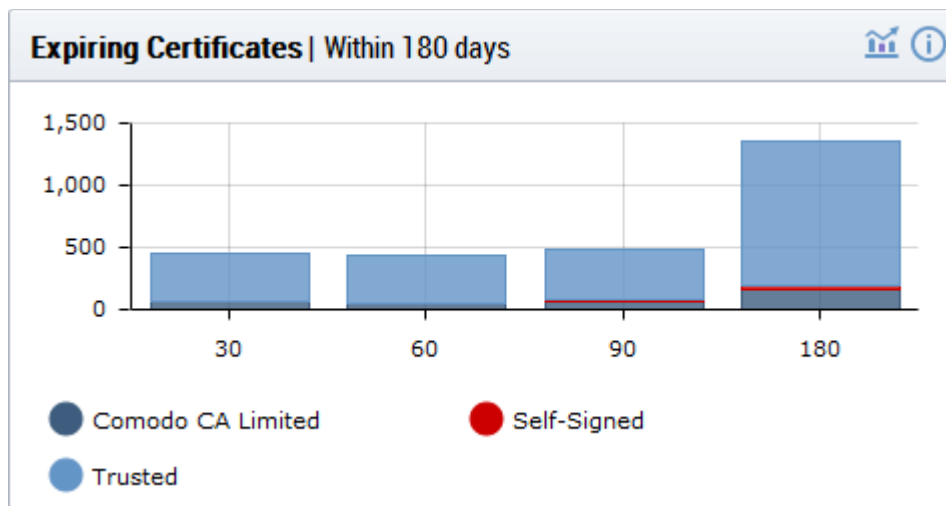
- **EV Expiring Organizations** - Organizations whose eligibility for accelerated EV validation will expire within

180 days.

- **Forward Secrecy** - The degree to which forward secrecy is supported on the web-servers hosting your certificates
- **Hosted by OS** - Details the server operating systems used to host your certificates (Windows, Linux etc)
- **RC4 Support** - The level of support for RC4 suites on the web-servers that host your certificates
- **Renegotiation Support** - The level of renegotiation support on the web-servers that host your certificates
- **Supported Protocols** - The types of encryption protocols supported by the web-servers that host your certificates
- **Certificates by port number** - The port numbers used for SSL traffic on the web-servers that host your certificates

Expiring Certificates

The 'Expiring Certificates' bar graph shows the number of certificates expiring within the next 30, 60, 90 and 180 days. Expiring certificates are further broken down according to signer. 'Trusted' certificates are those from other CAs which you may want to replace with Comodo certificates in order to benefit from CCM's management capabilities.



- Hovering the mouse cursor over a legend or graph displays the number of certificates in each category.
- Clicking on the information icon ⓘ displays a tool tip explaining the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart:

| COMMON NAME | ORGANIZATION | DEPARTMENT | EXPIRES |
|------------------------------------|----------------------|---------------|------------|
| *gehitachi.workforcehosting.com * | org1 | | 07/21/2015 |
| exch.bridgetree.com * | org1 | | 06/17/2015 |
| *comcastv.com * | OrganizationNumber12 | Department248 | |
| exchange.howardchem.com * | DCV_check_org | | 08/31/2015 |
| webmail.medcommbilling.com * | DCV_check_org | | 05/28/2015 |
| www.onedegreeevents.com * | DCV_check_org | | 04/12/2015 |
| contract.restorationhardware.com * | DCV_check_org | | 04/14/2015 |

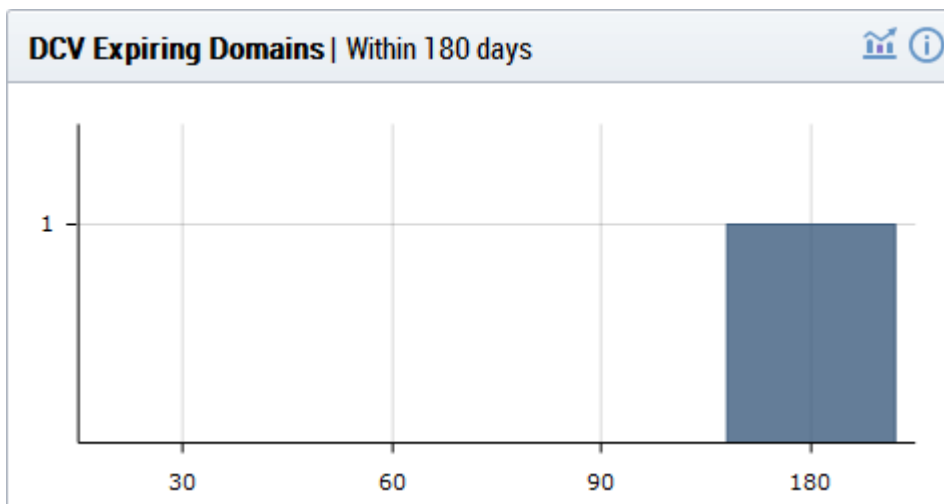
15 rows/page 1 - 15 out of 2716

Close

| 'Expiring Certificates Report' Table - Column Descriptions | |
|--|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Expires | The expiration date of the certificate. |



DCV Expiring Domains

The chart indicates how many of your domains are within 30, 60, 90 and 180 days of DCV (domain control validation) expiry. DCV validity lasts for one year so it is possible DCV might be approaching expiry even though your certificate is not. If DCV is allowed to expire, it will not mean your certificate becomes invalid/stops functioning. However, your next application for that domain will need to pass DCV again.



- Placing the mouse cursor over a legend or graph displays a tool-tip showing the number of domains within

that time-frame.

- Clicking on the information icon  displays a tool tip explaining the chart
- Clicking on the graph icon  displays a report with the breakdown of statistics shown in the chart:

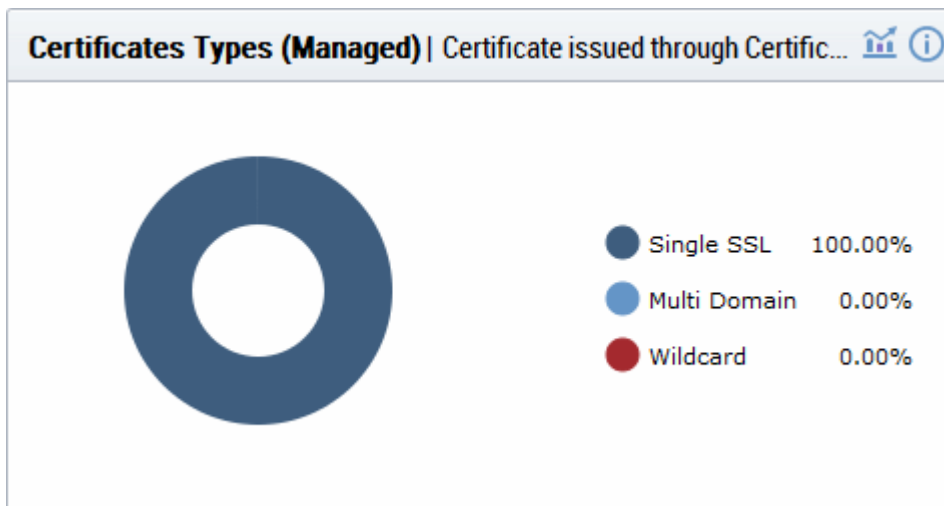
| NAME | DELEGATION STATUS | DATE REQUESTED | DCV STATUS |  |
|---------------|-------------------|----------------|------------|---|
| *.dithers.com | Approved | 09/05/2013 | Validated | |
| dithers.com | Approved | 09/05/2013 | Validated | |



15 rows/page 1 - 2 out of 2 

| 'DCV Expiring Domains Report' Table - Column Descriptions | |
|---|---|
| Column Header | Description |
| Name | The name of the domain. |
| Delegation Status | Indicates whether domain is active or inactive |
| Date Requested | Indicates the date on which the domain was requested. |
| DCV Status | Indicates the request/approval status of the domain. |

Certificate Types (Managed)

The 'Certificate Types' pie chart summarizes the different types of SSL certificates installed on servers in your network. (single domain, wildcard, multi-domain etc). This chart covers only 'managed' certificates issued through CCM.



- Hovering your mouse cursor over a legend item or section displays additional details such as the actual quantity of certificates of that type.
- Clicking on the information icon  displays a tool tip on the chart
- Clicking on the graph icon  displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | SSL TYPE |
|------------------------|----------------------|------------|------------------------------|
| abcdcomp.com (renewed) | ABCD Company | | Instant SSL |
| bestorg.com | Best Organization | | Instant SSL |
| capitalbus.com | Capital Business | | Instant SSL |
| duncangift.com | Dungan Gift Shop | | Instant SSL |
| elegantamp.com | Elegant Organization | | Comodo EV SSL Certificate |

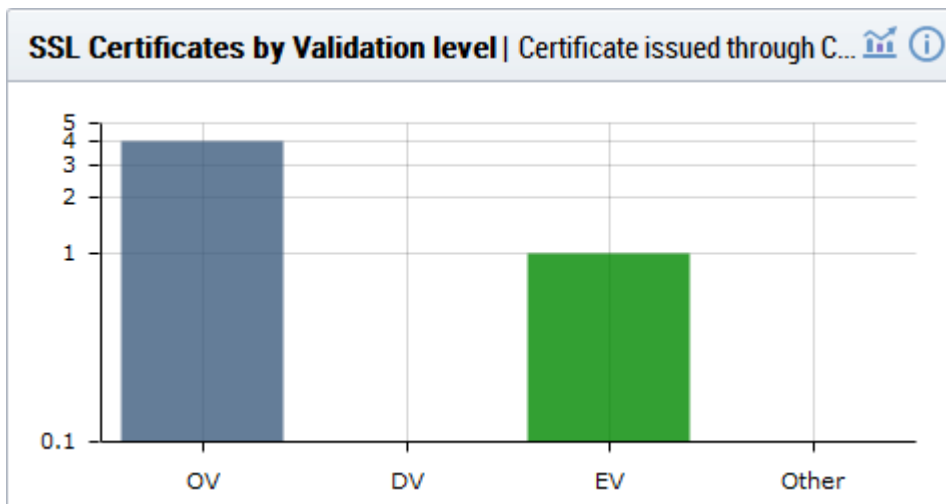
5 rows/page 1 - 5 out of 5

Close

| 'Managed Certificate Types Report' Table - Column Descriptions | |
|--|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| SSL Type | Indicates type of the certificate with its brand name |

Certificates by Validation Level

The chart displays the composition of your certificate portfolio according to certificate validation level. This includes the number of Domain Validated, Organization Validated and Extended Validation certificates on your network.



- Hovering the mouse cursor over a bar displays the exact number of certificates in that category.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the details icon 📊 displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | SUB TYPE |
|------------------------|----------------------|------------|----------|
| abcdcomp.com (renewed) | ABCD Company | | OV |
| bestorg.com | Best Organization | | OV |
| capitalbus.com | Capital Business | | OV |
| duncangift.com | Dungan Gift Shop | | OV |
| elegantamp.com | Elegant Organization | | EV |

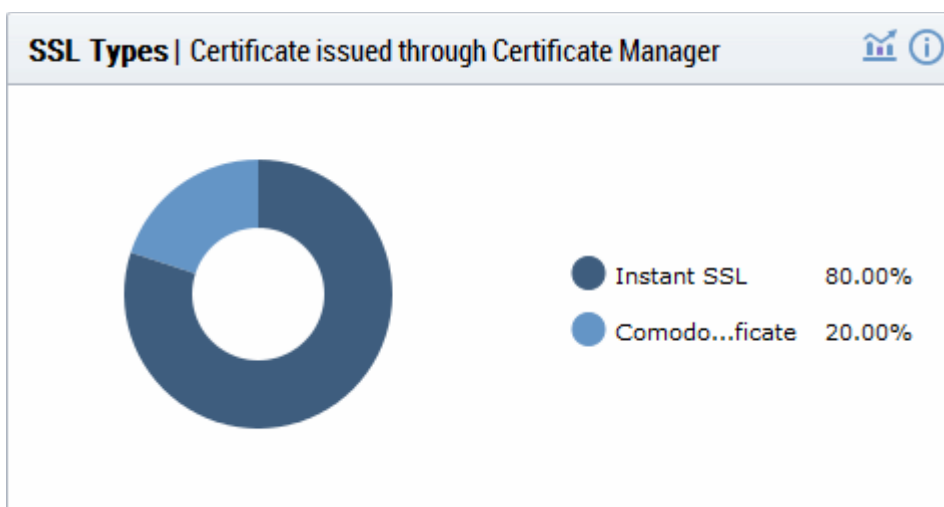
15 rows/page 1 - 5 out of 5

Close

| 'SSL Certificates by Validation Level Report' Table - Column Descriptions | |
|---|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Sub Type | Indicates validation level of the certificate, like Domain Validated, Organization Validated and Extended Validation. |

SSL Types

The 'SSL Types' chart details the quantities of SSL certificates issued by CCM according to certificate brand name.



- Hovering your mouse over a legend or sector displays additional details.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | SSL TYPE |
|------------------------|----------------------|------------|------------------------------|
| abcdcomp.com (renewed) | ABCD Company | | Instant SSL |
| bestorg.com | Best Organization | | Instant SSL |
| capitalbus.com | Capital Business | | Instant SSL |
| duncangift.com | Dungan Gift Shop | | Instant SSL |
| elegantamp.com | Elegant Organization | | Comodo EV SSL Certificate |

15 rows/page 1 - 5 out of 5

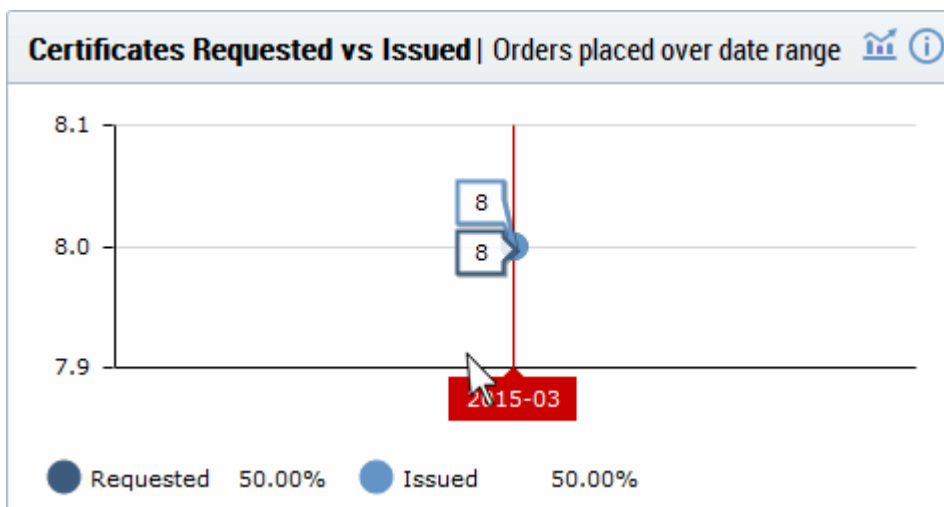
Close

| 'SSL Types Report' Table - Column Descriptions | |
|--|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| SSL Type | Indicates brand name of the certificate. |

Note: Certificates with 'Issued' status are shown with blue text

Certificates Requested vs Issued

The 'Certificates Requested vs Issued' graph allows you to view certificate issuance against certificate requests over time.



- Placing the mouse cursor over the graph nodes displays more details about the number of certificates that were requested and issued on that date.
- Clicking on the information icon ⓘ displays a tool tip on the chart

- Clicking on the details icon  displays a report with the breakdown of statistics shown in the chart

| CERTIFICATE TYPE | ORGANIZATION | DEPARTMENT | ORDER NUMBER | SERIAL NUMBER | TERM | STA |
|------------------|-------------------|------------|--------------|--|------|------|
| SSL | ABCD Company | | 1299179 | 4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1 | 365 | Issu |
| SSL | Best Organization | | 1304831 | 73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:1 | 365 | Issu |
| SSL | Capital Business | | 1304801 | E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:1 | 365 | Issu |
| SSL | Duncan Gift Shop | | 1304839 | 70:F9:12:B3:5D:96:76:86:C9:B9:44:16:76:7 | 365 | Issu |
| SSL | Elegant | | 1304800 | DE:EA:B3:FE:08:7F:48:F8:27:33:96:67:C7:2 | 365 | Revc |
| SSL | Elegant | | 1304836 | 6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B | 365 | Issu |
| Client cert | ABCD Company | | 1303940 | F3:49:8B:A9:29:24:60:64:7D:2D:32:B9:A3:2 | 1 | Revc |
| Client cert | Best Organization | | 1305101 | 38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:1 | 1 | Issu |

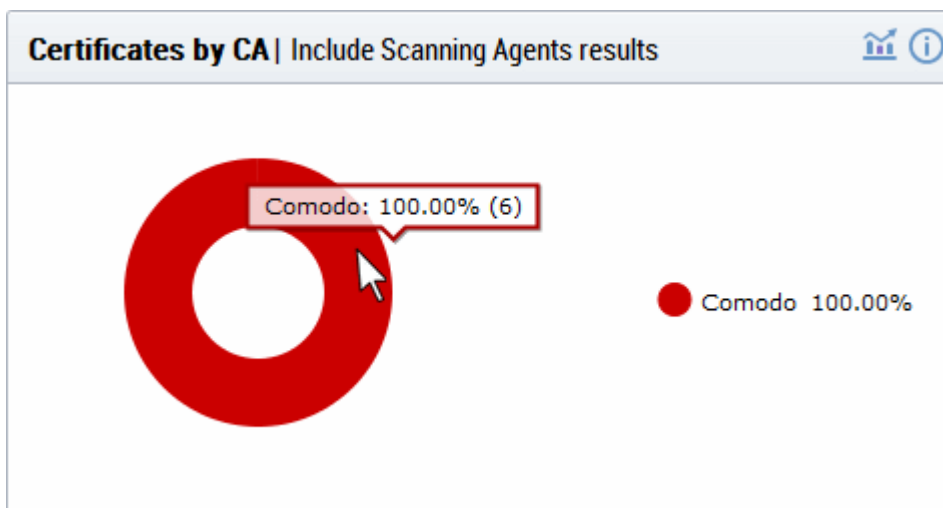
15 rows/page 1 - 8 out of 8



'Certificates Requested Vs Issued Report' Table - Column Descriptions

| Column Header | Description |
|------------------|---|
| Certificate Type | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Order Number | Indicates the number assigned by the Certification Authority (CA) for the request. |
| Serial Number | Displays the serial number of the certificate that is unique and can be used to identify the certificate. |
| Term | The length of time the certificate is (or will be) valid for from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process. |
| State | Indicates the current status of the certificate. |
| Requested | The date at which the certificate was requested by the end-user or the administrator |
| Collected | The date at which the certificate was collected by the end-user or the administrator |
| Expires | The date of expiry of the certificate |

Certificates by CA

The 'Certificates by CA' chart allows you to determine what percentage (%) of your certificates are publicly trusted by providing a break-down of certificates by signer. This includes all certificates signed by Certificate Authorities (CA) and those which are self-signed. It also highlights certificates from other CAs which you may want to replace with Comodo equivalents in order to benefit from CCM's management capabilities.



- Placing your mouse cursor over a legend or sector displays the number of certificates by that signer and their % of the total certificates.
- Clicking on the information icon  displays a tool tip on the chart
- Clicking on the graph icon  displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | VENDOR |
|------------------------|-------------------|------------|-------------------|
| bestorg.com | Best Organization | | Comodo CA Limited |
| abcdcomp.com (renewed) | ABCD Company | | Comodo CA Limited |
| capitalbus.com | Capital Business | | Comodo CA Limited |
| duncangift.com | Duncan Gift Shop | | Comodo CA Limited |
| dynacom.com (renewed) | Duncan Gift Shop | | Comodo CA Limited |
| elegantamp.com | Elegant | | Comodo CA Limited |

15 rows/page 1 - 6 out of 6

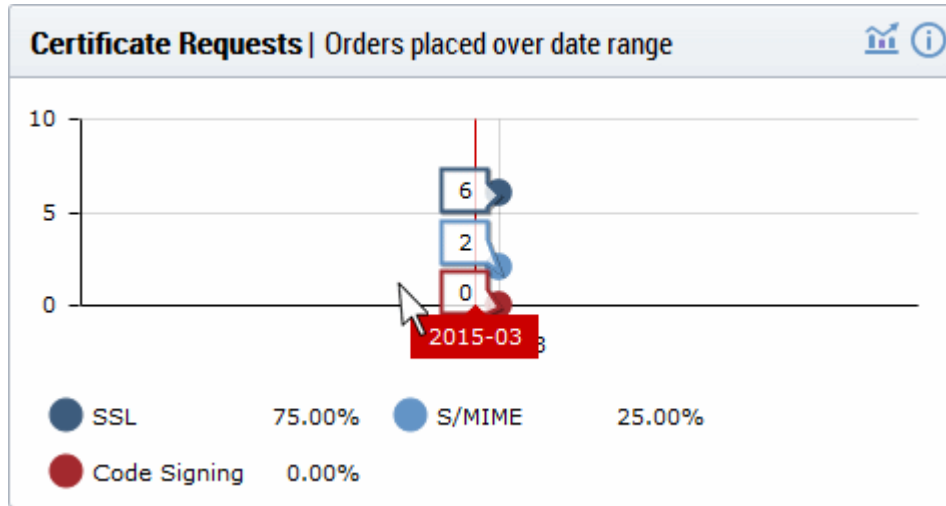
Close

| 'Certificates by CA Report' Table - Column Descriptions | |
|---|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Vendor | Shows the vendor that has issued the certificate. |

Note: Certificates with 'Issued' status are shown with blue text

Certificate Requests

The 'Certificates Requests' graph displays the number of CCM orders placed over time for SSL, S/MIME and Code Signing certificates.



- Hovering the mouse cursor over the nodes on the graph displays the exact number of certificates that were requested.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| CERTIFICATE TY | ORGANIZATION | DEPARTMENT | ORDER NUMBER | SERIAL NUMBER |
|----------------|-------------------|------------|--------------|---|
| SSL | ABCD Company | | 1299179 | 4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97 |
| SSL | Best Organization | | 1304831 | 73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:DE:AC:0 |
| SSL | Capital Business | | 1304801 | E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:C8:01:1 |
| SSL | Duncan Gift Shop | | 1304839 | 70:F9:12:B3:5D:96:76:86:C9:B9:44:16:76:72:3A:C0 |
| SSL | Elegant | | 1304800 | DE:EA:B3:FE:08:7F:48:F8:27:33:96:67:C7:2F:25:46 |
| SSL | Elegant | | 1304836 | 6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B:09:9A:1 |
| Client cert | ABCD Company | | 1303940 | F3:49:8B:A9:29:24:60:64:7D:2D:32:B9:A3:27:03:A9 |
| Client cert | Best Organization | | 1305101 | 38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:3 |

15 rows/page 1 - 8 out of 8

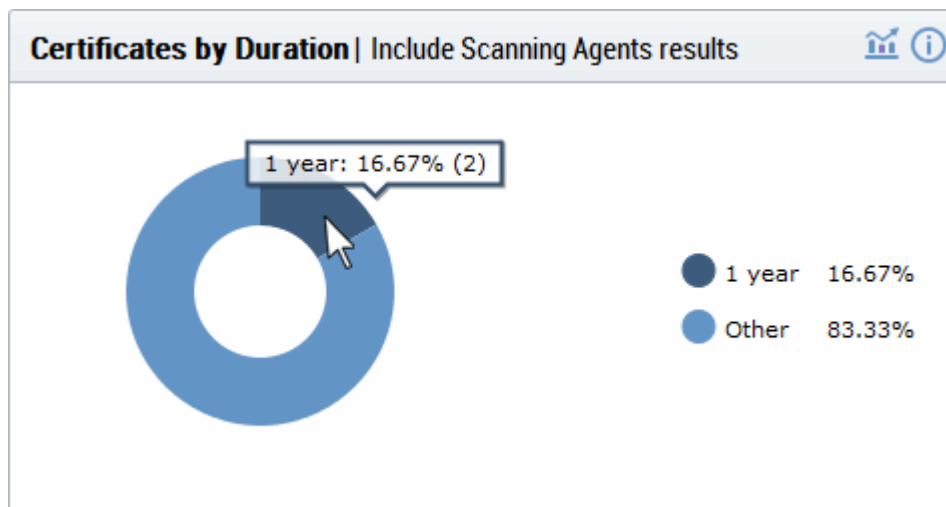
Close

| 'Certificates Requests Report' Table - Column Descriptions | |
|--|--|
| Column Header | Description |
| Certificate Type | The domain for which the certificate was requested / issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |

| | |
|---------------|---|
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Order Number | Indicates the number assigned by the Certification Authority (CA) for the request. |
| Serial Number | Displays the serial number of the certificate that is unique and can be used to identify the certificate. |
| Term | The length of time the certificate is (or will be) valid for from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process. |
| State | Indicates the current status of the certificate. |
| Requested | The date at which the certificate was requested by the end-user or the administrator |
| Collected | The date at which the certificate was collected by the end-user or the administrator |
| Expires | The date of expiry of the certificate |

Certificates by Duration

The 'Certificates by Duration' pie chart is a break-down of your certificates by term length.



- Hovering your mouse cursor over a legend or section displays the exact number of certificates with that term length and their percentage of the total.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| CERTIFICATE TY | ORGANIZATION | DEPARTMENT | ORDER NUMBER | SERIAL NUMBER |
|----------------|-------------------|------------|--------------|---|
| SSL | ABCD Company | | 1299179 | 4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97 |
| SSL | Best Organization | | 0 | |
| SSL | Capital Business | | 0 | |
| SSL | Duncan Gift Shop | | 0 | |
| SSL | Elegant | | 1304831 | 73:29:5D:E2:42:1E:85:B3:EB:43:3C:5D:A0:DE:AC:0 |
| SSL | Elegant | | 1304801 | E7:3F:B5:9E:FF:51:5F:FD:8C:1C:90:64:0F:C8:01:1 |
| SSL | ABCD Company | | 1304839 | 70:F9:12:B3:5D:96:76:86:C9:B9:44:16:76:72:3A:C0 |
| SSL | Best Organization | | 0 | |
| SSL | Elegant | | 1304800 | DE:EA:B3:FE:08:7F:48:F8:27:33:96:67:C7:2F:25:40 |
| SSL | Elegant | | 1304836 | 6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B:09:9A:0 |
| Client cert | ABCD Company | | 1303940 | F3:49:8B:A9:29:24:60:64:7D:2D:32:B9:A3:27:03:A9 |
| Client cert | Best Organization | | 1305101 | 38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:3 |

15 rows/page 1 - 12 out of 12

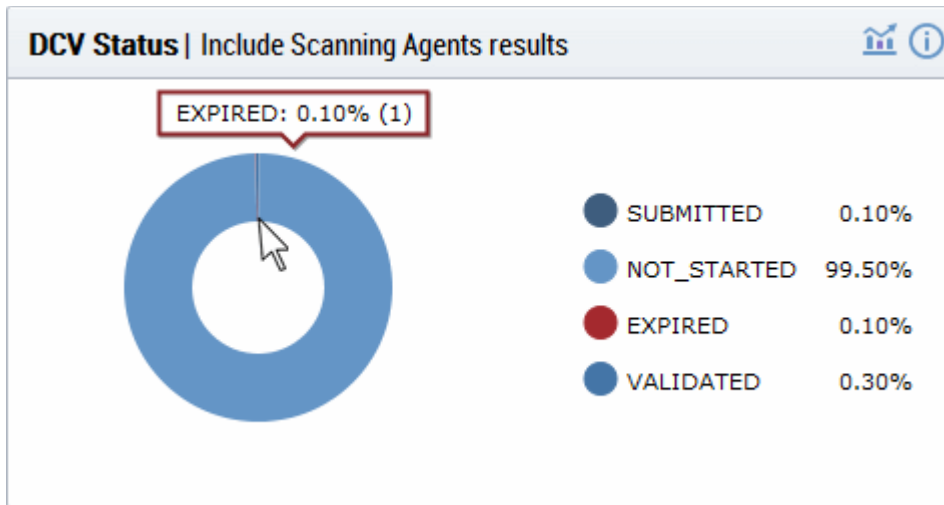
Close

| 'Certificates by Duration' Table - Column Descriptions | |
|--|---|
| Column Header | Description |
| Certificate Type | The domain for which the certificate was requested / issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Order Number | Indicates the number assigned by the Certification Authority (CA) for the request. |
| Serial Number | Displays the serial number of the certificate that is unique and can be used to identify the certificate. |
| Term | The length of time the certificate is (or will be) valid for from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process. |
| State | Indicates the current status of the certificate. |
| Requested | The date at which the certificate was requested by the end-user or the administrator |
| Collected | The date at which the certificate was collected by the end-user or the administrator |
| Expires | The date of expiry of the certificate |

DCV Status

The chart shows a summary of Domain Control Validation (DCV) status of domains registered within the CM. DCV is

required in order for Comodo to issue certificates to your domains and sub-domains. We advise customers to first complete DCV on their registrable domain (e.g. domain.com). Once the domain has passed DCV, then future certificate applications will be faster, because all sub-domains, including wildcards, will also be considered complete.



- Hovering your mouse cursor over a legend or section displays the quantity of domains with a particular status and their percentage of the total domains.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| NAME | DELEGATION STATUS | DATE REQUESTED | DCV STATUS | |
|----------------|-------------------|----------------|------------|--|
| abcdcomp.com | Approved | 08/28/2013 | | |
| bestorg.com | Approved | 08/29/2013 | | |
| capitalbus.com | Approved | 08/28/2013 | | |
| duncangift.com | Approved | 08/28/2013 | | |
| elegantamp.com | Approved | 08/29/2013 | | |

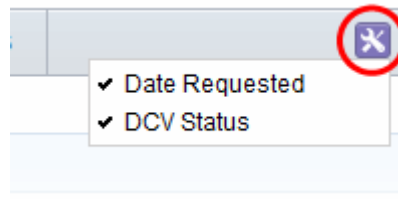
5 rows/page 1 - 5 out of 1003

Close

| 'DCV Status Report' Table - Column Descriptions | |
|---|--|
| Column Header | Description |
| Name | The name of the domain. |
| Delegation Status | Indicates the state of the domain within CCM. (Approved, Requested, etc.) |
| Date Requested | Indicates the date on which the domain was requested. |
| DCV Status | Indicates the validation state of domain within CCM. (Validated, Validated (revalidation) Expired (revalidation), Awaiting Submittal, etc.) |

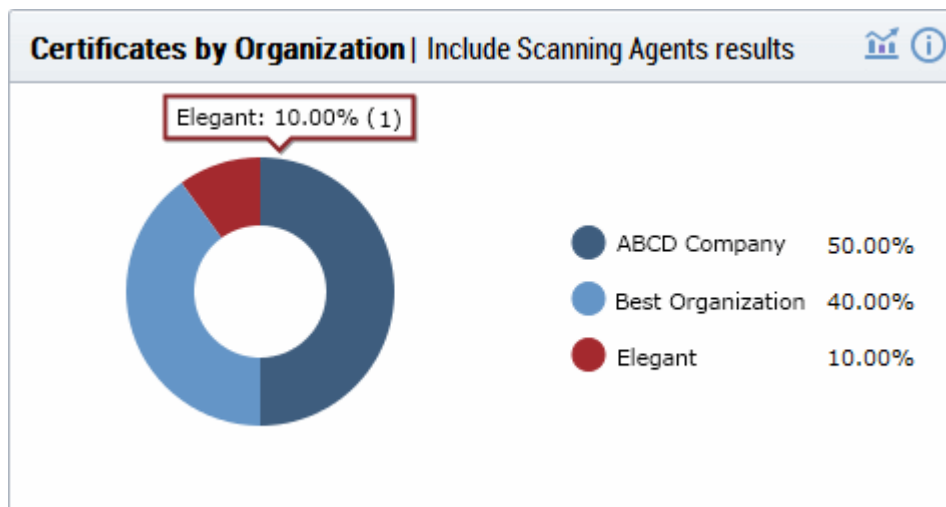
You can select the columns to be displayed by clicking the settings icon at the top right of the table and choosing the



columns.



Certificates by Organization

The 'Certificates by Organization' chart shows how many certificates have been issued to each Organization in your CCM account.



- Hovering your mouse cursor over a legend or section displays the precise number and percentage of total certificates issued to a particular Organization.
- Clicking on the information icon  displays a tool tip on the chart
- Clicking on the graph icon  displays a report with the breakdown of statistics shown in the chart

| CERTIFICATE TY | ORGANIZATION | DEPARTMENT | ORDER NUMBER | SERIAL NUMBER |
|----------------|-------------------|------------|--------------|---|
| SSL | ABCD Company | | 1304836 | 6C:D6:FE:FE:E5:07:CE:24:46:C0:EF:D0:1B:09:9A: |
| SSL | ABCD Company | | 1299179 | 4C:40:79:1F:31:93:64:9B:65:A0:55:EF:5F:1E:A8:97 |
| SSL | Best Organization | | 0 | |
| SSL | Elegant | | 0 | |
| Client cert | Best Organization | | 1305101 | 38:D4:BE:81:BE:BA:6A:D9:F3:7A:76:F9:16:C1:95:3 |

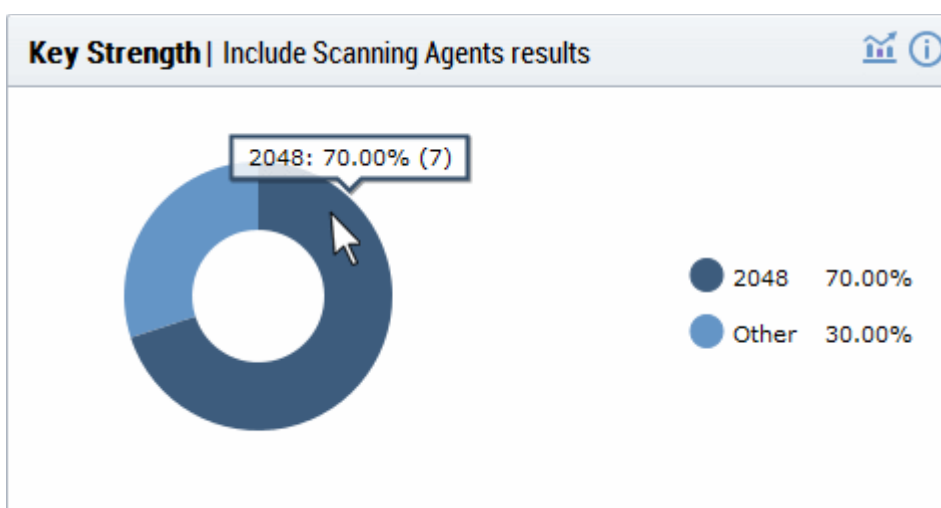
5 rows/page 6 - 10 out of 10

Close

| 'Certificates by Organization' Table - Column Descriptions | |
|--|---|
| Column Header | Description |
| Certificate Type | The domain for which the certificate was requested / issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Order Number | Indicates the number assigned by the Certification Authority (CA) for the request. |
| Serial Number | Displays the serial number of the certificate that is unique and can be used to identify the certificate. |
| Term | The length of time the certificate is (or will be) valid for from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process. |
| State | Indicates the current status of the certificate. |
| Requested | The date at which the certificate was requested by the end-user or the administrator |
| Collected | The date at which the certificate was collected by the end-user or the administrator |
| Expires | The date of expiry of the certificate |

Key Strength

The 'Key Strength' chart shows the composition of your certificate portfolio based on the size of their signature. This can be useful for identifying certificates which need to be replaced in order to be compliant with National Institute of Standards (NIST) recommendations. NIST has stated that all certificates, using the RSA algorithm, issued after 1st January 2014 should be of at least 2048 bit in key length.



- Placing your mouse cursor over a legend or sector displays the exact number of certificates with a particular signature size and their percentage of the total certificates.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | EXPIRES | KEY ALGORITHM | KEY SIZE |
|-----------------------|-------------------|------------|------------|---------------|----------|
| abcdcomp.com | ABCD Company | | 03/10/2016 | RSA | 2048 |
| elegantamp.com | Elegant | | | | 0 |
| abcdcorp.com | ABCD Company | | | | 0 |
| abcdmail.com | ABCD Company | | | | 0 |
| bestorg.com (renewed) | Best Organization | | 11/02/2015 | RSA | 2048 |

5 rows/page 1 - 5 out of 10

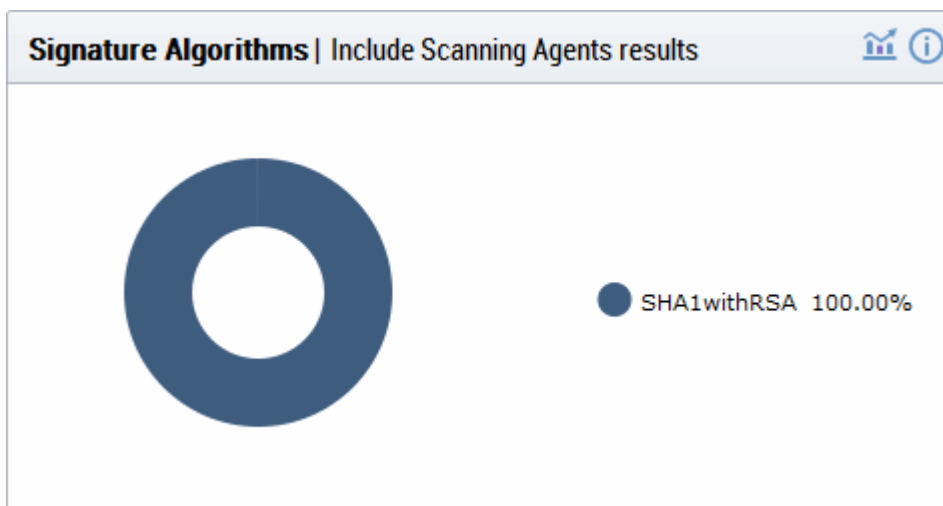
Close

| 'Key Strength Report' Table - Column Descriptions | |
|---|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Expires | The date of expiry of the certificate |
| Key Algorithm | Displays the type of algorithm used, by the public and private keys, for encryption. (RSA, DSA, EC, etc.) |
| Key Size | Displays the key size used, on the public and private keys, for encryption. (1024, 2048, 4096, etc.) |

Note: Certificates with 'Issued' status are shown with blue text

Signature Algorithm

The chart provides an overview of the algorithms used by your certificates to hash and sign data. This chart can be useful for identifying certificates using weaker algorithms which may need to be replaced before their expiry dates. Comodo recommends SHA-256 and upwards. MD5 has been proven insecure and Microsoft has stated its products will stop trusting SHA-1 code-signing and SSL certificates in 2016 and 2017 respectively.



For more details, see <http://www.comodo.com/e-commerce/SHA-2-transition.php>

- Placing your mouse cursor over a legend or sector displays the exact number of certificates using a particular signature algorithm and their percentage of the total certificates.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | EXPIRES | SIGNATURE ALGORITHM |
|-----------------------|-------------------|------------|------------|---------------------|
| abcdcomp.com | ABCD Company | | 03/10/2016 | SHA1withRSA |
| elegantamp.com | Elegant | | | |
| abcdcorp.com | ABCD Company | | | |
| abcdmail.com | ABCD Company | | | |
| bestorg.com (renewed) | Best Organization | | 11/02/2015 | SHA1withRSA |

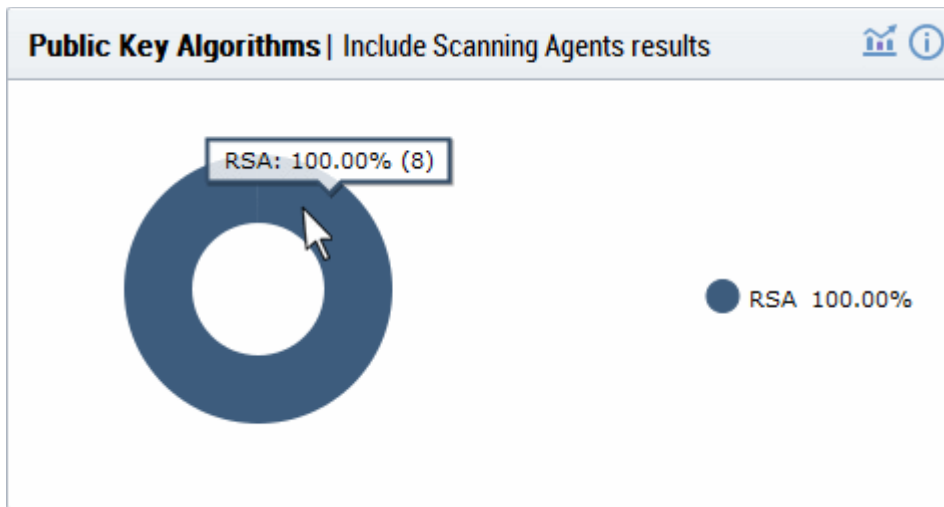
5 rows/page 1 - 5 out of 11

Close

| 'Signature Algorithm Report' Table - Column Descriptions | |
|--|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Expires | The date of expiry of the certificate |
| Signature Algorithm | Displays the type of signature algorithm used by the certificate. (SHA1 with RSA, SHA 256 with RSA, SHA384 with RSA, etc.) |

Public Key Algorithm

This chart provides an overview of the algorithms used to encrypt data by certificates on your network. Example algorithms include RSA, DSA and ECC.



- Placing your mouse cursor over a legend or sector displays the exact number of certificates using a particular public key algorithm and their percentage of the total certificates.
- Clicking on the information icon ⓘ displays a tool tip on the chart
- Clicking on the graph icon 📊 displays a report with the breakdown of statistics shown in the chart

| COMMON NAME | ORGANIZATION | DEPARTMENT | EXPIRES | SIGNATURE ALGORITHM | KEY ALGORITHM |
|-----------------------|-------------------|------------|------------|---------------------|---------------|
| abcdcomp.com | ABCD Company | | 03/10/2016 | SHA1withRSA | RSA |
| elegantamp.com | Elegant | | | | |
| abcdcorp.com | ABCD Company | | | | |
| abcdmail.com | ABCD Company | | | | |
| bestorg.com (renewed) | Best Organization | | 11/02/2015 | SHA1withRSA | RSA |

5 rows/page 1 - 5 out of 11

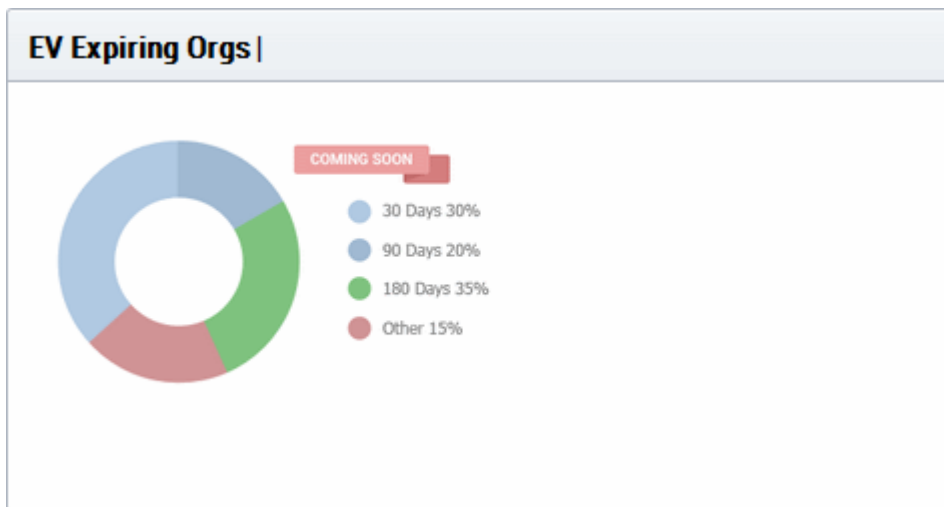
Close

| 'Public Key Algorithm Report' Table - Column Descriptions | |
|---|--|
| Column Header | Description |
| Common Name | The domain for which the certificate was issued. This domain name refers to the 'Common Name' field in the SSL certificate itself. |
| Organization | Name of the Organization that has been issued with the certificate. |
| Department | The specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Expires | The date of expiry of the certificate |

| | |
|---------------------|---|
| Signature Algorithm | Displays the type of signature algorithm used by the certificate. (SHA1 with RSA, SHA256 with RSA, SHA384 with RSA, etc.) |
| Key Algorithm | Displays the type of algorithm used, by the public and private keys, for encryption. (RSA, DSA, EC, etc.) |

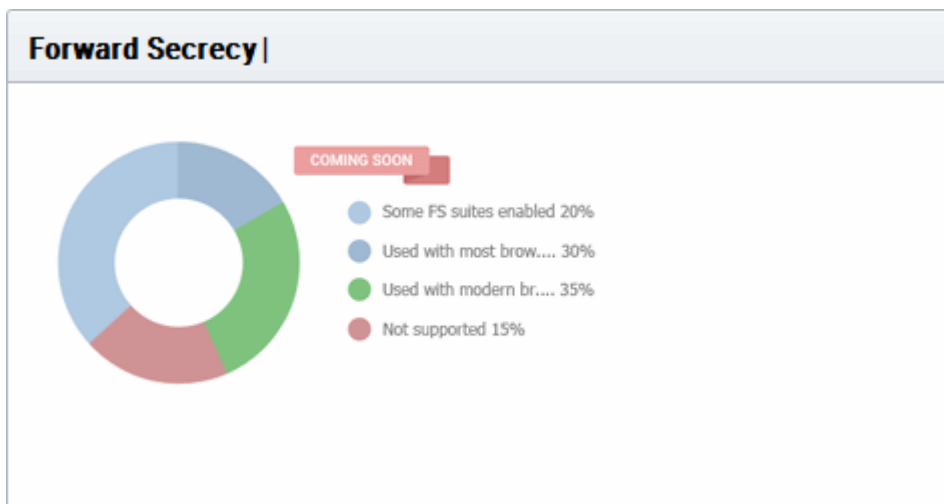
EV Expiring Organizations - coming soon

The chart displays the percentage of Organizations for which accelerated validation of one or more EV certificates will expire within 30, 90 and 180 days. Once an EV certificate has been validated for the high level domain (e.g. domain.com) it qualifies for EV Express and subsequent EV applications for that domain and it's sub-domains will be issued much more quickly (assuming address and contact details are not changed). EV Express status lasts for 13 months before it must be renewed by re-validating the details of the certificate on the high level domain.



Forward Secrecy Enabled - coming soon

The chart displays the percentage of certificates which are hosted on web-servers which have perfect forward secrecy fully or partially enabled. Forward secrecy prevents encrypted data from previous sessions from being decrypted in the event that the private key of the certificate is compromised.



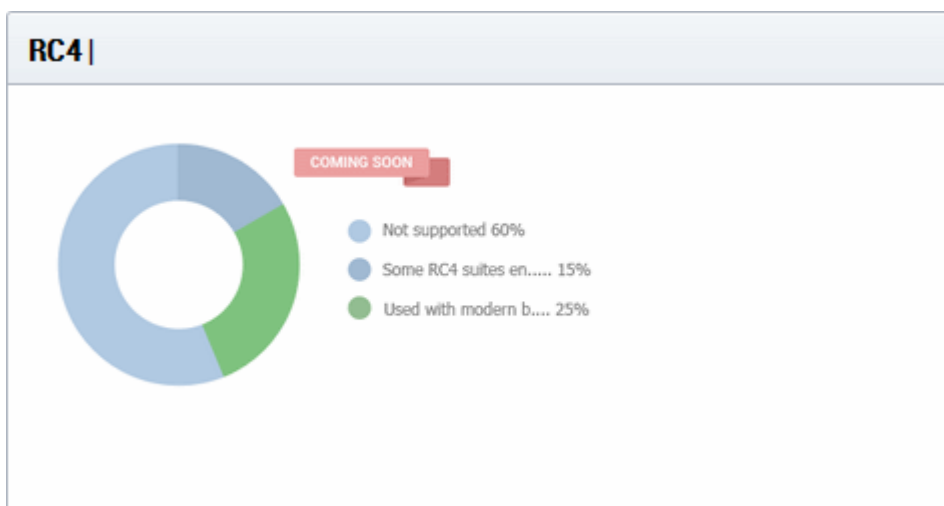
Hosted by OS - coming soon

The chart provides a visual break-down of the server operating systems used to host your certificates.



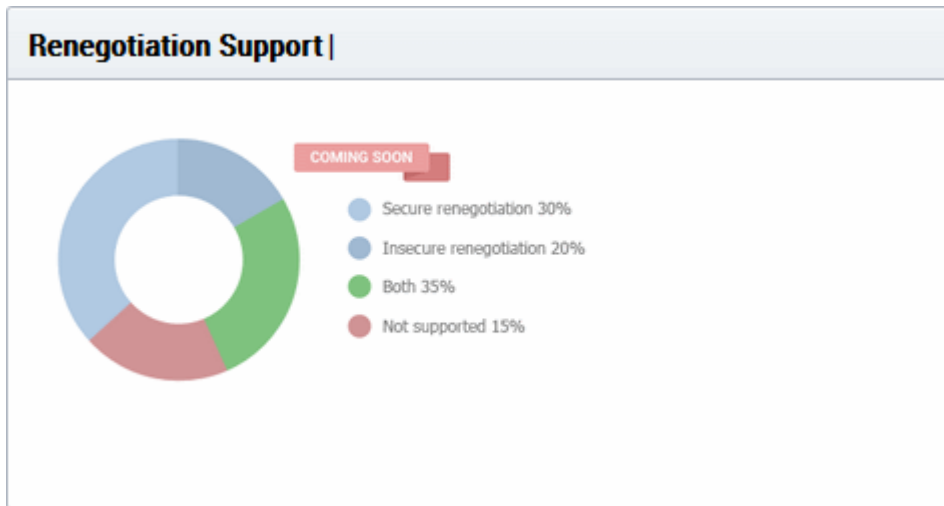
RC4 - coming soon

The chart indicates the degree to which the RC4 streaming cipher is supported by servers hosting your certificates. If your environment can operate without RC4, it is best practice to disable it.



Renegotiation Support - coming soon

Renegotiation is a feature that makes it possible to adjust the parameters of an SSL connection without disrupting the user experience by requiring an entirely new session. Take, for example, the case of an anonymous user browsing an e-commerce website who adds some products to the shopping cart then decides to login and purchase. Renegotiation allows the data from the 'anonymous' session to be transposed in a fluid and secure fashion. Unfortunately, security flaws were discovered in renegotiation in TLS 1 / SSL 3 which required a patch to fix. Unpatched web servers are shown here as 'Insecure renegotiation'.



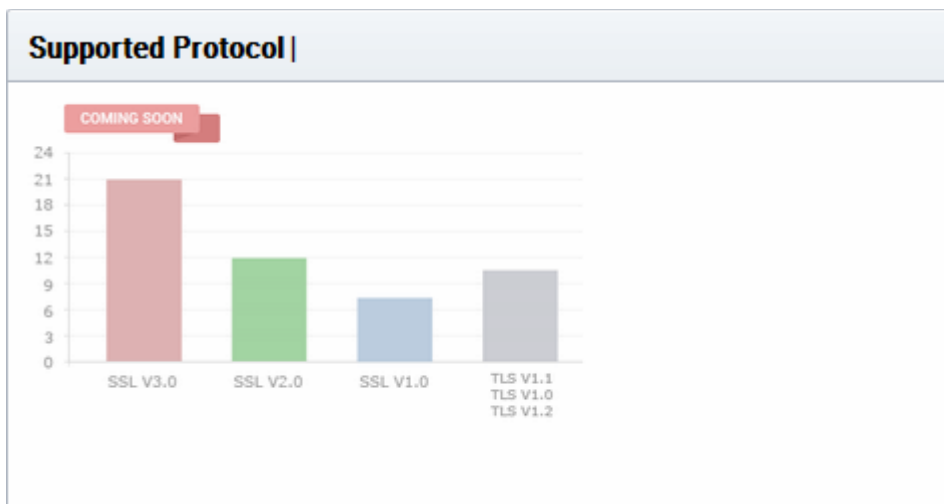
Supported Protocol - coming soon

Shows the support for various cryptographic protocols on the web servers which are used to host your certificates. While we recommend each customer to investigate the precise impact of disabling a given protocol by analyzing the browsers used by their visitors, Comodo would recommend the following:

TLS 1.1, 1.2 - Enable

SSL 3.0 / TLS 1.0 - Discretionary. Disable preferred *

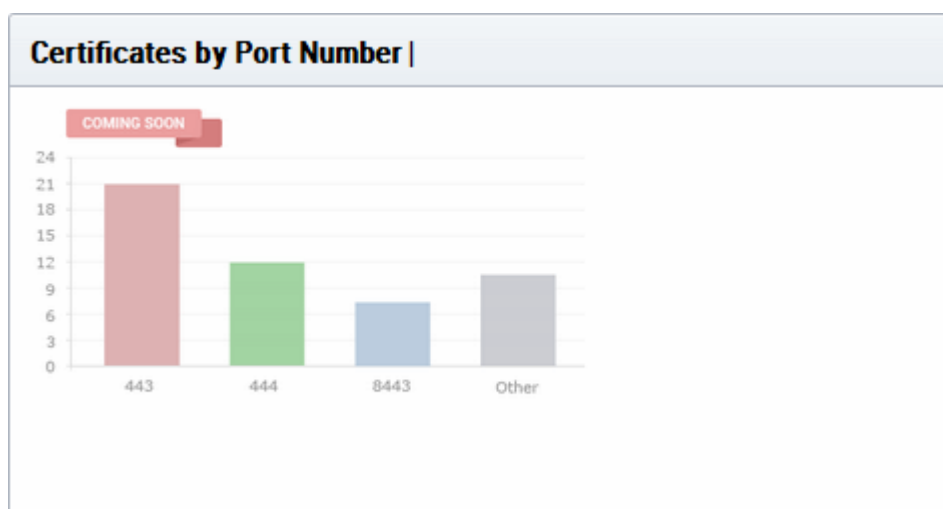
SSL 2.0 - Disable



* SSL 3.0 / TLS 1.0 is needed mainly for Windows XP / Internet Explorer 6.0 users. Microsoft have discontinued support for these systems and their use by the public has waned significantly. However, CCM customers *may* want to retain support in the short-medium term if widely supported by their user base.

Certificates by Port Number - coming soon

The chart shows the port numbers that are used for secure connections on web-servers that host your certificates.



3 Certificates Management

The 'Certificates' tab provides appropriately privileged administrators with the ability to request, collect, revoke and manage SSL, Client and Code Signing certificates.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|----------------------|--------------|------------|--------|------------|---------------|---------------|
| test.ccmqa.com[61] | org1 | | Issued | 01/14/2018 | Successful | Not scheduled |
| demo.ccmqa.local[60] | org2 | | Issued | 01/14/2018 | Not scheduled | Not scheduled |
| test.ccmqa.com[59] | org1 | | Issued | 01/14/2018 | Successful | Not scheduled |
| p1.ccmqa.local[58] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| l1.local[57] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |

It is divided into three main administrative areas, namely the SSL Certificates tab, the Client Certificates tab and the Code Signing Certificates tab.

This chapter provides guidance on the Certificates Management interface and explains the processes behind the administration and provisioning of SSL certificates, client certificates and code signing certificates. This chapter is divided into the following sections:

3.1 The SSL Certificates area - High level introduction to the SSL interface. Contains brief explanations of functionality and an overview of Comodo SSL certificate types.

3.1.2 Request and Issuance of SSL Certificates to Web Servers and Hosts - Detailed explanations of the entire application, provisioning and life management of SSL web server certificates.

3.2 The Client Certificates area - Introduction to the Client Certificate interface that covers basic interface functionality and the creation, import and management of certificate end-users.

3.2.5 Request and Issuance of Client Certificates to Employees and End-Users - Detailed explanations of the initiation, application, provisioning, collection and management of Client Certificates.

3.3 The Code Signing Certificates area - Introduction to the Code Sign Certificate interface that covers basic interface functionality and the application, import and management of code signing certificates.

3.3.4 Request and Issuance of Code Signing Certificates - Explains the initiation, application, requisition, collection and management of Code Signing Certificates.

3.4.The Device Certificates Area - Introduction to Device Certificates interface and covers explanations on viewing and managing Device Certificates issued to devices for authenticating themselves for secure connections like VPN.

3.4.2.Request and Issuance of Device Certificates - Explains the processes of enrollment of Device Certificates by Active Directory (AD) integration, SCEP enrollment and Web API.

Note: Administrators can also run a 'Discovery Scan' on their servers which will audit and monitor their entire network for all installed SSL certificates (including certificates issued by other vendors). Once completed, all discovered certificates are automatically imported into the 'Certificates Management' area. This feature is covered in greater detail in the **Certificate Discovery** section of this guide.

3.1 SSL Certificates Area

3.1.1 Overview of the Interface

The SSL Certificates Area provides MRAOs and nominated RAO / DRAO SSL administrators with the information and controls necessary to manage the life-cycle of SSL certificates for an Organization.

- MRAOs can request and manage SSL certificates for any Organization/Department. Can approve or decline certificate requests made for automatic installation and using the external application form for any Organization or Department.
- RAO SSL admins can request and manage certificates for their delegated Organization(s). Can approve or decline certificate requests made for automatic installation and using the external application form for their Organization.
- DRAO SSL admins can request SSL certificates for domains belonging to their delegated Department(s). Can approve or decline certificate requests made for automatic installation and using the external application form for their Organization.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|----------------------|--------------|------------|--------|------------|---------------|---------------|
| test.ccmqa.com[61] | org1 | | Issued | 01/14/2018 | Successful | Not scheduled |
| demo.ccmqa.local[60] | org2 | | Issued | 01/14/2018 | Not scheduled | Not scheduled |
| test.ccmqa.com[59] | org1 | | Issued | 01/14/2018 | Successful | Not scheduled |
| p1.ccmqa.local[58] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| l1.local[57] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |


© 2007-2017. All rights reserved.

Note: The SSL Certificates area is visible only to MRAO Administrators and RAO / DRAO SSL administrators. For more details refer to **1.2.3 Administrative Roles**.

| SSL Certificates Sub-tab - Table of Parameters | | |
|--|---------------------------------------|---|
| Column | | Description |
| Common Name | | The domain name that was used during the SSL certificate request. This domain name refers to the 'Common Name' in the SSL certificate itself. |
| Organization | | Name of the Organization that requested or has been issued with the certificate listed in the 'Common Name' column. |
| Department | | Indicates the specific Department of the Organization that is associated with the certificate. This column will be blank if a Department has not been delegated as the controlling entity. |
| Status | | Indicates the current status of the certificate. |
| | Requested | <p>The certificate application was made for auto-installation or using either the Self Enrollment Form or the Built-in application form. Once the applicant has requested the certificate, his/her request appears in the 'SSL Certificates' sub-tab with a 'Requested' state. The Administrator can "View", "Edit", "Approve" or "Decline" this request.</p> <p>A certificate can be requested by</p> <ul style="list-style-type: none"> • An applicant using the Self Enrollment Form. • An MRAO - for any Organization or Department - using Auto Installation feature, Self Enrollment Form or the Built In Application Form • An RAO SSL administrator- for Organizations and Departments which they have been delegated control. Can use Auto Installation feature, Self Enrollment Form or the Built In Application Form • A DRAO SSL administrator - for Departments of an Organization which they have been delegated control. Can use Auto Installation feature, Self Enrollment Form or the Built In Application Form |
| | Approved | <p>A certificate request that was made using the Auto Installation feature or the Self Enrollment Form has been approved by one of the following:</p> <ul style="list-style-type: none"> • An MRAO • An RAO SSL administrator of the Organization on whose behalf the request was made. • A DRAO SSL administrator of the Department on whose behalf the request was made. |
| | Applied | The request has been sent to the Certificate Authority (CA) for validation. In order to accelerate the validation process, the administrator can email PartnerValidation@comodo.com with the order number. |
| | Issued (number of found certificates) | The certificate was issued by CA and collected by Certificate Manager. A Blue font color (Issued) means that the certificate was issued by CA but was not installed. Placing the mouse cursor over the ' Common Name ' will display the name of the Vendor that is associated with this certificate. |

| SSL Certificates Sub-tab - Table of Parameters | | |
|--|---|--|
| Column | | Description |
| | | A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the 'State' column will display all the <i>IP address / Port</i> combinations that this certificate was found on. |
| | Expired | <p>The certificate is invalid because its term has expired. Placing the mouse cursor over the 'Common Name' will display the name of the Vendor that is associated with this certificate.</p> <p>A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the 'State' column will display all the <i>IP address / Port</i> combinations that this certificate was found on and will display a certificate expired warning.</p> |
| | Revoked | <p>The certificate is invalid because it has been revoked. Placing the mouse cursor over the 'Common Name' will display the name of the Vendor that is associated with this certificate.</p> <p>A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the 'State' column will display all the <i>IP address / Port</i> combinations that this certificate was found on and will display a certificate revoked warning.</p> |
| | Declined | <p>A certificate request that was made using the Self Enrollment Form or the Built-in Application Form has been rejected by one of the following:</p> <ul style="list-style-type: none"> • An MRAO - can decline any certificate requests from any Organization or Department • An RAO SSL administrator can decline certificate requests for Organizations over which they have been delegated control. • An DRAO SSL administrator can decline certificate requests for Departments over which they have been delegated control. |
| | Invalid | The Certificate Authority did NOT process the certificate request because of an error the applicant made in the enrollment form (e.g. CSR contains incorrect details). |
| | Rejected | The Certificate Authority rejected the request after a validation check. |
| | Unmanaged (n - number of found certificates) | <p>This state applies to certificates that were detected by a network Discovery Scan but were NOT ordered and issued through Comodo Certificate Manager (including any pre-existing Comodo certificates that may have been ordered from the website or partner API's). The red color (<i>Unmanaged</i>) indicates, that the certificate's term has expired. Placing the mouse cursor over the 'Common Name' will display the name of the Vendor that is associated with this certificate.</p> <p>A number in parentheses to the right of the certificate's status indicates how many servers this specific certificate is installed upon. Placing the mouse cursor over the 'State' column will display all the <i>IP address / Port</i> combinations that this certificate was found on.</p> |
| Expires | | Expiration term of the certificate. |
| Install State | | Indicates the current status of scheduled certificate installations: |
| | Not | The certificate is not scheduled for auto-installation. |

| SSL Certificates Sub-tab - Table of Parameters | | |
|---|---------------|---|
| Column | | Description |
| | Scheduled | |
| | Scheduled | The certificate is scheduled for auto-installation. |
| | Started | Certificate installation on the remote server has started as per the schedule |
| | Successful | Certificate was successfully installed on the remote server at the scheduled time |
| | Failed | Certificate installation on the remote server failed |
| Renewal State | | Indicates the current status of scheduled certificate auto-renewal |
| | Not Scheduled | The certificate is not scheduled for auto-renewal |
| | Scheduled | A schedule has been set for auto-renewal of the certificate |
| | Started | The auto-renewal process has been started as per the schedule |
| | Successful | The certificate has been auto-renewed and installed successfully |
| | Failed | Auto-renewal of the certificate has failed |
| <p>Note: The administrator can add more column headers from the drop-down button beside the last item in the column:</p> | | |

| SSL Certificates Sub-tab - Table of Parameters | | |
|--|--|--|
| Column | | Description |
| | | <div style="border: 1px solid black; padding: 5px;">  <ul style="list-style-type: none"> ✓ Status ✓ Expires ✓ Install state ✓ Renewal state Order Number Self-Enrollment Certificate ID IP address Issuer Serial Number Requester Requested External Requester Subject Alt Name City State Country Signature Algorithm Key Algorithm Key Size MD5 Hash SHA1 Hash Private Key Key Usage Extended Key Usage </div> |
| Order Number | | The order number of the certificate request as assigned by the Certificate Authority, when the request was made. |
| Self - Enrollment Certificate ID | | Displays the unique enrollment ID assigned to the certificate request. |
| IP address | | Displays all the IP address / Port combinations on which the certificate is installed. |
| Issuer | | Displays the details of the Certificate Authority that issued the certificate and the name of the certificate. |
| Serial Number | | Displays the serial number of the certificate that is unique and can be used to identify the certificate. |
| Requester | | Displays the name of the CCM administrator that has requested the certificate through the auto-install feature or the built-in enrollment form, or e-mail of end-user that has requested the certificate through the self-enrollment form. |
| Requested | | Displays the date of the certificate request. |
| External Requester | | Displays the the email address of the external requester on behalf of whom the administrator has requested the certificate through the built-in enrollment form. |

| SSL Certificates Sub-tab - Table of Parameters | | |
|---|---------|---|
| Column | | Description |
| Subject Alt Name | | Displays the names of domain(s) for which the certificate is used for. |
| City | | Displays the name of the city entered while creating the Organization / Department. |
| State | | Displays the name of the state/province entered while creating the Organization / Department. |
| Country | | Displays the name of the country entered while creating the Organization / Department. |
| Signature Algorithm | | Displays the signature algorithm of the public key of the certificate. |
| Key Algorithm | | Displays the type of algorithm used for the encryption. |
| Key Size | | Displays the key size used by certificate for the encryption. |
| MD5 Hash | | Displays the MD5 hash (thumbprint/fingerprint) for the certificate. |
| SHA1 Hash | | Displays the SHA1 hash (thumbprint/fingerprint) for the certificate. |
| Private Key | | Indicates whether the private key of the certificate is managed by CCM |
| Key Usage | | Indicates the capabilities of the certificate, in other words, the purposes served by the certificate, like website authentication, encryption and more. |
| Extended Key Usage | | Indicates the extended capabilities of the certificate. |
| Control Buttons Note: The type of control buttons that are displayed above the column header depends on the state of the selected certificate | Details | Allows the administrator to view information about the certificate (see SSL certificate 'Details' dialog description). |
| | Revoke | Revokes the certificate. |
| | Install | Uses the auto-installer feature to install the certificate on the target web server. See the section Automatic Installation and Renewal for more details. |
| | Replace | Replaces the existing certificate with a new one. Note: You will be prompted to specify new CSR. |
| | Approve | Approves certificate requests that were made for Auto Installation and using the auto-installation feature or the Self Enrollment Form and sends the request for the certificate to Comodo CA (the issuing Certificate Authority). Once submitted, the certificate State will change to 'Applied'. If the request is approved by Comodo CA, the certificate's state will change to 'Issued'. If the request was declined by Comodo CA because of incorrect enrollment details (for example, a mistake in the CSR or other form value), then 'State' will be listed as 'Invalid'. If the request was declined by Comodo CA for legal reasons then the certificate will have a status of 'Rejected'. Certificate requests can be approved by: An MRAO An RAO SSL administrator of the Organization on whose behalf the request was made. |

| SSL Certificates Sub-tab - Table of Parameters | | |
|--|---------------------------------|---|
| Column | | Description |
| | | A DRAO SSL administrator of the Department on whose behalf the request was made |
| | Decline | Declines the certificate request. This request will not be sent to Comodo Certificate Authority for processing. |
| | Edit | Enables administrator to edit SSL certificate parameters. This option is available only for certificates with a state of 'Requested', 'Rejected' or 'Invalid'. |
| | Renew | Clicking the 'Renew' button will open the 'Renew Certificate' dialog which will be pre-populated with the company and domain details of the existing certificate. Clicking 'OK' will submit the certificate renewal request. This control is available only for the certificates states of: Issued, Expired and Unmanaged. |
| | Set Auto Renewal & Installation | Create a schedule for auto-renewing a certificate in advance of its expiry, and to configure auto-installation of the renewed certificate. See the section Scheduling Automatic Renewal and Installation for more details. |

3.1.1.1 Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

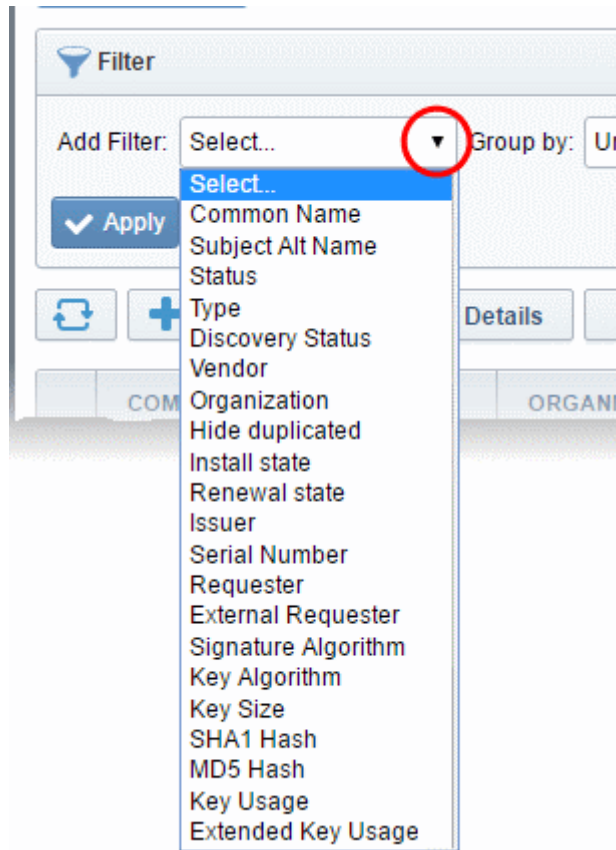
Administrators can search for particular SSL certificates using filters.



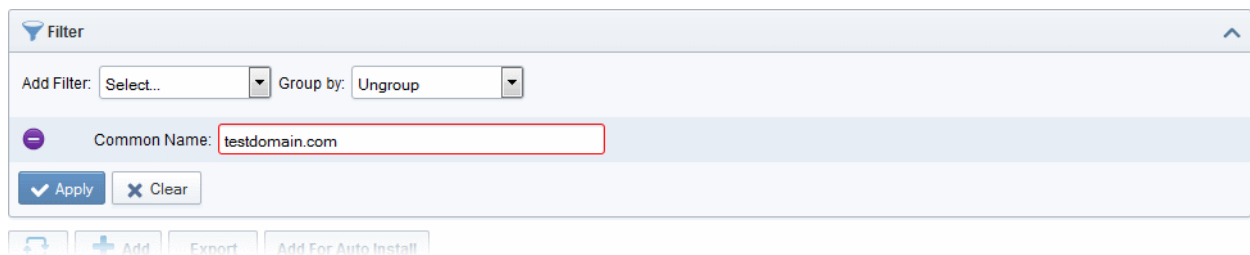
To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the results with other options that appears depending on the selection from the 'Add Filter' drop-down.

To add a filter

- Select a filter criteria from the 'Add Filter' drop-down



- Enter or select the filter parameter as per the selected criteria.



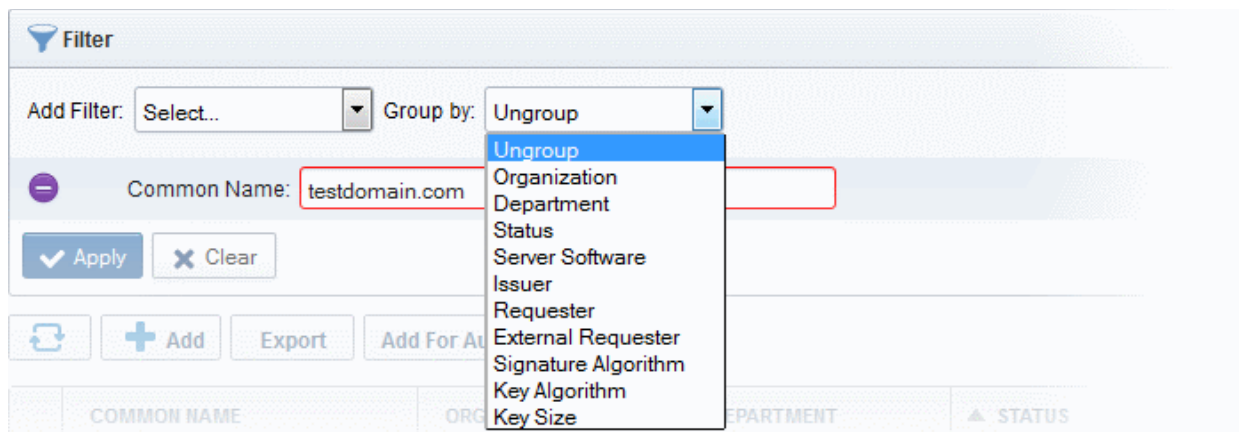
The available filter criteria and their filter parameters are given in the following table:

| Filter Criteria | Filter Parameter |
|------------------|---|
| Common Name | Enter the common name or domain name for the certificate fully or in part |
| Subject Alt Name | Enter the subject alternative name for the certificate fully or in part |
| Status | Choose the state of the certificate from the 'Status' drop-down |
| Type | Choose the type of the certificate from the 'Type' drop-down |
| Discovery Status | Choose the status, that is whether the certificate is deployed or not from the 'Discovery Status' drop-down |
| Vendor | Select the vendor of the certificate (CA) from the Vendor drop-down. |

| | |
|---------------------|--|
| Organization | Select the Organization and/or the Department to which the certificate belongs, from the 'Organization' and 'Department' drop-downs. |
| Hide Duplicated | Choose Hide Duplicated if you want duplicate certificates are not to be listed and select the 'Hide duplicated' check box. |
| Issuer | Enter the name of the issuer of the certificate |
| Serial Number | Enter the serial number of the certificate in full or part. |
| Requester | Enter the name of the CCM administrator that has requested the certificate through the auto-install feature or the built-in enrollment form, or e-mail of end-user that has requested the certificate through the self-enrollment form, in full or part. |
| External Requester | Enter the email address of the external requester on behalf of whom the administrator has requested the certificate through the built-in enrollment form, in full or part. |
| Signature Algorithm | Enter the signature algorithm of the certificate |
| Key Algorithm | Enter the key algorithm of the certificate |
| Key Size | Enter the key size in bits |
| SHA1 Hash | Enter the SHA1 Hash (thumbprint/fingerprint) of the certificate |
| MD5 Hash | Enter the MD5 Hash (thumbprint/fingerprint) of the certificate |
| Key Usage | Filter certificates by their key usage capabilities |
| Extended Key Usage | Filter certificates by their extended key usage capabilities |

Tip: You can add more than one filter at a time to narrow down the filtering. To remove a filter criteria, click the '-' button to the left if it.

- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter



For example, if you want to filter the certificates with a specific Common Name starting with 'testdomain.com' and group the results by their 'Status', then select 'Common Name' from the 'Add Filter' drop-down, enter 'testdomain.com' and select 'Status' from the 'Group by' drop-down. The certificates, having 'testdomain.com' in their common name will be displayed as a list, grouped based on their 'status'.

| | COMMON NAME | ORGANIZATION | DEPARTMENT | ▲ STATUS | EXPIRES | SERVER SOFTWARE | ✕ |
|-----------------------|-----------------------------|------------------------------|----------------------|-----------|------------|-----------------|---|
| [-] Requested | | | | | | | |
| <input type="radio"/> | testdomain.com | 123 | | Requested | | | |
| <input type="radio"/> | testdomain.com | OrganizationNumber21 | | Requested | | | |
| [-] Issued | | | | | | | |
| <input type="radio"/> | testdomain.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | |
| <input type="radio"/> | testdomain.com (renewed) | 123 | | Issued | 03/20/2016 | | |
| [-] Revoked | | | | | | | |
| <input type="radio"/> | onetestdomain.com (renewed) | 123 | | Revoked | 03/18/2016 | | |
| <input type="radio"/> | testdomain.com | OrganizationNumber11 | | Revoked | 09/06/2014 | | |
| [-] Expired | | | | | | | |
| <input type="radio"/> | testdomain.com | OrganizationNumber47 | | Expired | 09/06/2014 | | |
| <input type="radio"/> | testdomain.com | OrganizationNumber38 | | Expired | 09/07/2014 | | |

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'SSL certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

3.1.1.2 SSL Certificate 'Details' Dialog

The SSL Certificate Details dialog displays complete certificate details and also allows administrators to:

- Download the certificate in different formats for installation onto servers
- Upload the private key of the certificate for storage and management by the Private Key Store
- Download the private key of the certificate from the Private Key Store
- View the full certificate chain and installation details
- Resend the notification email to the requester of the issued certificate
- Restart Apache after auto-installation of the certificate

To view the SSL certificate details dialog, select the certificate from the Certificates > SSL certificates interface and

click the 'Details' button at the top.

The screenshot displays the 'SSL Certificate: test.ccmqa.com' window. At the top, it indicates '362 Days till expiration'. The window is divided into two main panes:

- CERTIFICATE DETAILS:** This pane shows the following information:
 - Common Name: test.ccmqa.com
 - State: Issued
 - Download The Certificate:
 - Order Number: 1675841
 - Vendor: Comodo CA Limited
 - Discovery Status: Not deployed
 - Self-Enrollment Certificate ID: 59
 - Type: Instant SSL
 - Server Software: Microsoft IIS 5.x and later
 - Server Software State
 - Term: 1 year
 - Owner: admin admin
 - Requested by: admin admin
 - External Requester
 - Requested: 01/13/2017
- CERTIFICATE CHAIN DETAILS:** This pane shows the certificate chain:
 - Root (AddTrust External CA Root)
 - Intermediate (AddTrust AB)
 - End Entity (AddTrust AB)
 Below the chain, the following details are listed:
 - Common Name: AddTrust External CA Root
 - Vendor: AddTrust AB
 - Term: 20 years
 - Valid From: 05/30/2000
 - Expires: 05/30/2020
 - Serial Number: 01
 - Signature Algorithm: SHA1WITHRSA
 - Public Key Algorithm: RSA
 - Public Key Size: 2048
 - MD5 Hash: 1d3554048578b03f42424dbf20730a3f
 - SHA1 Hash: 02faf3e291435468607857694df5e45b68851868
 - Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
 - Subject: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
 - Address1

A 'Close' button is located at the bottom center of the window.

The certificate details dialog contains two panes:

- **Certificate Details**
- **Certificate Chain Details**

Certificate Details

The top of the 'Certificate Details' pane displays the number of days remaining before the certificate expires. The lower section shows CCM and server related information about the certificate and contains various other controls. The precise contents of the 'Certificate Details' pane is dependent on the current 'State' of the certificate:

SSL Certificate with 'Issued' state

SSL Certificate with 'Unmanaged' state

365 Days till expiration

449 Days till expiration

CERTIFICATE DETAILS
Private Key

Common Name ditherscons.com

State **Issued**

Download The Certificate Select

Private Key Download Remove

Self Enrollment Passphrase

Show Pass-phrase

Order Number **1313045**

Vendor **Comodo CA Limited**

Discovery Status **Not deployed**

Self-Enrollment Certificate ID **77883**

Type **Instant SSL**

Server Software **AOL** Edit

Server Software State

Term **1 year**

Owner **Joe Dane** Resend Edit

Requested by **Joe A** Resend Edit

External Requester **johnsmith@dithers.com** Resend Edit

Requested **03/31/2015**

Approved **03/31/2015**

Expires **03/31/2016**

Comments Edit

Organization **Dithers Construction Company**

Department **Purchases Department**

Address1 **100, Raleigh Street**

Address2

Address3

City **Riverdale**

State/Province **Alabama**

Postal Code **123456**

Serial Number **81:72:02:EE:31:FF:7D:25:5E:09:2D:19:34:67:13:02**

Signature Algorithm **SHA1withRSA**

Public Key Algorithm **RSA**

Public Key Size **2048**

MD5 Hash **716b9f8788f5cbef48d866b59ddc5f8b**

SHA1 Hash **45103060d314f1423404998534f595b3b6996635**

Change Self Enrollment Passphrase

CERTIFICATE DETAILS

Common Name www.somedomain.org

State **Unmanaged**

Order Number **N/A**

Vendor **XXXXXXXXXX**

Discovery Status **Deployed**

IP Address(es) **XXXXXXXXXX**
XXXXXXXXXX

Alternative Names

Self-Enrollment Certificate ID **23179**

Type **Unmanaged**

Server Software **OTHER**

Server Software State

Term **3 years**

Expires **06/23/2016**

Serial Number **52:10:77:4A:AD:FE:DE:1E:C7:DA:CE:9D:54:DF:38:EE**

Signature Algorithm **SHA256withRSA**

Public Key Algorithm **RSA**

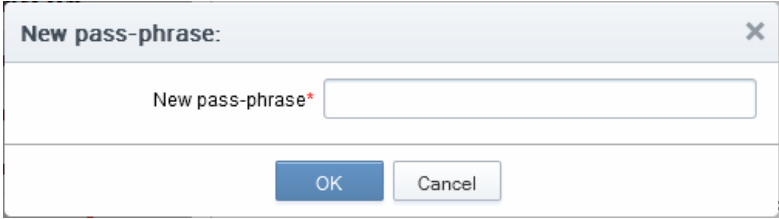
Public Key Size **2048**

MD5 Hash **e053b92d68492a901d1ab79828786af0**

SHA1 Hash **b42c5693c5300eee2798bdf79e2feb8d0e087407**

| SSL Certificates 'Details' Dialog - Table of Parameters | | |
|---|------------|--|
| Field | Type | Description |
| Common Name | Text Field | The domain name that was used during the SSL certificate request. This domain name refers to the 'Common Name' in the SSL certificate itself. |
| State | Text Field | State of the certificate (for the definitions see on the table above). |
| Download | Control | Allows the administrator to download the certificate in different formats. |
| Private Key | Control | <p>For the certificates enrolled by manually entering the CSR</p> <ul style="list-style-type: none"> Allows the administrator to upload the private key of the certificate for storage in the Private Key Store. <p>For the certificates enrolled by auto-generation of CSR by CCM and whose keys are managed by Private Key Store</p> <ul style="list-style-type: none"> Allows the administrator to download the private key of the certificate in .key format. <p>For more details, refer to the sections:</p> <ul style="list-style-type: none"> Uploading private key of a certificate Downloading the private key of a certificate <p>Note: The Private Key field is displayed only if the Private Key Store feature is enabled for your account and a Private Key Store controller is installed on your local network and configured. Refer to the section Private Key Store for more details.</p> |
| Pass Phrase | Text Field | <p>The Pass Phrase of the certificates enrolled by auto-generation of CSR by CCM and whose keys are managed by Private Key Store. The passphrase is displayed if 'Show Pass-phrase' checkbox is selected. This phrase is required to import the certificate on to any server, after downloading the certificate in .p12 format.</p> <p>Note: The Pass Phrase field is displayed only if the Private Key Store feature is enabled for your account and a Private Key Store controller is installed on your local network and configured. Refer to the section Private Key Store for more details.</p> |
| Order Number | Text Field | Order number of the certificate request. |
| Vendor | Text Field | A vendor that is associated with the certificate. The vendor for self-signed SSL certificates is ' Self-Signed '. |
| Discovery Status | Text Field | <p>There are two possible values: Not Deployed and Deployed.</p> <ul style="list-style-type: none"> Deployed - A certificate that is installed on the network (as found by the certificate discovery scan) Not Deployed - any certificate that is listed in the 'SSL Certificates' area but which was <i>not</i> detected as installed on the network during a certificate discovery scan. |
| Self-Enrollment Certificate ID | Text Field | Displays the unique ID of the certificate. |
| Type | Text Field | Displays the brand name of the certificate. |
| Server Software | Text Field | <p>Indicates the server type for which the certificate was issued.</p> <ul style="list-style-type: none"> Clicking 'View' allows you to view the installation status of the |

| SSL Certificates 'Details' Dialog - Table of Parameters | | |
|---|-------------|--|
| Field | Type | Description |
| | | <p>deployed certificate. Refer to the section Viewing the installation details of the certificate for more details.</p> <ul style="list-style-type: none"> Clicking 'Edit' allows you to change the Server Software for which the certificate is intended. |
| Server Software State | Text Field | Indicates the state of the server on which the certificate is installed. (For the definitions see on the table above). |
| Term | Text Field | The length of time the certificate is (or will be) valid for, from the time of issuance. For certificates that have not yet been approved, this is the certificate lifetime that was requested during the application process. |
| Owner | Text Field | Name of the 'Owner' of the certificate. The Owner of the certificate is the Administrator that first approved the request for the certificate. |
| Requested by | Text Field | Displays either: <ul style="list-style-type: none"> The email address of the end-user that requested this certificate using the Self Enrollment Application form <p>or</p> <ul style="list-style-type: none"> The name of the administrator that requested this certificate using the auto-install feature or the Built-In Application form. |
| External Requester | Text Field | The email address of the applicant on behalf of whom the administrator has applied for this certificate through the built-in application form in the CCM interface, as an alternative to making an applicant to complete the 'Self Enrollment' form . |
| Requested | Text Field | Date that the certificate was requested. |
| Approved | Text Field | Date that the certificate was approved. |
| Expires | Text Field | Date that the certificate expires. |
| Comments <i>(optional)</i> | Text Field | Information for administrator. |
| Organization | Text Field | Name of the Organization on behalf of which the certificate was requested |
| Department | Text Field | Name of the Department on behalf of which the certificate was requested |
| Address 1: Address 2: Address 3: City: State or Province: Postal Code: | Text Fields | Displays the address of the Organization as mentioned while requesting for the certificate. Only those address fields that were allowed to be displayed while applying for the certificate are shown here and the rest of the fields are displayed as "Details Omitted". |
| Serial Number | Text Field | Indicates the serial number of the certificate issued. |
| Signature Algorithm | Text Field | Displays the signature algorithm of the public key of the certificate |
| Public Key Algorithm | Text Field | Displays the encryption algorithm of the public key of the certificate |

| SSL Certificates 'Details' Dialog - Table of Parameters | | |
|---|------------|--|
| Field | Type | Description |
| Public Key Size | Text Field | Displays the key length of the public key in bits |
| Revoked | Text Field | Date that the certificate was revoked (if applicable.) |
| MD5 Hash | Text Field | Displays the MD5 Hash (thumbprint/fingerprint) value of the certificate |
| SHA1 Hash | Text Field | Displays the SHA1 Hash (thumbprint/fingerprint) value of the certificate |
| Key Usage | Text Field | Indicates the purpose(s) of the certificate. For example, authentication, encryption and more. |
| Extended Key Usage | Text Field | Indicates the extended capabilities of the certificate. |
| Change Pass Phrase | Control | <p>Enables the administrator to set or change the self-enrollment pass-phrase of the certificate. This phrase is required to revoke certificates should the situation arise.</p>  |

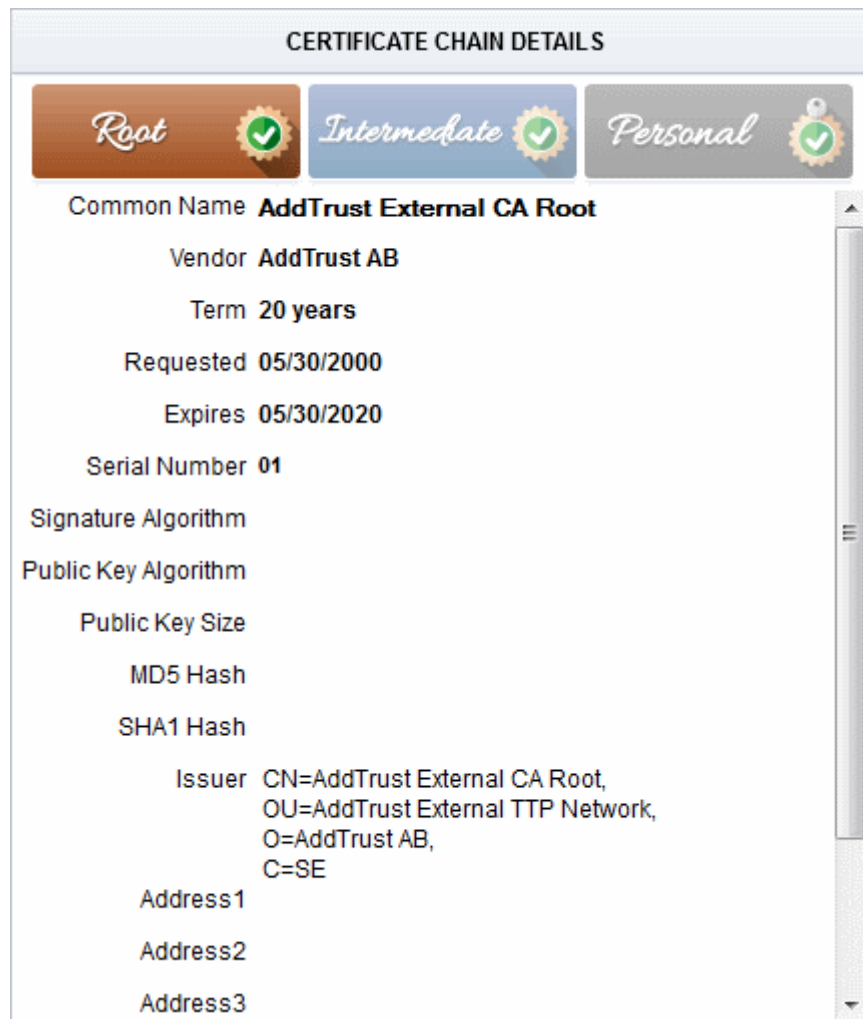
Following sections explain in detail on the tasks that can be accomplished from the 'Certificate Details' pane.

- [Uploading private key of a certificate for storage and management by the Private Key Store](#)
- [Downloading private key of a certificate](#)
- [Resending Notification Email for Certs with 'Issued' State](#)
- [Viewing Installation Details of Certificates](#)
- [Restarting Apache after Auto-Installation of SSL Certificate](#)

Certificate Chain Details

The 'Certificate Chain Details' pane displays the details of the 'Root' and 'Intermediate' certificates linked to the SSL certificate chain.

- Clicking on the 'Root', 'Intermediate' and the 'Personal' tabs, displays the certificate details of the Root, Intermediate and the self SSL certificate respectively.



3.1.1.2.1 Uploading Private Key of a Certificate for Storage and Management by the Private Key Store

The 'Details' dialog for SSL certificates with 'Issued' state allows the administrator to upload the private key associated with it, for storage and management by the Private Key Store configured in their local network. Managing the private key in the key store facilitates:

- Downloading the certificate in .pfx/.p12 format for importing on to any server
- Auto-uploading of the CSR during certificate renewal process

Prerequisite - Your account should have been enabled for Private Key Store feature. The Private Key Store controller should have been installed on your local network and configured from the Settings > Private Key Store interface. Refer to the section **Private Key Store** for more details.

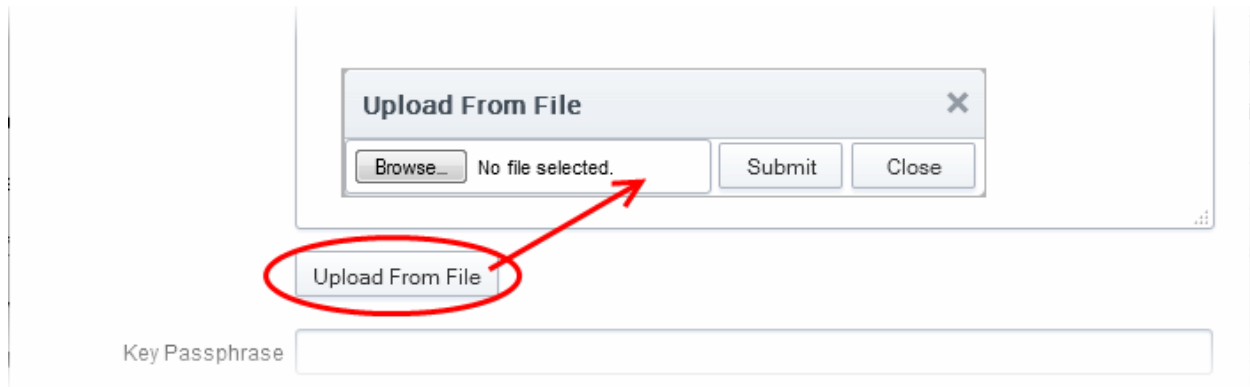
The 'Certificate Details' pane of the details dialog for the SSL certificate with the Issued state, displays a 'Upload' button beside the 'Private Key' field.

- Clicking the 'Upload' button will open the 'Upload Private Key' dialog.

- Enter the Private Key of the certificate

You can enter the private key associated with the certificate in two ways:

1. Directly paste the private key in the 'Paste Private Key here' text box
2. Save the private key as a text file and upload the file by clicking the 'Upload From File' button



- Enter a passphrase for the key

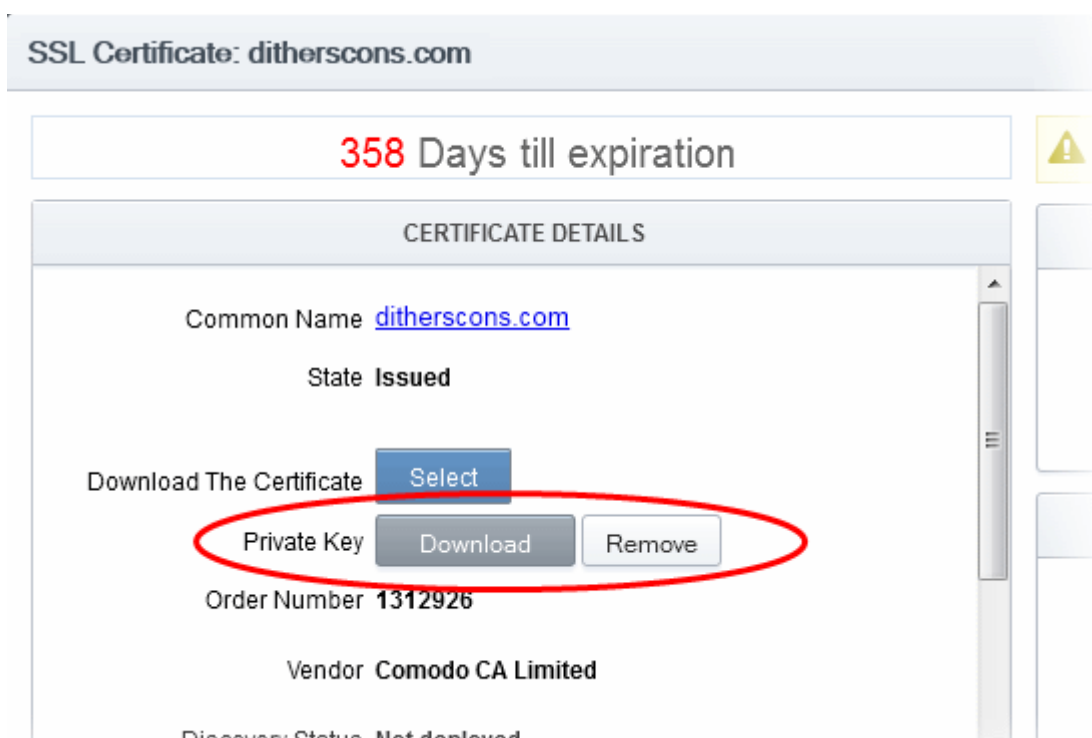
This passphrase is required for importing the certificate with the key pair on to the server for installation.

- Click 'OK'
- Close the 'Certificate Details' dialog

CCM will send a command to the controller to store the Private Key. The private key is now stored and managed by the Private Key Store. It will be indicated under the Private Key column in the 'SSL Certificates' area.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | SERVER SOFTWARE | PRIVATE KEY |
|-----------------|------------------------------|----------------------|---------|------------|-----------------|-------------|
| dithers.com | Dithers Construction Company | Purchases Department | Revoked | 04/06/2016 | | |
| dithers.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | Private Key |
| ditherscons.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | Private Key |
| ... | Dithers Construction | Purchases Department | Expired | ... | | |

Also, you can download the private key from the 'Certificate Details' dialog.



SSL Certificate: ditherscons.com

358 Days till expiration

CERTIFICATE DETAILS

Common Name ditherscons.com

State **Issued**

Download The Certificate

Private Key

Order Number **1312926**

Vendor **Comodo CA Limited**

Discovery Status: Not deployed

3.1.1.2.2 Downloading private key of a certificate

The 'Details' dialog for SSL certificates with Private Keys stored at the Private Key Store allows the administrator to download the private key in .key format.

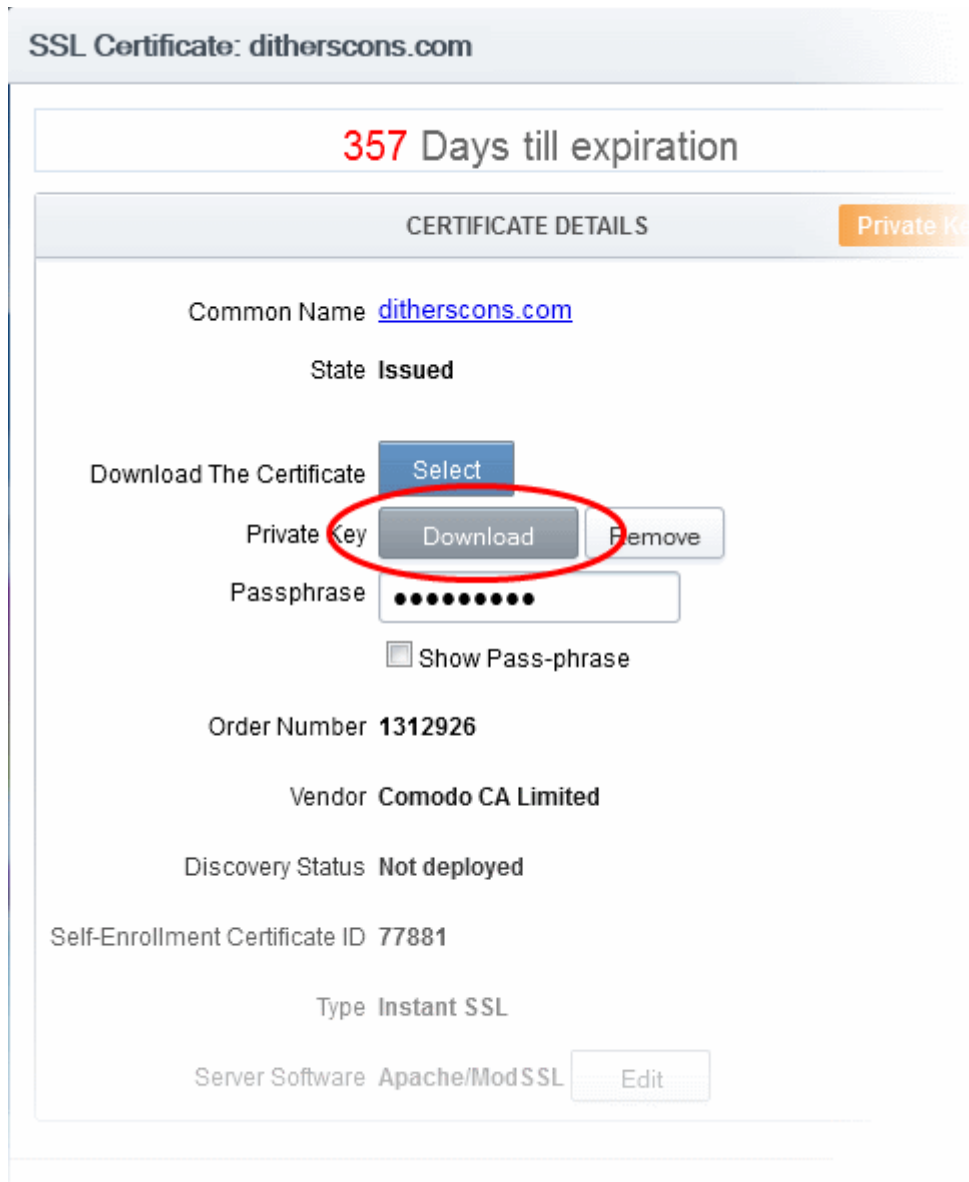
Limitations - The private key can be downloaded only for the certificates whose private keys are managed by the private key store. This includes:

- Certificates applied using auto-CSR generation feature in CCM. Refer to the section **Method 3 - Built-in Enrollment Form - Auto CSR Generation** for more explanation on using the Auto-CSR generation feature.
- Certificates for which the private keys were manually uploaded to the Private Key Store. Refer to the section **Uploading Private Key of a Certificate for Storage and Management by the Private Key Store** for more details.

In order to download a private key, the administrator should have been logged-in to CCM through a computer in the same local network on which the Private Key Store controller is installed and should have a personal authentication certificate installed on the computer.

During the download process, CCM sends a download command to the controller. The controller requests for authentication of the administrator and checks for authentication certificate. Once authenticated, the private key controller enables the administrator to download the private key in .key format directly from it, without uploading it to CCM. This ensures that the private key does not leave your network though CCM initiates the download.

The 'Certificate Details' pane of the details dialog for the SSL certificate with managed private key, displays a 'Download' button beside the 'Private Key' field.



SSL Certificate: ditherscons.com

357 Days till expiration

CERTIFICATE DETAILS Private Key

Common Name ditherscons.com

State **Issued**

Download The Certificate Select

Private Key Download Remove

Passphrase

Show Pass-phrase

Order Number **1312926**

Vendor **Comodo CA Limited**

Discovery Status **Not deployed**

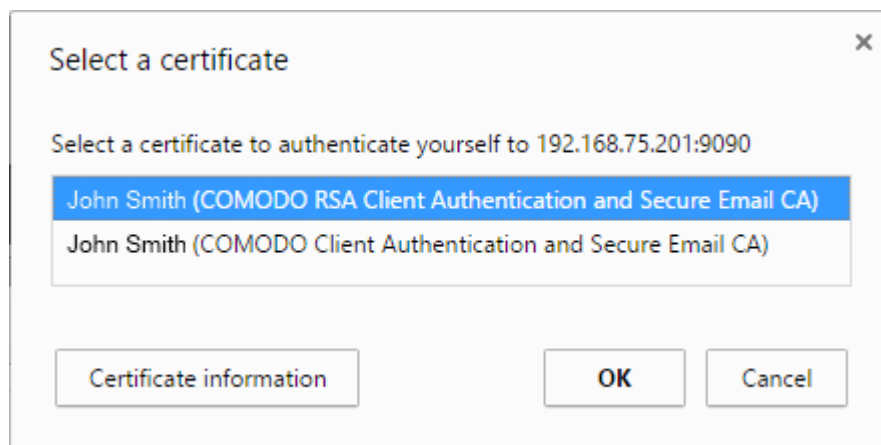
Self-Enrollment Certificate ID **77881**

Type **Instant SSL**

Server Software **Apache/Mod SSL** Edit

- Clicking the 'Download' button will send a command to the Private Key Store controller.

The private key storage controller will request for authentication and search for the personal authentication certificate of the administrator in the computer from which the administrator has logged-in. If more than one certificate is found, the Select Certificate dialog will be displayed for the administrator to choose the certificate.



Select a certificate

Select a certificate to authenticate yourself to 192.168.75.201:9090

- John Smith (COMODO RSA Client Authentication and Secure Email CA)
- John Smith (COMODO Client Authentication and Secure Email CA)

Certificate information OK Cancel

- Choose the certificate for authentication and click OK.

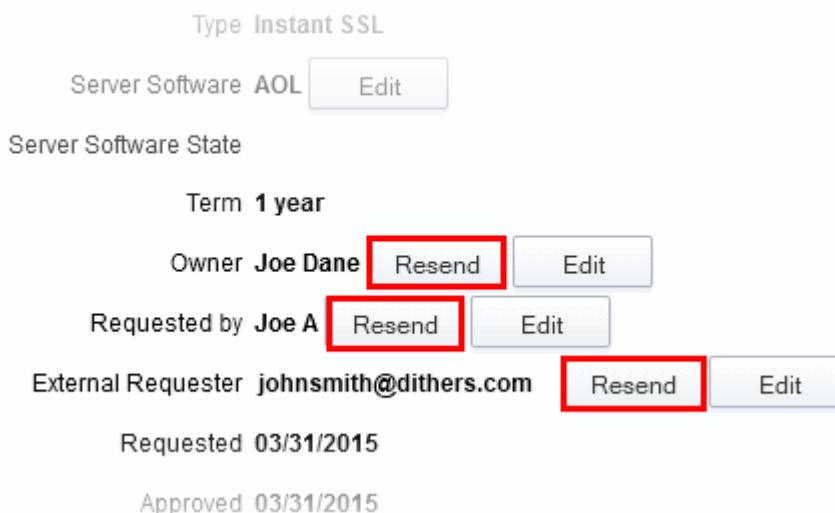
Upon authentication verification, the download dialog will be displayed, enabling the administrator to download the private key in .key format.

3.1.1.2.3 Resending Notification Email for Certs with 'Issued' State

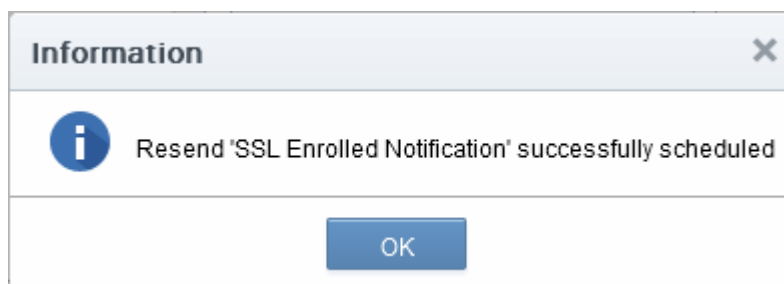
The 'Details' dialog for SSL certificates with 'Issued' state allows the administrator to resend the 'Certificate Enrolled' notification to the domain control administrator. the applicant that applied for the certificate through the **Self Enrollment Form** and/or the applicant on behalf of whom the administrator has applied for the certificate through the **Built-in Enrollment Form**.

An automated notification email for collection of certificate will be sent to the Domain Administrator once CCM issues the Certificate. However, if the certificate is not downloaded by the domain administrator for a long time, CCM administrator can resend the notification for certificate collection.

The 'Certificate Details' pane of the details dialog for the SSL certificate with the Issued state, displays a 'Resend' button beside the Owner and Requested by and External Requester (if applicable) fields.



- Clicking the 'Resend' button will create a schedule for CCM to resend the notification email.



3.1.1.2.4 Viewing Installation Details of Certificates

The 'Details' dialog for SSL certificates added for auto installation to IIS or Apache, allows the administrator to view the installation state of the certificate.

- The 'Certificate Details' pane of the details dialog for the SSL certificate added for auto installation, displays a 'View' button beside the 'Server Software' field.

Self-Enrollment Certificate ID 77875

Type **Instant SSL**

Server Software **Microsoft IIS 5.x and later**

View

Edit

Server Software State **Active**

Term **1 year**


Owner **admin 1**

Resend

Edit

- Clicking the 'View' button will display a Nodes dialog that provides the details on the Agent responsible for auto-installation, the node server upon which the certificate is installed and the installation status.

Nodes ✕



| NAME | COMMON NAME | PROTOC | IP ADDRESS | PORT | STATUS | SSL |
|----------------------------------|-----------------|--------|------------|------|-----------|-------------------------|
| Server IIS 123 52 | | | | | Active | |
| <input type="checkbox"/> dithers | ditherscons.com | HTTPS | * | 9443 | Installed | 1306124 |

15 rows/page 1 - 1 out of 1 ⏪ ⏩

Close

3.1.1.2.5 Restarting Apache after Auto-Installation of SSL Certificate

The Apache will need to be restarted to finalize the installation of the SSL certificate. Administrators can do this remotely from the CCM interface by clicking the 'Restart' button on the 'Certificate Details' pane of the details dialog.

Self-Enrollment Certificate ID 77875

Type **Instant SSL**

Server Software **Apache/ModSSL**

View

Edit

Server Software State **Restart Required**

Restart

Term **1 year**

Owner **admin 1**

Resend

Edit

- Clicking 'Restart' will reboot the server. After rebooting, the 'Server Software State' will change to 'Active'.

3.1.1.3 Comodo SSL Certificates

3.1.1.3.1 Definition of Terms

Validation Levels

OV: Organization Validated certificates include full business and company validation from a certificate authority using currently established and accepted manual vetting processes.

EV: Browsers with EV support display more information for EV certificates than for previous SSL certificates. Microsoft Internet Explorer 7, Mozilla Firefox 3, Safari 3.2, Opera 9.5, and Google Chrome all provide EV support.

Certificate Types

SDC: Single Domain Certificates will secure a single fully qualified domain name.

WC: Wildcard Certificates will secure the domain and unlimited sub-domains of that domain.

MDC: Multi-Domain Certificates will secure up to 100 different domain names on a single certificate.

| Certificate Name | Type | Validation Level | Description | Maximum Term Length |
|---|------|------------------|---|---------------------|
| Comodo Trial SSL Certificate | SDC | OV | Secures a single domain | 30 days |
| Comodo Intranet SSL Certificate | SDC | OV | Secures a single internal host | 1 year - 3 years |
| Comodo InstantSSL Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| Comodo InstantSSL Pro Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| Comodo PremiumSSL Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| Comodo PremiumSSL Wildcard Certificate | WC | OV | Secures domain and unlimited sub-domains of that domain | 1 year - 3 years |
| Comodo PremiumSSL Legacy Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| Comodo PremiumSSL Legacy Wildcard Certificate | WC | OV | Secures domain and unlimited sub-domains of that domain | 1 year - 3 years |
| Comodo SGC SSL Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| Comodo SGC SSL Wildcard Certificate | WC | OV | Secures domain and unlimited sub-domains of that domain | 1 year - 3 years |
| EliteSSL Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| GoldSSL Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| PlatinumSSL Certificate | SDC | OV | Secures a single domain | 1 year - 3 |

| Certificate Name | Type | Validation Level | Description | Maximum Term Length |
|---|------|------------------|---|---------------------|
| | | | | years |
| PlatinumSSL Wildcard Certificate | WC | OV | Secures domain and unlimited sub-domains of that domain | 1 year - 3 years |
| PlatinumSSL Legacy Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| PlatinumSSL Legacy Wildcard Certificate | WC | OV | Secures domain and unlimited sub-domains of that domain | 1 year - 3 years |
| PlatinumSSL SGC Certificate | SDC | OV | Secures a single domain | 1 year - 3 years |
| PlatinumSSL SGC Wildcard Certificate | WC | OV | Secures domain and unlimited sub-domains of that domain | 1 year - 3 years |
| Comodo Multi-Domain SSL Certificate | MDC | OV | Secure multiple Fully Qualified domains on a single certificate | 1 year - 3 years |
| Comodo EV SSL Certificate | SDC | EV | Secures a single domain | 1 year - 2 years |
| Comodo EV SGC SSL Certificate | SDC | EV | Secures a single domain | 1 year - 2 years |

3.1.2 Request and Issuance of SSL Certificates to Web Servers and Hosts

There are two broad methods an SSL administrator can use to request and install certificates:

- **Automatic installation** - Administrators can configure CCM to automatically create certificate requests for their domains and then automatically install the certificate on the web server. When a certificate is nearing expiry, a CSR is automatically generated and forwarded for administrative approval. Once issued by CA, the certificate will be collected and automatically installed on the web server. The auto-installation feature must be enabled for your account. Refer to the section [Automatic Installation and Renewal](#) for more details.
- **Manual Installation** - SSL administrators, or the applicants authorized by them, can also obtain certificates via CCM's applications forms. The applicant will then need to manually install the certificate on the target web server. Refer to the section [Request, Installation and Renewal using Application Forms](#) for more details.

Summary of steps for requesting and issuing an SSL certificate:

- Applicant confirms completion of the [prerequisites](#);
- A certificate request is made via the certificate auto-installer or an application form as explained [above](#).
- The certificate will appear in the 'SSL Certificates' area of Comodo Certificate Manager with the state 'Requested'. The MRAO, RAO SSL or DRAO SSL administrator (as applicable) will receive an email notification that a certificate request is awaiting approval.
- The certificate request will then need to be checked and approved or declined by appropriately privileged

SSL Administrator. If it is approved then the request will be forwarded to Comodo CA for validation and issuance or rejection.

- If the certificate is applied through CCM interface for automatic installation, the certificate will be issued and its state will be changed to 'Issued' in the 'Certificates Management' area. The administrator can choose to install the certificate remotely by clicking the 'Install' button in the CCM interface.
- If the certificate is applied through the an application form, a collection mail will be sent to the applicant which contains a link to the certificate collection form (see section **Certificate Collection** for more details). The applicant can manually download and install the certificate.
- Once an administrator has approved the request, that administrator becomes the 'Owner' of the request. At this stage, the administrator can also choose to 'View', 'Edit' or 'Decline' the request. See **Certificate Request Approval** for more details.
- The applicant will be designated as 'Requester' of the certificate. If the applicant does not exist then CCM will automatically add this applicant as a new 'End-user' at the time the certificate enrollment form is successfully submitted.

3.1.2.1 Prerequisites

- The domain for which the SSL certificate is to be issued has been enabled for SSL certificates, has been pre-validated by Comodo through **DCV** process and that the domain has been activated for account by your Comodo account manager. All certificate requests made on 'pre-validated' domains or sub-domains thereof are issued automatically. If you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.
- For applications using Enterprise Controller mode, the administrator has installed the Certificate Controller on a control server and configured it to communicate with the remote hosts. (See the section **Agents** for more details.)
- For applications using CCM Controller mode, the administrator has installed the agent on all hosts on which certificates are to be automatically installed. The Agent is responsible for creating the CSR, fetching the certificates and installing it in the host. (See the section **Agents** for more details.)
- The administrator has created at least one Organization/Department that the domain will belong to. (See chapter **'Settings - Organizations'**- for more details.)
- If the administrator wishes to enable **external SSL applications**, that the administrator has checked the 'Self Enrollment' box in the **SSL tab** of the 'Create/Edit' Organizations dialog box (see screen-shot below)

Edit Organization: Dithers

General | EV Details | Client Certificate | **SSL Certificate** | Code Signing Certificate | Device Certificate | Email Template

Self Enrollment

Access Code*

Sync. Expiration Date

Sync. Month

Sync. Day (1 - 31)

Web API

Secret Key*

SSL Types

Server Software

- If the administrator wishes to enable external SSL application using the Self Enrollment Form, that the administrator has specified an **Access Code** in the **SSL tab** of the 'Create/Edit' Organizations dialog box (see screen-shot). Comodo recommends using a mixture of alpha and numeric characters that cannot not easily be guessed.
- For the Built-in and the Self Enrollment Forms, the applicant has already created the Certificate Signing Request (CSR) using their web server software prior to beginning the application. This helps avoid potential errors on the certificate application form by allowing the common name (CN) to be automatically drawn from the CSR. Please note that CSR must be at least 2048 bit and must contain at least the following fields:

Common Name (Fully Qualified Domain Name)
 Organization
 Organization Unit
 Locality
 State/Province
 Country (2 character ISO code)

- **Optional:** The administrator has checked the '**Sync. Expiration Date**' box and specified the day of the month upon which the certificate will expire.

3.1.2.2 Automatic Installation and Renewal

Comodo Certificate Manager has the ability to automatically install SSL certificates on Apache Tomcat, Apache/ModSSL ApacheSSL, and IIS servers. There are two available modes:

| Enterprise Controller Mode | CCM Controller Mode |
|---|--|
| Requires one-time installation of the certificate controller software on a central control server inside your network. The controller communicates with each remote host and coordinates automatic CSR generation and certificate installation. See Method 1 - Enterprise Controller Mode | Requires an agent to be installed on each individual web server. These agents communicate with CCM to coordinate automatic CSR generation and certificate installation. See Method 2 - CCM Controller Mode |

Note: Currently CCM supports auto-installation only for 'Instant SSL' from Comodo CA. Other certificate types will be enabled for auto-installation in future versions. For more details on Comodo SSL Certificate types, refer to the section [Comodo SSL Certificates](#).

1. Enterprise Controller Mode

- i. Certificate Controller software is installed on a host in your network. This controller will communicate with your remote web-hosts and will automatically apply for and install certificates on them. The controller is configured through a web-interface and can be configured to communicate directly with Comodo CA infrastructure through a proxy server.
- ii. The controller periodically polls CCM for certificate requests for remote servers. If a request exists, it will automatically generate a CSR for the web server and present the application for administrator approval via the CCM interface. On approval, the agent will submit the CSR to Comodo CA and track the order number. Once the certificate is issued by CA, the controller will download the certificate and allow the administrator to install the certificate from the CCM interface.
- iii. Auto-installation/renewal is available for the following server types:
 - Apache/Mod SSL
 - Apache - SSL
 - Apache Tomcat
 - Microsoft IIS 1.x to 4.x (Server 2000 - 2008R2)
 - Microsoft IIS 5.x and above (Server 2000 - 2008R2)

Refer to the section [Method 1 - Enterprise Control Mode](#) for a tutorial on automatic installation of Certificates on remote web servers

2. CCM Controller Mode

- i. This mode requires an agent to be installed on each of the web servers for which certificate auto-installation/renewal is required.
- ii. The agent periodically polls CCM for certificate requests for web servers enabled for automatic certificate installation. If a request exists, it will automatically generate a CSR for the web server and present the application for administrator approval via the CCM interface. On approval, the agent will submit the CSR to Comodo CA and track the order number. Once the certificate is issued by the CA, the agent will download the certificate and allow the administrator to install the certificate from the CCM interface.
- iii. The auto-installation/renewal is available for the following server types:
 - Apache/Mod SSL
 - Apache - SSL
 - Apache Tomcat
 - Microsoft IIS 1.x to 4.x (Server 2000 - 2008R2)
 - Microsoft IIS 5.x and above (Server 2000 - 2008R2)

Refer to the section [Method 2 - CCM Controller Mode](#) for a tutorial on automatic installation of Certificates on web servers.

Background Note: It is possible for one Organization to have multiple certificates for different domain names. See the section [5.2.2.4.2 General Settings - Table of Parameters](#) if you would like to read more about this at this time.

3.1.2.2.1 Method 1 - Enterprise Controller Mode

Enterprise Controller mode enables administrators to automatically install certificates on any remote server on the network. Certificate Controller software needs to be installed on a control server and this software will communicate with web-hosts on your network. If a new certificate is requested, the controller will coordinate with the host to generate a CSR, submit it to Comodo CA, collect the certificate and install it. The certificate controller software is accessible through a dedicated web-interface and can be configured to communicate with Comodo CA through a company owned proxy server for additional security.

Certificate Manager Administrator can add remote servers for automatic installation of certificates through the Discovery > Agents interface.

Note: The Certificate Controller software should have been installed on the control server prior to the application for a certificate for a remote server. Refer to the section **Agents** for more details on installing the controller and the section **Configuring the Certificate Controller Agent through Web Interface** for more details on configuring the controller to connect to Comodo CA through a proxy server (optional).

To add remote servers to the certificate controller

- Click the 'Discovery' tab and choose the 'Agents' sub-tab

The screenshot shows the 'Agents' sub-tab in the 'Discovery' section. A table lists agents, with 'Agent org1 52' selected. The 'Edit' button is circled in red, with an arrow pointing to the 'Edit Agent' dialog box. In the dialog, the 'Servers' tab is also circled in red. The dialog shows a table with one server: 'Server IIS org1 50' by 'Microsoft IIS 7.x' in an 'Active' state.

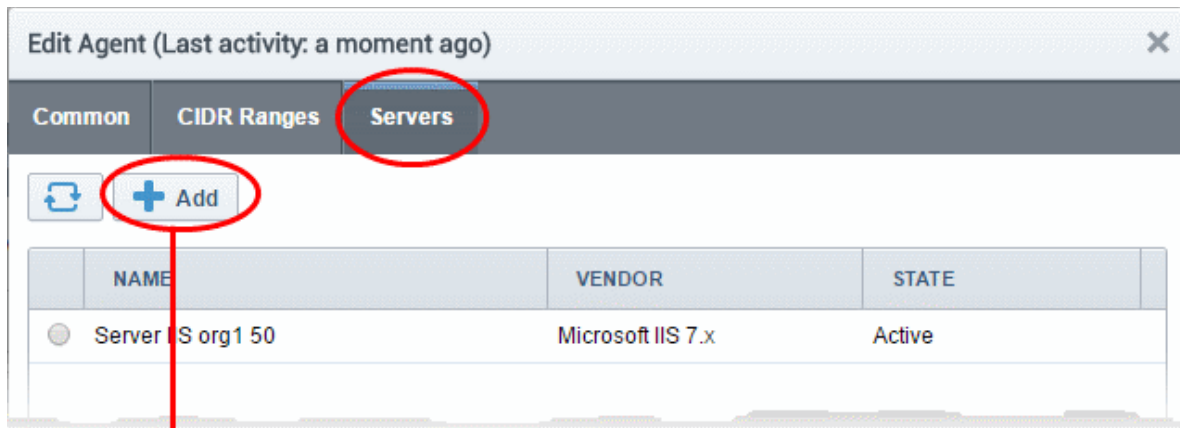
| NAME | ALTERNATIVE NAME | ORGANIZATION | DEPARTMENT | ACTIVE | STATUS |
|---------------|------------------|--------------|------------|-------------------------------------|--------|
| Agent org1 52 | | org1 | | <input checked="" type="checkbox"/> | Con... |

| NAME | VENDOR | STATE |
|--------------------|-------------------|--------|
| Server IIS org1 50 | Microsoft IIS 7.x | Active |

- Select the controller, click 'Edit' at the top to open the 'Edit Agent' dialog and open the 'Servers' tab

The server on which the controller is installed will be displayed in the list of servers.

- Click 'Add' to associate a remote server with the controller. The 'Add Web Server' dialog will open.



Add Web Server ✕

*-required fields

Name*

Vendor*

State Init

Remote

IP address / Port* . . .

Username

Password

| Add Web Server - Table of Parameters | | |
|--------------------------------------|-----------|--|
| Field Name | Type | Description |
| Name | String | Enables the Administrator to enter the name of the server. |
| Vendor | Drop-down | Enables the Administrator to select the vendor of the server. |
| State | | Indicates whether or not the server is initialized. |
| Path to web server | String | Enables the Administrator to specify the network path for the server. Required only for Apache 2.x and Apache Tomcat servers. |
| Remote | Checkbox | Enables the Administrator to specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected. |
| IP Address / Port | String | Enables the Administrator to specify the IP address and connection port of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected. |

| Add Web Server - Table of Parameters | | |
|--------------------------------------|--------|--|
| User Name | String | For IIS server - Enables the Administrator to specify the username of the administrator for logging-into the server. For Apache - Enables the Administrator to specify the private key file path to enable agent to access the server Note: This field will be enabled only if 'Remote' is selected. |
| Password | String | For IIS server - Enables the Administrator to specify the login password for the administrator account for logging into the server For Apache - Enables the Administrator to specify the passphrase of the private key file path Note: This field will be enabled only if 'Remote' is selected. |

- Enter the parameters and click 'OK'. The server will be added to the controller. It will take a few minutes for the server to become 'Active'.

The screenshot shows the 'Servers' tab in the Comodo Certificate Manager. The table contains the following data:

| NAME | VENDOR | STATE |
|--------------------|-------------------|--------|
| Remote Server | Microsoft IIS 7.x | Init |
| Server IIS org1 50 | Microsoft IIS 7.x | Active |

Navigation controls show 15 rows/page and 1 - 2 out of 2 pages. Buttons for 'OK' and 'Cancel' are visible at the bottom.

Once the remote server is added to the controller, administrators can apply for certificates for domains on the server in the 'Certificates Management' > 'SSL Certificates' area.

- Repeat the process to add more remote servers

To enroll a certificate for auto-installation

- Click the 'Certificates' tab and choose the 'SSL Certificates' sub-tab
- Click the 'Add' button

The built-in application form for SSL Enrollment will appear.

Request New SSL Certificate

***-required fields**

Organization* ⓘ

Department*

[Click here to edit address details](#)

Certificate Type*

Certificate Term*

Server Software*

CSR

Provide CSR Autogenerate CSR and Manage Private Key

CSR*

Max CSR size is 32K

Certificate Parameters

Common Name*

Requester

External Requester ⓘ

Comments

Renewal & Installation

Auto renew days before expiration

Create new key pair

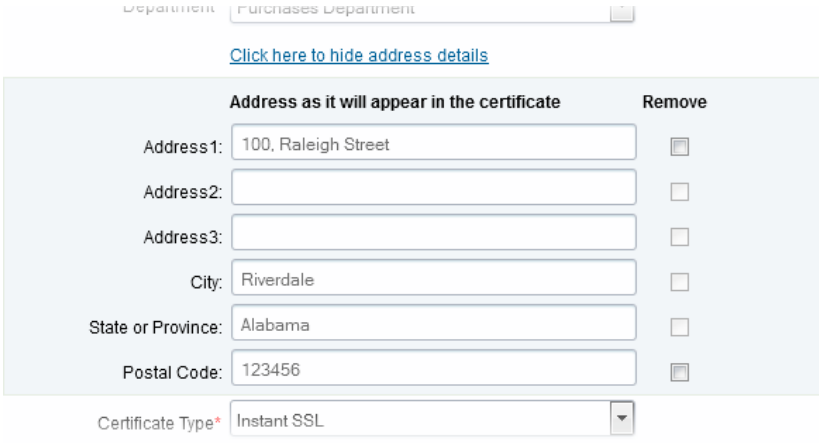
Auto install renewed certificate

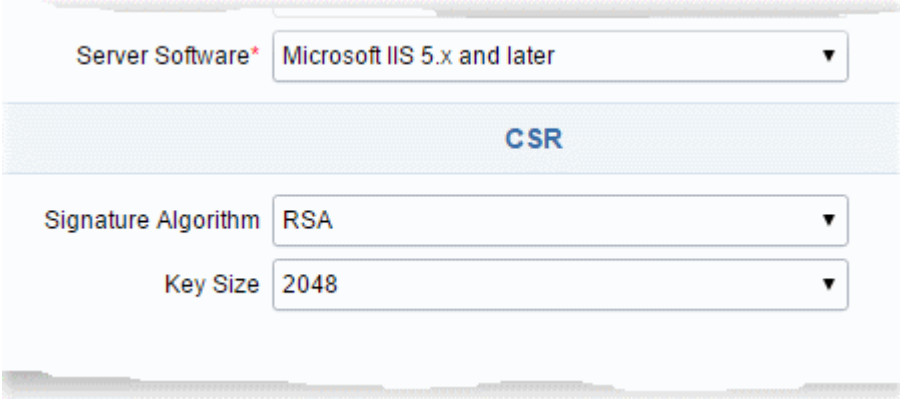
Auto install initial certificate

Subscriber Agreement

Predefined test SSL license text for test customer[2]...

I agree.* Scroll to bottom of the agreement to activate check box.

| Form Element | Type | Description |
|---------------------------------------|-----------------------|---|
| Organization <i>(required)</i> | Drop-down list | Choose the Organization that the SSL certificate will belong to. |
| Department <i>(required)</i> | Drop-down list | Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'. |
| Click here to edit address details | <i>Text Fields</i> | <p>Clicking this link will expand the address fields.</p>  <p>The address fields are auto-populated from the details in the 'General Properties' tab of the Organization or Department on whose behalf this certificate request is being made.</p> <p>These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.</p> |
| Certificate Type <i>(required)</i> | <i>Drop-down list</i> | <p>Choose the certificate type that you wish to add for auto-installation. See Comodo SSL Certificates for a list of certificate types.</p> <p>The specific certificate types displayed in the drop-down list depends on the SSL Types allowed for the selected Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p> <p>Note: Currently CCM supports auto-installation only for the 'Instant SSL' certificate type. Other certificate types will be enabled for auto-installation in the future versions.</p> |
| Certificate Term <i>(required)</i> | <i>Drop-down list</i> | <p>Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years. See Comodo SSL Certificates for a list of certificate types and term lengths.</p> <p>The validity periods available for a particular Organization depends on its configuration. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for</p> |

| Form Element | Type | Description |
|---|-----------------------|---|
| | | more details. |
| Server Software <i>(required)</i> | <i>Drop-down list</i> | Select the server software on which the certificate is to be installed. Auto-installation is supported only on the following server types: <ul style="list-style-type: none"> • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x • Microsoft IIS 5.x and above |
| CSR | | |
| Provide CSR/Autogenerate CSR and Manage Private Key | | Leave these fields blank. After a successful application, the certificate controller will co-ordinate with the web server to create the CSR and submit it to Comodo CA. Once you choose 'Auto install initial certificate' under ' Renewal & Installation ' in this form, these fields will disappear. |
| CSR <i>(required)</i> | | |
| Get CN from CSR <i>(optional)</i> | | You can choose the signature algorithm to be used by the public key of the certificate and the key size for the certificate under 'CSR'. |
| Upload CSR <i>(optional)</i> | |  |
| Certificate Parameters | | |
| Common Name <i>(required)</i> | <i>Text Field</i> | Type the domain that the certificate will be issued to. |
| Requester <i>(auto-populated)</i> | <i>Text Field</i> | The 'Requester' is field is auto-populated with the name of the administrator making the application. |
| External Requester <i>(optional)</i> | <i>Text Field</i> | Enter the email address of an external requester on whose behalf the application is made. Note: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question). The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden. |
| Comments <i>(optional)</i> | <i>Text Field</i> | Enter your comments on the certificate. This is optional. |
| Renewal and Installation | | |

| Form Element | Type | Description |
|--|--------------------------------|--|
| Auto Renew | <i>Checkbox and text field</i> | Enable to auto-renew the certificate when it is nearing expiry. You can also choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA. |
| Create new key pair | <i>Checkbox</i> | Select this option if you want a new key pair is to be generated for the renewal certificate. Leaving it unselected means CCM will re-use the existing key pair of the expiring certificate. |
| Auto install renewed certificate | <i>Checkbox</i> | Select this option if you want the renewed certificate be auto-installed. |
| Auto install initial certificate | <i>Checkbox</i> | Select this option to mark this certificate for auto-installation. After completing the form, the auto-installation wizard will allow you to select the nodes on which the certificate should be installed and to create an installation schedule. |
| Subscriber Agreement (<i>required</i>) | <i>Control</i> | You must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox. |

- Click 'OK' to submit the application

The 'Set Auto Renewal & Installation' dialog will be displayed with the 'Nodes' interface opened. The 'Nodes' interface displays a tree structure of servers associated with the Certificate Controller and the domains hosted on them.

| NAME | COMMON NAME | PROTOC | IP ADDRESS | PORT | STATUS | SSL |
|---|-------------------|--------|------------|------|--------|--------|
| Server IIS org1 50 | | | | | | Active |
| <input type="radio"/> self.ccmqa.local | self.ccmqa.local | HTTP | * | 8443 | No SSL | |
| <input type="radio"/> Default Web Site | Default Web Site | HTTP | * | 80 | No SSL | |
| Server IIS ACME | | | | | | Active |
| <input checked="" type="radio"/> test.ccmqa.com | fortest.ccmqa.com | HTTPS | * | 8444 | No SSL | |
| <input type="radio"/> ms1.ccmqa.com | ms1.ccmqa.com | HTTPS | * | 443 | No SSL | |

- Select the domain from the remote server for which you wish to install a SSL certificate and click 'Next'.

The 'Schedule' interface will be displayed enabling you to choose whether you wish to manually install the certificate from the CCM interface or set a schedule for auto-installation.

Set Auto Renewal & Installation

1 Nodes — 2 **Schedule** — 3 Port — 4 EULA

Manual
 Certificate installation must be started manually.

Schedule
 Certificate installation will be started during selected time period.

Time zone: UTC+00:00 - GMT, UCT, UTC, WET, EGST

Start not earlier than: 01/18/2017

Time Of Day

Run Between: 00 : 19 00 : 19

Day of Week

Run Only: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Close < Back Next >

- If you want to manually install the certificate from the CCM interface, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule', select your time zone, and set a time period. The controller will generate the CSR and submit it to Comodo the next time it polls CCM after the scheduled time.
- Click 'Next'.

The 'Port' interface will open.

Set Auto Renewal & Installation

1 Nodes — 2 Schedule — 3 **Port** — 4 EULA

ms1.ccmqa.com 8445

Wrong server configuration: HTTP on 443 port or HTTPS on 80.

Default node port will be used. New binding on port 8445 will be created

Close < Back Next >

- Specify the HTTPS port for installing the certificate, (**Default = 9443**)
- Click 'Next'. The EULA interface will open.

Set Auto Renewal & Installation X

1 Nodes ————— 2 Schedule ————— 3 Port ————— 4 **EULA**

Subscriber Agreement:

Predefined test SSL license text for test customer[2]...

Print

I agree.* *Scroll to bottom of the agreement to activate check box.*

- Read the EULA fully and accept to by the selecting 'I Agree' checkbox.
- Click 'OK' to save your application.

The certificate will be added to the SSL Certificates interface and its status will be displayed as 'Requested'.

| Dashboard | | | | | |
|---|---------------|--------------|------------|-----------|---------|
| Certificates | | | | | |
| Discovery | | | | | |
| Reports | | | | | |
| Admins | | | | | |
| Settings | | | | | |
| SSL Certificates | | | | | |
| Client Certificates | | | | | |
| Code Signing Certificates | | | | | |
| Device Certificates | | | | | |
| Filter | | | | | |
| <input type="button" value="Refresh"/> <input type="button" value="+ Add"/> <input type="button" value="Export"/> | | | | | |
| | COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES |
| <input type="radio"/> | ccmqa.com[67] | org1 | | Invalid | |
| <input type="radio"/> | ccmqa.com[72] | org1 | | Applied | |
| <input type="radio"/> | ccmqa.com[68] | org1 | | Requested | |
| <input type="radio"/> | ccmqa.com[66] | Advanced | | Invalid | |

- The CSR for the requested certificate will be generated automatically. After the CSR has been created, the 'Approve' button will appear at the top when you select the certificate in the list:

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Approve' button is circled in red. Below it, an 'Approval Message' dialog box is open, containing a text area with the message: 'SSL Cert for ccmqa.com is approved'. The dialog box has 'OK' and 'Cancel' buttons at the bottom.

| | COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES |
|----------------------------------|---------------|--------------|------------|-----------|---------|
| <input type="radio"/> | ccmqa.com[67] | org1 | | Invalid | |
| <input type="radio"/> | ccmqa.com[72] | org1 | | Applied | |
| <input checked="" type="radio"/> | ccmqa.com[68] | org1 | | Requested | |
| <input type="radio"/> | ccmqa.com[66] | Advanced | | Invalid | |

- Click the 'Approve' button to approve the request, enter an approval message and click 'OK'.

On approval, the CSR will be submitted to Comodo CA to apply for the certificate. The certificate status will change to 'Applied'.

The screenshot shows the same 'Certificates' section. The certificate for 'ccmqa.com[68]' now has a status of 'Applied'. The row for this certificate is circled in red.

| | COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRE |
|----------------------------------|---------------|--------------|------------|---------|----------|
| <input type="radio"/> | ccmqa.com[67] | org1 | | Invalid | |
| <input type="radio"/> | ccmqa.com[72] | org1 | | Issued | 01/19/20 |
| <input checked="" type="radio"/> | ccmqa.com[68] | org1 | | Applied | |
| <input type="radio"/> | ccmqa.com[66] | Advanced | | Invalid | |

The controller will track the order number and will download the certificate once it is issued. The certificate will be stored and its status will change to 'Issued'.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|----------------------|--------------|------------|---------------|-------------------|----------------------|----------------------|
| ccmqa.com[67] | org1 | | Invalid | | Not scheduled | Not scheduled |
| ccmqa.com[68] | org1 | | Issued | 01/19/2018 | Not scheduled | Not scheduled |
| ccmqa.com[66] | Advanced | | Invalid | | Not scheduled | Not scheduled |
| ccmqa.com[69] | org1 | | Invalid | | Not scheduled | Not scheduled |

To check whether the Certificate Controller has stored the certificate

- Click 'Discovery' > 'Agents'
- Select the controller and click 'Commands' button

You will see successful execution of 'Store Certificate' command.

Network Assets Discovery Tasks **Agents**

Filter

Download Agent Edit Delete Nodes **Commands**

| NAME | ALTERNATIVE NAME | ORGANIZATION | DEPARTMENT | ACTIVE | STATUS |
|----------------------|------------------|--------------|------------|-------------------------------------|--------|
| Agent org1 52 | | org1 | | <input checked="" type="checkbox"/> | Com... |

Commands

Queue Schedule history

Details Restart

| NAME | DATE | STATE |
|--------------------------|----------------------------|-------------------|
| Store Certificate | 01/18/2017 12:22:20 | Successful |
| Generate Certificate | 01/18/2017 12:20:34 | Successful |
| Discover Target Servers | 01/18/2017 12:18:39 | Successful |
| Generate Certificate | 01/17/2017 18:56:11 | Successful |
| Generate Certificate | 01/17/2017 18:54:01 | Canceled |

The certificate is stored on the server by the agent. If you have set a schedule for automatic installation in the Schedule step while applying for the certificate, it will be installed automatically at the scheduled time. If you have selected 'Manual' in the Schedule step, you can manually initiate the installation process or schedule for auto-installation, from the 'Certificates' > 'SSL Certificates' interface of the CCM console.

To manually initiate auto-installation of a certificate

- Select the certificate from the 'Certificates' > 'SSL Certificates' interface and click 'Install'

The screenshot shows the 'SSL Certificates' interface with a table of certificates. The 'Install' button is circled in red, and a red arrow points from it to the 'Install Certificate' wizard. The wizard is currently on the 'Nodes' step, showing a table of nodes to install the certificate on.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRE |
|--|--------------|------------|--------|----------|
| <input checked="" type="radio"/> ccmqa.com[68] | org1 | | Issued | 01/19/20 |
| <input type="radio"/> ccmqa.local[52] | org1 | | Issued | 01/14/20 |
| <input type="radio"/> demo.ccmqa.local[60] | ccm8 | | Issued | 01/14/20 |

| NAME | COMMON NAME | PROTOC | IP ADDRESS | PORT | STATUS | SSL |
|--|-------------------|--------|------------|------|--------|-------------------------|
| Server IIS org1 50 Active | | | | | | |
| <input type="checkbox"/> test.ccmqa.com | fortest.ccmqa.com | HTTPS | * | 8444 | Failed | 1675873 |
| <input type="checkbox"/> ms1.ccmqa.com | ms1.ccmqa.com | HTTPS | * | 443 | No SSL | |
| <input checked="" type="checkbox"/> ccmqa.com | ccmqa.com | HTTPS | * | 8443 | No SSL | |
| <input type="checkbox"/> Default Web Site | Default Web Site | HTTP | * | 80 | No SSL | |

The 'Install Certificate' wizard will start with the 'Nodes' interface. The node upon which the certificate is to be installed is pre-selected.

- If you want to install the same certificate to additional nodes or to a different node, select the node(s) as required
- Click 'Next'.

The 'Ports' interface will open.

- Specify the port and click 'Next'. The 'Schedule' interface will open.

- If you want to instantly install the certificate, select 'Install now'
- If you want to install the certificate at a later time, select 'Schedule', then select your time zone, and set a time period. The certificate will be installed on the remote server when the certificate controller polls CCM for the first time, within the set time period.
- Click 'OK'

The certificate installation will begin instantly or at the scheduled time as set in the 'Schedule' interface. Once the installation commences, the 'Install State' of the certificate will change to 'Started'.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|-----------------------|--------------|------------|---------|------------|---------------|---------------|
| ccmqa.com[68] | org1 | | Issued | 01/19/2018 | Started | Scheduled |
| ccmqa.local[52] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| demo.ccmqa.local[60] | org2 | | Issued | 01/14/2018 | Not scheduled | Not scheduled |
| fortest.ccmqa.com[65] | org1 | | Invalid | | Not scheduled | Not scheduled |

When installation is complete:

- IIS servers and Tomcat servers - The certificate will be activated immediately and the install state will change to 'Successful'.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE |
|-----------------|--------------|------------|--------|------------|---------------|
| ccmqa.com[68] | org1 | | Issued | 01/19/2018 | Successful |
| ccmqa.local[52] | org1 | | Issued | 01/14/2019 | Not scheduled |

- Apache servers - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.

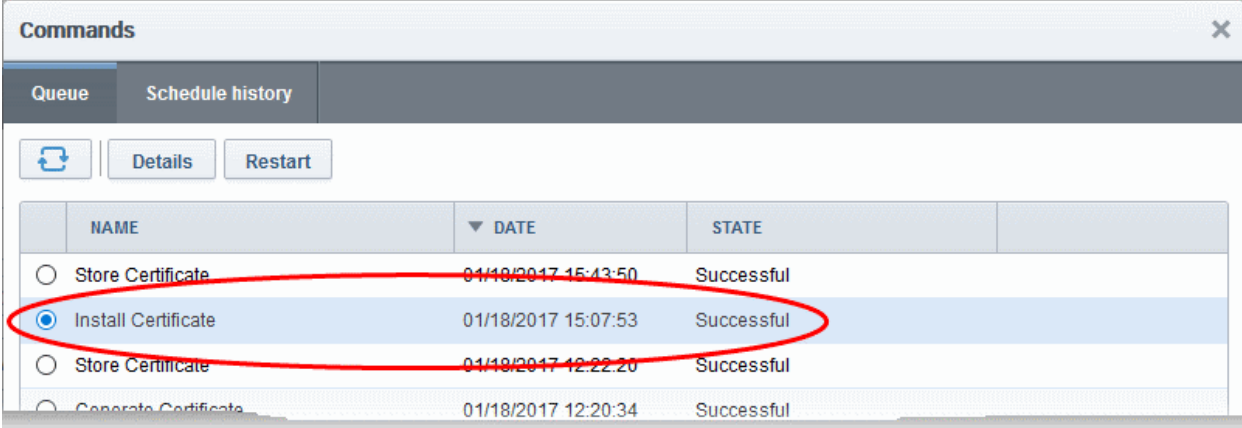
| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE |
|-----------------|--------------|------------|--------|------------|------------------|
| ccmqa.com[72] | org1 | | Issued | 01/19/2018 | Restart Required |
| ccmqa.local[52] | org1 | | Issued | 01/14/2019 | Not scheduled |

Tip: The server can be restarted from CCM through the **Certificate Details** dialog. For more details, refer to the section **Restarting Apache after Auto-Installation of SSL Certificate**.

After restarting the server, the certificate will be activated and the 'Install State' will change to 'Successful'.

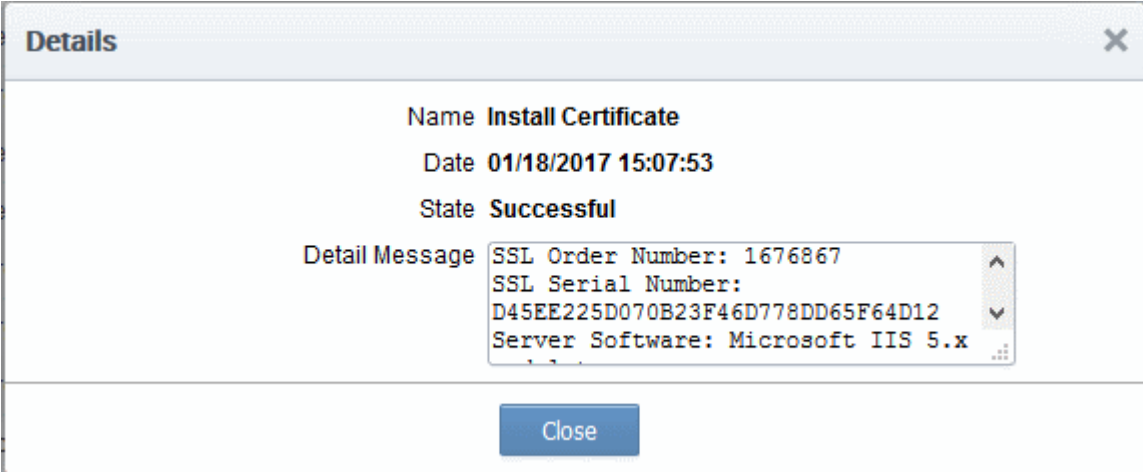
- To check whether the controller has installed the certificate, click Discovery > Agents
- Select the controller and click the 'Commands' button

You will see successful execution of 'Install Certificate' command.



| | NAME | DATE | STATE |
|----------------------------------|----------------------|---------------------|------------|
| <input type="radio"/> | Store Certificate | 01/18/2017 15:43:50 | Successful |
| <input checked="" type="radio"/> | Install Certificate | 01/18/2017 15:07:53 | Successful |
| <input type="radio"/> | Store Certificate | 01/18/2017 12:22:20 | Successful |
| <input type="radio"/> | Generate Certificate | 01/18/2017 12:20:34 | Successful |

- To view command details, select the command and click the 'Details' button at the top.



Name Install Certificate

Date 01/18/2017 15:07:53

State Successful

Detail Message

```
SSL Order Number: 1676867
SSL Serial Number:
D45EE225D070B23F46D778DD65F64D12
Server Software: Microsoft IIS 5.x
```

Close

3.1.2.2.2 Method 2 - CCM Controller Mode

Administrators can request and install new certificates for domains hosted on different web servers from the 'Certificate Management - SSL Certificates' area. 'CCM Controller Mode' requires an agent to be installed on each web server upon which the certificates are to be auto-installed/renewed. Refer to the section [Agents](#) for more details on installing the agent.

To enroll a certificate for auto-installation

- Click the 'Certificates' tab and choose the 'SSL Certificates' sub-tab
- Click the 'Add' button

The built-in application form for SSL Enrollment will appear.

Request New SSL Certificate ✕

***-required fields**

Organization* ⓘ Refresh

Department*

[Click here to edit address details](#)

Certificate Type*

Certificate Term*

Server Software*

CSR

Provide CSR Autogenerate CSR and Manage Private Key

CSR*

Max CSR size is 32K

Certificate Parameters

Common Name*

Requester

External Requester ⓘ

Comments

Renewal & Installation

Auto renew days before expiration

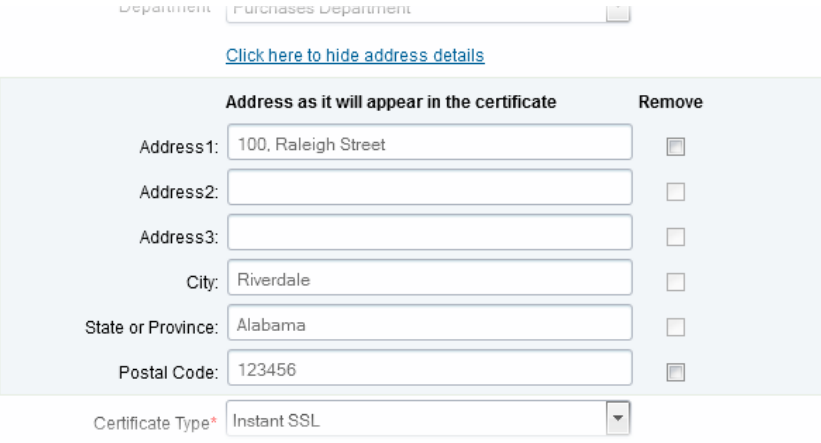
Create new key pair

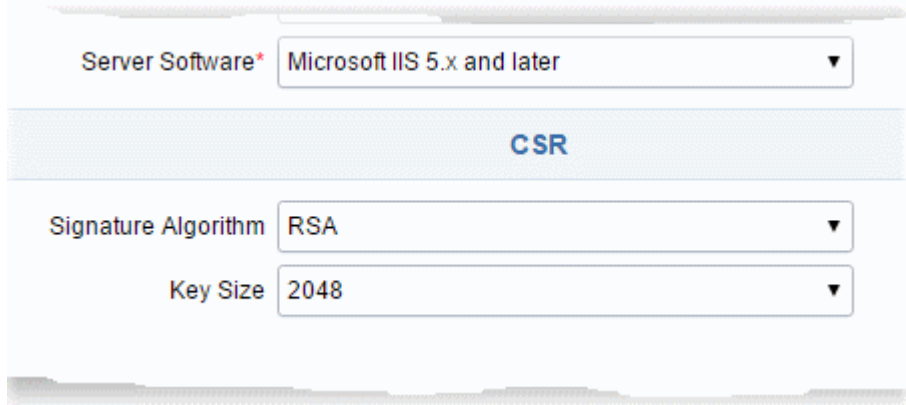
Auto install renewed certificate

Auto install initial certificate

Subscriber Agreement

I agree.* *Scroll to bottom of the agreement to activate check box.*

| Form Element | Type | Description |
|--------------------------------------|----------------|---|
| Organization (<i>required</i>) | Drop-down list | Choose the Organization that the SSL certificate will belong to. |
| Department (<i>required</i>) | Drop-down list | Choose the Department that the SSL certificate will belong to. For the certificate to be applied to all departments, choose 'Any'. |
| Click here to edit address details | Text Fields | <p>Clicking this link will expand the address fields.</p>  <p>The address fields are auto-populated from the details in the 'General Properties' tab of the Organization or Department on whose behalf this certificate request is being made.</p> <p>These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.</p> |
| Certificate Type (<i>required</i>) | Drop-down list | <p>Choose the certificate type that you wish to add for auto-installation. See Comodo SSL Certificates for a list of certificate types.</p> <p>The specific certificate types displayed in the drop-down list depends on the SSL Types allowed for the selected Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p> <p>Note: Currently CCM supports auto-installation only for the 'Instant SSL' certificate type. Other certificate types will be enabled for auto-installation in future versions.</p> |
| Certificate Term (<i>required</i>) | Drop-down list | <p>Choose the validity period of the certificate. For example, 1 year, 2 years, 3 years. See Comodo SSL Certificates for a list of certificate types and term lengths.</p> <p>The validity periods available for a particular Organization depends on its configuration. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more</p> |

| Form Element | Type | Description |
|---|-----------------------|--|
| | | details. |
| Server Software <i>(required)</i> | <i>Drop-down list</i> | Select the server software on which the certificate is to be installed. Auto-installation is supported only on the following server types: <ul style="list-style-type: none"> • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x • Microsoft IIS 5.x and above |
| CSR | | |
| Provide CSR/Autogenerate CSR and Manage Private Key | | Leave these fields blank. After a successful application, the certificate controller will co-ordinate with the web server to create the CSR and submit it to Comodo CA. Once you choose 'Auto install initial certificate' under ' Renewal & Installation ' in this form, these fields will disappear. |
| CSR <i>(required)</i> | | |
| Get CN from CSR <i>(optional)</i> | | You can choose the signature algorithm to be used by the public key of the certificate and the key size for the certificate under 'CSR'. |
| Upload CSR <i>(optional)</i> | |  |
| Certificate Parameters | | |
| Common Name <i>(required)</i> | Text Field | Type the domain that the certificate will be issued to. |
| Requester <i>(auto-populated)</i> | Text Field | The 'Requester' is field is auto-populated with the name of the administrator making the application. |
| External Requester <i>(optional)</i> | | Enter the email address of an external requester on whose behalf the application is made. Note: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question). The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden. |
| Comments <i>(optional)</i> | Text Field | Enter your comments on the certificate. This is optional. |
| Renewal and Installation | | |

| Form Element | Type | Description |
|--|-------------------------|--|
| Auto Renew | Checkbox and text field | Enable to auto-renew the certificate when it is nearing expiry. You can also choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA. |
| Create new key pair | Checkbox | Select this option if you want a new key pair is to be generated for the renewal certificate. Leaving it unselected means CCM will re-use the existing key pair of the expiring certificate. |
| Auto install renewed certificate | Checkbox | Select this option if you want the renewed certificate be auto-installed. |
| Auto install initial certificate | Checkbox | Select this option to mark this certificate for auto-installation. After completing the form, the auto-installation wizard will allow you to select the nodes on which the certificate should be installed and to create an installation schedule. |
| Subscriber Agreement (<i>required</i>) | Control | You must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox. |

- Click 'OK' to submit the application

The 'Set Auto Renewal & Installation' dialog will be displayed with the 'Nodes' interface open. The 'Nodes' interface displays a list of agents installed on your servers for different Organizations and Departments. A list of server nodes is shown under each Agent.

- Select the domain on which you wish to install a certificate and click Next.

The 'Schedule' interface will open, allowing you to install the certificate manually from the CCM interface or to set a schedule for auto-installation.

Set Auto Renewal & Installation

1 Nodes — 2 **Schedule** — 3 Port — 4 EULA

Manual
 Certificate installation must be started manually.

Schedule
 Certificate installation will be started during selected time period.

Time zone: UTC+00:00 - GMT, UCT, UTC, WET, EGST

Start not earlier than: 01/18/2017

Time Of Day

Run Between: 00 : 19 00 : 19

Day of Week

Run Only: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Close < Back Next >

- If you want to manually install the certificate from the CCM interface, select 'Manual'
- If you want to install the certificate at a scheduled time, select 'Schedule' then select your time zone and a 'not earlier than' time. The controller will generate a CSR and submit it to Comodo CA the first time it polls CCM after the 'not earlier than' time. Use the check-boxes at the bottom to limit which days of the week that the installation should run.
- Click 'Next'.

The 'Port' interface will open.

Set Auto Renewal & Installation

1 Nodes — 2 Schedule — 3 **Port** — 4 EULA

ms1.ccmqa.com 8445

Warning: Wrong server configuration: HTTP on 443 port or HTTPS on 80.

Info: Default node port will be used. New binding on port 8445 will be created

Close < Back Next >

- Specify the HTTPS port for installing the certificate, (**Default = 9443**)
- Click 'Next'. The EULA interface will open.

Set Auto Renewal & Installation X

1 Nodes ————— 2 Schedule ————— 3 Port ————— 4 **EULA**

Subscriber Agreement:

Predefined test SSL license text for test customer[2]...

Print

I agree.* *Scroll to bottom of the agreement to activate check box.*

- Read the EULA fully and accept it by selecting the 'I Agree' checkbox.
- Click 'OK' to save your application.

The certificate will be added to the SSL Certificates interface and its status will change to 'Requested'.

| Dashboard | | | | | |
|---|---------------|--------------|------------|-----------|---------|
| Certificates | | | | | |
| Discovery | | | | | |
| Reports | | | | | |
| Admins | | | | | |
| Settings | | | | | |
| SSL Certificates | | | | | |
| Client Certificates | | | | | |
| Code Signing Certificates | | | | | |
| Device Certificates | | | | | |
| Filter | | | | | |
| <input type="button" value="Refresh"/> <input type="button" value="+ Add"/> <input type="button" value="Export"/> | | | | | |
| | COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES |
| <input type="radio"/> | ccmqa.com[67] | org1 | | Invalid | |
| <input type="radio"/> | ccmqa.com[72] | org1 | | Applied | |
| <input type="radio"/> | ccmqa.com[68] | org1 | | Requested | |
| <input type="radio"/> | ccmqa.com[66] | Advanced | | Invalid | |

- The CSR for the requested certificate will be generated automatically. After the CSR is created, the approve button will appear at the top when you select the certificate in the list.

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Approve' button is circled in red. Below it, an 'Approval Message' dialog box is open, containing a text area with the message: 'SSL Cert for ccmqa.com is approved'. The dialog box has 'OK' and 'Cancel' buttons at the bottom.

| | COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES |
|----------------------------------|---------------|--------------|------------|-----------|---------|
| <input type="radio"/> | ccmqa.com[67] | org1 | | Invalid | |
| <input type="radio"/> | ccmqa.com[72] | org1 | | Applied | |
| <input checked="" type="radio"/> | ccmqa.com[68] | org1 | | Requested | |
| <input type="radio"/> | ccmqa.com[66] | Advanced | | Invalid | |

- Click the 'Approve' button to approve the request, enter the approval message in the 'Approval Message' dialog and click 'OK'.

On approval, the CSR will be submitted to Comodo CA to apply for the certificate. The certificate status will change to 'Applied'.

The screenshot shows the same 'Certificates' section as before, but the status of the certificate 'ccmqa.com[68]' has changed from 'Requested' to 'Applied'. The row for 'ccmqa.com[68]' is circled in red.

| | COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES |
|----------------------------------|---------------|--------------|------------|---------|----------|
| <input type="radio"/> | ccmqa.com[67] | org1 | | Invalid | |
| <input type="radio"/> | ccmqa.com[72] | org1 | | Issued | 01/19/20 |
| <input checked="" type="radio"/> | ccmqa.com[68] | org1 | | Applied | |
| <input type="radio"/> | ccmqa.com[66] | Advanced | | Invalid | |

The controller will track the order number then collect and store the certificate once it is issued. The certificate status

will change to 'Issued'.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|----------------------|--------------|------------|---------------|-------------------|---------------|---------------|
| ccmqa.com[67] | org1 | | Invalid | | Not scheduled | Not scheduled |
| ccmqa.com[68] | org1 | | Issued | 01/19/2018 | Not scheduled | Not scheduled |
| ccmqa.com[66] | Advanced | | Invalid | | Not scheduled | Not scheduled |
| ccmqa.com[69] | org1 | | Invalid | | Not scheduled | Not scheduled |

To check whether the controller has stored the certificate:

- Click 'Discovery' > 'Agents'
- Select the controller and click the 'Commands' button

You will see successful execution of 'Store Certificate' command.

Network Assets Discovery Tasks **Agents**

Filter

Download Agent Edit Delete Nodes **Commands**

| NAME | ALTERNATIVE NAME | ORGANIZATION | DEPARTMENT | ACTIVE | STATUS |
|----------------------|------------------|--------------|------------|-------------------------------------|-----------|
| Agent org1 52 | | org1 | | <input checked="" type="checkbox"/> | Completed |

Commands

Queue Schedule history

Details Restart

| NAME | DATE | STATE |
|--------------------------|----------------------------|-------------------|
| Store Certificate | 01/18/2017 12:22:20 | Successful |
| Generate Certificate | 01/18/2017 12:20:34 | Successful |
| Discover Target Servers | 01/18/2017 12:18:39 | Successful |
| Generate Certificate | 01/17/2017 18:56:11 | Successful |
| Generate Certificate | 01/17/2017 18:54:01 | Canceled |

The certificate is stored on the server by the agent. If you created a schedule for automatic installation in the Schedule step, it will be installed automatically at the scheduled time. If you selected 'Manual', you can initiate the auto-installation process from the 'Certificates' > 'SSL Certificates' interface:

To manually initiate auto-installation of a certificate

- Select the certificate from the 'Certificates' > 'SSL Certificates' interface and click 'Install'

The screenshot shows the 'Install Certificate' wizard in the Comodo Certificate Manager. The wizard is divided into three steps: 1. Nodes, 2. Port, and 3. Schedule. The 'Nodes' step is active, displaying a table of nodes. The 'ccmqa.com' node is selected with a checked checkbox. The table columns are NAME, COMMON NAME, PROTOC, IP ADDRESS, PORT, STATUS, and SSL.

| NAME | COMMON NAME | PROTOC | IP ADDRESS | PORT | STATUS | SSL |
|--|-------------------|--------|------------|------|--------|-------------------------|
| <input checked="" type="checkbox"/> Server IIS org1 50 | | | | | Active | |
| <input type="checkbox"/> test.ccmqa.com | fortest.ccmqa.com | HTTPS | * | 8444 | Failed | 1675873 |
| <input type="checkbox"/> ms1.ccmqa.com | ms1.ccmqa.com | HTTPS | * | 443 | No SSL | |
| <input checked="" type="checkbox"/> ccmqa.com | ccmqa.com | HTTPS | * | 8443 | No SSL | |
| <input type="checkbox"/> Default Web Site | Default Web Site | HTTP | * | 80 | No SSL | |

The 'Install Certificate' wizard will start with the 'Nodes' interface. The node upon which the certificate is to be installed is pre-selected.

- If you want to install the same certificate to additional nodes or to a different node, select the node(s) as required
- Click 'Next'.

The 'Ports' interface will open.

- Specify the port and click 'Next'. The 'Schedule' interface will open.

- If you want to instantly install the certificate, select 'Install now'
- If you want to install the certificate at a later time, select 'Schedule', then select your time zone, and set a 'not earlier than' date. The certificate will be installed on the server when the controller polls CCM for the first time after the 'Not earlier than' date.
- Click 'OK'

Once installation commences, the 'Install State' of the certificate will change to 'Started':

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE | RENEWAL STATE |
|-----------------------|--------------|------------|---------|------------|---------------|---------------|
| ccmqa.com[68] | org1 | | Issued | 01/19/2018 | Started | Scheduled |
| ccmqa.local[52] | org1 | | Issued | 01/14/2019 | Not scheduled | Not scheduled |
| demo.ccmqa.local[60] | org2 | | Issued | 01/14/2018 | Not scheduled | Not scheduled |
| fortest.ccmqa.com[65] | org1 | | Invalid | | Not scheduled | Not scheduled |

When installation is complete:

- IIS servers and Tomcat servers - The certificate will be activated immediately and the install state will change to 'Successful'.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE |
|-----------------|--------------|------------|--------|------------|---------------|
| ccmqa.com[68] | org1 | | Issued | 01/19/2018 | Successful |
| ccmqa.local[52] | org1 | | Issued | 01/14/2019 | Not scheduled |

- Apache servers - The certificate will become active after the server is restarted. The install state will change to 'Restart Required'.

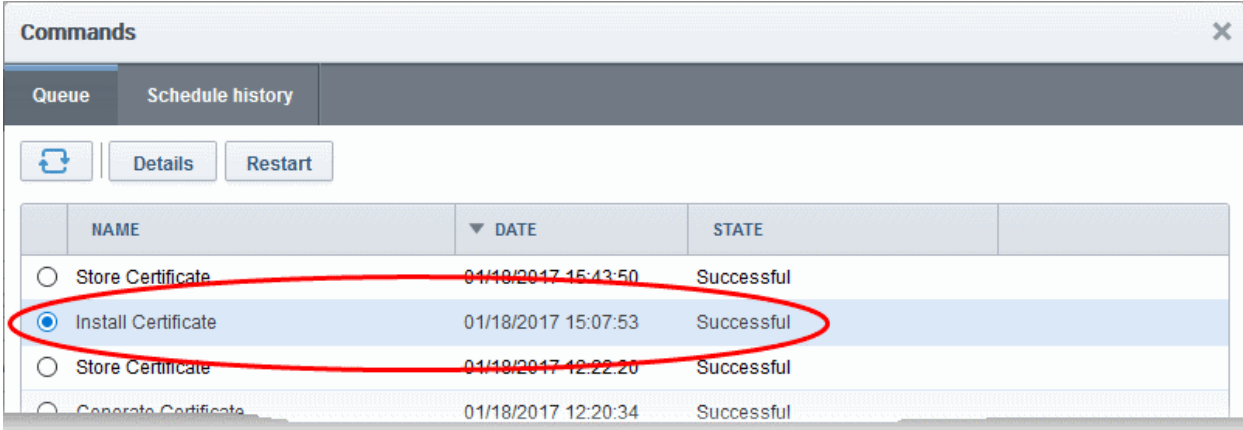
| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | INSTALL STATE |
|-----------------|--------------|------------|--------|------------|------------------|
| ccmqa.com[72] | org1 | | Issued | 01/19/2018 | Restart Required |
| ccmqa.local[52] | org1 | | Issued | 01/14/2019 | Not scheduled |

Tip: The server can be restarted from CCM through the **Certificate Details** dialog. For more details, refer to the section **Restarting Apache after Auto-Installation of SSL Certificate**.

After restarting the server, the certificate will be activated and the 'Install State' will change to 'Successful'.

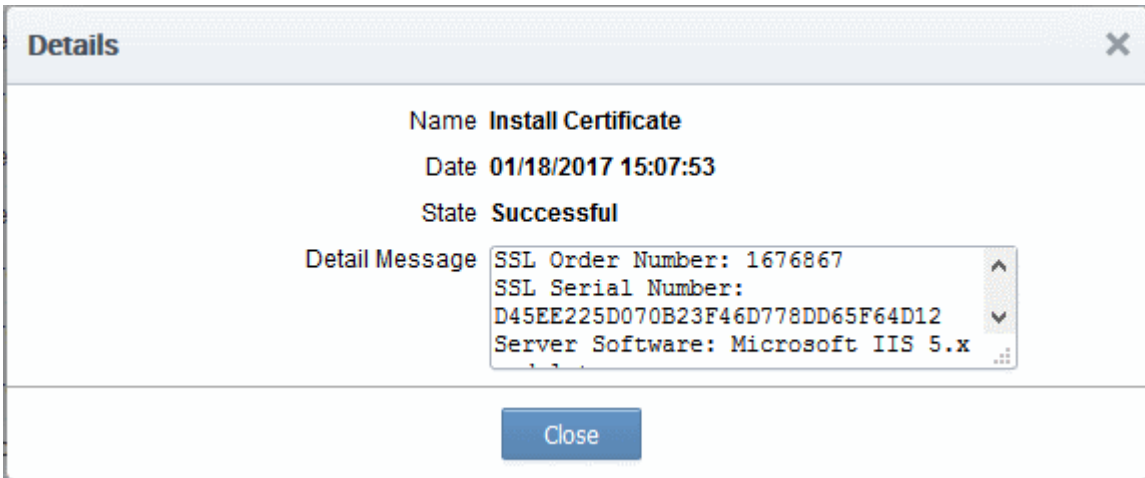
- To check whether the controller has installed the certificate, click Discovery > Agents
- Select the controller and click the 'Commands' button

You will see successful execution of 'Install Certificate' command.



| | NAME | DATE | STATE |
|----------------------------------|----------------------|---------------------|------------|
| <input type="radio"/> | Store Certificate | 01/18/2017 15:43:50 | Successful |
| <input checked="" type="radio"/> | Install Certificate | 01/18/2017 15:07:53 | Successful |
| <input type="radio"/> | Store Certificate | 01/18/2017 12:22:20 | Successful |
| <input type="radio"/> | Generate Certificate | 01/18/2017 12:20:34 | Successful |

- To view command details, select the command and click the 'Details' button at the top.



Name Install Certificate

Date 01/18/2017 15:07:53

State Successful

Detail Message

```
SSL Order Number: 1676867
SSL Serial Number:
D45EE225D070B23F46D778DD65F64D12
Server Software: Microsoft IIS 5.x
```

Close

3.1.2.3 Initiating SSL Enrollment using Application Forms

The SSL Administrators or the applicants authorized by them can make request for certificates to be installed on to the web servers by submission of application forms. On successful submission and validation by Comodo CA, the certificate will be issued and a notification email will be sent to the applicant. The applicant can download the certificate and install it on to respective web server.

CCM offers two types of SSL application forms:

- The Self Enrollment Form** - Administrators can apply or direct applicants to the request form to order SSL certificates. Applicants using this method must validate their application to Certificate Manager by:
 - Entering the appropriate **Access Code** for the Organization or Department. The Access Code is a mixture of alpha and numeric characters that the applicant needs to provide in order to authenticate the request to Certificate Manager.
and
 - The email address they enter must be from the domain that the certificate application is for. This domain must have been assigned to the Organization or Department.

Refer to the section **Method 1 - Self Enrollment Form** for a tutorial on applying for and installing certificates through the self-enrollment form.

- The Built-in Application Form** - Administrators can login and request SSL certificates using the built-in application form available at the Certificates Management > SSL Certificates area. The Built-in application form allows the administrator to enroll for SSL certificates in two ways:
 - Manual CSR Generation** - The administrator needs to generate the certificate signing request (CSR) at

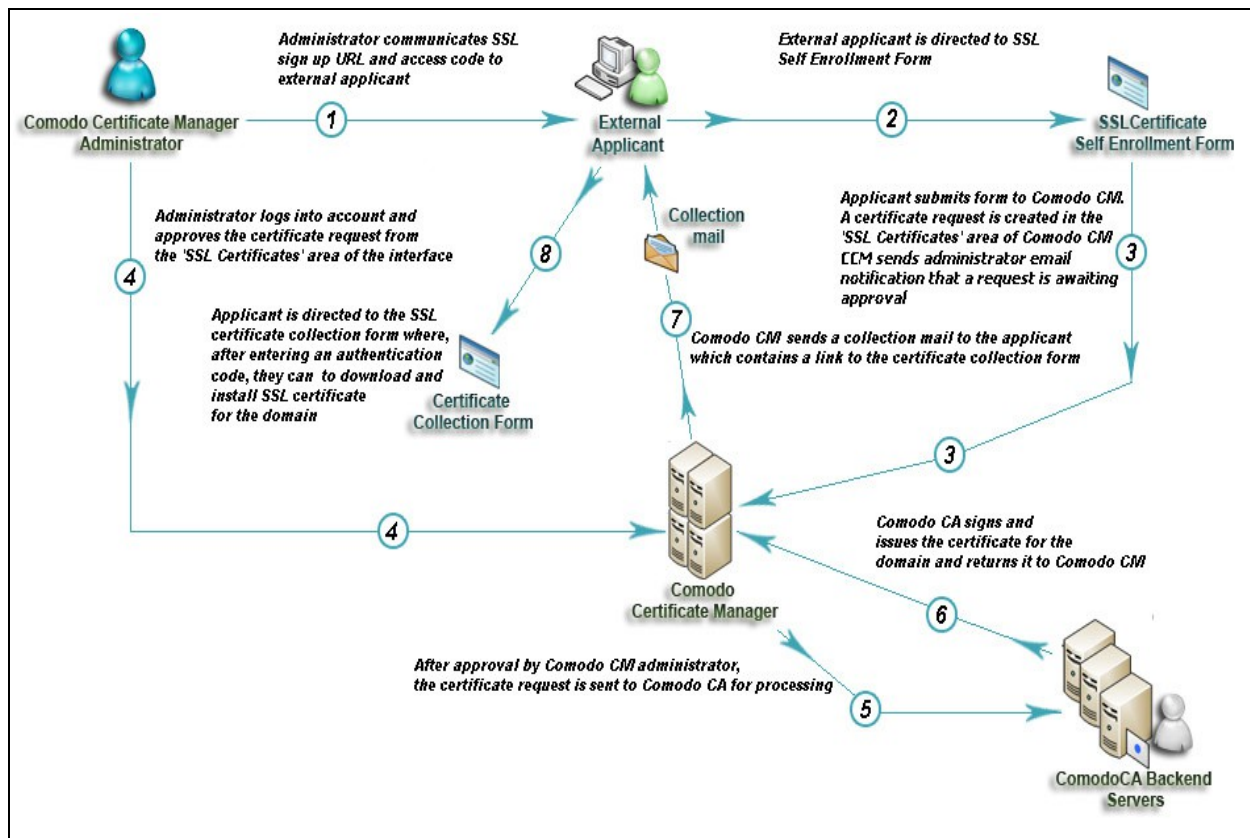
the server on which the certificate needs to be installed and enter the CSR in to the application form. Refer to the section **Method 2 - Built-in Enrollment Form - Manual CSR Generation** for a tutorial on applying for and installing certificates.

- ii. **Auto CSR Generation** - CCM can generate the CSR for the domain name with the private key stored by the Private Key Store controller installed on a server at the customer premises. On completion of certificate issuance, the administrator can download the certificate with the public/private key pair from CCM and import to the server(s) on which it needs to be installed. Refer to the section **Method 3 - Built-in Enrollment Form - Auto CSR Generation** for a tutorial on applying for and installing certificates.

On successful completion of application submission, the certificate will be added to the Certificates Management > SSL Certificates area with the status 'Requested'. An appropriately privileged SSL administrator should **approve** the request. On approval, CCM will forward the application to Comodo CA. After validating the application, the CA will issue the certificate and the certificate status will be changed to 'Issued'. A collection email will be sent to the administrator or the applicant. The applicant can collect, download and install the certificate in the respective web server. For more details on collection of the certificate, refer to the section **Certificate Collection**. For more details on downloading and installing the certificate, refer to the section **Downloading and Importing SSL Certificates**.

Background Note: It is possible for one Organization to have multiple certificates for different domain names. See **5.2.2.3.2 General Settings - Table of Parameters** if you would like to read more about this at this time.

3.1.2.3.1 Method 1 - Self Enrollment Form



3.1.2.3.1.1 Initiating the Self Enrollment Process

After completing the **prerequisite steps**, the administrator needs to communicate enrollment details to all and any end-users they wish to issue SSL certificates to (for example, via email). The communication must contain the

following information:

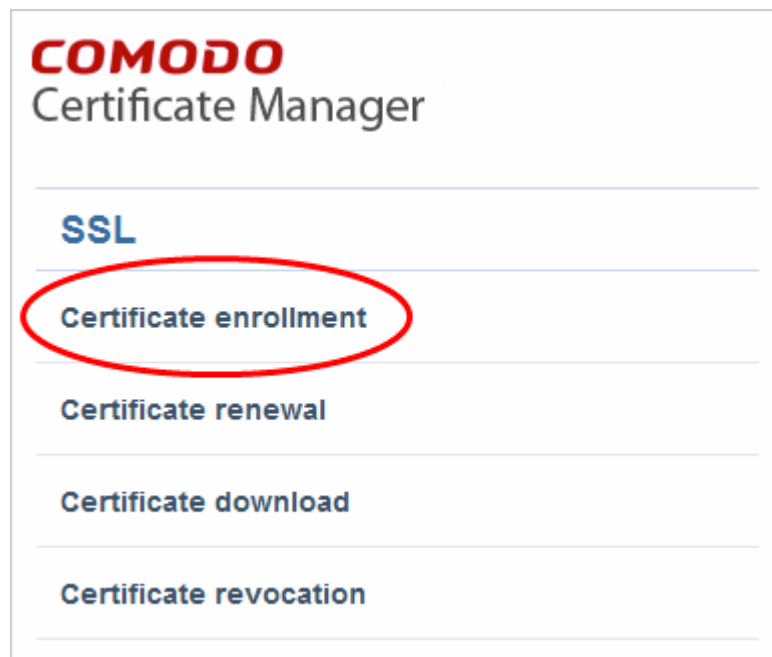
1. A link to the Self Enrollment Form - [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/ssl](https://cert-manager.com/customer/[REAL CUSTOMER URI]/ssl)
2. The Access Code specified in the Organization or Department's **SSL settings tab**.

Furthermore, the email address that the applicant enters at the self-enrollment form must match a domain that has been assigned to the Organization or Department.

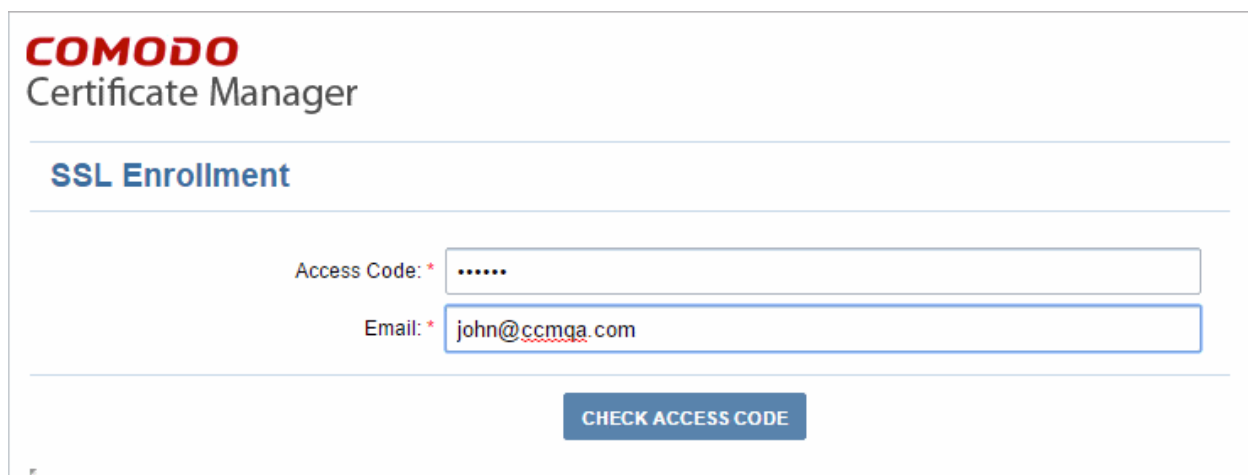
3.1.2.3.1.2 The Self Enrollment Form

The application form for SSL certificates is hosted, by default, at: [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/ssl](https://cert-manager.com/customer/[REAL CUSTOMER URI]/ssl)

End-users should be directed to this page using the administrators preferred communication method. Please refer to the preceding section, **Initiating the Self Enrollment Process** for more details.



- Clicking the 'Certificate enrollment' link will open the self enrollment form

A screenshot of the 'SSL Enrollment' form in the Comodo Certificate Manager. The form has a header with the 'COMODO Certificate Manager' logo and the title 'SSL Enrollment'. Below the title, there are two input fields: 'Access Code: *' with a masked value '.....' and 'Email: *' with the value 'john@ccmqa.com'. At the bottom of the form, there is a blue button labeled 'CHECK ACCESS CODE'.

- Before proceeding to the full application form, the applicant has to authenticate the request by:
 - Entering the correct Access Code for the Organization or Department
 - Entering an email address from a domain that has been assigned to that Organization or Department.

- Clicking the 'Check Access Code' will contact CCM to authenticate that the applicant has the right to apply for a certificate
- If both Access Code and E-mail address are successfully verified then the applicant will move onto the full certificate application form:

COMODO
Certificate Manager

SSL Enrollment

Access Code: *

Email: * john@ccmqa.com

[Click here to edit address details](#)

Certificate Type: * Instant SSL

Certificate Term: * 1 year

Server Software: * AOL

CSR: *

GET CN FROM CSR UPLOAD CSR Warning: CSR size is 32K

Common Name: *

Renew: Auto renew _____ days before expiration

Please provide a pass-phrase. A pass-phrase is necessary for certificate revocation and renewal.

Pass-phrase: _____

Re-type pass-phrase: _____

External Requester: _____

Acceptable format:

- email@domain.com
- email.1@domain.com, email.2@domain.com

Comments: _____

Predefined test SSL license text for test customer[2]...

Subscriber Agreement

I Agree. Scroll to bottom of the agreement to activate check box.

PRINT

ENROLL RESET

The external applicant need not be an existing user in the CM, but the person's email address must be from the same domain as the common name, else the application cannot proceed.

Clicking 'Get Common Name from CSR' will automatically populate the 'Common Name' field and if relevant, the 'SAN' field with the domain name(s) in the CSR - Helping to avoid errors. This feature is especially useful while applying for MDCs where the application could contain upto 100 domains in the SAN field.

The applicant can directly upload the CSR saved as .txt file by clicking 'Upload CSR'. The CSR field will be auto-populated with the CSR from the text file.

The applicant can configure for auto-renewal of the certificate, upon its expiry.

The Passphrase entered here is required for the purposes of certificate revocation.

The applicant must accept the 'Terms and Conditions' before submitting the form. The 'I Agree' checkbox becomes active only on scrolling down the page till the end.

- The 'Access Code' and 'E-mail' address fields will be pre-populated.
- The domain that the user specifies in the 'CN' field must be the same domain as the applicant's E-mail

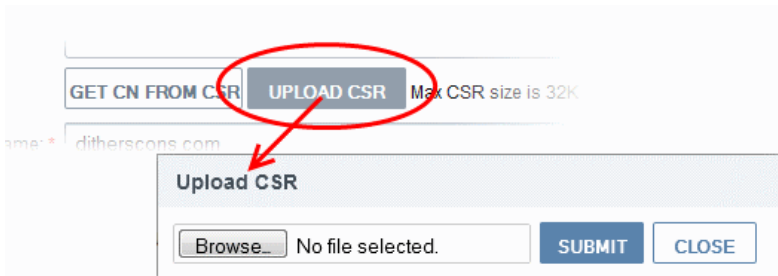
address. The applicant MUST be able to receive emails at this address.

- Comodo provide a range of CSR generation documents designed to assist Administrators and external applicants through the CSR creation process. For a list of these documents, please visit: https://support.Comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0 . (Select 'CSR generation' section and web server software).
- It is possible for Certificate Manager Account holders to use their own, custom form templates rather than the default form supplied by Comodo. Contact your account manager for more details on enabling this functionality and for submitting custom banners for application forms

3.1.2.3.1.3 Form Parameters

| Form Element | Type | Description |
|-------------------------------|------------|---|
| Access Code <i>(required)</i> | Text Field | <p>An Access Code identifies a particular Organization or Department and is used to authenticate certificate requests that are made using the Self-Enrollment form.</p> <p>Organizations and Departments are uniquely identified by combination of the Organization's 'Access Code' and the 'Common Name' (domain) specified in 'General' properties. Multiple Organizations or Departments can have the same Access Code OR the same Common Name - but no single entity can share both.</p> <p>Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form.</p> <p>Applicants that request a certificate using the Self Enrollment Form will need to enter this code.</p> |

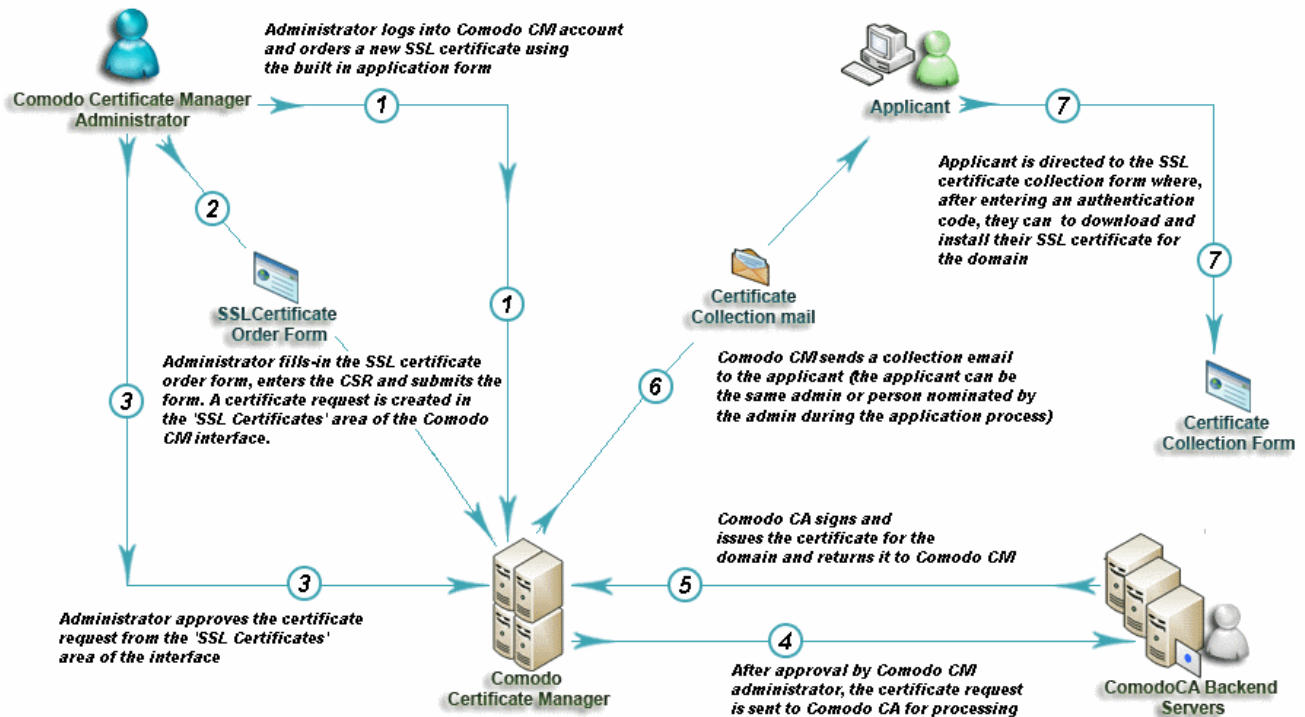
| Form Element | Type | Description |
|--|----------------|---|
| Email (<i>required</i>) | Text Field | Applicant should enter their full email address. The email address must be for a domain that has been assigned to the Organization or Department. |
| Address Details Displayed on clicking the Click here to edit address details link. Address 1: Address 2: Address 3: City: State or Province: Postal Code: (all auto-populated) | Text Fields | Clicking the link 'Click here to edit address' details displays the address fields. The address fields are auto-populated from the details in the ' General Settings ' tab of the Organization or Department on whose behalf this certificate request is being made. These fields cannot be modified but, in the case of OV level certificates , the applicant can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For EV level certificates , it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down. |
| Certificate Type (<i>required</i>) | Drop-down list | Applicant should select certificate type. For a list of Comodo SSL certificate types, see the section Comodo SSL Certificates . The specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization , Customize an Organization's SSL Certificate Types and SSL Types for more details. |
| Certificate Term (<i>required</i>) | Drop-down list | Applicant should select the life time of the certificate chosen from the 'Certificate Type ' drop-down. The available term lengths for different certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization , Customize an Organization's SSL Certificate Types and SSL Types for more details. |
| Server Software (<i>required</i>) | Drop-down list | Applicant should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from the Comodo's support portal here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0 |
| CSR (<i>required</i>) | Text Field | A Certificate Signing Request (CSR) is required to be entered into this field in order for Comodo CA to process your application and issue the certificate for the domain. The CSR can be entered in two ways: <ul style="list-style-type: none"> • Pasting the CSR directly into this field • Uploading the CSR saved as a .txt file by clicking the 'Upload CSR' button |

| Form Element | Type | Description |
|-------------------------------------|------------|--|
| | | <p>Background: In public key infrastructure systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information. Upon uploading or pasting the CSR, the form will automatically parse the CSR.</p> <p>Administrators that require assistance to generate a CSR should consult the Comodo knowledge article for their web server type here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1</p> <p>Special Note regarding MDC applications: The CSR you generate only needs to be for the single 'Common Name' (aka the 'Primary Domain Name'). You should type the additional domains that you require in the 'Subject Alternative Name' field on this form.</p> |
| Get CN from CSR (<i>optional</i>) | Control | <p>Once the CSR has been entered correctly, clicking this button will auto-populate the Common Name (CN) field. Using this method helps to avoid human error by ensuring the domain name mentioned in the application form exactly match that in the CSR. If the domain name mentioned in this application form do not match that in the CSR, then Comodo CA will not be able to issue the certificate.</p> <p>Special Note regarding MDC applications: In order to successfully order a Multi-Domain Certificate, the applicant need only list the additional domains in the SAN field on this form. In certain circumstances, however, the applicant may have created a CSR that already contains these Subject Alternative Names. In this case, clicking the 'Get CN from CSR' button will also auto-populate the 'Subject Alternative Names' form fields as well as the 'Common Name' field.</p> |
| Upload CSR (<i>optional</i>) | Control | <p>The applicant can upload the CSR saved as a .txt file in the local computer, instead of copying and pasting the CSR into the CSR field - helping to avoid errors.</p>  |
| Common Name (<i>required</i>) | Text Field | Applicants should enter the correct fully qualified domain name for the |

| Form Element | Type | Description |
|--|------------|---|
| | | <p>Organization or Department</p> <p>Single Domain certificates - enter domain name using the form: domain.com.</p> <p>Wildcard Certificates - enter domain name using the form: *.domain.com.</p> <p>Multi-Domain Certificates - enter the primary domain name using the form: domain.com.</p> |
| Renew | Check box | Allows applicants to specify whether the certificate should be automatically renewed when it is nearing expiry. Applicants can also choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, CCM will automatically submit the renewal application to the CA with a CSR generated using the same parameters as the existing certificate. |
| Subject Alternative Names <i>(required for Multi-Domain certificates)</i> | Text Field | If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain listed in this field should be separated by a comma. |
| Pass Phrase <i>(optional)</i> | Text Field | This phrase is needed to revoke the certificate when using the external revocation page at: https://cert-manager.com/customer/real_customer_uri/ssl?action=revoke |
| Re-type Pass Phrase <i>(required if specified in the field above)</i> | Text Field | Confirmation of the above. |
| External Requester <i>(optional)</i> | Text Field | Applicants should enter the full email address of the user on behalf of whom the application is made. The email address must be from the same domain name for which the certificate is applied. The certificate collection email will be sent to this email address. |
| Comments <i>(optional)</i> | Text Field | Applicant can enter information for the administrator. |
| Subscriber Agreement | Checkbox | <p>Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox.</p> <p>Note: The Subscriber Agreement will differ depending on the type of SSL certificate selected from the 'Certificate Type' drop-down. If Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate is selected, The 'I Agree' checkbox will not be shown and the agreement will be taken as accepted, when the user submits the application.</p> |
| Enroll | Control | Submits the application and enrolls the new certificate request. |
| Reset | Control | Clears all data entered on the form. |

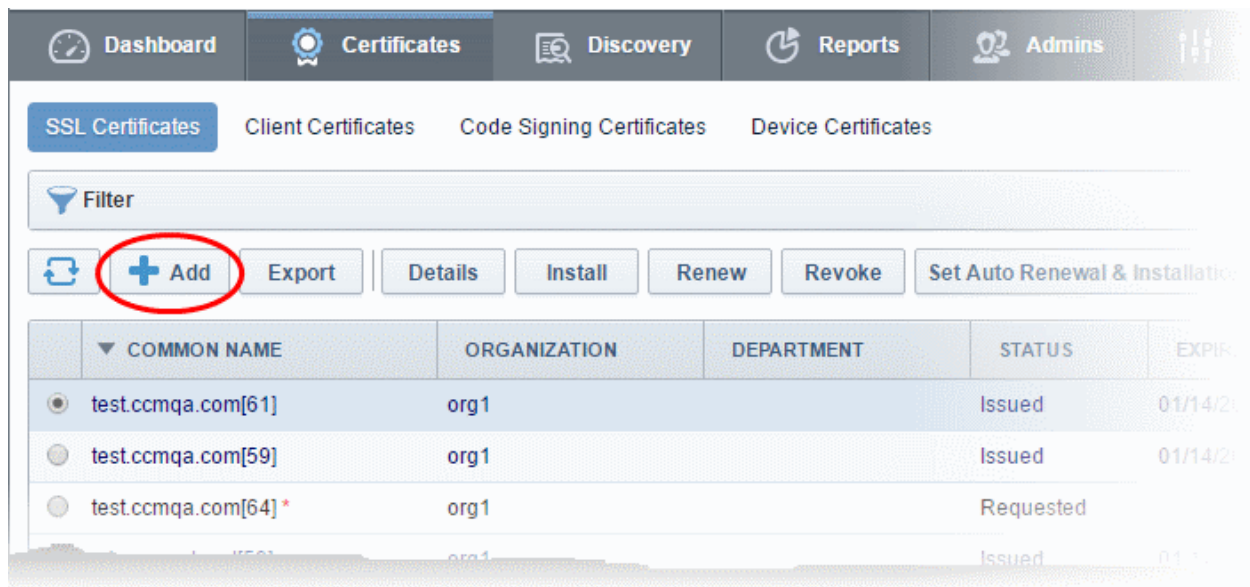
Note: In addition to the standard fields in the Self Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

3.1.2.3.2 Method 2 - Built-in Enrollment Form - Manual CSR Generation



3.1.2.3.2.1 Accessing the Built-in Application Form

Certificate Manager administrators can apply for new certificates directly from the 'Certificate Management - SSL Certificates' area by clicking the 'Add' button (as shown).



Clicking the 'Add' button will open the built-in 'Request New SSL Certificate' form. The next sections of this guide will explain this form in more details.

3.1.2.3.2.2 The Built-In Application Form

The built in SSL certificate application form is very similar to the Self Enrollment Form but does not require an Access Code:

Request New SSL Certificate

*-required fields

Organization* ⓘ

Department*

[Click here to edit address details](#)

Certificate Type*

Certificate Term*

For manually entering the CSR generated at the server, the administrator should choose 'Provide CSR'.

Provide CSR Autogenerate CSR and Manage Private Key

CSR*

Max CSR size is 32K

The address details are auto-populated based on the Organization and Department selected. These details cannot be edited. If required, the administrator can select the address fields to be omitted in the certificate by clicking this link.

The administrator can directly upload the CSR saved as a .txt file by clicking 'Upload CSR'. The CSR field will be auto-populated with the CSR from the text file.

Clicking Get 'CN from CSR' will automatically populate the 'Common Name' field and if relevant, the 'Subject Alternative Names' field with the domain names in the CSR, helping to avoid errors. This feature is especially useful during the application for MDCs, where the application could contain up to 100 domain names in SAN field.

Certificate Parameters

Common Name*

Requester

External Requester

Comments

Telephone*

The administrator can specify the email address of the external applicant on behalf of whom the application is made. The external applicant will also receive the certificate collection email.

Renewal & Installation

Auto renew days before expiration

Create new key pair

Auto install renewed certificate

Auto install initial certificate

Administrators can choose for automatic installation and renewal of applied certificate. These features are supported only for certain certificate types and server types.

Subscriber Agreement

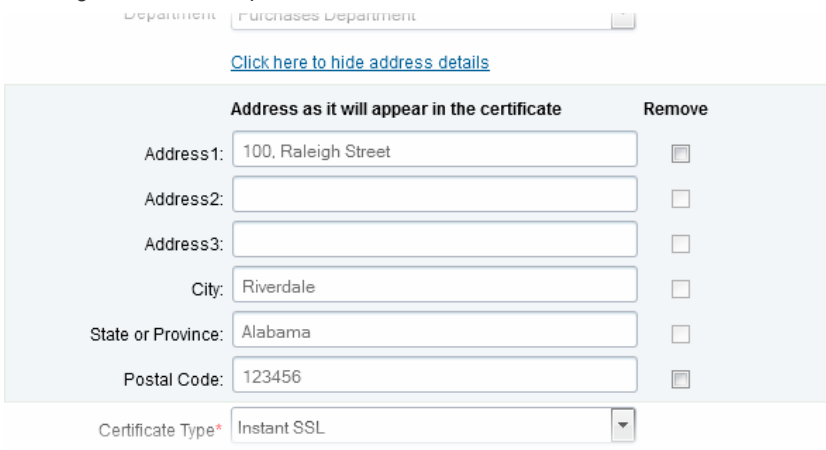
Predefined test SSL license text for test customer[2]...

I agree.* Scroll to bottom of the agreement to activate check box.

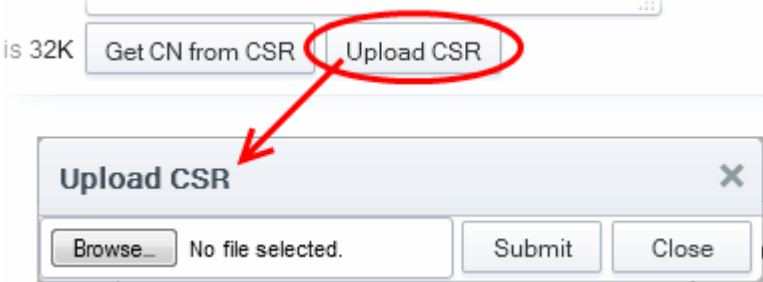
The administrator must read the agreement fully and accept the terms and conditions before submitting the form.

Note: Each type of certificate has a slightly different form.

3.1.2.3.2.3 Form Parameters

| Form Element | Type | Description |
|--------------------------------------|----------------|--|
| Organization (<i>required</i>) | Drop-down list | Administrators should choose the Organization that the SSL certificate will belong to. |
| Department (<i>required</i>) | Drop-down list | Administrators should choose the Department that the SSL certificate will belong to. |
| Click here to edit address details | Text Fields | <p>Clicking this link will expand the address fields.</p>  <p>The address fields are auto-populated from the details in the 'General Properties' tab of the Organization or Department on whose behalf this certificate request is being made.</p> <p>These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>For EV level certificates, it is mandatory to include organization name, address, incorporating or registration agency, certificate requester and contract signer. It is not possible to remove these fields from the Comodo EV or Comodo EV MDC forms.</p> |
| Certificate Type (<i>required</i>) | Drop-down list | <p>Type of the certificate that the applicant wishes to order. See section Comodo SSL Certificates for a list of certificate types.</p> <p>The specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p> |
| Certificate Term (<i>required</i>) | Drop-down list | <p>Administrators should select the term length of the certificate. See section Comodo SSL Certificates for a list of certificate types and term lengths.</p> <p>The term lengths of specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p> |
| Server Software (<i>required</i>) | Drop-down list | The administrator should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from Comodo support portal here: |

| Form Element | Type | Description |
|---|----------------------|---|
| | | https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0 |
| CSR | | |
| Provide CSR/Autogenerate CSR and Manage Private Key | <i>Radio Buttons</i> | <p>If the administrator applies for the certificate after creating the CSR, he/she should choose 'Provide CSR' and enter the CSR in the next field.</p> <p>If the administrator had set up the Private Key Store and wants CCM to create CSR he/she has to choose 'Autogenerate CSR and Manage Private Key'. Refer to the next section Method 3 - Built-in Enrollment Form - Auto CSR Generation for more details.</p> <p>Background: In public key infrastructure systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information. Upon uploading or pasting the CSR, the form will automatically parse the CSR.</p> <p>Administrators that require assistance to generate a CSR should consult the Comodo knowledgebase article for their web server type here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1</p> <p>Special Note regarding MDC applications: The CSR you generate only needs to be for the single 'Common Name' (aka the 'Primary Domain Name'). You should type the additional domains that you require in the 'Subject Alternative Name' field' on this form.</p> |
| CSR (<i>required</i>) | <i>Text Field</i> | <p>The Certificate Signing Request (CSR) is required to be entered into this field in order for Comodo CA to process your application and issue the certificate for the domain.</p> <p>The CSR can be entered in two ways:</p> <ul style="list-style-type: none"> • Pasting the CSR directly into this field • Uploading the CSR saved as a .txt file by clicking the 'Upload CSR' button |
| Get CN from CSR (<i>optional</i>) | <i>Control</i> | <p>Once the CSR has been pasted correctly, clicking this button will auto-populate the Common Name (CN) field. Using this method helps to avoid human error by ensuring the domain name mentioned in the application form exactly match that in the CSR. If the domain name mentioned in this application form do not match that in the CSR, then Comodo CA will not be able to issue the certificate.</p> <p>Special Note regarding MDC applications: In order to successfully order a Multi-Domain Certificate, the applicant need only list the additional domains in the SAN field on this form. In certain circumstances, however, the applicant may have created a CSR that already contains these Subject Alternative</p> |

| Form Element | Type | Description |
|---|------------|--|
| | | Names. In this case, clicking the 'Get CN from CSR' button will also auto-populate the 'Subject Alternative Names' form fields as well as the 'Common Name' field. |
| Upload CSR (<i>optional</i>) | Control | <p>The applicant can upload the CSR saved as a .txt file in the local computer, instead of copying and pasting the CSR into the CSR field - helping to avoid errors.</p>  |
| Certificate Parameters | | |
| Common Name (<i>required</i>) | Text Field | Type the domain that the certificate will be issued to. Single Domain certificates - enter domain name using the form: domain.com. Wildcard Certificates - enter domain name using the form: *.domain.com. Multi-Domain Certificates: enter the primary domain name using the form: domain.com. |
| Subject Alternative Names (<i>required for Multi Domain certificates</i>) | Text Field | If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain should be separated by a comma. |
| Requester (<i>auto-populated</i>) | Text Field | The 'Requester' is field is auto-populated with the name of the administrator making the application. |
| External Requester (<i>optional</i>) | | <p>As an alternative to making an applicant complete the 'Self Enrollment form', the administrator can complete the application themselves using this built-in form and specify an 'External Requester'.</p> <p>Entering the email address of an external requester in this field will mean that person will also receive a certificate collection email.</p> <p>Note: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question.) The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden.</p> |
| Comments (<i>optional</i>) | Text Field | Enables administrator to add comments. |
| Renewal & Installation | | |
| Auto renew | | Leave these fields blank if you plan to manually install the certificate. |
| Create new key pair | | Background Note: CCM supports auto-installation and renewal of SSL certificates. Auto-installation/renewal |
| Auto install renewed | | |

| Form Element | Type | Description |
|--|----------------|--|
| certificate | | is available for the following server types: |
| Auto install initial certificate | | <ul style="list-style-type: none"> • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x (Server 2000 - 2008R2) • Microsoft IIS 5.x and above (Server 2000 - 2008R2) <p>Administrators can configure automatic installation and renewal through the options under 'Automatic & Renewal'.</p> <p>These fields will appear only if you choose:</p> <ul style="list-style-type: none"> • SSL certificate type enabled for auto-installation • Server software type enabled for auto-installation <p>CCM currently supports auto-installation only for 'Instant SSL' from Comodo CA. Other certificate types will be enabled for auto-installation in future versions.</p> <p>For more details on enrollment of SSL Certificates for auto-installation, refer to the section Automatic Installation and Renewal</p> |
| Subscriber Agreement (<i>required</i>) | <i>Control</i> | <p>Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox.</p> <p>Note: The Subscriber Agreement will differ depending on the type of SSL certificate selected from the 'Certificate Type' drop-down. If Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate is selected, The 'I Agree' checkbox will not be shown and the agreement will be taken as accepted, when the user submits the application.</p> |
| OK | <i>Control</i> | Submits the application to Certificate Manager for approval. If the form was completed correctly then the certificate will appear in the 'SSL' area with the state 'Requested'. |
| Cancel | <i>Control</i> | Cancels the application. |

Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

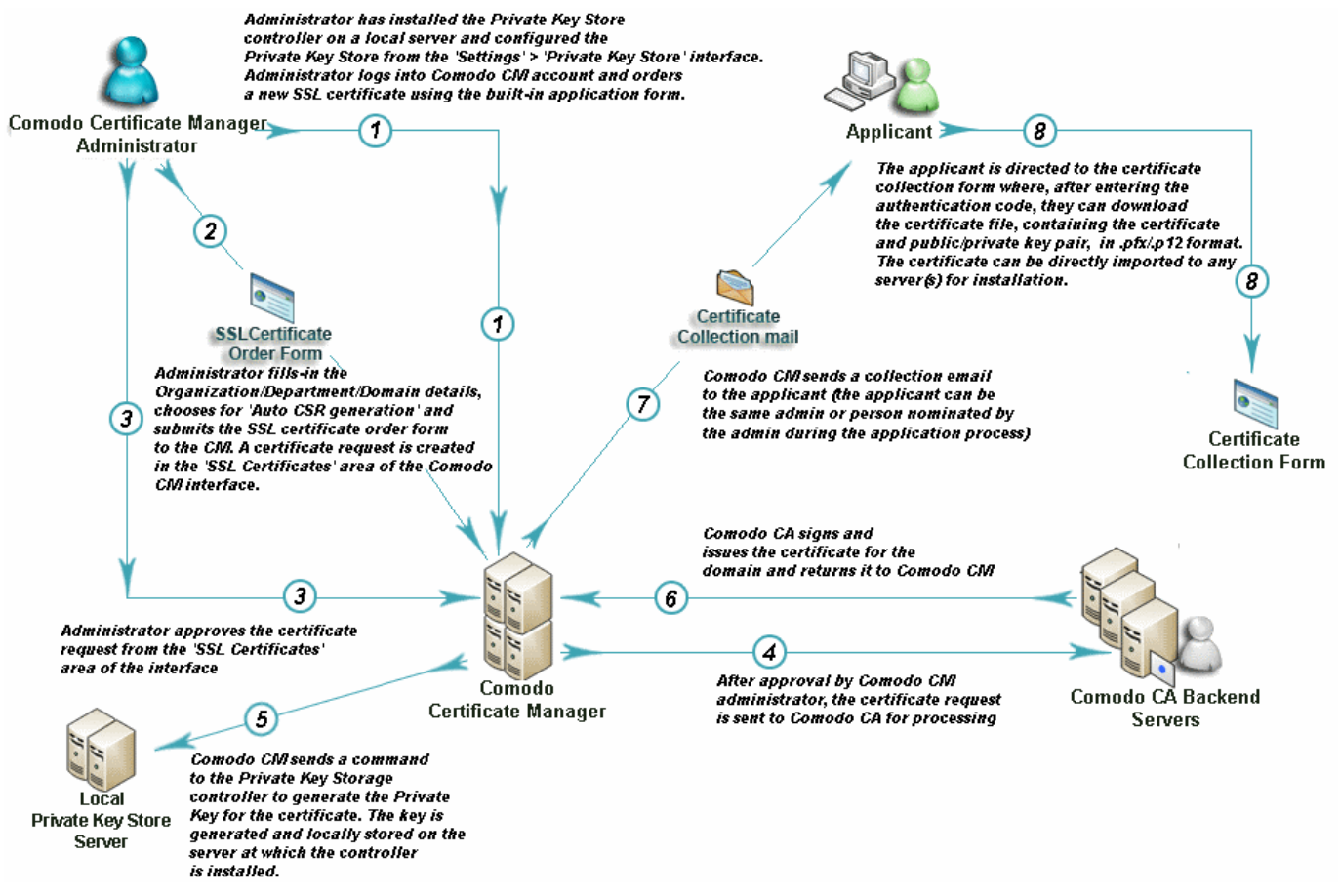
3.1.2.3.3 Method 3 - Built-in Enrollment Form - Auto CSR Generation

As an alternative to manually generating a CSR, CCM can automatically generate a CSR at the point of application. CCM will generate a CSR using the details entered in the Organization/Department, Common name, and server software fields of the application. During the CSR generation process, CCM sends a command to generate the private key for the certificate to the Private Key Store controller. This controller is installed on a local server in the customer network and configured from the 'Settings' > 'Private Key Store' interface. The private key is stored in a database created by the controller on the local server and does not leave your network. It is not uploaded to CCM.

Upon approval and issuance, the certificate can be collected by the administrator or the applicant from the 'Certificate Details' dialog or from the collection form. During collection, CCM retrieves the private key from the Private Key Store through an encrypted channel and integrates with the certificate, enabling the certificate to be downloaded in .pfx or .p12 format. The certificate can be imported and installed on to any server(s).

Prerequisite - The auto-CSR generation feature needs the Private Key Store controller installed on a local server

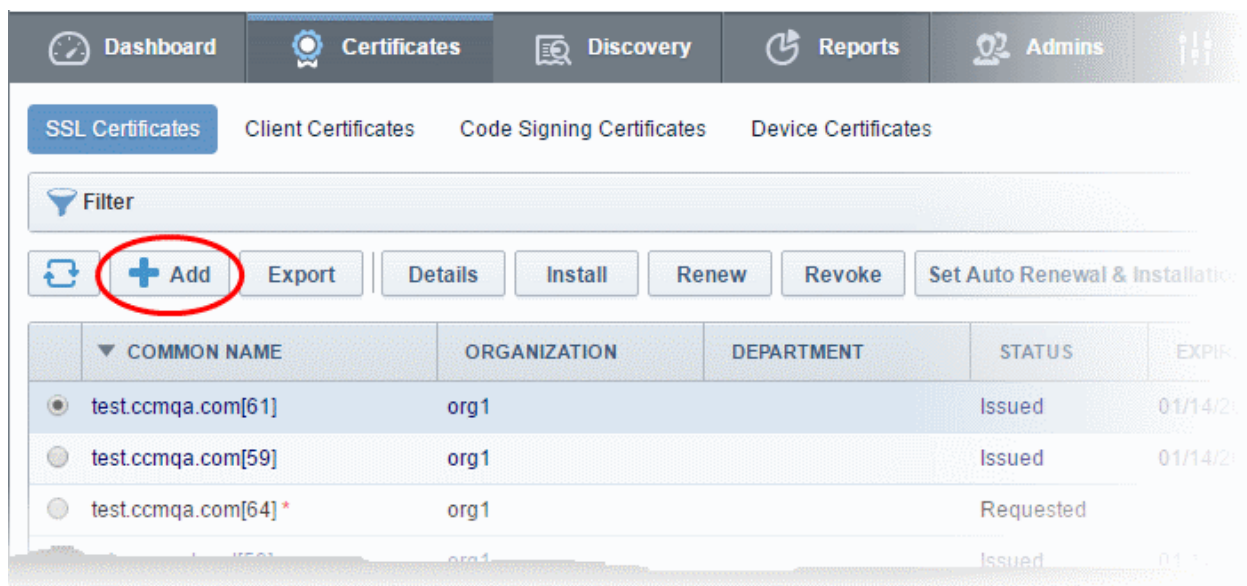
and configured to connect to CCM for receiving command and generate and store the private keys. Refer to the section **Private Key Store** for more details.



3.1.2.3.3.1 The Built-In Application Form

To access the Built-in application form

- Click the 'Certificates' tab and choose 'SSL Certificates'



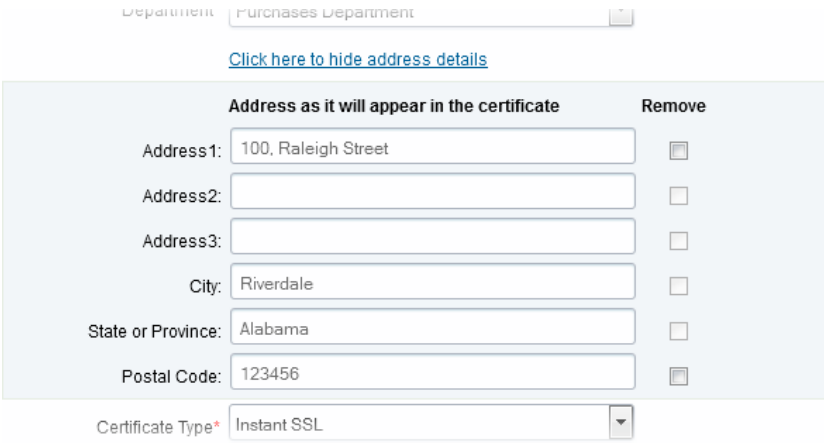
- Click the 'Add' button to open the built-in 'Request New SSL Certificate' form. The next sections of this guide will explain this form in more detail.

Note: Each type of certificate has a slightly different form.

The screenshot shows the 'Request New SSL Certificate' form with several sections and callouts:

- Organization and Department:** Dropdown menus for 'Organization' (Advanced) and 'Department' (ANY). A 'Refresh' button is next to the Organization dropdown. A callout box states: "The address details are auto-populated based on the Organization and Department selected. These details cannot be edited. If required, the administrator can select the address fields to be omitted in the certificate by clicking this link." A link 'Click here to edit address details' is visible below the Department dropdown.
- Certificate Details:** Fields for 'Certificate Type' (Instant SSL), 'Certificate Term' (1 year), and 'Server Software' (Apache/ModSSL).
- CSR Section:** Radio buttons for 'Provide CSR' and 'Autogenerate CSR and Manage Private Key' (selected). Below are 'Signature Algorithm' (RSA) and 'Key Size' (2048) dropdowns. A callout box states: "For CCM to generate the CSR, the administrator should choose 'Autogenerate CSR and Manage Private Key' and specify the signature algorithm and key size."
- Key Passphrase Section:** Radio buttons for 'Manual' (selected) and 'No Passphrase'. A 'Passphrase*' field with a 'Generate' button and a 'Verify*' field are present. A 'Show Passphrase' checkbox is also there. A callout box states: "The Passphrase entered here is required for downloading the certificate by the administrator or the external requester".
- Certificate Parameters Section:** Fields for 'Common Name*', 'Requester' (Admin MRAO), 'External Requester', 'Comments', and 'Telephone*'. A callout box states: "The administrator can specify the email address of the external applicant on behalf of whom the application is made. The external applicant will also receive the certificate collection email."
- Renewal & Installation Section:** Checkboxes for 'Auto renew' (30 days before expiration), 'Create new key pair', 'Auto install renewed certificate', and 'Auto install initial certificate'. A callout box states: "Administrators can choose for automatic installation and renewal of applied certificate. These features are supported only for certain certificate types and server types."
- Subscriber Agreement Section:** A text area containing 'Predefined test SSL license text for test customer[2]...'. A callout box states: "The administrator must read the agreement fully and accept the terms and conditions before submitting the form."
- Footer:** 'Print' button, 'I agree.* Scroll to bottom of the agreement to activate check box' checkbox, and 'OK'/'Cancel' buttons.

3.1.2.3.3.2 Form Parameters

| Form Element | Type | Description |
|--------------------------------------|----------------|---|
| Organization (<i>required</i>) | Drop-down list | Administrators should choose the Organization that the SSL certificate will belong to. |
| Department (<i>required</i>) | Drop-down list | Administrators should choose the Department that the SSL certificate will belong to. |
| Click here to edit address details | Text Fields | <p>Clicking this link will expand the address fields.</p>  <p>The address fields are auto-populated from the details in the 'General Properties' tab of the Organization or Department on whose behalf this certificate request is being made.</p> <p>These fields cannot be modified but, in the case of OV level certificates, the administrator can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>For EV level certificates, it is mandatory to include organization name, address, incorporating or registration agency, certificate requester and contract signer. It is not possible to remove these fields from the Comodo EV or Comodo EV MDC forms.</p> |
| Certificate Type (<i>required</i>) | Drop-down list | <p>Type of the certificate that the applicant wishes to order. See section Comodo SSL Certificates for a list of certificate types.</p> <p>The specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p> |
| Certificate Term (<i>required</i>) | Drop-down list | <p>Administrators should select the term length of the certificate. See section Comodo SSL Certificates for a list of certificate types and term lengths.</p> <p>The term lengths of specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p> |

| Form Element | Type | Description |
|--|-----------------------|--|
| Server Software (<i>required</i>) | <i>Drop-down list</i> | The administrator should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from Comodo support portal here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0 |
| CSR | | |
| Provide CSR/Autogenerate CSR and Manage Private Key | <i>Radio Buttons</i> | For CCM to automatically generate the CSR for the certificate, the administrator should choose 'Autogenerate CSR and Manage Private Key'. |
| Signature Algorithm | <i>Drop-down</i> | The administrator should choose the signature algorithm to be used by the certificate. |
| Key Size | <i>Drop-down</i> | The administrator should choose the key size for the certificate. |
| Key Passphrase | | |
| Key Phrase Manual/No Passphrase | <i>Radio buttons</i> | Allows the administrator to provide passphrase protection for downloading the certificate. The passphrase can be manually entered or auto generated. <ul style="list-style-type: none"> Choose 'Manual' to provide pass-phrase protection Choose No Pass-phrase, to allow the certificate to be downloaded without entering the pass-phrase |
| Pass-Phrase | <i>Text Field</i> | Enter the pass-phrase if Manual is chosen. For CCM to automatically generate the passphrase, click 'Generate'. You need to store the passphrase in a safe location, as it is needed to download the certificate. To view the passphrase, select 'Show Passphrase' checkbox. |
| Verify | <i>Text Field</i> | Reenter the passphrase for confirmation, if chosen to be manually specified. |
| Certificate Parameters | | |
| Common Name (<i>required</i>) | <i>Text Field</i> | Type the domain that the certificate will be issued to. Single Domain certificates - enter domain name using the form: domain.com. Wildcard Certificates - enter domain name using the form: *.domain.com. Multi-Domain Certificates: enter the primary domain name using the form: domain.com. |
| Subject Alternative Names (<i>required for Multi Domain certificates</i>) | <i>Text Field</i> | If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain should be separated by a comma. |
| Requester (<i>auto-populated</i>) | <i>Text Field</i> | The 'Requester' is field is auto-populated with the name of the administrator making the application. |

| Form Element | Type | Description |
|---|-------------------|--|
| External Requester (<i>optional</i>) | | <p>As an alternative to making an applicant complete the 'Self Enrollment form', the administrator can complete the application themselves using this built-in form and specify an 'External Requester'.</p> <p>Entering the email address of an external requester in this field will mean that person will also receive a certificate collection email.</p> <p>Note: The 'Requester' will still be the administrator that is completing this form (to view this, open the 'Certificates Management' area and click 'View' next to the certificate in question.) The email address of the 'External Requester' will be displayed as the 'External Requester' in the 'View' dialog of an issued certificate. This field is not required when requesting for EV SSL certificate and hence will be hidden.</p> |
| Comments (<i>optional</i>) | <i>Text Field</i> | Enables administrator to add comments. |
| Renewal & Installation | | |
| Auto renew | | Leave these fields blank if you plan to manually install the certificate. |
| Create new key pair | | <p>Background Note:</p> <p>CCM supports auto-installation and renewal of SSL certificates. Auto-installation/renewal is available for the following server types:</p> <ul style="list-style-type: none"> • Apache/Mod SSL • Apache - SSL • Apache Tomcat • Microsoft IIS 1.x to 4.x (Server 2000 - 2008R2) • Microsoft IIS 5.x and above (Server 2000 - 2008R2) <p>Administrators can configure automatic installation and renewal through the options under 'Automatic & Renewal'.</p> <p>These fields will appear only if you choose:</p> <ul style="list-style-type: none"> • An SSL certificate type enabled for auto-installation • Server software type enabled for auto-installation <p>CCM currently supports auto-installation only for 'Instant SSL' from Comodo CA. Other certificate types will be enabled for auto-installation in future versions.</p> <p>For more details on enrollment of SSL Certificates for auto-installation, refer to the section Automatic Installation and Renewal</p> |
| Auto install renewed certificate | | |
| Auto install initial certificate | | |
| Subscriber Agreement (<i>required</i>) | <i>Control</i> | |
| OK | <i>Control</i> | Submits the application to Certificate Manager for approval. If the form was completed correctly then the certificate will appear in the 'SSL' area with the state 'Requested'. |
| Cancel | <i>Control</i> | Cancels the application. |

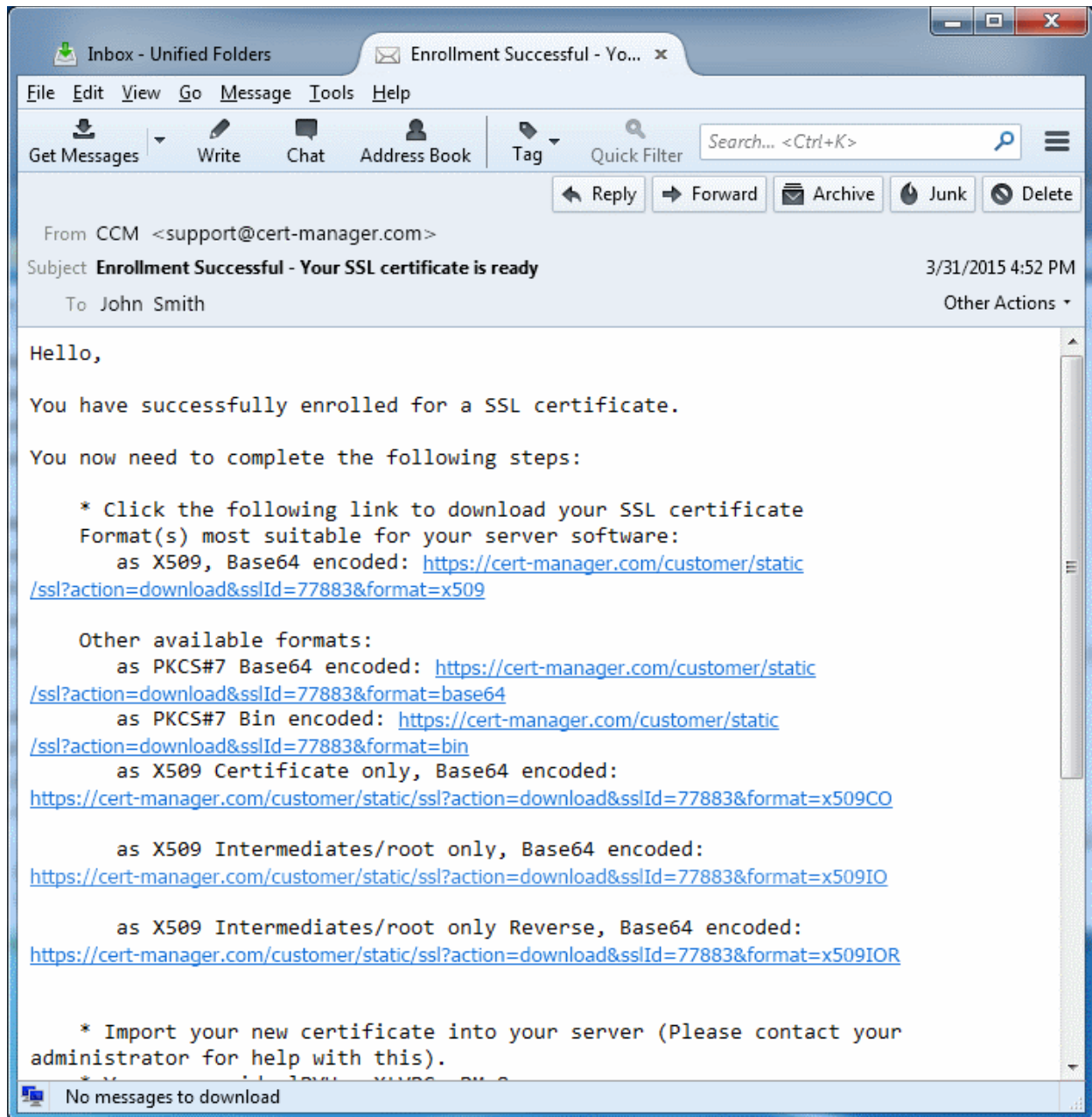
Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

3.1.2.3.4 Certificate Collection

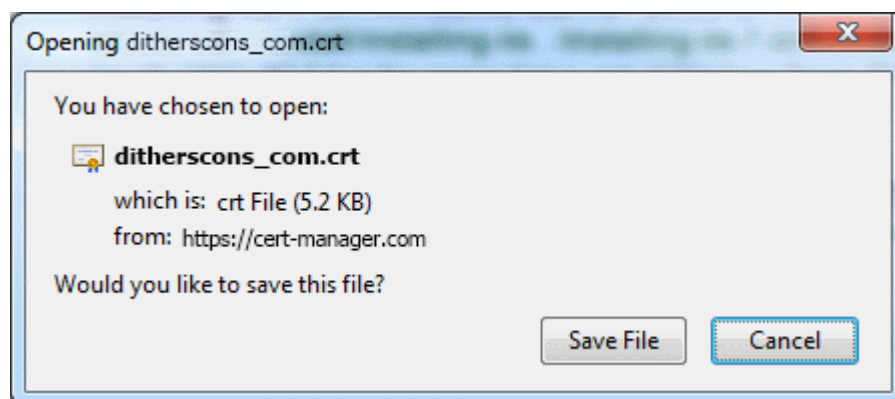
After Comodo CA has issued the certificate applied through the Built-in application form or the Self-enrollment form, the next stage of the provisioning process is for the applicant to download their certificate. Once the certificate has been issued, Comodo Certificate Manager will automatically send a collection email to the applicant. The certificate can be downloaded by the applicant by clicking the link in the email. Also, the issued SSL certificate can be downloaded by an MRAO, RAO SSL or DRAO SSL administrator from the **SSL Certificate Details dialog** accessed from the 'Certificates Management' > 'SSL certificates' tab.

3.1.2.3.4.1 Collection of SSL Certificate Through Email

1. Once the certificate has been issued, Comodo Certificate Manager will automatically send a collection email to the applicant. This can be either an external applicant using the self enrollment method or a CCM administrator using the built-in application form.) The email will contain a summary of the certificate details, a link to the certificate collection form and a unique certificate ID that will be used for validation.



- Having clicked the link in the collection email, the end-user will be able to download the certificate file.



3.1.2.3.4.2 Collection of SSL certificate by Administrator

The issued certificate can also be downloaded and provided to the applicant from the **SSL Certificate Details dialog**. Click the 'Details' button at the top after selecting the issued certificate from the SSL Certificates tab of the

Certificate management interface.

The screenshot displays the Comodo Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Reports, and Admins. Below these, there are sub-tabs for SSL Certificates, Client Certificates, Code Signing Certificates, and Device Certificates. A 'Filter' section is present, followed by action buttons: Add, Export, Details (circled in red), Install, Renew, Revoke, and Set Auto Renewal & Install. Below the buttons is a table of certificates with columns: COMMON NAME, ORGANIZATION, DEPARTMENT, STATUS, and EXPIRES. Two certificates are listed, both for 'test.ccmqa.com' with status 'Issued'. The first certificate has a radio button selected (circled in red). A red arrow points from this radio button to the 'Details' view below. The 'Details' view for 'SSL Certificate: test.ccmqa.com' shows fields for Common Name, State, Order Number (1675873), Vendor (Comodo CA Limited), Discovery Status (Not deployed), Self-Enrollment Certificate ID (61), and Type (Instant SSL). The 'Download The Certificate' button is highlighted, and a dropdown menu is open, showing options: PKCS#7 Base64, PKCS#7 Binary, X509 Base64, X509 Certificate only, X.509 Intermediate(s)/Root, and X.509 Root/Intermediate(s). A 'Select' button is at the bottom of the dropdown, with a mouse cursor over it.

The resulting dialog contains options to download the issued certificate in several formats at its top:

- Click the 'Select' button
- Click the appropriate button to download the certificate in desired format.

If the private key of the certificate is managed by CCM at the Private Key Store configured at the local network, the administrator then have the option to download certificates in .pfx/.p12 format containing the public/private key pair so, for example, it may be exported to another web server.

Only the administrators that are authenticated by their client certificate at the computer from which they are accessing the CCM, can download the certificate in .p12 format.

3.1.2.3.5 Downloading and Importing SSL Certificates

Once the application process has been successfully completed, the applicant needs to download the certificate,

save it to a secure place on their hard drive and import it into the certificate store of their computer.

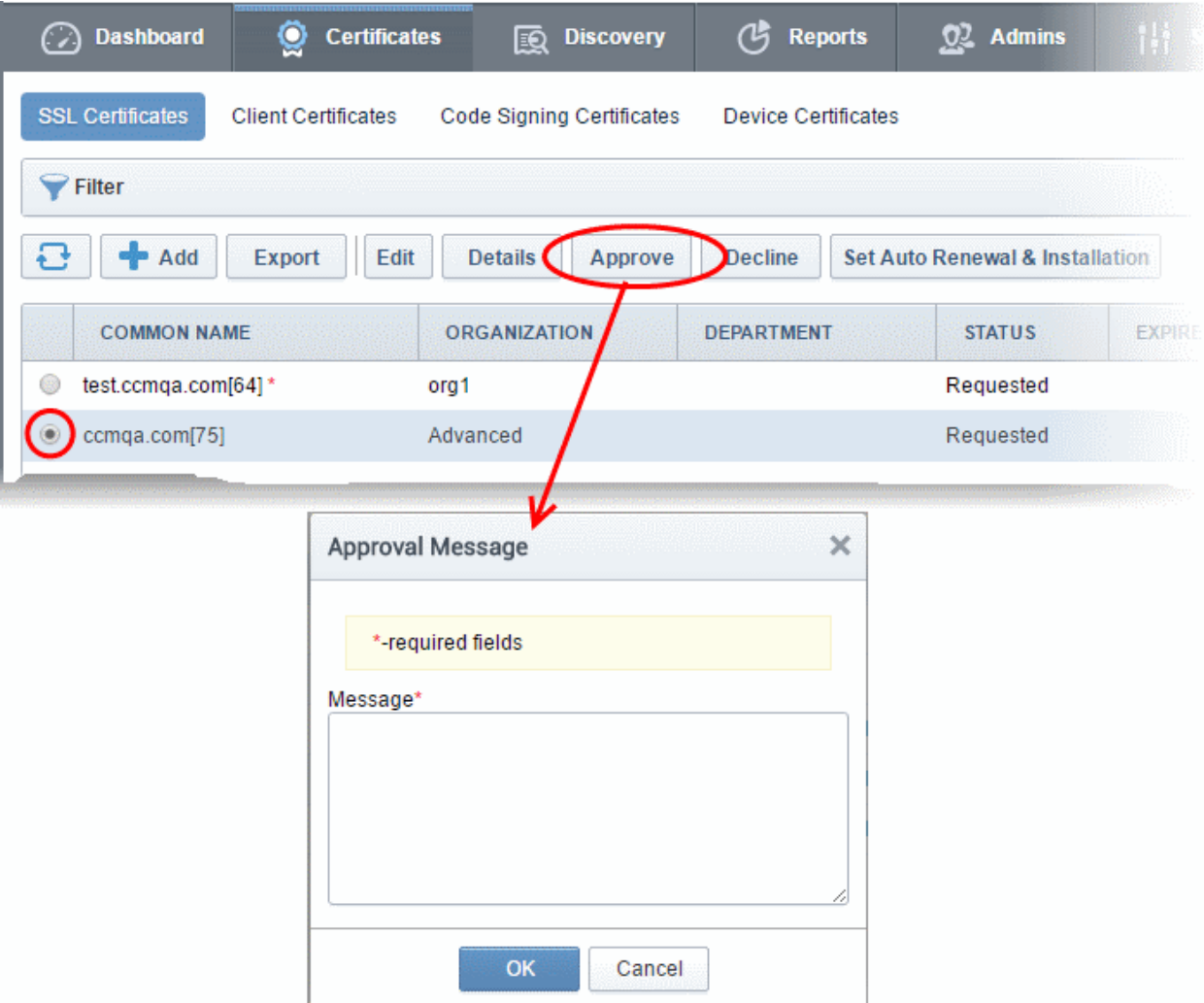
The precise installation process depends on the web server type and a range of installation guides are available at the Comodo support website at:

https://support.Comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav

First select the Comodo certificate type and then choose the appropriate web server software to view a detailed guide explaining the import process.

3.1.2.4 Certificate Requests - Approving, Declining, Viewing and Editing

A certificate request will appear in the 'SSL Certificates' area after the applicant has successfully applied for a certificate using either the **Auto Installer**, the **Self Enrollment Form** or the **Built-in application form**. Use the filter option to view all the certificates that are in 'Requested' state. Select the certificate that you want to approve, decline, view or edit.



The screenshot shows the 'SSL Certificates' section of the Comodo Certificate Manager. The 'Approve' button is circled in red. Below it, an 'Approval Message' dialog box is open, featuring a text area for a message and 'OK' and 'Cancel' buttons.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRE |
|----------------------|--------------|------------|-----------|--------|
| test.ccmqa.com[64] * | org1 | | Requested | |
| ccmqa.com[75] | Advanced | | Requested | |

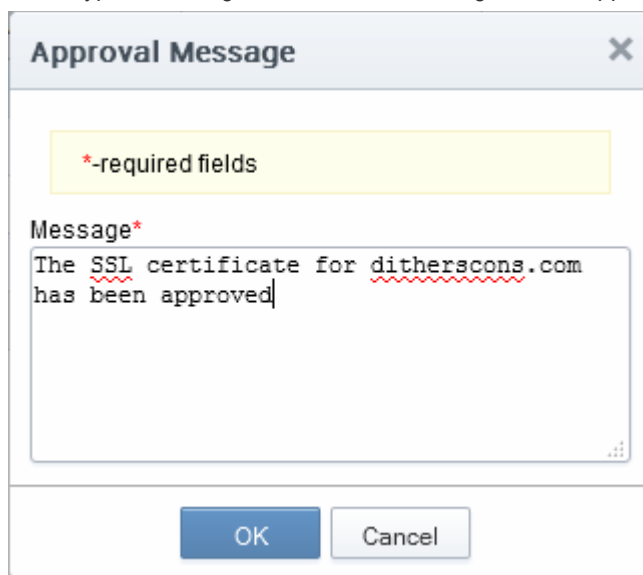
- At this point, the certificate request has NOT been submitted to Comodo CA and is pending approval from a Certificate Manager administrator. (If the application was made by an administrator, that administrator can, of course, approve their own request.)

If the administrator does not want to submit this request, they should click the 'Decline' button.

Note: Declining a certificate request will change the certificate status to 'Declined'. If an 'SSL Declined' Notification has been set up then an email will be automatically sent to the requester informing them that the request has been declined.

However, this request can still be 'Approved' at any time in the future by a 'MRAO', 'RAO SSL' or 'DRAO SSL' administrator with appropriate privileges.

- If the administrator wishes to view the details of the request, they should click the 'Details' button at the top after selecting the checkbox next to the certificate name.
- If the administrator wishes to modify the request they should click the 'Edit' button. (for example, administrators may wish to correct certain request fields in the application before submitting to Comodo CA for processing).
- To approve the request and submit the application to Comodo CA for processing, administrators should click the 'Approve' button at the top.
 - After clicking the 'Approve' button, an 'Approval Message' box will be displayed. This allows the Administrator to type a message that will be sent along with the approval notification email.



- Click 'OK' to add the message and send the approval email.

Note: The **SSL Approved Notification** should have been set up for the requester to receive the email notification.

- Once the Administrator has approved the request and submitted it to Comodo CA, the certificate state will be displayed as 'Approved'. If the request has applied by Comodo CA, the state of the certificate is changed to the proper value - 'Applied' (It also can be rejected by CA). Next, if validation is successful, then Comodo will send a **Certificate Collection** email to the certificate requester and the 'State' of the certificate will change to one of 'Issued'.

Please see the '**SSL Certificates**' chapter for full details of the options available in this area.

3.1.2.5 Certificate Renewal

SSL certificates can be renewed manually or automatically:

Manual

There are two broad ways to manually renew certificates via CCM:

- SSL administrators can renew certificates from the SSL certificates interface. Jump to **Certificate Renewal by Administrators** for more details.
- External applicants can renew using the self-renewal form. Jump to **Certificate Renewal by the End-User** for more details.

Automatic

Administrators can configure automatic renewal of SSL certificates. Jump to [Scheduling Automatic Renewal and Installation](#) for more details.

3.1.2.5.1 Certificate Renewal by Administrators

The SSL Certificates interface allows administrators to renew both managed certificates and unmanaged certificates. As the name suggests, unmanaged certificates are those are listed in CCM but which are not currently managed by CCM. These are usually certificates identified during discovery scans but not originally ordered using CCM. The processes for renewing managed and unmanaged certificates are different.

| Managed Certificates | Unmanaged Certificates |
|---|--|
| <p>A 'managed certificate' is a certificate which has been issued, via CCM, to a specific combination of domain and Organization.</p> <p>You will need to submit a CSR the first time you apply for a certificate for any such combination. After issuance, this certificate will become 'managed'.</p> <p>'Managed' certificates are those with CCM statuses of 'Issued', 'Applied' or 'Requested'</p> <p>For renewals of 'managed' certificates, you will typically not need to submit a CSR because CCM shall re-use the existing CSR.</p> | <p>An 'unmanaged certificate' is a certificate which was found installed on servers during a discovery scan but was not issued via CCM.</p> <p>You will need to submit a new CSR during renewal of an 'Unmanaged' certificate because CCM does not have one on record. After issuance, this certificate will become 'managed'.</p> |

General note: If you moved a domain from one Organization to another or modified the address details of an Organization, then you are effectively creating a new certificate application, not 'renewing' a certificate. In these circumstances, you will also have to submit a new CSR.

Renewing a 'Managed' Certificate

If the administrator wishes to renew a managed certificate, they should select the radio button beside it and click the 'Renew' button at the top.

The screenshot shows the 'SSL Certificates' section of the Comodo Certificate Manager. At the top, there are tabs for 'SSL Certificates', 'Client Certificates', and 'Code Signing Certificates'. Below the tabs, there is a filter section with a dropdown menu set to 'Issued'. Below the filter, there are buttons for 'Apply' and 'Clear'. Below that, there are buttons for 'Add', 'Export', 'Add For Auto Install', 'Details', 'Renew', 'Revoke', and 'Replace'. The 'Renew' button is circled in red. Below the buttons is a table with columns: COMMON NAME, ORGANIZATION, DEPARTMENT, STATUS, EXPIRES, and SERVER SOFTWARE. The table contains three rows of certificates. The second row, for 'ditherspayments.com', is selected, and a red arrow points from the 'Renew' button to this row.

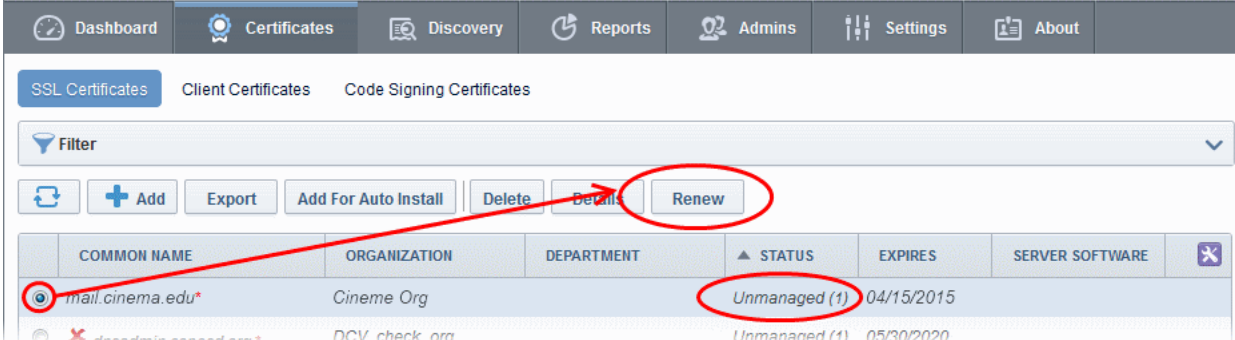
| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | SERVER SOFTWARE |
|---------------------|------------------------------|----------------------|--------|------------|-----------------|
| ditherscons.com | 123 | | Issued | 03/20/2016 | Active |
| ditherspayments.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | |
| ccmda.com | Dithers Construction | Purchases Department | Issued | 03/31/2016 | |

- On clicking 'Renew', CCM will automatically request a renewal with the same details as the existing certificate.
- Once issued, the renewed certificate will become available for collection and installation. Refer to the

section [Certificate Collection](#) for more details.

Renewing an 'Unmanaged' Certificate

If the administrator wishes to renew an unmanaged certificate, they should select the radio button beside it and click the 'Renew' button at the top.



The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Renew' button is circled in red. A red arrow points from the 'Renew' button to the 'Unmanaged (1)' status of a certificate in the table below. The certificate has a common name of 'mail.cinema.edu*' and expires on 04/15/2015.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | SERVER SOFTWARE |
|------------------|--------------|------------|---------------|------------|-----------------|
| mail.cinema.edu* | Cineme Org | | Unmanaged (1) | 04/15/2015 | |
| ... | ... | ... | ... | ... | ... |

- Clicking the 'Renew' button will open the 'Renew SSL Certificate' form. This form is similar to the **Built-in Enrollment form** with the company and domain details pre-populated from the existing certificate. If needed, administrators can select a new certificate type and edit its details.

*-required fields

Organization*

Department*

Certificate Type*

Certificate Term*

Server Software*

CSR*

Max CSR size is 32K

Common Name*

Subject Alternative Names
(optional, comma separated)

Requester

External Requester

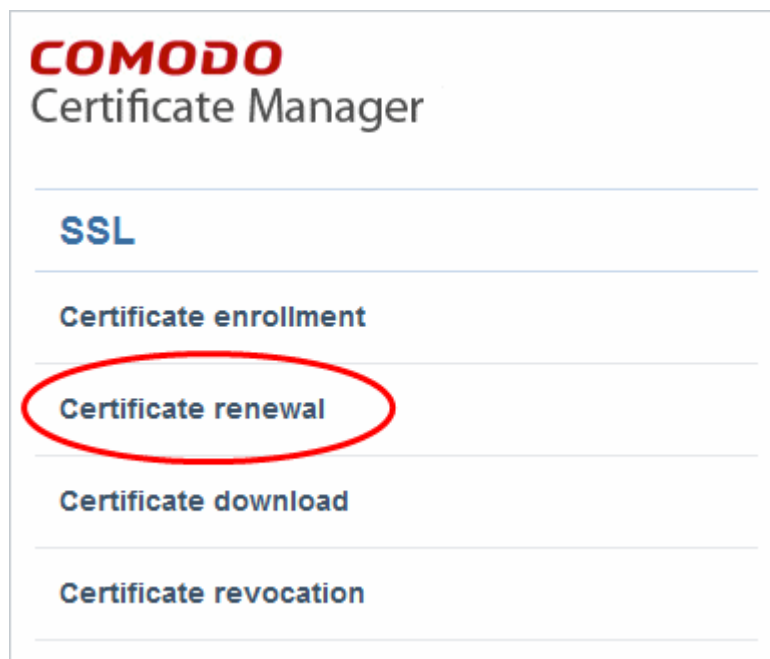
Comments

- Administrators should next paste or upload a new CSR, accept the Certificate Subscriber Agreement and click the OK button.
- CCM will place a request for the new certificate
- Once issued, the renewed certificate can be collected and installed. Refer to the section **Certificate Collection** for more details. After installation, the status of the certificate changes to 'Managed'.

3.1.2.5.2 Certificate Renewal by the End-User

End-users can renew their certificates through the self renewal application form.

- The self renewal form is hosted by default at [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/ssl](https://cert-manager.com/customer/[REAL CUSTOMER URI]/ssl).



- Clicking the Certificate renewal link will open the self renewal form

The image shows a screenshot of the 'SSL Renew' form in the Comodo Certificate Manager. The form has a white background with a blue header 'COMODO Certificate Manager' and a sub-header 'SSL Renew'. Below the sub-header, there are two input fields. The first field is labeled 'Your Certificate ID: *' and contains the value '77881'. The second field is labeled 'Pass-phrase: *' and contains a series of black dots. At the bottom of the form, there is a blue button labeled 'RENEW'.

- Before proceeding to the full renewal application form, the user has to authenticate the request by:
 - Entering the correct certificate ID. The certificate ID is available from the certificate collection email and in the 'Certificates' > 'SSL' interface. Administrators may need to communicate the certificate ID to external applicants.
 - Entering the certificates renewal/revocation passphrase. This phrase was created during enrollment for the original certificate..
- Clicking 'Renew' will automatically renew the certificate with the same details as in the existing certificate.
- Once issued, the renewal certificate can be collected and installed. Refer to the section **Certificate Collection** for more details.

3.1.2.5.3 Scheduling Automatic Renewal and Installation

To configure auto-renewal (and optionally auto-installation):

- Go to 'Certificates' > 'SSL Certificates' > select a certificate > Click the 'Set Auto-renewal and Installation' button.
- This dialog allows administrators to enable auto-renewal and to specify the number of days in advance of expiry that the renewal process should begin.
- Selecting 'Auto-installation' will start a configuration wizard. Auto-installation is possible only for managed

certificates and requires the installation of controller software. A full run-down of how to set up auto-installation can be found at [Automatic Installation and Renewal](#).

To configure auto-renewal of an SSL Certificate

- Click the 'Certificates' tab and choose 'SSL Certificates'
- Select the certificate you want to auto-renew and click the 'Set Auto-Renewal & Installation' button:

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. Under 'SSL Certificates', a table lists two certificates: 'c2.local[53]' and 'c3.local[55]'. The 'c2.local[53]' certificate is selected. A red circle highlights the 'Set Auto Renewal & Installation' button in the top toolbar. A red arrow points from this button to a dialog box titled 'Set Auto Renewal & Installation 'c2.local''. The dialog box contains the following options:

- Auto renew days before expiration
- Create new key pair
- Auto install renewed certificate
- Auto install selected certificate

At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

Set Auto Renewal & Installation - Table of Parameters

| | |
|----------------------------------|--|
| Auto Renew | Enable to auto-renew the certificate when it is nearing expiry. You can also choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, the certificate controller will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA. |
| Create new key pair | Select if you want a new key pair to be generated for the renewal certificate. Leaving it unselected means CCM will re-use the existing key pair of the expiring certificate. |
| Auto install renewed certificate | <p>Select if you want to automatically install the renewed certificate on its web server. After selecting this option and clicking 'OK', the 'Set Auto Renewal & Installation' wizard will begin. The wizard is similar to scheduling auto-installation for a new certificate. For guidance on the wizard, refer to the explanation in Method 1 - Enterprise Controller Mode.</p> <p>After you have completed the wizard, the 'Renewal State' of the certificate will change from 'Not scheduled' to 'Scheduled'.</p> <ul style="list-style-type: none"> • If you set an installation schedule in the wizard, the certificate will be auto-installed on the specified date. • If you instead chose 'Manual' in the schedule step of the wizard, you can select the certificate and click the 'Install' button to initiate auto-installation. Refer to 'Manually initiate auto-installation of a certificate' for more details. |

| | |
|-----------------------------------|---|
| Auto install selected certificate | Select this option if you want the currently selected certificate to be auto-installed on its web server. On selecting this option and clicking OK , the 'Set Auto Renewal & Installation' wizard will begin. For guidance on this, refer to the explanation of the wizard |
|-----------------------------------|---|

3.1.2.6 Certificate Revocation, Replacement and Deletion

In the 'SSL Certificates' sub-tab of 'Certificates' interface explained [above](#), the administrator has also the option to revoke, renew, replace or delete a certificate.

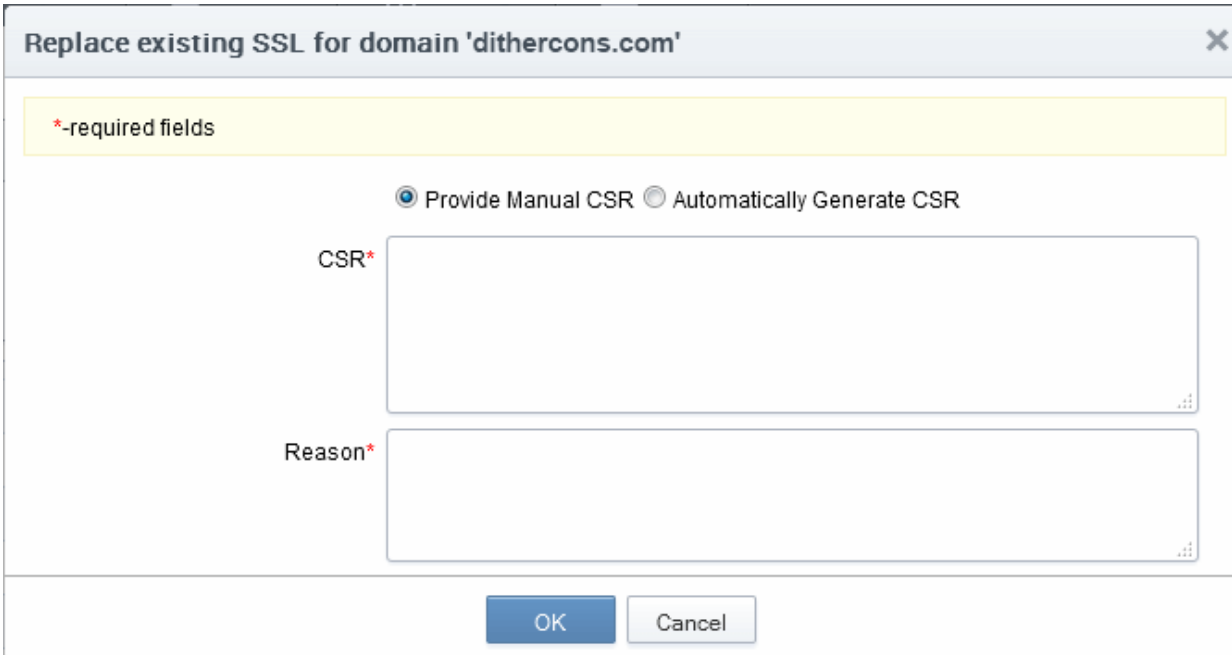
- If the Administrator wishes to revoke a certificate, they should first select the certificate and click the 'Revoke' button at the top.
 - After clicking the 'Revoke' button, a 'Revoke reason' message box will be displayed. This allows the administrator to type a message that will be sent along with the revoke notification email.



- Click 'OK' to add the message and send the revoke email.

Note: The [SSL Revoked Notification](#) should have been set up for the requester to receive the email notification.

- If the administrator wishes to replace an existing certificate, they should select the checkbox beside it and click the 'Replace' button at the top. Clicking the 'Replace' button will open the 'Replace existing SSL' dialog which requires a new CSR and reason for replacing the certificate.



Replace existing SSL for domain 'dithercons.com'

*-required fields

Provide Manual CSR Automatically Generate CSR

CSR*

Reason*

OK Cancel

The administrator can choose to:

- Manually upload a new CSR for the new certificate. Refer to the section [Method 2 - Built-in Enrollment Form - Manual CSR Generation](#) for more details
- Instruct CCM to generate a CSR and manage the private key associated with the new certificate at the Private Key Store configured at the local network. Refer to the section [Method 3 - Built-in Enrollment Form - Auto CSR Generation](#) for more details
- If the administrator wishes to delete a certificate, they should select the checkbox beside it and click the 'Delete' button at the top.

Please see the '[SSL Certificates](#)' chapter for full details of the options available in this area.

3.2 The Client Certificates Area

3.2.1 Overview

The 'Client Certificates' area allows administrators to manage end-users client certificates and their owners' details.

Visibility of the 'Client Certificates' area is restricted to:

- MRAO administrators - can view the client certificates and end-users of any Organization or Department.
- RAO S/MIME administrators - can view the client certificates and end-users of Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO S/MIME administrators- can view the client certificates and end-users of Departments that have delegated to them.

| NAME | EMAIL | ORGANIZATION | DEPARTMENT |
|------------|---------------------------|------------------------------|----------------------|
| Alice | alice@abcdcomp.com | ABCD Company | |
| Bob Smith | bob@bestorg.com | Best Organization | |
| Dave | dave@abcdcomp.com | ABCD Company | |
| John Smith | johnsmith@coradithers.com | Dithers Construction Company | Purchases Department |
| Thomas | thomass@elegantamp.com | Elegant | |

| 'Client Certificates' table | | |
|-----------------------------|-----------------|---|
| Column Name | | Description |
| Name | | End-user's name. |
| Email | | End-user's email address. |
| Organization | | Name of the Organization that the end -user belongs to. |
| Department | | Name of the Department that the end-user belongs to (if applicable) |
| Control Buttons | Add | Allows the administrator to add a new end-user and configure a client certificate for that user |
| | Export | Export the currently displayed list to a spreadsheet in .csv format |
| | Import from CSV | Enables the administrator to import list of new end-users in .csv format into the Certificate Manager database. |
| | Refresh | Updates the currently displayed list of users. Will remove any users that have been recently deleted and add any that have been recently created. Will update details such as Organization, email etc if those details have recently changed. |
| Certificate Control Buttons | Edit | Enables the administrator to edit the end-user's details. |
| | Delete | Enables the administrator to delete the end-user. |
| | Certs | Enables the administrator to view/manage the end-user's Client certificates. |

Note: The types of certificate control buttons that are displayed in the table header depends on the state of the

| 'Client Certificates' table | | |
|-----------------------------|--|-------------|
| Column Name | | Description |
| selected certificate | | |

3.2.1.1 Sorting and Filtering Options

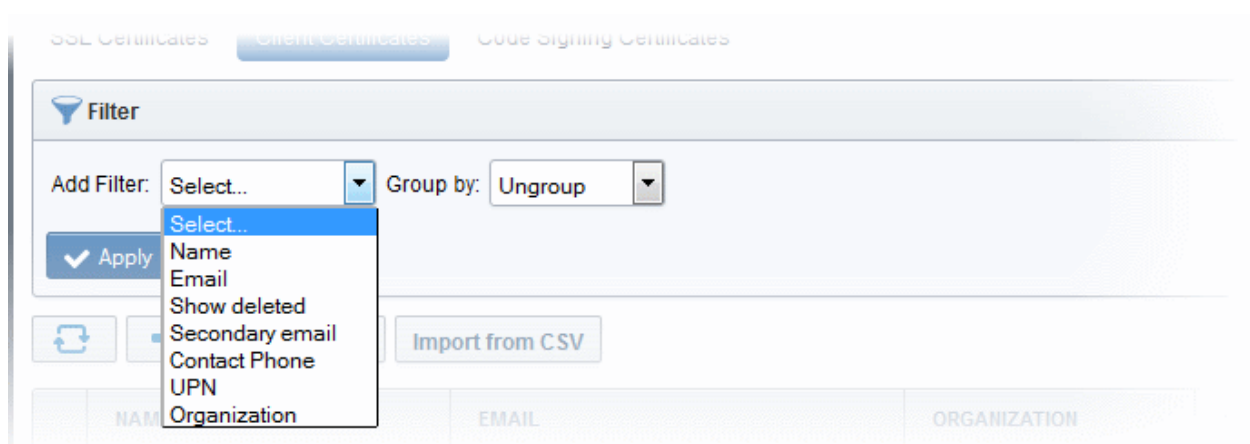
- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular client certificates by using filters.



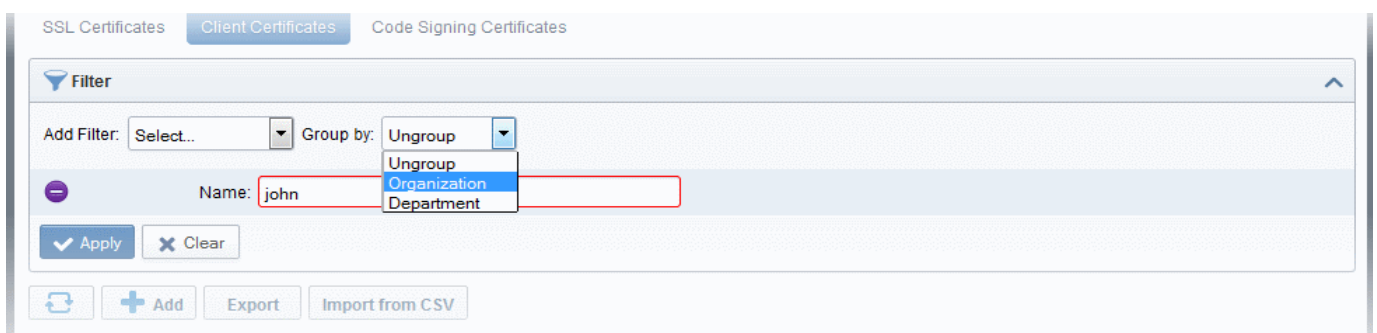
To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.

For example, if you want to filter the certificates with 'Name' and group with 'Organization', select 'Name' from the 'Add Filter' drop-down:



Tip: You can add more than one filter at a time to narrow down the filtering. To remove a filter criteria, click the '-' button to the left if it.

- Enter part or full name in the Name field.
- Select 'Organization' from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:

The screenshot shows the 'Client Certificates' interface. At the top, there is a navigation bar with tabs for Dashboard, Certificates, Discovery, Reports, Admins, Settings, and About. Below this, there are sub-tabs for SSL Certificates, Client Certificates (selected), and Code Signing Certificates. A filter section is visible with the text 'Filter is applied'. It includes an 'Add Filter' dropdown set to 'Select...', a 'Group by' dropdown set to 'Organization', and a search input field containing 'john'. Below the search field are 'Apply' and 'Clear' buttons. Underneath the filter section are buttons for 'Refresh', '+ Add', 'Export', and 'Import from CSV'. The main content area is a table with columns for NAME, EMAIL, ORGANIZATION, and DEPARTMENT. The table shows two entries under the 'org1' organization, both for 'John Smith' with email 'johnsmith@abcdcomp.com'. The second entry is further categorized under 'Dithers Construction Company' with a 'Purchases Department'.

| | NAME | EMAIL | ORGANIZATION | DEPARTMENT |
|----------------------------------|------------|---------------------------|------------------------------|----------------------|
| [-] org1 | | | | |
| <input type="radio"/> | John Smith | johnsmith@abcdcomp.com | org1 | |
| [-] Dithers Construction Company | | | | |
| <input type="radio"/> | John Smith | johnsmith@coradithers.com | Dithers Construction Company | Purchases Department |

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Client Certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

3.2.1.2 'Certs' Dialog

Clicking the 'Certs' button at the top after selecting the check box next to a end-user's name will list all the client certificates belonging to that end-user. Certificates are listed in chronological order (newest first). If a certificate has been revoked, then the date of revocation is displayed in the 'Revoked' column.

This interface allows the administrator to revoke, download, view and send invitation for that certificate. (See below).

Certificates for: johnsmith@coradithers.com

Filter

Send Invitation Invitation not sent View Revoke

| | ORDERED | REVOKED | EXPIRES | CERTIFICATE TYPE | ORDER NUMBER | SERIAL NUMBER | |
|--|------------------|------------------|------------|-----------------------------|--------------|------------------|-------|
| | 03/19/2015 10:36 | 03/30/2015 11:11 | 03/19/2016 | High Persona Validated Cert | 1305101 | 38:D4:BE:81:BE:1 | Revok |
| | 03/25/2015 16:01 | 03/30/2015 11:11 | 03/25/2016 | High Persona Validated Cert | 1308491 | 66:A2:E4:63:34:C | Revok |
| | 03/30/2015 11:46 | | 03/30/2016 | High Persona Validated Cert | 1311952 | 1A:74:23:8A:54:8 | Down |
| | 03/30/2015 13:28 | | 03/30/2016 | High Persona Validated Cert | 1312005 | 76:DB:5D:33:CB:1 | Down |

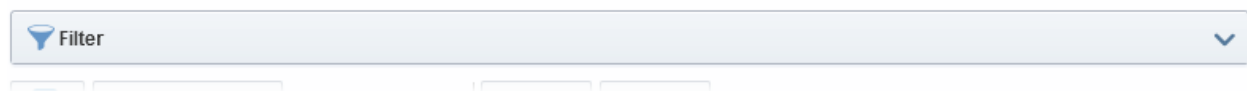
15 rows/page 1 - 4 out of 4

Close

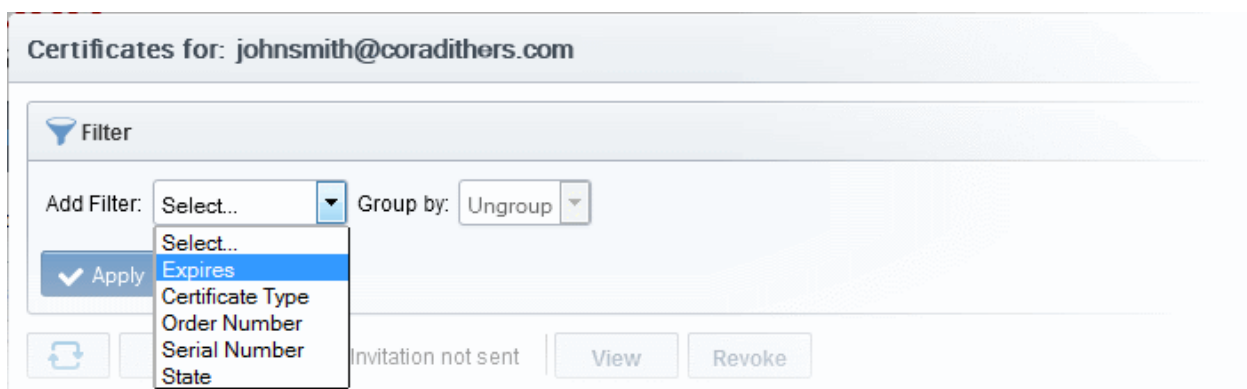
Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for a particular certificate by using filters.



To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down.



The options available are:

- Expires - Allows you to filter certificates that are expiring in next 3, 7, 14, 30, 60 and 90 days
- Certificate Type - Allows you to filter certificates based on their validation type
- Order Number - Allows you to search for a certificate with a specific order number
- Serial Number - Allows you to search for a certificate with a specific serial number
- State - Allows you to filter certificates based on their states
- Choose the filter and enter the parameters.

- Click the 'Apply' button. The results will displayed based on the filters selected / entered.
- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

| Client Certificate 'Cert' Dialog - Table of Parameters | | |
|--|--------|--|
| Controls | Type | Description |
| View | Button | Allows administrators to view an end-user's certificate. See Viewing End-User's certificate for more details. |
| Revoke | Button | Allows administrators to revoke an end-user's certificate. Once revoked, the date and time of revocation is displayed in this column. |
| Download | Button | Allows administrators to download a copy of the end-user's certificate. * |
| Send Invitation | Button | Enables the administrator to send an email to the end-user with instructions on how to apply for/collect their client certificate. See 'Request and issuance of 'Client Certificates to Employees and End-Users' for an explanation of the process from this point. |
| Refresh | Button | Reloads the list. |

*Comodo Certificate Manager creates a copy of each end-user's certificate which it saves on the server. This duplicate certificate is protected in two ways:

The key pair of each end-user's certificate is encrypted by a master public key. See the **'Encryption and Key Escrow'** section for more details;

- Password protected with an administrator set password. The end-user will be asked for this password every time he wish to download a certificate.

Comodo Certificate Manager stores the individual private keys of end-user's client certificates so that they can be retrieved at a later date by the administrator or end-user. Due to the highly sensitive and confidential nature of this feature, all end-users' key pairs are stored in encrypted form so that they cannot be easily stolen or compromised. Each end-user's key pair is encrypted using a 'master' public key that is stored by CCM. In order to decrypt this end-user's key pair the administrator must paste the corresponding 'master' private key into the space provided. Admin can set a password to protect access to private key in .p12 file as well. The Administrator is able to bypass the PIN but should be aware that not all programs will subsequently allow the certificate to be imported if they do so. The following is a summary of browsers in which it is possible to import .p12 with empty password field.

| Browser | Windows 8 | Windows 7 | Vista | XP | Mac |
|----------------|-----------|-----------|-------|----|-----|
| IE 6 | - | - | - | ✓ | - |
| IE 7 | - | - | ✓ | ✓ | - |
| IE 8 and above | ✓ | ✓ | ✓ | ✓ | - |
| FF 2 | ✓ | ✓ | ✓ | ✓ | ✓ |
| FF 3 and | ✗ | ✗ | ✗ | ✗ | ✗ |

| | | | | | |
|---------------|---|---|---|---|---|
| above | | | | | |
| Opera 9 | ✓ | ✓ | ✓ | ✓ | ✓ |
| Opera 10 | ✓ | ✓ | ✓ | ✓ | ✓ |
| Google Chrome | ✓ | ✓ | ✓ | ✓ | ✓ |
| Safari | ✓ | ✓ | ✓ | ✓ | ✓ |

WARNING! If an administrator downloads an end-user's certificate, this certificate will be revoked.

3.2.2 Adding Cert End-Users

There are several methods of adding end-users to Organizations in Certificate Manager.

- **Manually adding end-users**
- **Loading multiple end-users from a comma separated values (.csv) file**
- **Auto Creation of end-users via certificate Self Enrollment Forms**

Note: A new End-User will also be created and added to this interface when an SSL certificate application is made through the SSL Self Enrollment form. If the applicant does not already exist as an end-user when the form is submitted then a new end-user will be created with the name 'requesterSSL <DOMAIN.com>' (where DOMAIN.com = the domain name for which the application is being made) This End-User will automatically be assigned membership of the Organization that the SSL Certificate was ordered for but will not own a Client Certificate.

3.2.2.1 Manually Adding End-Users

- Click 'Certificates Management' - > 'Clients Cert' at the top left of the CCM interface;
- Click the 'Add' button to open the 'Add New Person' form:

Add New Person [X]

*-required fields

Organization: Dithers Construction Company

Department: None

Domain: coradithers.com

Email Address*: johnsmith@coradithers.com

First Name*: John

Middle Name:

Last Name*: Smith

Secret ID: ab123cde45f

Validation Type: Standard

Principal Name: [] [Copy email]

[OK] [Cancel]

- Click 'OK' to add the end-user to Comodo Certificate Manager.
- An end-user's details can be modified at any time by clicking the 'Edit' button at the top after selecting the checkbox next to their name in the main list of end-users. If any information in this dialog is changed, with the exception of Secret ID, any previously issued client certificates for this email address shall be automatically revoked. CCM maintains a username history. If the username is changed, the Administrator will still be able to search for the client certificates using both the old name and the new name.
- 'Validation Type' drop down will only be visible if enabled by your Comodo account manager.

3.2.2.1.1 'Add New Person' form - Table of Parameters

| Form Element | Type | Description |
|---------------|----------------|--|
| Organization | Drop down menu | Administrator should select the Organization that they wish the new end-user to belong to. |
| Department | Drop down menu | If required, the administrator should specify the Department that the end-user is to belong to. |
| Domain | Drop down menu | Administrator should select the domain from which to issue from the drop down menu. This drop-down will only display domains that have been correctly delegated to the Organization/Department selected earlier. |
| Email Address | Text Field | Administrator should enter the email address of the end-user. The email address must be for the domain belonging to the Organization. |
| First Name | Text Field | Administrator should enter the first name of the end-user. |

| Form Element | Type | Description |
|-----------------|----------------|---|
| Middle Name | Text Field | If required, the administrator should enter the middle name of the end-user. |
| Last Name | Text Field | Administrator should enter the last name of the end-user. Note: The combined length of First Name and the Last name should not exceed 64 characters. |
| Secret ID | Text Field | A 'Secret ID' (or 'Secret Identifier'/SID) is used to identify the details of an existing end-user in CCM. Assigning SIDs to users will simplify the client certificate enrollment process for those users and therefore help eliminate errors. This is because, as the details of the user are already stored, the end-user need only specify the email address If the administrator wishes to allow enrollment by Secret ID then they must fill out this field. |
| Validation Type | Drop Down Menu | Note: The 'Validation Type' drop down will only be visible if enabled by your Comodo account manager. Allows the administrator to specify the type of client certificate that is issued to an applicant. The difference between the two lies in the degree of user authentication is carried out prior to issuance. The two options are 'Standard' and 'High'. 'Standard' certificates can be issued quickly and take advantage of the user authentication mechanisms that are built into CCM. A user applying for a 'Standard Personal Validation' certificate is authenticated using the following criteria: <ul style="list-style-type: none"> • User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization • The Organization has been independently validated by a web-trust accredited Certificate Authority as the owner of that domain • User must know either a unique Access Code or Secret ID that should be entered at the certificate enrollment form. These will have been communicated by the administrator to the user via out-of-band communication. • User must be able to receive an automated confirmation email sent to the email address of the certificate that they are applying for. The email will contain a validation code that the user will need to enter at the certificate collection web page. 'High Personal Validation' certificates require that the user undergo the validation steps listed above AND <ul style="list-style-type: none"> • Face-to-Face meeting with the issuing Organization Note: The additional validation steps must be completed PRIOR to the administrator selecting 'High Personal Validation' type. |
| Principal Name | Text Field | The Administrator can enter the email address that should appear as principal name in the certificate to be issued. Note: For the Organizations/Departments enabled for Principal Name support, the client certificates issued to the end-users of the Organization/Department will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative |

| Form Element | Type | Description |
|--------------|--------|--|
| | | <p>Name(SAN) field. If included, the Principal Name will be the primary email address of the end-user to whom the certificate is issued. But this can be customized at a later time by editing the end-user if Principal Name Customization is enabled for the Organization/Department.</p> <p>The Administrator can check whether an Organization or Department is enabled for Principal Name support from the Settings interface by clicking Settings > Organizations > Edit button in the row of the respective Organization name > Client Cert tab or Settings > Organizations > Department button in the row of the respective Organization name > Edit button in the row of the respective Department > Client Cert tab.</p> <p>This field will be disabled for the Organizations for which the Principal Name support is not enabled. If the Principal Name support is enabled for an Organization and not enabled for the Department belonging to the Organization, this field will be auto populated with the email address entered in the Email Address field.</p> |
| Copy E-Mail | Button | Auto-fills the Principal Name field with the email address entered in the E-mail Address field. |

3.2.2.2 Loading Multiple End-Users from a Comma Separated Values (.csv) File

Administrators can import list of end-users into CCM in comma separated values (.csv) format. After importing the list, your employees then only need to complete the self enrollment with their secret code.

Note: The ability to loading multiple end-users from a .csv file functionality is only available to MRAO, RAO S/MIME and DRAO S/MIME administrators.

3.2.2.2.1 Procedure Overview

Summary of required steps for adding end-users by loading a .csv file:

1. Administrator generates a .csv file using containing a list of end-users. .csv files can be exported directly from spreadsheet programs such as Excel or Open Office Calc.
2. Administrator loads the .csv file by clicking the 'Load from CSV' button in the 'Certificates Management' > 'Client Certificates' interface
3. CCM sends an email notification containing a link to the self-enrollment form and the secret identifier to each end-user included in the .csv file.

Note: For the CM to automatically send the notification emails to the end-users, the administrator should have configured for this by selecting the checkbox 'Send invitations on successful upload' in the Import persons from CSV dialog while loading the .csv file. If not configured, the administrator should manually send an email containing a link to the self-enrollment form and the secret identifier to each end-user. For more details refer to section **The Import Process**.

4. End-users collect and install their certificates.

3.2.2.2.2 Requirements for .csv file

The fields per user in the .csv differs for Organizations depending on whether or not the Principal Name Support is enabled for the Organization. For more details on the principal Name Support, refer to **Settings > Organisations > Creating a New Organisation > Client Cert Settings tab**.

3.2.2.2.1 For Organizations with Principal Name Support Enabled

There are 12 potential fields per user that can be imported via .csv. 6 are **mandatory** and there is one conditionally mandatory value. The 12 potential fields are as follows:

- First Name
- Middle Name
- Last Name
- Email Address (Primary)
- Alternative Email Address(es)
- Validation Type
- Organization
- Department
- Secret Identifier
- Phone
- Country
- Principal Name

- Each entry should have 12 fields. Even the optional fields without values must be included but should be left blank ("").
- 'Department' will be mandatory if the administrator that is importing is a DRAO S/MIME. MRAO, RAO S/MIME (and DRAO S/MIME administrators that are also MRAO or RAO S/MIME administrators) have the option to leave this field blank. See **3.2.2.2.3.General Rules** for more details.
- The 'Secret ID' value can be used to add a layer of authentication to the process. If specified, the user will need to type the identifier at the certificate enrollment form to complete the process.
- With the exception of the 'Secret ID' and 'Phone', make sure the fields are imported using characters as specified below. (including commas (,) and quotation marks (" ")).

The following table explains the requirements and formats of the values.

| Values | First Name | Middle Name | Last Name | Email Address (primary) | Email Addresses (Alternative) | Validation Type | Organization | Department | Secret ID | Phone | Country | Principal Name |
|--------------------------------|------------|-------------|-----------|-------------------------|--------------------------------|-----------------|--------------|------------|-----------|-------|--------------------------|----------------|
| Required | Yes | | Yes | Yes | Yes | | Yes | | | | Yes | |
| Min Length (characters) | 1 | 0 | 1 | 3 | 3 | | 1 | 0 | 0 | 0 | 2 | 1 |
| Max Length (characters) | 128 | 128 | 128 | 128 | 128 | | 128 | 128 | 128 | 128 | 2 | 128 |
| Format | | | | Valid email address | Valid email address, separated | | | | | | Valid two letter country | |

| | | | | | by space | | | | | | code | |
|--------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|-------------------------------------|--------------------------------------|---|-----|-----|-----|-----|--------------|-----|
| Character s allowed | A-Z, a-z, 0-9, ',';', ''; | A-Z, a-z, 0-9, ',';', ''; | A-Z, a-z, 0-9, ',';', ''; | A-Z, a- z, 0-9, ',';', ''; | A-Z, a-z, 0-9, ',', -', '_' | 'high' , empt y or 'stan dard' | ANY | ANY | ANY | ANY | A-Z, a- z | ANY |

Example:

"First1", "Middle1", "Last1", "User----1-al@abc.com", "User----1-sec-al@abc.com", "standard", "System", "sysdep", "Secret1", 380487000001, "UA", "User----1-al@abc.com"

Note: If an Organization is enabled for Principal Name support and a Department belonging to the Organization is not enabled for Principal Name support, when loading end-users of the Department, the Principal Name field must be included but should be left blank.

The Administrator can check whether an Organization or Department is enabled for Principal Name support from the Settings interface by clicking **Settings > Organizations > Edit button in the row of the respective Organization name > Client Cert tab** or **Settings > Organizations > Department button in the row of the respective Organization name > Edit button in the row of the respective Department > Client Cert tab**.

3.2.2.2.2 For Organizations without Principal Name Support

There are 11 potential fields per user that can be imported via .csv. 6 are **mandatory** and there is one conditionally mandatory value. The 11 potential fields are as follows:

- First Name
- Middle Name
- Last Name
- Email Address (Primary)
- Alternative Email Address(es)
- Validation Type
- Organization
- Department
- Secret Identifier
- Phone
- Country

- Each entry should have 11 fields. Even the optional fields without values must be included but should be left blank ("").
- 'Department' will be mandatory if the administrator that is importing is a DRAO S/MIME. MRAO, RAO S/MIME (and DRAO S/MIME administrators that are also MRAO or RAO S/MIME administrators) have the option to leave this field blank. See **3.2.2.2.3.General Rules** for more details.
- The 'Secret ID' value can be used to add a layer of authentication to the process. If specified, the user will need to type the identifier at the certificate enrollment form to complete the process.
- With the exception of the 'Secret ID' and 'Phone', make sure the fields are imported using characters as specified below. (including commas (,) and quotation marks (" ")).

The following table explains the requirements and formats of the values.

| Values | First Name | Middle Name | Last Name | Email Address (primary) | Email Address (Alternative) | Validation Type | Organization | Department | Secret ID | Phone | Country |
|--------------------------------|--|--|--|--|--|-----------------------------|--------------|------------|-----------|-------|-------------------------------|
| Required | Yes | | Yes | Yes | Yes | | Yes | | | | Yes |
| Min Length (characters) | 1 | 0 | 1 | 3 | 3 | | 1 | 0 | 0 | 0 | 2 |
| Max Length (characters) | 128 | 128 | 128 | 128 | 128 | | 128 | 128 | 128 | 128 | 2 |
| Format | | | | Valid email address | Valid email address, separated by space | | | | | | Valid two letter country code |
| Characters allowed | A-Z, a-z, 0-9, ' ', '!', '@', '#', '\$', '%', '&', '*', '^', '_' | A-Z, a-z, 0-9, ' ', '!', '@', '#', '\$', '%', '&', '*', '^', '_' | A-Z, a-z, 0-9, ' ', '!', '@', '#', '\$', '%', '&', '*', '^', '_' | A-Z, a-z, 0-9, ' ', '!', '@', '#', '\$', '%', '&', '*', '^', '_' | A-Z, a-z, 0-9, ' ', '!', '@', '#', '\$', '%', '&', '*', '^', '_' | 'high', empty or 'standard' | ANY | ANY | ANY | ANY | A-Z, a-z |

Example:

"First1","Middle1","Last1","User----1-al@abc.com","User----1-sec-al@abc.com","standard","System","sysdep","Secret1",380487000001,"UA",

3.2.2.2.3 General Rules

The import will fail if:

- All the lines are not having the 12/11 fields as required.
- Any **mandatory** field as explained in **2.2.2.2.2.Requirements for .csv file** is missing
- The Organization does not exist
- The Department, if present, does not exist
- The Department, if present, does not exist for the specified Organization
- The Primary Email Address is not in a valid format or the email domain cannot be determined
- The domain of the Primary Email Address is not delegated to the Organization or is not active.
- The domain of the Primary Email Address is not delegated to the Department (if Department is supplied)
- The Secondary Email Address (if supplied) is not in a valid format or the email domain cannot be determined
- The domain of the Secondary Email Address is not delegated to the Organization or is not activate.
- The domain of the Secondary Email Address is not delegated to the Department (if Department is supplied)

- The administrator attempting the import does not have the correct permissions for the Organization and/or Department:
 - MRAO administrators have permission to import for any valid Organization or Department. MRAOs may leave the 'Department' field blank.
 - RAO S/MIME administrators have permission to import for Organizations (and any subordinate Departments) that have been delegated to them. RAO S/MIME may leave the 'Department' field blank.
 - DRAO S/MIME administrators have permission to import for Departments that have delegated to them. DRAO S/MIME administrators *cannot* leave the 'Department' field blank unless they are also an RAO S/MIME for the same Organization.

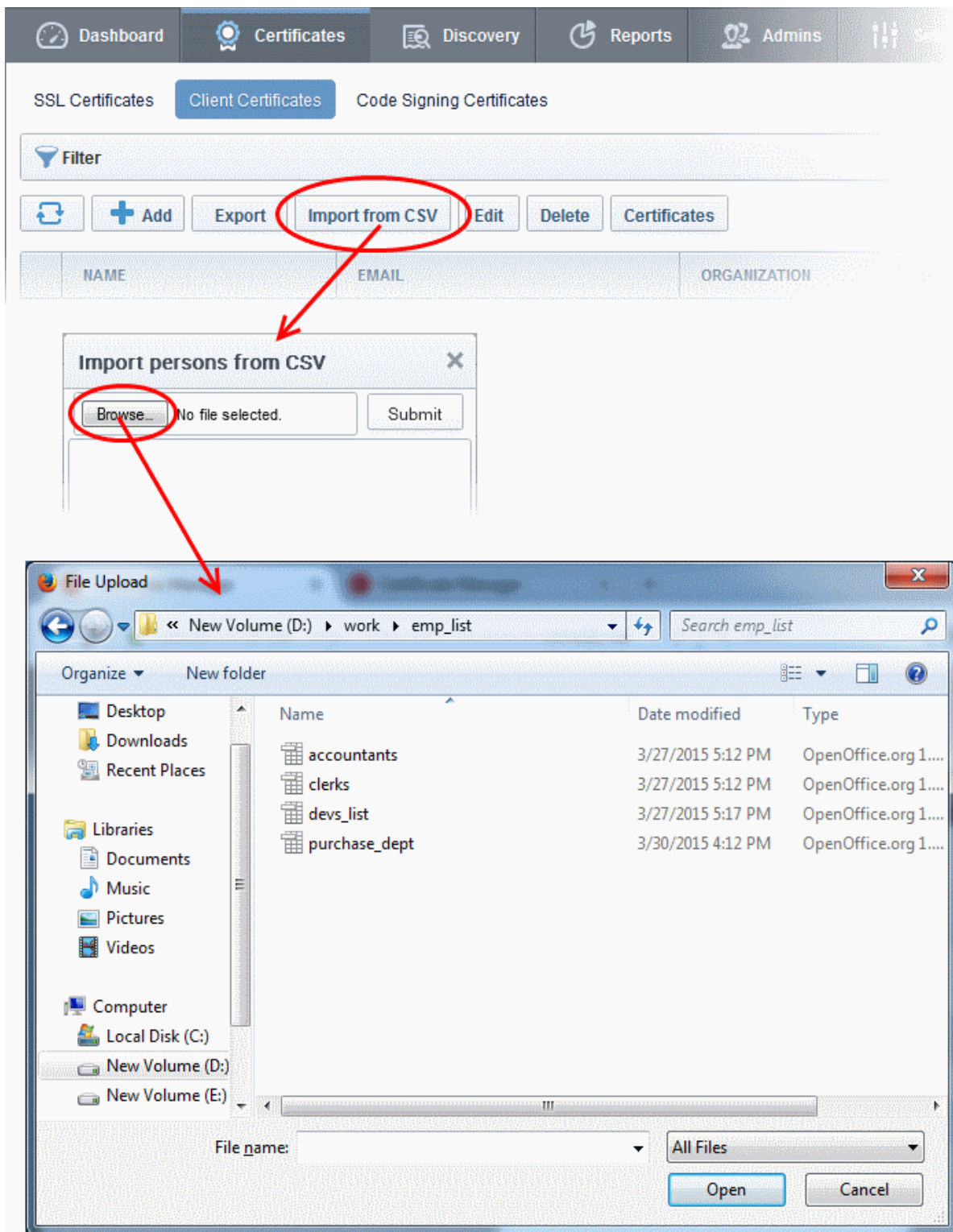
3.2.2.2.4 The Import Process

To load the .csv file

- Click 'Import from CSV' in 'Certificates Management' > 'Client Certificates' interface

The 'Import from CSV' dialog will appear.

- Click the 'Browse' button and navigate to the .csv file

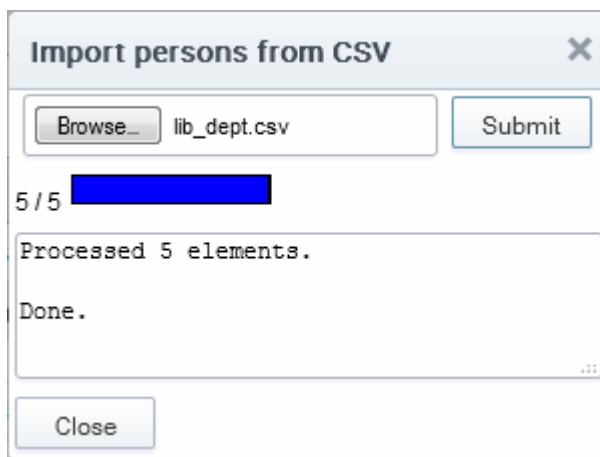


- Click 'Submit'.

The import status will be indicated. You will see a progress bar indicating that information is being uploaded:



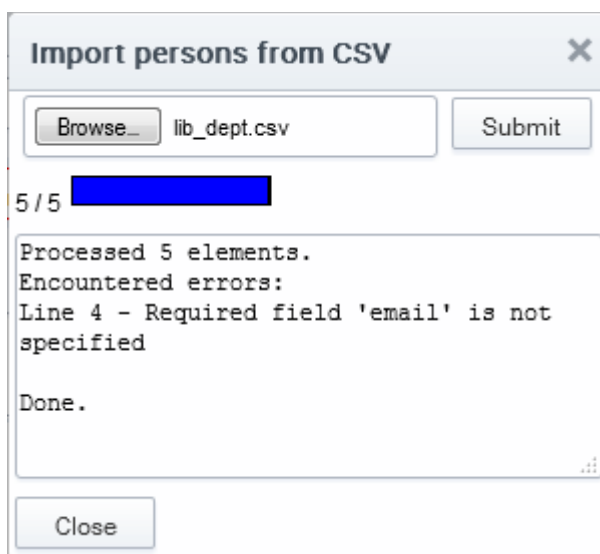
CCM will inform you when the process is finished:



All imported users appear in the list of end-users in the 'Client Certificates' section and notification emails containing a link to the [self-enrollment form](#) and the secret ID will be automatically sent to the imported end-users, if the checkbox 'Send invitations on successful upload' is selected.

3.2.2.2.5 Errors in .csv file

CCM will inform you if there is an error in the .csv file (mandatory fields are missing, for example).



Only the end-users included in the lines without errors will be loaded to CCM and the end-users included in the lines with errors will not be loaded.

3.2.2.3 Auto Creation of End-Users via Certificate Self Enrollment Form

End-users applying via the SSL or Client Certificate enrollment form are automatically added to the 'Certificate Management - Client Certificates' area.

For more details see: [Request and issuance of client certificates to employees and end-users](#)

3.2.3 Editing End-Users

All end-user details can be modified at any time by clicking the 'Edit' button after selecting the end-user's name.

Edit Person
✕

*-required fields

Organization

Department

Domain

Email Address* @coradithers.com

First Name*

Middle Name

Last Name*

[Reset Secret ID](#)

Validation Type

Principal Name

- If any information in this dialog is changed, with the exception of 'Secret ID', any previously issued client certificates for this email address shall be automatically revoked.
- For security reasons, the 'Secret ID' field is not displayed. If the SID needs to be changed, administrator can click the [Reset Secret ID](#) link.
 - On clicking the link, the Secret ID text box will be displayed, enabling the administrator to specify a new SID.

Last Name*

Secret ID

[Don't Reset Secret ID](#)

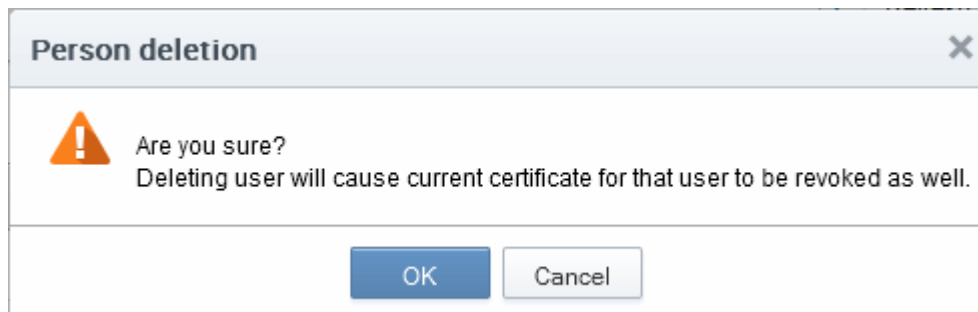
Validation Type

- To change the SID, the administrator can type a new SID in this field.
 - To retain the existing SID, the administrator can click the [Don't Reset Secret ID](#) link.
- 'Validation Type' drop down will only be visible if enabled by your Comodo account manager. For an explanation of validation types, see 'Validation Type' in the **'Add New Person'** table of parameters.
- Renaming an end-user does not affect the search and filtering actions in the Client Certificates Interface. CCM allows the administrators to search for particular user or client certificates using both the old name and the new name in case a username is changed.
- To customize the Principal Name for the end-user, type the new Principal Name as it should appear in the in the Subject Alternative Name (SAN) field of the certificate in the Principal Name field. To revert the Principal Name to the email address of the end-user, click the 'Copy E-Mail' button. This button will be available only if this feature is enabled for your account.

Full details of the fields available when editing an existing end-user are available in the section '[Add New Person form - table of parameters](#)'.

3.2.4 Deleting an End-User

An Administrator can delete any end-user by clicking 'Delete' button after selecting the end-user's name.



Once the end-user is deleted, their certificate will be revoked.

3.2.5 Request and Issuance of Client Certificates to Employees and End-Users

End-users can be enrolled for client certificates (a term which covers email certificates, end-user authentication certificates and dual-use certificates) in three ways:

- **Self Enrollment of End-Users by Access Code** - Involves directing the end-users to apply for their own client certificate by accessing the self enrollment form. The Administrator has to inform the end-user of the URL at which the self-enrollment form is hosted and the access code of the Organization to which the end-user belongs. This should be done by out-of-band communication such as email. See the section **Self Enrollment by Access Code** for more details.
- **Self Enrollment of End-Users by Secret Identifier** - Involves directing the end-users to apply for their own client certificate by accessing the self enrollment form. The Administrator has to inform the end-user of the URL at which the self-enrollment form is hosted and the Secret Identifier of the Organization to which the end-user belongs. This should be done by out-of-band communication such as email. See the section **Self Enrollment by Secret Identifier** for more details.
- **Enrollment by Administrator's Invitation** - Involves sending invitation mails to end-users previously added to CCM. The Administrators can send the invitation mail from the CCM interface itself. The invitation mail will contain a validation link and instructions for the end-users to download and install their certificates. See the section **Enrollment by Invitation** for more details.

3.2.5.1 Self Enrollment by Access Code

This section explains how the administrator can direct the end-user for self-enrollment using the access code specified for the Organization and how the end-user can apply for, collect, download and install their certificate.

3.2.5.1.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for S/MIME certificates, has been pre-validated by Comodo and that the domain has been activated by your Comodo account manager. (i.e. if you wish to issue client certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo).

However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.

- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See [Creating a New Organization](#) and [Editing an Existing Organization](#) for more details on adding a domain to an Organization.
- The RAO S/MIME or DRAO S/MIME administrator has been delegated control of this Organization or Department
- The administrator has **checked** the 'Self Enrollment' box in the '**Client Cert**' tab of the 'Create/Edit' Organizations dialog box.

The screenshot shows the 'Edit Organization: Dithers Construction Company' dialog box with the 'Client Certificate' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with the following tabs: General, EV Details, Client Certificate (selected), SSL Certificate, Code Signing Certificate, and Email Template. The 'Client Certificate' tab contains the following settings:

- Self Enrollment:
- Access Code*:
- Web API:
- Secret Key*: OrgID: 3875
- Allow Key Recovery by Master Administrators:
- Allow Key Recovery by Organization Administrators:
- Allow Principal Name:
- Allow Principal Name Customization:
- Client Cert Types:
- Key Usage Template:

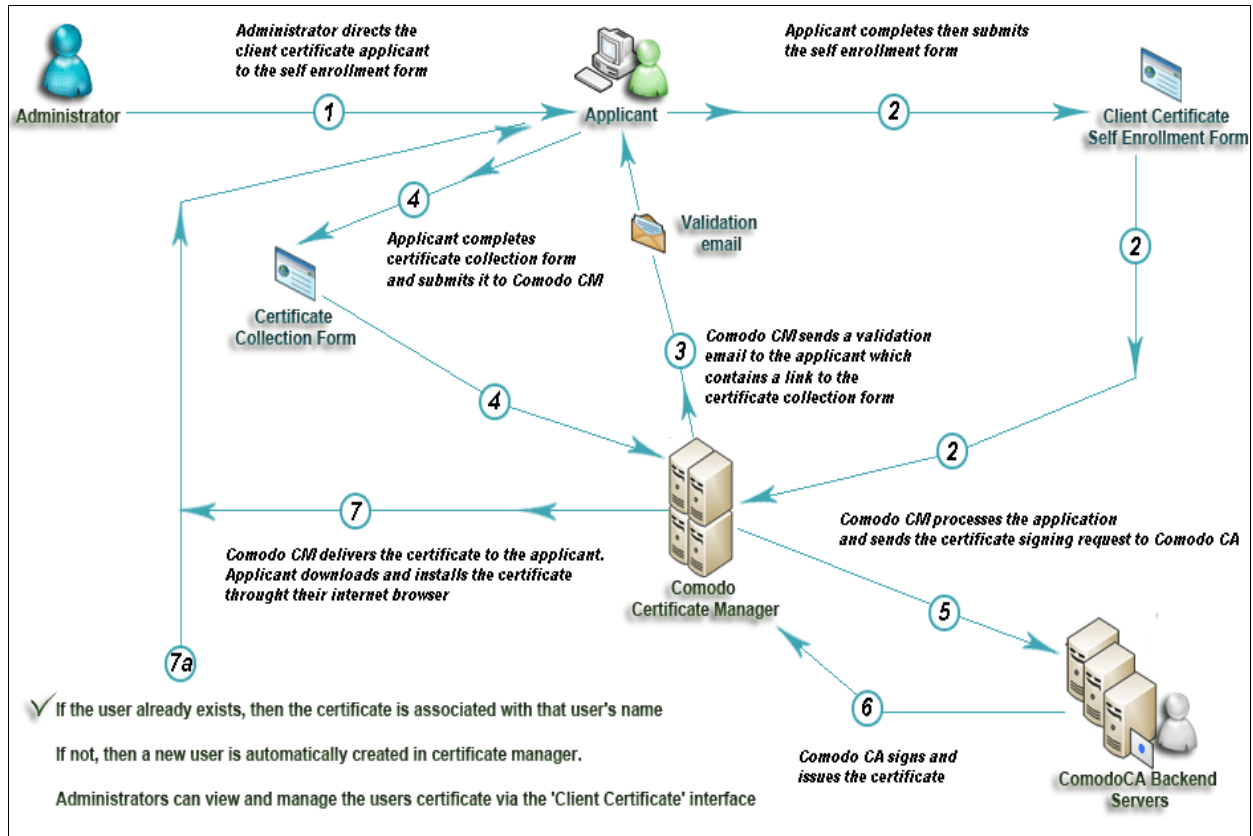
At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- The administrator has **specified an Access Code** in the '**Client Cert**' tab of the 'Create/Edit' Organizations dialog box. This should be a mixture of alpha and numeric characters that cannot easily be guessed.

3.2.5.1.2 Procedure Overview

1. Administrator confirms completion of the [prerequisite steps](#).
2. Administrator directs the personal certificate applicant to the 'Access Code' based Self Enrollment Form - making sure the application is done from the end-user's computer (see section [Initiating the enrollment process](#)).
3. Applicant completes then submits the Self Enrollment Form, specifying the correct Access Code for the Organization's domain. (See section [The Self Enrollment Form](#))
4. CCM sends a validation mail to the applicant which contains a link to the Account Validation form and a request code. (See section [Validation of the Application](#) for more details)
5. Applicant completes the Account Validation form. The certificate request is sent to Comodo CA servers. If the application is successful, the applicant will be able to download and install their personal certificate. (See section [Certificate Collection..](#))
6. If the applicant already exists as an 'End-User' (viewable in the '[Client Certificates](#)' area of 'Certificates

Management' section) then the certificate will be added to their account. If the applicant does not exist as an 'End-User' then CCM will automatically add this applicant as a new 'End-user' at the point of certificate issuance. If the applicant already exists as an Administrator (visible in '**Admin Management**') but not as a (client certificate) 'End-User' then CCM will automatically add this applicant as a new 'End-user' to the 'Client Certificates' area'. ([Click here](#) for further details)



3.2.5.1.3 Initiating the Enrollment Process

After completing the **prerequisite** steps, administrators need to communicate enrollment details to all and any end-users they wish to issue client certificates to. The communication must contain the following information:

1. A link to the Access Code based Self Enrollment Form - [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/smime?action=enroll&swt=ac](https://cert-manager.com/customer/[REAL CUSTOMER URI]/smime?action=enroll&swt=ac)
2. The client access code specified in that Organization's **Client Cert settings tab**.


These details can be informed to the applicant by the any preferred out-of-band communication method like email. The end-user can access the form at the given URL, fill-in with the necessary details and submit it.

Please Note:

The domain of the email address that the end-user specifies in the Self Enrollment Form **MUST** match a 'Common Name' (domain) associated with an **Organization or Department within an Organization**. The applicant **MUST** be able to receive emails at this address.

The access code the end-user enters at the Self Enrollment Form **MUST** match the access code specified by the administrator for that specific Organization.

3.2.5.1.3.1 The Access Code Based Self Enrollment Form


Certificate Manager

S/MIME Certificate Enroll

Access Code: *

First Name: *

Middle Name:

Last Name: *

Email: *

Certificate Type: *

Self Enrollment Passphrase: * i

Re-type Self Enrollment Passphrase: *

1

Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS DESCRIBED HEREIN.

I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.

3.2.5.1.3.2 Form Parameters

| Form Element | Type | Description |
|------------------------|------------|--|
| Access Code(required) | Text Field | This is the Access Code specified for the Organization or Department. |
| First Name (required) | Text Field | Applicant should enter their first name |
| Middle Name (optional) | Text Field | If required, the applicant should enter their middle name |
| Last Name (required) | Text Field | Applicant should enter their last name |

| | | |
|--------------------------------|------------|--|
| Email (required) | Text Field | Applicant should enter their full email address. The Email address must be for the domain belonging to the Organization. |
| Pass-Phrase (required) | Text Field | This phrase is needed to renew or revoke the certificate should the situation arise. |
| Re-type Pass-Phrase (required) | Text Field | Confirmation of the above |
| Eula Acceptance (required) | Checkbox | Applicant must accept the terms and conditions before submitting the form. |
| Enroll | Control | Submits the application and enrolls the applicant for the client certificate. |
| Cancel | Control | Clears all data entered on the form |

Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section **Custom Fields** for more details.

After completing the form and clicking the 'Enroll' button, a confirmation dialog will be displayed...

COMODO
Certificate Manager

Confirmation

You have requested a S/MIME Certificate with the follow details:

Email: johnsmith@coradithers.com,
Name: John Smith.

We have sent you an email containing an enrollment link in order to complete the rest of the enrollment process.

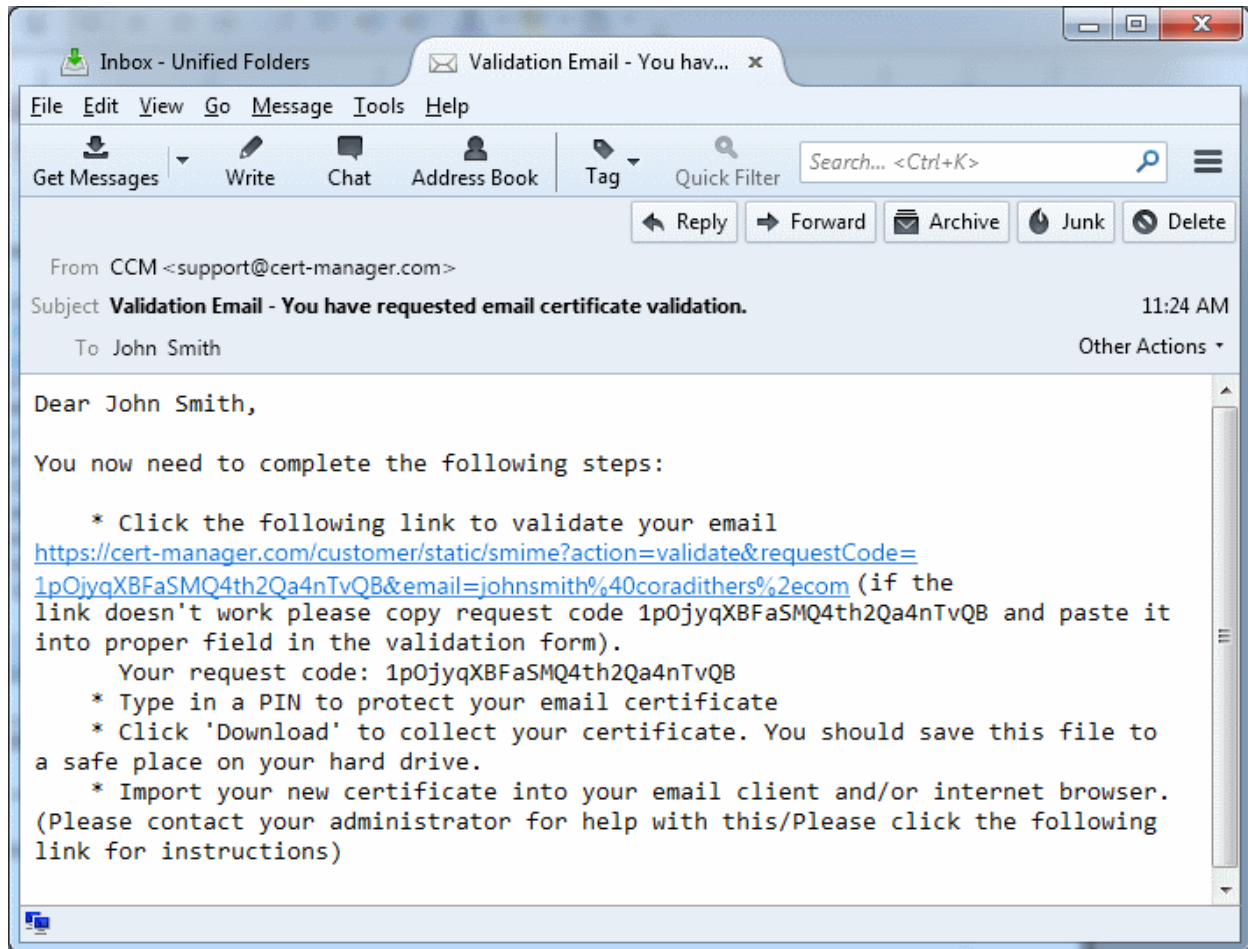
[BACK](#)

...and the applicant will receive an email containing a URL for validating the application, a request validation code and instructions for downloading the certificate. Upon clicking the link, the end-user will be taken to the Account Validation form. See the section **Validation of the Application** for more details. On completion of the validation process, a certificate collection form will appear, enabling the end-user to download and save the certificate. See the section **Certificate Collection** for more details.

3.2.5.1.4 Validation of the Application

The applicant will receive a validation email on successful submission of the **Self Enrollment Form** and after being processed at Comodo.

The validation email will contain a link to the Account Validation form. The link will also contain a randomly generated 'Request Code' that the end-user will need in order to validate that they are the correct applicant. Simply clicking on the link in the email will automatically populate the request 'Code' and 'Email' fields in the Account Validation form.



Note: It is possible for administrators to modify the contents of these emails in the 'Email Templates' area under the 'Settings' tab.

Upon clicking the link the applicant will be taken to the validation form.

COMODO


Certificate Manager

Account Validation

Code: *

Email: *

Certificate Type: *

PIN: 

Re-type PIN:

Select address fields to remove from the certificate.

| Address as it will appear in certificate | Remove |
|---|--------------------------|
| Address1: <input type="text" value="Mount Road"/> | <input type="checkbox"/> |
| Address2: <input type="text"/> | <input type="checkbox"/> |
| Address3: <input type="text"/> | <input type="checkbox"/> |
| City: <input type="text" value="Riverdale"/> | <input type="checkbox"/> |
| State or province: <input type="text" value="Alabama"/> | <input type="checkbox"/> |
| Postal Code: <input type="text" value="123456"/> | <input type="checkbox"/> |
| Employee ID: * <input type="text"/> | |

VALIDATE

CANCEL

| Form Element | Type | Description |
|---|------------|---|
| Code (required) | Text Field | The validation request code. This field is auto-populated when the applicant clicks the validation link contained in the email. |
| E-mail (required) | Text Field | Email address of the applicant. This field is auto-populated. |
| PIN (required) | Text Field | The applicant should specify a PIN for the certificate to protect the certificate. |
| Re-type PIN (required) | | Confirmation of the above. |
| Select address fields to remove from the certificate (optional) | Checkboxes | By default, the address details are displayed in the View Certificate Details dialog. The applicant can hide these details selectively in the View Certificate Details dialog by selecting the 'Remove' checkboxes beside the required address fields. Click here for more details. |
| Validate | Control | Completes the validation process and enables the applicant to download the certificate |
| Cancel | Control | Clears all data entered on the form |

Selecting Address Fields to be Removed from the Certificate

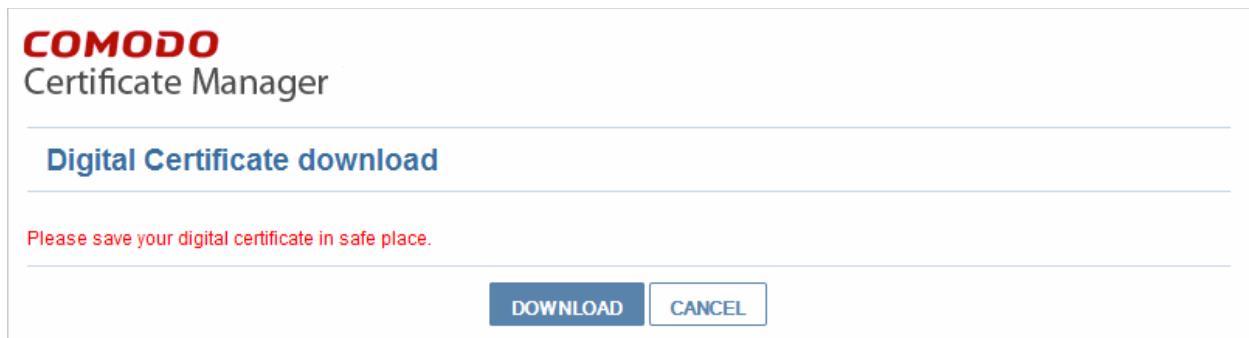
The following address fields...

- Address1;
- Address2;
- Address3;
- City;
- State/Province;
- Postal Code.

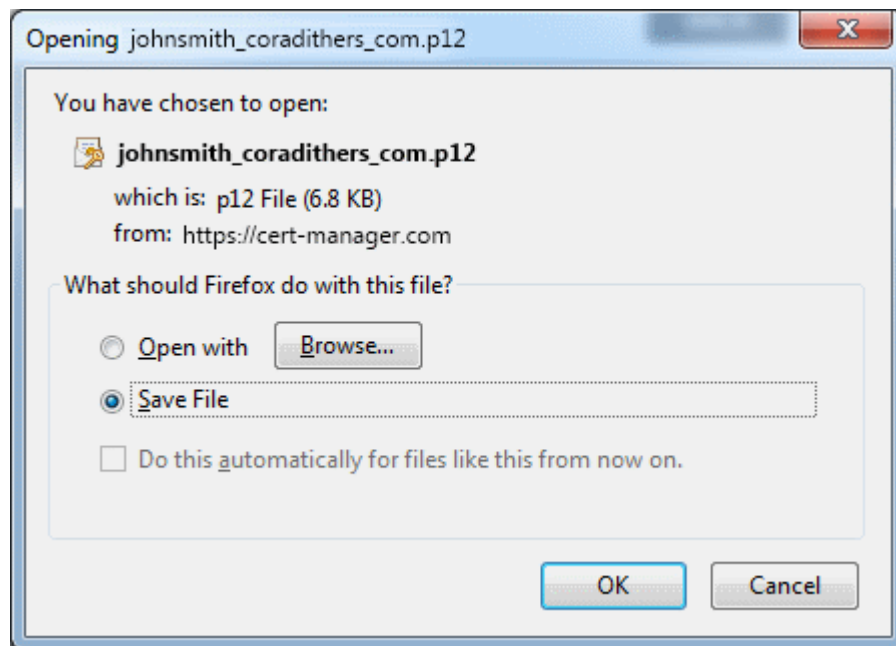
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' checkboxes below beside the corresponding field. The selected details will not be included in the certificate that is issued. The 'View Certificate Details' dialog will state 'Details Omitted' next to these fields.

3.2.5.1.5 Certificate Collection

Upon successful submission of the Account Validation form, a download dialog will be displayed enabling the applicant to download and save the certificate.



The applicant can collect the certificate by clicking 'Download' and save the file in a safe location in his/her computer.



CCM will deliver the certificate to the end-user in PKCS#12 file format (.p12 file). The PIN specified in the PIN fields is used to protect access to this .p12 file. The end-user will be asked for this PIN when he/she imports the certificate into the certificate store of their machine.

New end-users: If the end-user does not already exist in Certificate Manager (viewable in the 'Client Certificates' area of 'Certificates Management' section) then he/she will be automatically created and added as a new end-user belonging to the Organization for which the certificate was issued. This new end-user will now be viewable in the **Client Certificates Sub-tab** of the interface with the following parameters:

- **Name:** The name that the end-user specified at the **Client Self Enrollment Form**
- **Email:** The email address that the certificate was issued to (as specified at the **Client Self Enrollment Form**)
- **Organization:** Name of the Organization to which this end-user belongs to.
- **Existing end-users:** If the end-user already exists, then the certificate will be associated with their end-user name.

See section '**The Client Certificates Area**' for more information regarding end-user and client certificate management.

3.2.5.2 Self Enrollment by Secret Identifier

This section explains how the administrator can direct the end-user for self-enrollment using the Secret Identifier specified for the Organization and how the end-user can apply for, collect, download and install their certificate.

3.2.5.2.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for S/MIME certificates, has been pre-validated by Comodo and that the domain has been activated by your Comodo account manager. (i.e. if you wish to issue client certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo).

However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.

- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See **Creating a New Organization** and **Editing an Existing Organization** for more details on adding a domain to an Organization.
- The RAO S/MIME or DRAO S/MIME administrator has been delegated control of this Organization or Department
- The administrator has **checked** the "Web API" box in the '**Client Cert**' tab of the 'Create/Edit' Organizations dialog box.

Edit Organization: Dithers Construction Company [X]

General | EV Details | **Client Certificate** | SSL Certificate | Code Signing Certificate | Email Template

Self Enrollment

Access Code* 654321

Web API

Secret Key* ab123cde45f OrgID: 3875

Allow Key Recovery by Master Administrators

Allow Key Recovery by Organization Administrators

Allow Principal Name

Allow Principal Name Customization

Client Cert Types

Key Usage Template

- The administrator has specified a Secret ID for the user using either the 'Add User' or 'Edit User' dialog boxes or when 'Importing from .csv'. The secret code should be a mixture of alpha and numeric characters that cannot easily be guessed.

Add New Person [X]

*-required fields

Organization: Dithers Construction Company

Department: Purchases Department

Domain: coradithers.com

Email Address*: johnsmith@coradithers.com

First Name*: John

Middle Name:

Last Name*: Smith

Secret ID: ab123cde45f

Validation Type: High

OK Cancel

3.2.5.2.2 Procedure Overview

- Administrator confirms completion of the **prerequisite steps**.
- Administrator directs the personal certificate applicant to the 'Secret Identifier' based Self Enrollment Form - making sure the application is done from the end-user's computer (see section **Initiating the enrollment process**).
- Applicant completes then submits the Self Enrollment Form, specifying the correct Secret Identifier assigned to him/her. (See section **The Self Enrollment Form**)
- The certificate request is sent to Comodo CA servers. If the application is successful, the applicant will be able to download and install their personal certificate. (See the section **Certificate Collection**)

3.2.5.2.3 Initiating the Enrollment Process

After completing the **prerequisite steps**, administrators need to communicate enrollment details to each end-user, they wish to issue client certificates to. The communication must contain the following information:

1. A link to the Secret Identifier based Self Enrollment Form - [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/smime?action=enroll&swt=si](https://cert-manager.com/customer/[REAL CUSTOMER URI]/smime?action=enroll&swt=si)
2. The secret identifier specified for the end-user.


These details can be informed to the applicant by the any preferred out-of-band communication method like email. The end-user can access the form at the given url, fill-in with the necessary details and submit it.

Please Note: The domain of the email address that the end-user specifies in the Self Enrollment Form **MUST** match a 'Common Name' (domain) associated with an **Organization or Department within an Organization**. The applicant **MUST** be able to receive emails at this address.

The Secret Identifier the end-user enters at the Self Enrollment Form **MUST** match the identifier specified for him/her by the administrator.

3.2.5.2.3.1 Secret Identifier Based Self Enrollment Form

The applicant needs to fill the application form, shown below.


Certificate Manager

Digital Certificate Download

Enter your Digital ID information

Fill in all required fields.

Email Address: *

Secret identifier: *

Certificate Type: *

Annual Renewal Self Enrollment Passphrase

The Annual Renewal Self Enrollment Passphrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. Do not lose it. You will need it when you want to revoke or renew your Digital ID.

Annual Renewal Self Enrollment Passphrase: *

Confirm Annual Renewal Self Enrollment Passphrase: *

Password:

This value will be used as password to protect access to your Digital ID.

Password:

Confirm Password:

Select address fields to remove from the certificate.

| | Address as it will appear in certificate | Remove |
|--------------------|--|--------------------------|
| Address1: | <input type="text" value="100, Raleigh Street"/> | <input type="checkbox"/> |
| Address2: | <input type="text"/> | <input type="checkbox"/> |
| Address3: | <input type="text"/> | <input type="checkbox"/> |
| City: | <input type="text" value="Riverdale"/> | <input type="checkbox"/> |
| State or province: | <input type="text" value="Alabama"/> | <input type="checkbox"/> |
| Postal Code: | <input type="text" value="123456"/> | <input type="checkbox"/> |

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE

THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.

3.2.5.2.3.2 Form Parameters

| Form Element | Type | Description |
|--|------------|---|
| Email Address (required) | Text Field | Applicant should enter their full email address. The Email address must be for the domain belonging to the Organization. |
| Secret identifier (required) | Text Field | Applicant should enter the Secret ID specified for him/her. This should have been communicated to the applicant by the administrator. |
| Annual Renewal Pass-Phrase (required) | Text Field | This phrase is needed to renew or revoke the certificate should the situation arise. |
| Password (required) | Text Field | The applicant should specify a password for the certificate. This is needed for accessing the certificate e.g. while exporting the certificate for backup and while importing the certificate to restore the certificate from the backup. The password should be entered in the first text box and reentered in the second text box for confirmation. The password should be of at least eight characters. |
| Select address fields to remove from the certificate (optional) | Checkboxes | By default, the address details are displayed in the View Certificate Details dialog. The applicant can hide these details selectively in the View Certificate Details dialog by selecting the 'Remove' checkboxes beside the required address fields. Click here for more details. |
| Eula Acceptance (required) | Checkbox | Applicant must accept the terms and conditions before submitting the form. |
| Enroll | Control | Submits the application and enrolls the applicant for the client certificate. |
| Cancel | Control | Clears all data entered on the form |

Note: In addition to the standard fields in the Enrollment form, custom fields such as 'Employee Code, Telephone' can be added by the MRAO Administrator. Refer to the section [Custom Fields](#) for more details.

Selecting Address Fields to be Removed from the Certificate

The following address fields...

- Address1;
- Address2;
- City;
- State/Province;
- Postal Code.

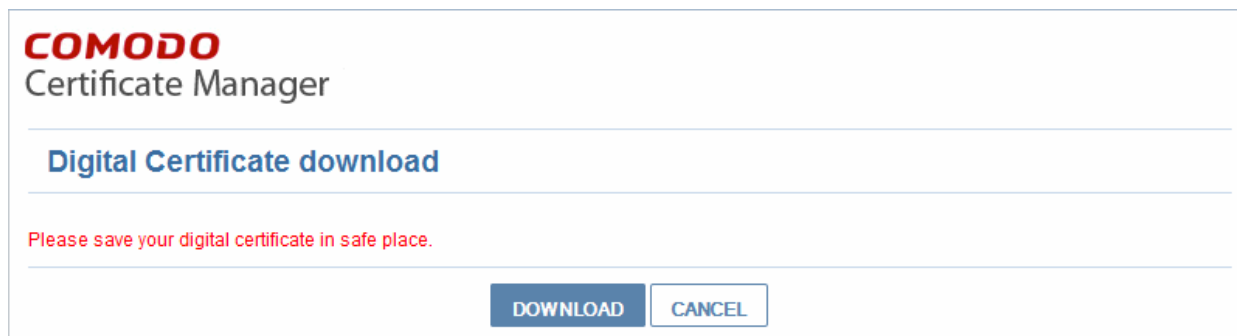
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' checkboxes below beside the corresponding field. The selected details will not be included in the certificate that is issued. The 'View Certificate Details' dialog will state 'Details Omitted' next to these fields.

After completing the form and clicking the 'Submit' button a certificate collection form will appear, enabling the end-user to download and save the certificate. See the section [Certificate Collection](#) for more details.

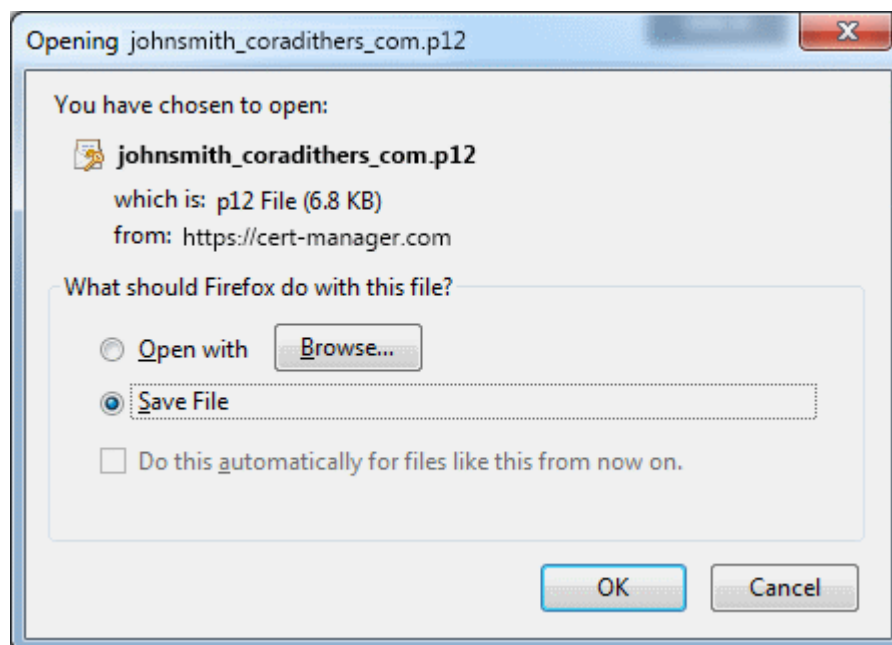
Note: It is possible for CCM Account holders to use their own, custom form templates rather than the default form supplied by Comodo. See your Comodo account manager for more details on enabling this functionality.

3.2.5.2.4 Certificate Collection

Once the enrollment form is submitted, a download dialog will be displayed enabling the applicant to download and save the certificate.



The applicant can collect the certificate by clicking 'Download' and save the file in a safe location in his/her computer.



CCM will deliver the certificate to the end-user in PKCS#12 file format (.p12 file). The PIN specified in the password fields is used to protect access to this .p12 file. The end-user will be asked for this PIN when he/she imports the certificate into the certificate store of their machine.

3.2.5.3 Enrollment by Invitation

This section explains how the administrator can invite the end-user for enrollment from the CCM interface and how the end-user can apply for, collect, download and install their certificate.

3.2.5.3.1 Prerequisites

- The domain from which the client certificate is to be issued has been enabled for S/MIME certificates, has been pre-validated by Comodo and that the domain has been activated by your Comodo account manager. (i.e. if you wish to issue client certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo).

However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.

- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See **Creating a New Organization** and **Editing an Existing Organization** for more details on adding a domain to an Organization.
- The RAO S/MIME or DRAO S/MIME administrator has been delegated control of this Organization or Department
- The administrator has added the end-user(s) to the Certificates Management > Client Certificates area of CCM.

3.2.5.3.2 Procedure Overview

Client certificates can be provisioned to the employees and end-users by inviting them for enrollment.

Overview of stages:

1. Administrator confirms completion of the **prerequisite steps**.
2. Administrator sends invitation for enrollment to the end-users from the Comodo CM interface. (see section **Initiating the Enrollment Process**)
3. CCM sends an Invitation mail to the end-user which contains a link to the User Registration Form. (See section **Validation of the Email Address** for more details)
4. The end-user completes the User Registration form. The certificate request is sent to Comodo CA servers. If the registration is successful, the end-user will be able to download and install their personal certificate. (See the section **Certificate Collection**)

3.2.5.3.3 Initiating the Enrollment Process

After completing the **prerequisite steps**, administrators need to send invitations to the end-users.

To send invitation administrator should:

- Click Certificate Management > Client Certificates. The list of end-users added previously will be displayed.
- Click 'Certs' button at the top after selecting the checkbox beside the end-user's name;
- In the dialog that appears press 'Send Invitation' button. (See screenshot below).

The screenshot shows the Comodo Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Reports, Admins, Settings, and About. Below these, there are sub-tabs for SSL Certificates, Client Certificates, and Code Signing Certificates. A 'Filter' dropdown is visible. Below the filter, there are buttons for Add, Export, Import from CSV, Edit, Delete, and Certificates. A table lists certificates with columns for NAME, EMAIL, ORGANIZATION, and DEPARTMENT. The first row is for John Smith (johnsmith@coradithers.com) at Dithers Construction Company, Purchases Department. A modal window titled 'Certificates for: johnsmith@coradithers.com' is open, showing a 'Send Invitation' button and a table with columns: ORDERED, REVOKED, EXPIRES, CERTIFICATE TYPE, ORDER NUMBER, and SERIAL NUMBER. The table is empty, displaying 'There is no data to display'. A 'Close' button is at the bottom of the modal.

After clicking 'Send Invitation', the 'Confirm Invitation' dialog will be displayed:

The 'Confirm Invitation' dialog box displays the following information:

- First Name: **John**
- Middle Name: (empty)
- Last Name: **Smith**
- Email Address: **johnsmith@coradithers.com**
- Organization: **Dithers Construction Company**
- Department: (empty)
- Certificate Type*: **High Persona Validated Cert** (dropdown menu)
- Term*: **1 year** (dropdown menu)

At the bottom, there are 'OK' and 'Cancel' buttons.

The confirmation dialog displays the details of the user and allows the administrator to choose the client certificate

type and the term.

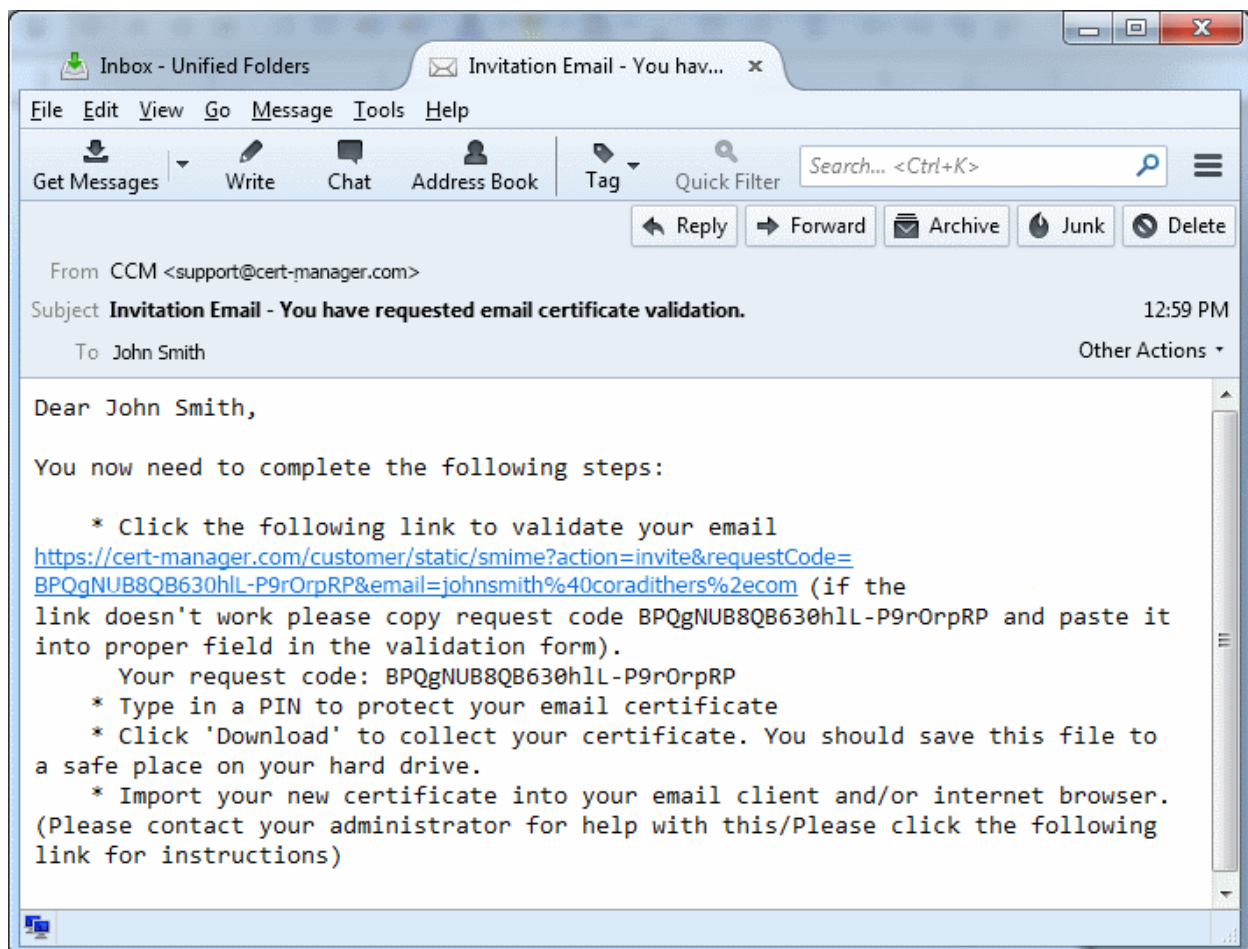
- Certificate Type - If your Organization's account has been enabled for High Personal Validated Certificates AND the administrator has specified a 'Validation Type' of 'High' * for this user THEN the 'Certificate Type' value will be a drop down menu rather than flat text. This menu will offer a choice between sending an invitation for a 'High Personal Validated' or a "Standard Personal Validated" certificate. The default choice is 'High Personal Validated'.
- Certificate Term - You can choose the term length for the certificate to be issued to the end-user. The 'Term' drop-down displays the term options allowed for your Organization.
- Upon clicking 'OK', an invitation email will be sent to the end-user.

The email will contain the URL of the certificate validation form, a request validation code and instructions for downloading the certificate. The request code will be contained within the URL so that applicants can simply click the link or copy and paste the URL in their browser. See the section Validation of the Email Address for more details. On completion of the validation and user registration processes, a certificate collection form will appear, enabling the end-user to download and save the certificate. See the section **Certificate Collection** for more details.

3.2.5.3.4 Validation of the Email Address


The end-user will receive an Invitation email on the administrator clicking the 'Send Invitation' button.

The invitation email will contain a link to the User Registration form. The link will also contain a randomly generated 'Request Code' that the end-user will need in order to validate that they are the correct applicant. Simply clicking on the link in the email will automatically populate the request 'Code' and 'Email' fields in the User Registration form.



Note: It is possible for administrators to modify the contents of these emails in the 'Email Templates' area under the 'Settings' tab.

Upon clicking the link the applicant will be taken to the user registration form.



Certificate Manager

User Registration

Code: *

Email: *

Certificate Type:

PIN: i

Re-type PIN:

Self Enrollment Passphrase: * i

Re-type Self Enrollment Passphrase: *

Select address fields to remove from the certificate.

| Address as it will appear in certificate | Remove |
|--|--------------------------|
| Address1: <input type="text" value="100, Raleigh Street"/> | <input type="checkbox"/> |
| Address2: <input type="text"/> | <input type="checkbox"/> |
| Address3: <input type="text"/> | <input type="checkbox"/> |
| City: <input type="text" value="Riverdale"/> | <input type="checkbox"/> |
| State or province: <input type="text" value="Alabama"/> | <input type="checkbox"/> |
| Postal Code: <input type="text" value="123456"/> | <input type="checkbox"/> |
| Employee ID: * <input type="text"/> | |

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.

| Form Element | Type | Description |
|---|------------|---|
| Code (required) | Text Field | The validation request code. This field is auto-populated when the applicant clicks the validation link contained in the email. |
| Email (required) | Text Field | Email address of the applicant. This field is auto-populated. |
| PIN (required) | Text Field | The applicant should specify a PIN for the certificate to protect the certificate. |
| Re-type PIN (required) | Text Field | Confirmation of the above. |
| Pass-Phrase (required) | Text Field | The end-user needs to enter a pass-phrase for their certificate. This phrase is needed to revoke the certificate should the situation arise. |
| Select address fields to remove from the certificate (optional) | Checkboxes | By default, the address details are displayed in the View Certificate Details dialog. The applicant can hide these details selectively in the View Certificate Details dialog by selecting the 'Remove' checkboxes beside the required address fields. Click here for more details. |
| EULA Acceptance (required) | Checkbox | Applicant must accept the terms and conditions before submitting the form. |
| Submit | Control | Submits the application. |
| Cancel | Control | Clears all data entered on the form |

Selecting Address Fields to be Removed from the Certificate

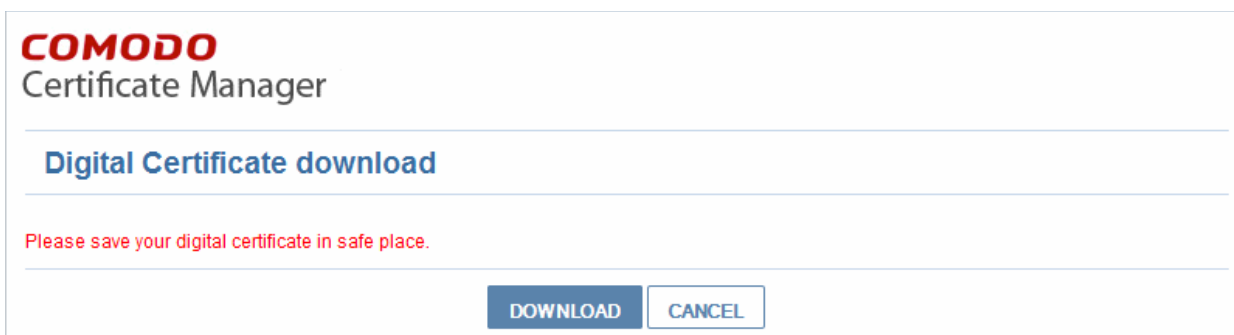
The following address fields...

- Address1;
- Address2;
- Address3;
- City;
- State/Province;
- Postal Code.

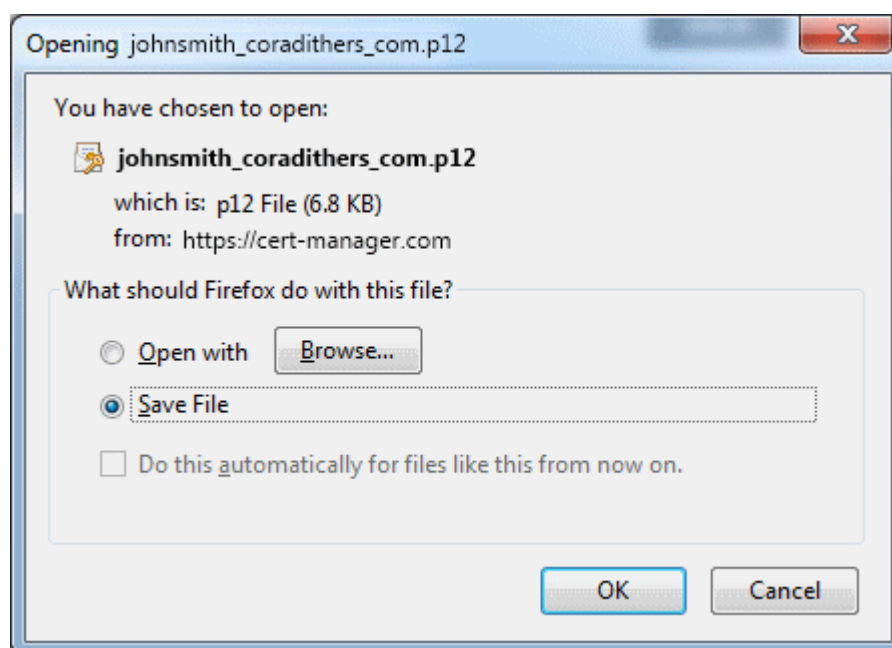
...are automatically populated with the address details of the Organization or Department that the user belongs to. The applicant can choose to remove these details from the client certificate by selecting the 'Remove' checkboxes below beside the corresponding field. The selected details will not be included in the certificate that is issued. The 'View Certificate Details' dialog will state 'Details Omitted' next to these fields.

3.2.5.3.5 Certificate Collection

Upon successful submission of the Account Validation form, a download dialog will be displayed enabling the applicant to download and save the certificate.



The applicant can collect the certificate by clicking 'Download' and save the file in a safe location in his/her computer.



CCM will deliver the certificate to the end-user in PKCS#12 file format (.p12 file). The pass-code specified in the PIN fields is used to protect access to this .p12 file. The end-user will be asked for this PIN when he/she imports the certificate into the certificate store of their machine.

See section '[The Client Certificates Area](#)' for more information regarding end-user and client certificate management.

3.2.6 Revocation of Client Certificates

The client certificates belonging to any end-user can be revoked by two ways:

- The Administrator can revoke the client certificate belonging to any end-user, from the Certs dialog accessible by clicking [Certificates Management](#) > [Client Certificates](#) > clicking [Certs](#) button at the top after selecting the checkbox beside the end-user's name. See the section '[Certs' Dialog](#)' for more details;
- The end-user can directly revoke their client certificate. See the section [Revocation of Client Certificates by End-Users](#) for more details.

3.2.6.1 Revocation of Client Certificates by End-Users

End-users can revoke their client certificates on their own, when a necessity arises. On such an occasion, the end-user can request the administrator. The Administrator can direct the end-user to access the revocation interface hosted at <https://cert-manager.com/customer/Comodo/S/MIME?action=revoke>. The pass-phrase set for the certificate is required for revoking the certificate by the end-user.

3.2.6.1.1 Procedure Overview

1. The end-user requests for access to the self revocation interface to the Administrator.
2. The Administrator directs the end-user to the revocation interface hosted at [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/S/MIME?action=revoke](https://cert-manager.com/customer/[REAL CUSTOMER URI]/S/MIME?action=revoke)
3. The end-user accesses the revocation interface and fills the revocation form with the email address and the pass-phrase set by him/her during self-enrollment or User Registration and submits the form.
4. The client certificate is revoked.

3.2.6.1.2 Revocation form

COMODO
Certificate Manager

S/MIME Certificate Revocation

Email: *

Self Enrollment Passphrase: *

3.2.6.1.3 Form Parameters

| Form Element | Type | Description |
|------------------------|------------|---|
| Email (required) | Text Field | The end-user should enter their full email address. |
| Pass Phrase (required) | Text Field | The end-user should enter the pass-phrase of the client certificate. This Pass-phrase must be the same as entered during self enrollment or in the User Registration form . |
| Revoke | Control | Revokes the certificate |
| Cancel | Control | Cancel the process. |

3.2.7 Viewing End-User's Certificate

Administrators can view the certificates applied for, downloaded by or issued to the end-users from the Client Certificates area.

Selecting the person whose certificate is to be viewed and clicking the 'Certs' button at the top will open the 'Certificates for...' dialog.

Certificates for: johnsmith@coradithers.com

Filter

Send Invitation Invitation not sent View Revoke

| | ORDERED | REVOKED | EXPIRES | CERTIFICATE TYPE | ORDER NUMBER | SERIAL NUMBER | |
|----------------------------------|------------------|------------------|------------|-----------------------------|--------------|-------------------|-------|
| <input type="radio"/> | 03/19/2015 10:36 | 03/30/2015 11:11 | 03/19/2016 | High Persona Validated Cert | 1305101 | 38:D4:BE:81:BE:F | Revok |
| <input type="radio"/> | 03/25/2015 16:01 | 03/30/2015 11:11 | 03/25/2016 | High Persona Validated Cert | 1308491 | 66:A2:E4:63:34:C | Revok |
| <input checked="" type="radio"/> | 03/30/2015 11:46 | | 03/30/2016 | High Persona Validated Cert | 1311952 | 1A:74:23:8A:54:8! | Down |
| <input type="radio"/> | 03/30/2015 13:28 | | 03/30/2016 | High Persona Validated Cert | 1312005 | 76:DB:5D:33:CB:! | Down |

15 rows/page 1 - 4 out of 4

Close

- Select the certificate that you want to view the details and click the 'View' button at the top.

Client Certificate: John Smith <johnsmith@coradithers.com>
✕

State **Downloaded**

Ordered **03/30/2015**

Type **static High Persona Validated Cert**

Certificate Term **1**

Cert subject **John Smith <johnsmith@coradithers.com>**

Principal Name

Address1 **Raleigh Street**

Address2

Address3

City **Riverdale**

State/Province **Alabama**

Postal Code **1234**

Collected **03/30/2015**

Revoked

Expires **03/30/2016**

Order Number **1311952**

Serial Number **1A:74:23:8A:54:85:7A:6F:23:CD:89:28:99:48:B0:45**

Key Escrow **No recovery**

Employee ID **123**

Close

| Client Certificate 'View' Dialog - Table of Parameters | | |
|--|------------|--|
| Field | Type | Description |
| State | | Indicates the current status of the certificate. |
| | Invited | The end-user has been sent an invitation email by the Administrator |
| | Requested | The request has been sent to the Certificate Authority (CA) for approval. |
| | Applied | The end-user has validated the email and applied for the certificate. |
| | Issued | The certificate was issued by CA and collected by Certificate Manager. A Blue font color (Issued) means that the certificate was issued by CA but was not installed. |
| | Downloaded | The end-user has downloaded the certificate. |
| | Revoked | The certificate in question is invalid because it was revoked . |
| | Expired | The certificate in question is invalid because it's term has expired. |
| | Rejected | CA rejected the request after validation check. |
| Ordered | Numeric | Date of the request made by CCM to CA |

| Client Certificate 'View' Dialog - Table of Parameters | | |
|---|-------------|---|
| Field | Type | Description |
| Type | Text Field | Type of the client certificate, prefixed with the customer name. |
| Certificate Term | Text Field | The life term of the certificate |
| Cert subject | Text Field | Name and email address of the end-user |
| Principal Name | Text Field | Principal name included in the certificate |
| Address 1: Address 2: Address 3: City: State or Province: Postal Code: | Text Fields | Displays the address of the Organization as mentioned while requesting for the certificate. Only those address fields that were allowed to be displayed while applying for the certificate are shown here and the rest of the fields are displayed as "Details Omitted". |
| Collected | Numeric | Date of the collection of certificate by CCM from CA |
| Revoked | Numeric | Date of the revocation of the certificate |
| Expires | Numeric | Expiry date of the certificate. |
| Order Number | Numeric | Order number of the certificate request made to CA. |
| Serial Number | Numeric | Serial number of the certificate. |
| Key Escrow | | Indicates whether Key Escrow is available for certificate recovery by the administrator. |

3.3 The Code Sign Certificates Area

The Code Signing Certificates area provides administrators with the information and controls necessary to issue and manage the life-cycle of code signing certificates for their respective Organization/Department.

Visibility of the 'Code Signing Certificates' area is restricted to:

- MRAO administrators - can request, issue and manage the code signing certificates and their end-users of any Organization or Department.
- RAO Code Signing administrators - can request, issue and manage the code signing certificates and their end-users of Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Code Signing administrators - can request, issue and manage the code signing certificates and their end-users of Departments that have been delegated to them.

Note: Comodo also offer the ability for companies to simplify the code signing process using our **Code Signing on Demand** service. The service is available in both hosted and cloud versions can sign .EXE, .DLL, .CAB, .MSI, .JS, .VBS, .PS1, .OCX, .SYS, .WSF, .CAT, .MSP, .CPL, .EFI. formats. Please contact your account manager if you wish to enable this feature.

| NAME | EMAIL | ORDER NUMBER | STATE | ORGANIZATION | DEPARTMENT | EXPIRES | CODE SIGNING ON DEMAND |
|------------------|-------------------------|--------------|--------|------------------------------|------------|------------|-------------------------------------|
| Alfred | alfred@dithercons.com | 1502130 | Issued | Dithers Construction Company | | 11/18/2016 | <input type="checkbox"/> |
| Bumpsted Dagwood | bumpsted@dithercons.com | 1501523 | Issued | Dithers Construction Company | | 11/17/2016 | <input checked="" type="checkbox"/> |

Code Sign Certificates area - Table of Parameters

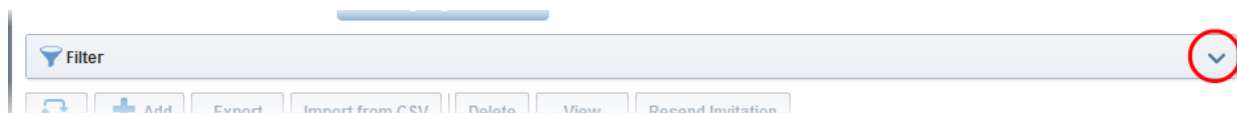
| Field Name | | Description |
|---------------------|------------|--|
| Name | | Name of the applicant/developer |
| Email | | Email address of the applicant/developer |
| Order Number | | Order number of the certificate request made to CA. |
| State | | Indicates the current status of the certificate. |
| | Init | Applies only for Code Signing certificates added for Code Signing on Demand (CSD) service. Indicates that the process for issuing the certificate for the developer has been initiated by the agent. |
| | Invited | The applicant has been sent an invitation email by the Administrator |
| | Requested | The request has been sent to the Certificate Authority (CA) for approval. |
| | Applied | The applicant has validated the email and applied for the certificate. |
| | Issued | The certificate was issued by CA and collected by Certificate Manager, but not downloaded by the applicant. For the certificates issued for CSD, the agent will automatically download the certificate. |
| | Downloaded | The applicant has downloaded the certificate. |
| | Revoked | The certificate in question is invalid because it was revoked . |
| | Expired | The certificate in question is invalid because it's term has expired. |
| | Rejected | CA rejected the request after validation check. |
| Organization | | Name of the Organization to which the applicant belongs. |
| Department | | Name of the Department to which the applicant belongs. |
| Expires | | Expiry date of the certificate. |
| Code | | Indicates whether the certificate is enrolled for CSD service or not. |

| Code Sign Certificates area - Table of Parameters | | |
|---|-------------------|---|
| Field Name | | Description |
| Signing on Demand | | Note: This column is displayed only if Code Signing on Demand is enabled for your account. |
| Control Buttons | Add | Allows the administrator to add new end-user for the process of issuing code signing certificate |
| | Export | Allows administrators to save the list of code signing certificates in CSV format |
| | Import from CSV | Allows administrators to import a list of code signing certificates into Comodo CM in comma separated values (.csv) format. |
| | Refresh | Updates the currently displayed list of users. Will remove any users that have been recently deleted and add any that have been recently created. Will update details such as Organization, email etc if those details have recently changed. |
| Certificate Control Buttons Note: The types of certificate control buttons that are displayed above the table header depends on the state of the selected certificate | View | Allows to view information about the certificate (see Code Sign certificate "View" dialog description) |
| | Resend Invitation | Re-sends the invitation email to the applicant (thus validating the applicant's email address and enabling them to request their certificate) |
| | Revoke | Revokes the certificate. |
| | Delete | Deletes the certificate. |

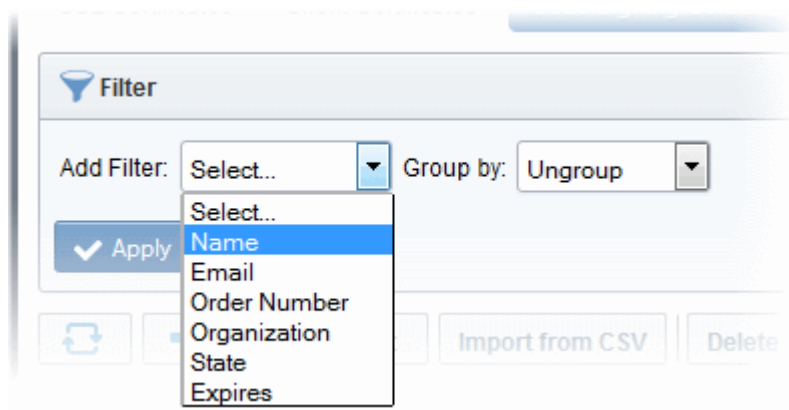
3.3.1 Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular code signing certificate by using filters.

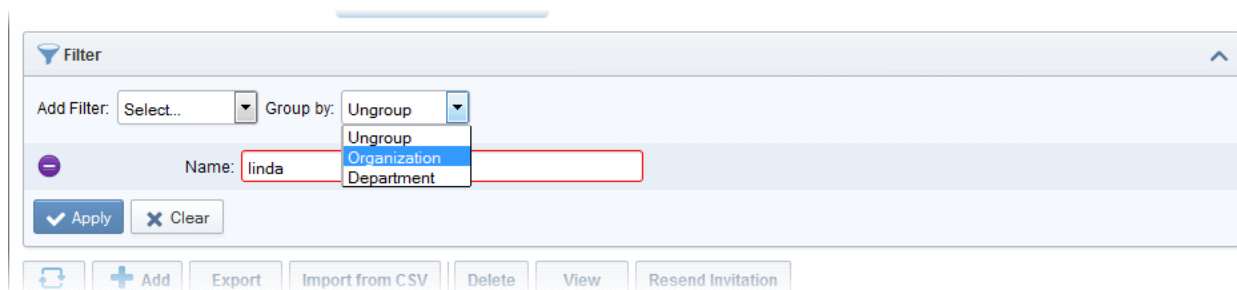


To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



For example, if you want to filter the certificates with 'Name' and group with 'Organization', select 'Name' from the 'Add Filter' drop-down:

- Enter part or full name in the Name field.
- Select 'Organization' from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed.

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Code Signing Certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

3.3.2 Code Sign Certificates View Dialog

Clicking the 'View' button after selecting a certificate listed in the Code Sign Certificates tab will open a panel containing a summary of that certificate's details.

Code Signing Certificate ✕

Name **Bumpsted Dagwood**

State **Issued**

Order Number **1501523**

Email **bumpsted@dithercons.com**

Contact email

Organization **Dithers Construction Company**

Term **1 year**

Invited

Requested **11/17/2015**

Collected **11/17/2015**

Downloaded

Expires **11/17/2016**

Serial Number **C7:F0:F5:7E:46:B5:6B:6A:0D:9C:D2:B0:36:66:53:96**

Suspend Notifications

Close

| Code Sign Certificate 'View' Dialog - Table of Parameters | | |
|---|------------|--|
| Field Element | Type | Description |
| Name | Text Field | Name of the applicant. |
| State | | Indicates the current status of the certificate. |
| | Invited | The applicant has been sent an invitation email by the Administrator |
| | Requested | The request has been sent to the Certificate Authority (CA) for approval. |
| | Applied | The applicant has validated the email and applied for the certificate. |
| | Issued | The certificate was issued by CA and collected by Certificate Manager, but not downloaded by the end-user. |
| | Downloaded | The end-user has downloaded the certificate. |
| | Revoked | The certificate in question is invalid because it was revoked . |
| | Expired | The certificate in question is invalid because it's term has expired. |
| | Rejected | CA rejected the request after validation check. |
| Order Number | Numeric | Order number of the certificate request made to CA. |
| Email | Text Field | End-user's email address. |
| Contact Email | Text Field | Contact email address or alternative email address of the applicant. The contact email address may be the customer facing email address like |

| Code Sign Certificate 'View' Dialog - Table of Parameters | | |
|---|------------|---|
| | | support@company.com, sales@company.com etc. |
| Organization | Text Field | Name of the Organization to which the end-user belongs. |
| Term | Numeric | The life term of the certificate |
| Invited | Numeric | Date at which invitation was sent to the end-user |
| Requested | Numeric | Date of the request made by CCM to CA |
| Collected | Numeric | Date of the collection of certificate by CCM from CA |
| Downloaded | Numeric | Date of download of certificate by the end-user |
| Expires | Numeric | Expiry date of the certificate. |
| Serial Number | Numeric | The serial number of the certificate as assigned by the CA. |
| Suspend Notifications | Checkbox | Selecting this checkbox will disable all the automated notifications for events like certificate download, expiry, revocation from the CCM to the administrator and the end-user, for this certificate. |

3.3.3 Adding Certificates to be Managed

There are several methods of adding certificates to the Code Sign Certificates area of Certificate Manager.

- **Manually adding certificates**
- **Loading multiple certificates from a comma separated values (.csv) file**
- **Auto Creation of end-users by initiating self enrollment**

3.3.3.1 Manually Adding Certificates

The code signing certificates for both 'Code Signing on Demand' (CSD) and manual signing can be added from the 'Certificates' > 'Code Signing Certificates' interface.

- Click 'Certificates' > 'Code Signing Certificates'
- Click the 'Add' button to open the 'Add New Code Signing Certificate' form.

Add New Code Signing Certificate

*-required fields

Organization

Department

Domain

Email Address* @dthercons.com

Term

Full Name*

Contact email

Code Signing on Demand

Signature Algorithm

Key Size

Subscriber Agreement

EULA

I agree.* *Scroll to bottom of the agreement to activate check box.*

| Add New Code Signing Certificate dialog - Table of parameters | | |
|---|------------|--|
| Field | Type | Description |
| Organization | Drop-down | Select the Organization to which the applicant belongs. |
| Department | Drop-down | Select the Department to which the applicant belongs. |
| Domain | Drop-down | Select the domain pertaining to the Department |
| Term | Drop-down | Select the term of the certificate. |
| Email Address | Text field | Enter the email address of the applicant. |
| Full Name | Text field | Full name of the applicant. |
| Contact Email | Text field | Enter the contact email address of the applicant that should be included in the certificate. The contact email address may be the customer facing email address like support@company.com, sales@company.com etc. |
| Code Signing on Demand | Checkbox | Select this checkbox, if you wish to issue this certificate to the developer for Code Signing on Demand (CSD). Prerequisites: <ul style="list-style-type: none"> The Comodo Code Signing service should have been setup for your account The applicant should have been added as a 'Developer' to CCM. Refer to the next chapter Code Signing on Demand for more details. Note: This option will be available only if CSD service is enabled for your account. |
| Signature Algorithm | Drop-down | Appears only if 'Code Signing on Demand' is selected. Choose the signature algorithm to be used by the certificate. |
| Keysize | Drop-down | Appears only if 'Code Signing on Demand' is selected. Choose the key-size (in bits) by the certificate. |
| Subscriber Agreement | Text field | Appears only if 'Code Signing on Demand' is selected. Displays the End-User License Agreement (EULA) for the certificate. Read through the EULA and accept to it by selecting the 'I agree' checkbox for the application to proceed. |

- Complete the 'Add New Code Signing Certificate' form.
- Click 'OK'.

If the applicant is an existing user, the corresponding certificate will be automatically added to CCM. If the applicant is a new user, an invitation mail will be sent to initiate self enrollment process. Refer to **Request and issuance of code signing certificates** for more details on self enrollment.

3.3.3.2 Loading Multiple Certificates from a Comma Separated Values (.csv) File

Administrators can import a list of code signing certificates into Comodo CM in comma separated values (.csv) format. After importing the list, the certificates belonging to existing users will be automatically added and invitation emails will be sent to new users automatically to initiate the self enrollment process, Refer to **Request and issuance of code signing certificates** for more details on self enrollment.

Note: Only the certificates for manual signing can be added by importing the users from a .csv file. The developers for issuance of certificates for Code Signing on Demand cannot be imported from a .csv file.

3.3.3.2.1 Procedure Overview

Summary of required steps for adding certificates by loading a .csv file:

1. Administrator generates a .csv file using containing a list of the certificates. .csv files can be exported directly from spreadsheet programs such as Excel or Open Office Calc.
2. Administrator loads the .csv file to CCM by clicking 'Load from CSV' in 'Certificates Management' > 'Code Sign Certificates' interface.

3.3.3.2.2 Requirements for .csv file

- There are 6 potential values per certificate that can be imported in CCM, but 4 are mandatory. As long as each user listed in the .csv file has at least these four elements then they can be added into the system.
- The 6 potential values are as follows. Mandatory values are highlighted in red. Make sure to export with the commas (,) and the quotation marks (") as specified below
 "Organization", "Department", "Term", "Email Address", "Full Name", "Contact Email Address"
- The following table explains the requirements and formats of the values.

| Values | Organization | Department | Term | Email Address | Full Name | Contact Email Address |
|-------------------------|--------------|------------|----------|-----------------------------------|------------------------------|-----------------------------------|
| Required | Yes | No | Yes | Yes | Yes | No |
| Min Length (characters) | 1 | 0 | 1 | 3 | 1 | 3 |
| Max Length (characters) | 128 | 128 | 1 | 128 | 64 | 128 |
| Format | | | integer | Valid email address | Valid name | Valid email address |
| Characters allowed | ANY | ANY | 01/05/10 | A-Z, a-z, 0-9, '!', ' ', '_', '@' | A-Z, a-z, 0-9, '!', ' ', '_' | A-Z, a-z, 0-9, '!', ' ', '_', '@' |

Example:

"Test Organization", "Test Department", "1", "jsmith@example.org", "JOHN SMITH", "jsmith@alternativeemail.com"

3.3.3.2.3 Uploading .CSV File

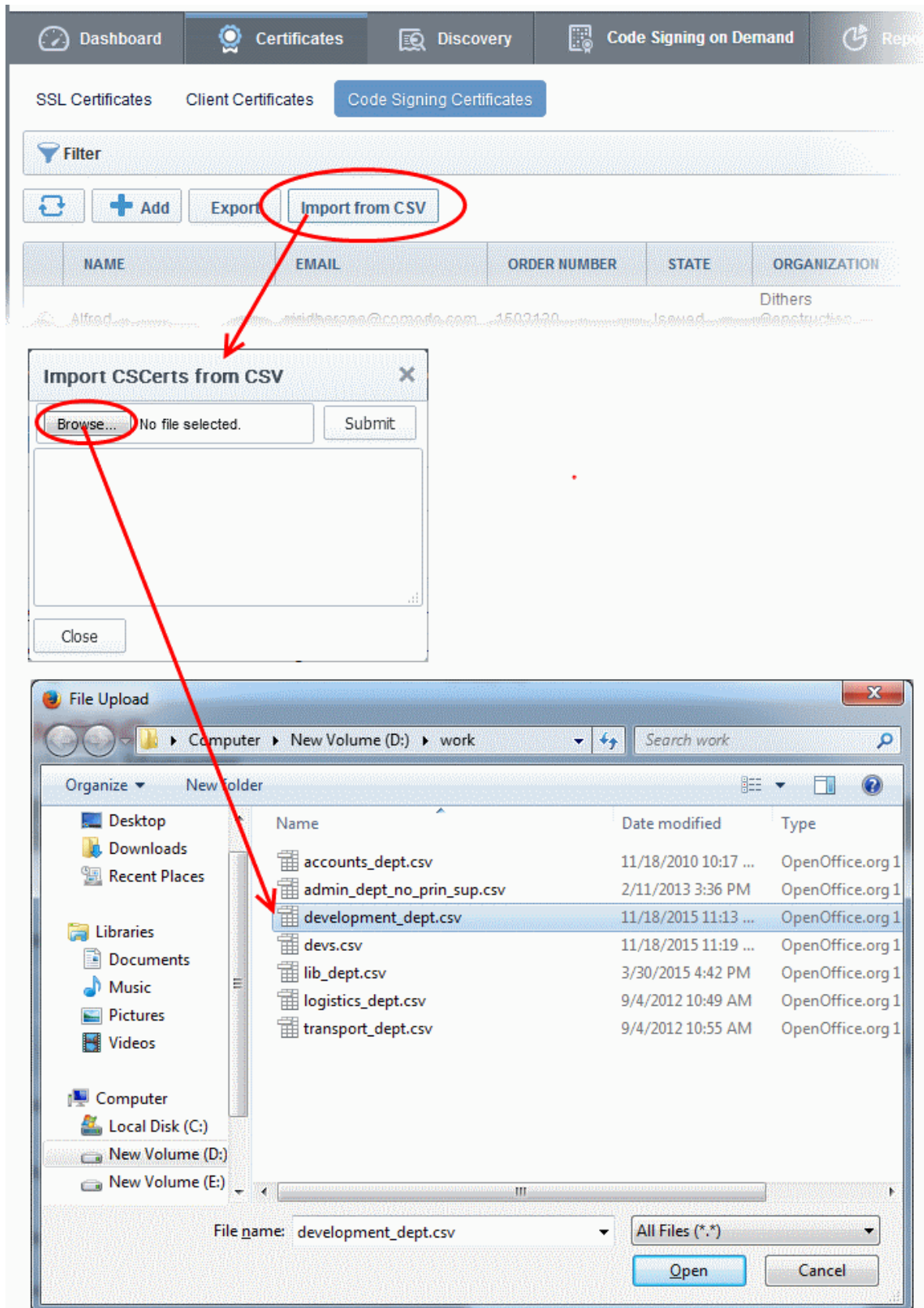
The CSV file containing the list of users in the format described in the section **above**, can be uploaded to CCM, for importing the applicants from it.

To upload the .csv file

- Click the 'Import from CSV' button above the table header in the 'Certificates' > 'Code Signing Certificates' interface.

The 'Import CSCerts from CSV' dialog will appear.

- Click the 'Browse' button, and navigate to the in .csv file, and click on 'Submit'.



An import status dialog box is displayed. You will see a progress bar indicating that information is being uploaded. On successful completion, all the imported data will appear in the list of certificates in 'Code Sign Certificates' and 'Organization' areas.



3.3.3.3 Auto Creation of End-Users by Initiating Self Enrollment

Certificates issued to end-users by the self enrollment process initiated by an Administrator are automatically added to the 'Certificate Management - Code Sign Certificates' area. For more details see: [Request and issuance of code signing certificates](#).

3.3.4 Request and Issuance of Code Signing Certificates

3.3.4.1 Prerequisites

- The domain for which the code signing certificate is to be issued has been enabled for Code Signing certificates, has been pre-validated by Comodo and that the domain has been made activated by your Comodo account manager. (i.e. if you wish to issue code signing certs to end-user@mycompany.com, then mycompany.com must have been pre-validated by Comodo.) All certificate requests made on 'pre-validated' domains or sub-domains thereof are issued automatically.

However, if you request a certificate for a brand new domain, then this domain will first have to undergo validation by Comodo. Once validated, this new domain will be added to your list of pre-validated domains and future certificates will be issued immediately.

- The domain from which the client certificates are to be issued has been delegated to the Organization or Department. See [Creating a New Organization](#) and [Editing an Existing Organization](#) for more details on adding a domain to an Organization.
- The RAO Code Signing or DRAO Code Signing administrator has been delegated control of this Organization or Department
- The MRAO or delegated RAO administrator has enabled Code Signing Certificates for the Organization by selecting the 'Enabled' checkbox in the '[Code Signing tab](#)' of the 'Add New/Edit' Organizations dialog box (see screen-shot below)

The screenshot shows a dialog box titled "Edit Organization: ABCD Company" with a close button (X) in the top right corner. Below the title bar is a tabbed interface with six tabs: "General", "EV Details", "Client Certificate", "SSL Certificate", "Code Signing Certificate" (which is selected and highlighted), and "Email Template". A yellow highlighted box contains the text: "When checkbox is selected 'Code Signing' certificates could be enrolled for this particular Organization or Department." Below this box is a light gray area containing the text "Enabled" followed by a checked checkbox. At the bottom of the dialog are two buttons: "OK" and "Cancel".

3.3.4.2 Procedure Overview

The Code Signing Certificates can be provisioned to the employees and end-users using a self-enrollment process.

Overview of stages:

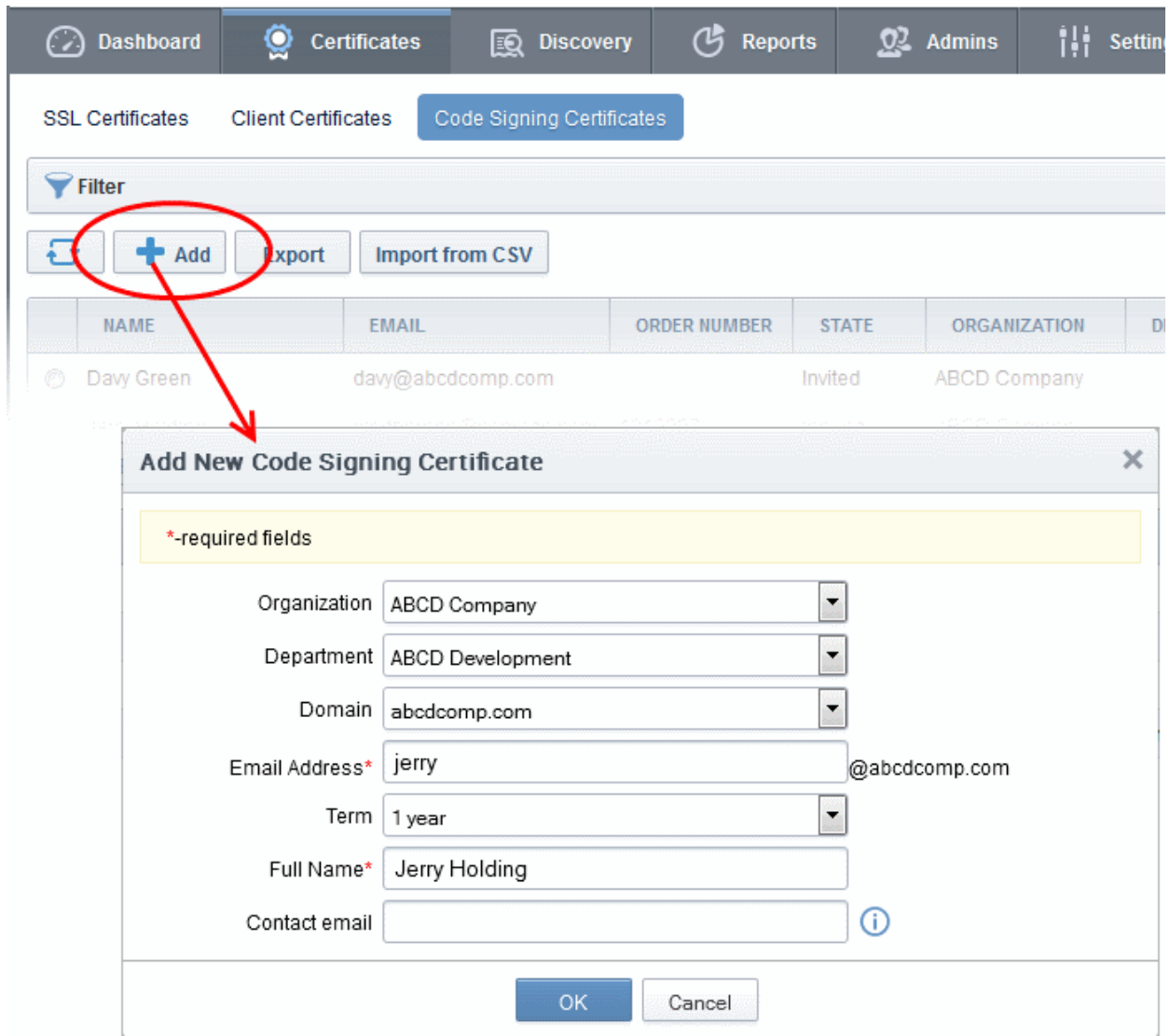
1. The administrator confirms the completion of the **prerequisite steps**.
2. The administrator sends an invitation email to the end-user for enrollment.
3. End-user validates the email address, completes the online form for auto-generation of CSR and requests for the certificate.
4. The certificate request is sent to Comodo CA servers by CCM.
5. If the application is successful, CCM sends an email with a download link to the end-user, enabling to download the certificate.
6. The certificate will be automatically added to the end-user account in CCM and will be manageable from the 'Code Sign Certificates' area.

3.3.4.3 Initiating the Enrollment Process

After completing the **prerequisite steps**, Administrators need to send an invitation to the end-user.

To send invitation and initiate the process

- Click the Add button from the 'Code Sign Certificates' area. This will open 'Add New Code Signing Certificate' dialog.



| Add New Code Signing Certificate dialog - Table of parameters | | |
|---|------------|--|
| Field | Type | Description |
| Organization | Drop-down | Select the Organization to which the applicant belongs. |
| Department | Drop-down | Select the Department to which the applicant belongs. |
| Domain | Drop-down | Select the domain pertaining to the Department |
| Term | Drop-down | Select the term of the certificate. |
| Email Address* | Text field | Enter the email address of the applicant. The invitation message will be sent to this address. This will be validated before commencing the request process. |
| Full Name* | Text field | Enter the Full name of the applicant. |
| Contact Email | Text field | Enter the contact email address of the applicant that should be included in the certificate. The contact email address may be the customer facing email address like support@company.com, sales@company.com etc. |

Fields marked with * are mandatory.

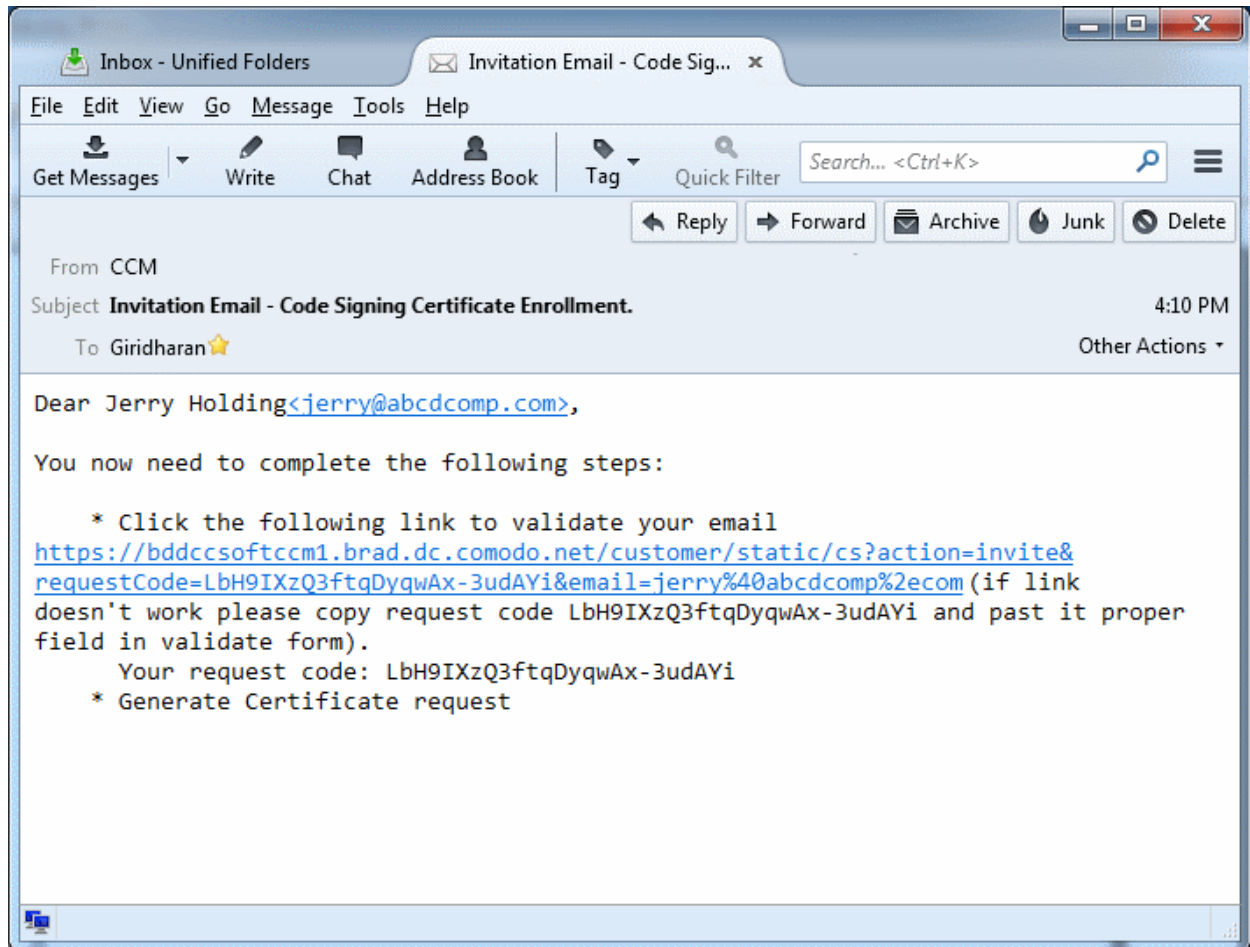
- Fill the necessary details and click 'OK'.

An invitation email will be automatically sent to the applicant. The certificate status will be set to 'INVITED' and added to 'Code Signing Certificates' area of CCM.

Note: For the new applicants added by **importing a .csv file**, the invitations will be sent automatically.

3.3.4.4 Validation of Email address and Requisition

The applicant will receive an invitation email with a link to validate his/her email address. An example is shown below.



Note: It is possible for administrators to modify the contents of these emails in the 'Email Templates' area under the 'Settings' tab.

Upon clicking the link in the mail, the email address will be validated and the applicant will be taken to user registration page.

COMODO

Certificate Manager

User Registration

Code: *

Email: *

Private Key Options

Key Size (bits):

Subscriber Agreement:

CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS PRESENTED HEREIN. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR CREATE A CERTIFICATE MANAGER ACCOUNT OR USE OR ACCESS CERTIFICATE MANAGER AND CLICK "DECLINE" BELOW.

The terms and conditions set forth below (the "Agreement") constitute a binding agreement between you (the "Company" or "you") and Comodo CA Limited ("Comodo") with respect to your or your employee's creation and use of your Certificate Manager account and the related

PRINT

I Agree*

Scroll to bottom of the agreement to activate check box.

When you click the button below, your browser will generate a new private key.

GENERATE

Form Parameters


| Form Element | | Type | Description |
|------------------------------|----------|------------|---|
| Code (<i>required</i>) | | Text Field | The Code field will be auto-populated with the certificate request code, on clicking the validation link in the email. If not, the end-user can copy the request code from the email and paste in this field. |
| Email (<i>required</i>) | | Text Field | The email address of the applicant. This field will be auto-populated. |
| Advanced Private Key Options | CSP | Drop Down | The applicant can select the cryptographic service provider for the certificate from the drop-down (Default = Microsoft Cryptographic Provider v1.0) |
| | Key Size | Drop Down | The applicant can select the key size for the private key of the certificate (Default = 2048 bit) Note: The private key is generated locally by the crypto module of the browser/ operating system. The key never leaves the computer and no |

| Form Element | Type | Description |
|---|----------|--|
| | | copy is ever transmitted to the certificate issuer. Comodo does not collect a copy of the private key at any time and cannot be recovered if it is lost. The certificate is useless without it. Hence the end-users are strongly advised to backup their private key, during certificate installation process. |
| Exportable | Checkbox | The applicant can choose whether or not the certificate is exportable. |
| User Protected | Checkbox | If enabled, you will be asked to set password and security levels during the certificate collection process. Windows will prompt you for a password and/or your permission every time you access your certificate to code sign. |
| Subscriber Agreement (<i>required</i>) | Checkbox | Applicant must accept the terms and conditions before submitting the form. |
| Generate | Control | Starts the certificate generation process. |

The applicant needs to fill-in the form, accept to the subscriber agreement by reading it and selecting the checkbox 'I Agree' and click the 'Generate' button. The certificate request will be automatically generated and a request will be sent to CCM.

COMODO
Certificate Manager

Info



Your application was accepted, you will be notified by email when your certificate is ready for collection

The certificate status will be set to 'REQUESTED' in the Code Sign Certificates area. CCM will process the request and send a certificate request to Comodo CA Server. The certificate status will be set to 'APPLIED'

3.3.4.5 Downloading and Installing the Certificate

The CCM will collect the certificate from the server and send a notification mail to the applicant with a link to download the certificate. The certificate status will be changed to 'ISSUED' in Code Sign Certificates area. The applicant can follow the link and download the certificate. The certificate status will be changed to 'DOWNLOADED' in CCM. The certificate can be installed by the user and used to digitally sign the executables.

3.4 The Device Certificates Area

3.4.1 Overview

The 'Device Certificates' area allows administrators to manage certificates issued to devices that have been enrolled to CCM via Active Directory or self-enrollment. In addition to the request and issuance of device certificates, CCM is capable of issuing certificates from Private Certificate Authorities. Please contact your Comodo account manager to add a Private CA to your CCM account.

Note: Device certificates are not enabled by default. Please contact your Comodo account manager if you would like to add them to your account.

Device certificates can be issued via Active Directory/NDES, SCEP, self enrollment or by API. See '[Request and Issuance of Device Certificates](#)' for more details.

Visibility of the 'Device Certificates' area is restricted to:

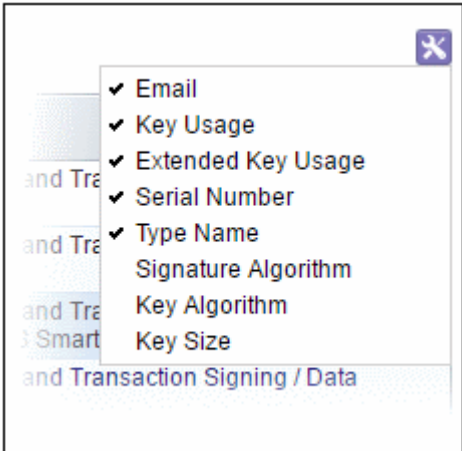
- MRAO administrators - can view device certificates and end-users of any Organization or Department.
- RAO Device Cert administrators - can view the device certificates of Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO Device Cert administrators- can view the device certificates of Departments that have delegated to them.

| COMMON NAME | ORDER NUMBER | EMAIL | STATUS | ORGANIZATION | DEPARTMENT | EXPIRES | KEY USAGE |
|--------------------------------------|--------------|------------------|------------|------------------------------|------------|------------|-------------------|
| comodo.com | 61025783 | admin@comodo.com | Issued | Diflers Construction Company | | 04/11/2019 | Digital Signature |
| comodotest | 60316903 | admin@comodo.com | Downloaded | Comodo SE | SE Support | 04/08/2018 | Digital Signature |
| comodotest | 60312986 | admin@comodo.com | Downloaded | Comodo SE | SE Support | 04/08/2018 | Digital Signature |
| 98ac1b76-80b7-4a77-89c7-a3920a9e1be9 | 55053229 | | Revoked | Comodo SE | | 03/07/2019 | Digital Signature |
| clofcswin10.comododev.com | 53988797 | | Applied | Comodo SE | SE Support | | |
| clofcswin10.comododev.com | 53979940 | | Applied | Comodo SE | SE Support | | |
| clofcsadcs.comododev.com | 53310686 | | Downloaded | Comodo SE | SE Support | 02/25/2018 | Digital Signature |
| clofcswin10.comododev.com | 53304880 | | Downloaded | Comodo SE | SE Support | 02/25/2018 | Digital Signature |
| clofcswin10.comododev.com | 53303738 | | Downloaded | Comodo SE | SE Support | 02/25/2018 | Digital Signature |

'Device Certificates' table

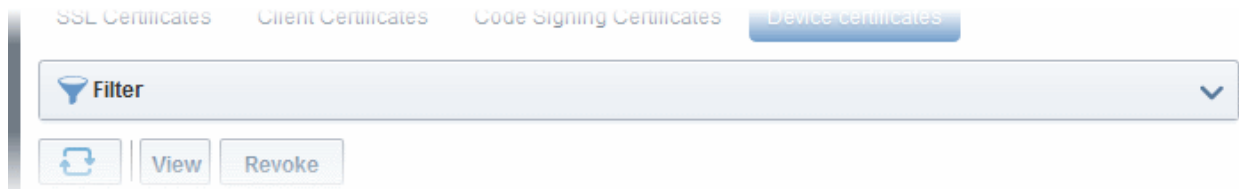
| Column Name | Description |
|-------------------|--|
| Common Name | The name of the device for which the certificate was issued . The device name is used as the 'Common Name' in the Device Certificate itself. |
| Order Number | The order number of the certificate. |
| Email | The email address of the applicant that was provided during self-enrollment. |
| Status | The current status of the certificate: |
| Awaiting Approval | A device certificate request has been placed with CCM using the self-enrollment method. |
| Requested | A device certificate request has been placed with CCM by either (i) the MS Agent installed on the AD server to which the device is enrolled (ii) by the device through SCEP or (iii) through an API call by the Mobile Device Manager (MDM) software used by the Organization. Administrators can "View", "Edit", "Approve", "Decline" or 'Revoke' the request. |

| 'Device Certificates' table | | |
|---|------------|---|
| Column Name | | Description |
| | Declined | A certificate request that was made using the Self Enrollment Form has been rejected by one of the following: <ul style="list-style-type: none"> • An MRAO - can decline any certificate requests from any Organization or Department • An RAO Device Cert administrator can decline certificate requests for Organizations over which they have been delegated control. • An DRAO Device Cert administrator can decline certificate requests for Departments over which they have been delegated control. |
| | Applied | The request has been approved and sent to Comodo CA. |
| | Issued | The certificate has been issued by Comodo CA and collected by CCM. |
| | Downloaded | The certificate has been downloaded by the MS agent or the device. |
| | Expired | The certificate is invalid because its term has expired. |
| | Revoked | The certificate is invalid because it was revoked. |
| | Rejected | The certificate request was declined by the administrator. |
| Organization | | Name of the Organization that the certificate belongs to. |
| Department | | Name of the Department that the certificate belongs to (if applicable) |
| Expires | | Expiration date of the certificate. |
| Key Usage | | Indicates the purposes of the certificate. Purposes include signing, non repudiation, authentication, encryption and more. |
| Extended Key Usage | | Indicates the extended capabilities of the certificate. |
| Serial Number | | Unique number which identifies the certificate. |
| Type Name | | The name of the device certificate. |
| <p>Note: The administrator can add more column headers from the drop-down button beside the last item in the column:</p> | | |

| 'Device Certificates' table | | |
|--|------------------------|--|
| Column Name | | Description |
| | |  |
| Signature Algorithm | | Displays the signature algorithm of the public key of the certificate. |
| Key Algorithm | | Displays the type of algorithm used for the encryption. |
| Key Size | | Displays the key size used by certificate for the encryption. |
| Control Buttons | Refresh | Updates the currently displayed list of certificates.. |
| Certificate Control Buttons Note: The types of certificate control buttons that are displayed in the table header depends on the state of the selected certificate | View | Displays a summary of details about the selected certificate. (see the description under 'Viewing Device Certificate Details'). |
| | Approve / Decline | Enables administrators to approve or decline the certificate request via self enrollment. |
| | Revoke | Enables administrators to revoke the certificate. |
| | Resend Collection Link | Enables administrators to resend the device certificate collection email. See section ' Resending Device Certificate Collection Email ' for more details. |

3.4.1.1 Sorting and Filtering Options

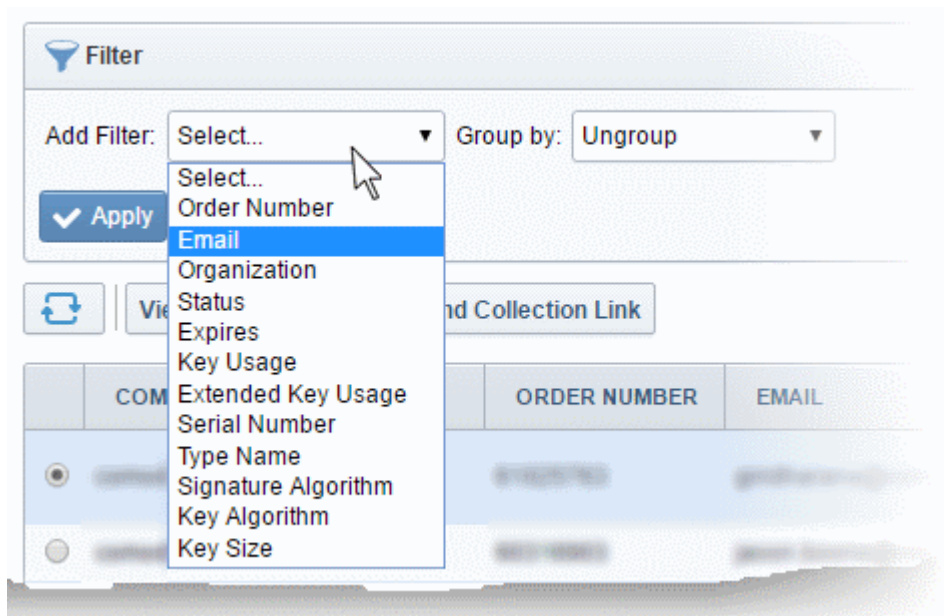
- Clicking on any column header except the 'Common Name' sorts items in alphabetical order.
- Administrators can search for particular device certificates using filters.



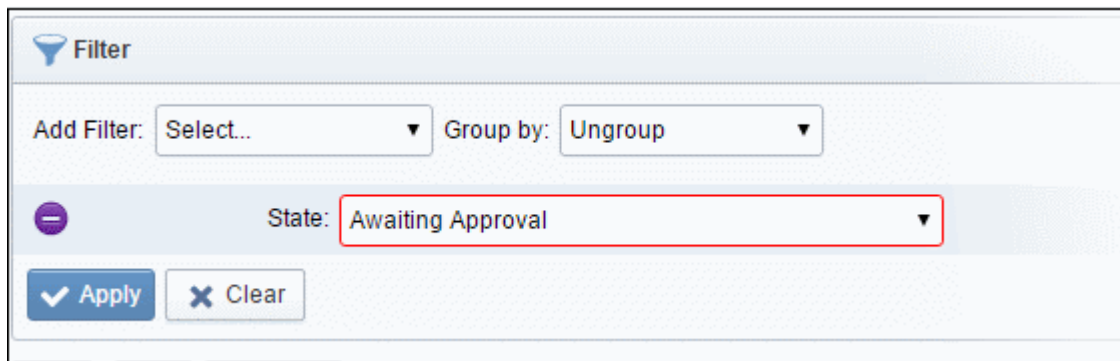
To apply filters, click anywhere on the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the results with other options that appears depending on the selection from the 'Add Filter' drop-down.

To add a filter

- Select a filter criteria from the 'Add Filter' drop-down



- Enter or select the filter parameter as per the selected criteria.



The available filter criteria and their filter parameters are given in the following table:

| Filter Criteria | Filter Parameter |
|-----------------|--|
| Order Number | Search for a particular order number. |
| Email | Find certificates by applicant email address |

| | |
|---------------------|--|
| Organization | Find certificates belonging to a specific Organization and/or Department |
| Status | Filter by certificate status. |
| Expires | Find certificates which expire within a certain number of days. |
| Key Usage | Filter certificates by their key usage capabilities |
| Extended Key Usage | Filter certificates by their extended key usage capabilities |
| Serial Number | Enter the serial number of the certificate in full or part. |
| Type Name | Filter certificates by their type. |
| Signature Algorithm | Filter by signature algorithm of the certificate |
| Key Algorithm | Filter by key algorithm of the certificate |
| Key Size | Filter by key size in bits |

Tip: You can add more than one filter at a time to narrow down your search. To remove a filter criteria, click the '-' button to the left of it.

- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter

For example, if you want to find certificates whose type names start with 'test' and group the results by their 'Status', then select 'Type Name' from the 'Add Filter' drop-down, enter 'test' and select 'Status' from the 'Group by' drop-down.

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you re-open the 'Device certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button before exiting.

3.4.1.2 Viewing Certificate Details

Click the 'View' button after selecting a certificate in the 'Device Certificates' tab to open a panel containing a summary of that certificate's details.

Device Certificate
✕

Details

Email **fiatliena@gmail.com**

State **Downloaded**

Order Number **1676179**

Organization **Bar**

Department

Requested **01/16/2017**

Collected **01/16/2017**

Downloaded **01/16/2017**

Expires **01/17/2019**

Serial Number **08:13:DB:F8:D7:B8:DD:38:44:4D:1C:1F:BB:C4:FF:FD**

Key Usage **Digital Signature
Key Encipherment**

Extended Key Usage **1.3.6.1.5.5.7.3.4
1.3.6.1.5.5.7.3.2**

Optional fields

State or province name **Tamil Nadu**

Country name **IN**

Organization name **Dithers**

Organization unit name **Marketing**

Locality name **Chennai**

Common name **Demo-NDES**

Suspend Notifications

Close

| Device Certificate 'View' Dialog - Table of Parameters | | |
|--|-------------------|---|
| Field Element | Value | Description |
| Name | | The name of the certificate as populated in the Common Name field. |
| State | Awaiting Approval | A device certificate request has been placed with CCM using the self-enrollment method. |
| | Requested | A request has been received for the certificate. Requests need to be approved by the administrator. |
| | Declined | A certificate request that was made using the self-enrollment form has been rejected by an administrator. |
| | Applied | The request has been approved and sent to Comodo CA. |

Device Certificate 'View' Dialog - Table of Parameters

| | | |
|-----------------------|-------------|--|
| | Issued | The certificate has been issued by the CA and collected by CCM. |
| | Downloaded | The certificate has been downloaded by the MS agent or the device. |
| | Expired | The certificate in question is invalid because its term has expired. |
| | Revoked | The certificate in question is invalid because it was revoked . |
| | Rejected | CA rejected the request after a validation check. |
| Order Number | Numeric | Order number of the certificate. |
| Organization | Text Field | Name of the Organization to which the device certificate belongs. |
| Department | Text Field | Name of the Department to which the device certificate belongs. |
| Requested | Numeric | Date the certificate request was sent to Comodo CA from CCM. |
| Collected | Numeric | Date the certificate was collected by CCM from Comodo CA |
| Downloaded | Numeric | Date the certificate was downloaded by the end-user |
| Expires | Numeric | Expiry date of the certificate. |
| Serial Number | Numeric | The serial number of the certificate as assigned by the CA. |
| Key Usage | Text Field | Displays the key usage capabilities |
| Extended Key Usage | Numeric | Displays the extended key usage capabilities |
| Optional fields | Text Fields | Available for certificates applied for via the self-enrollment method. Displays details such as organization name, common name and more. |
| Suspend Notifications | Checkbox | Will disable automatic notifications to administrators and end users for events like certificate download, expiry and revocation. |

3.4.2 Request and Issuance of Device Certificates

Device Certificates can be issued to devices in four ways:

- **Through Active Directory** - The device certificates can be requested for and issued to devices that are enrolled to the Active Directories added to CCM, through Network Device Enrollment Service (NDES). See the section for **Issuance of Device Certificates through Active Directory** more details.
- **Through SCEP** - CCM has the SCEP server integrated. Administrators can push a configuration profile to the devices for enrollment of certificates to CCM. See the section for **Issuance of Device Certificates through SCEP** more details.
- **Through API Integration** - Mobile Device Management (MDM) solutions can be integrated to CCM through API. Administrators can apply configuration profiles to managed devices to enroll for certificates to CCM. For details on API integration refer to the document at https://help.comodo.com/uploads/helpers/CCM_Device_Cert_Enroll_API.pdf
- **Through Self Enrollment** - Device certificates can be requested by applicants using the self-enrollment form. The self-enrollment form will be available by clicking the link provided by an administrator. See **Issuance of Device Certificate through Self-Enrollment** for more details.

3.4.2.1 Issuance of Device Certificates through Active Directory

Prerequisites:

- The Active Directory Certificate Service (AD CS) has been installed on the AD server with NDES role
- The AD server has been added to CCM by installing the MS Agent and must be connected. The Agent must have been enabled as CA Proxy during its installation. Refer to the section for **MS Agents for AD server Integration** more details.
- An RAO/DRAO Device Cert administrator has been delegated control of this Organization or Department

Procedure Overview:

- The AD Domain Administrator creates a Group Policy Object (GPO) with a certificate template and applies to the devices.
- The Devices generate the certificate request and forward them to NDES configured with the MS Agent as CA Proxy.
- NDES forwards the certificate requests to the MS Agent. The Agent creates certificate requests and forwards them to CCM.
- The certificate requests are added to the Certificates > Device Certificates interface for Approval. The state of the certificate will be 'Requested'.
- An MRAO, RAO or DRAO with appropriate privileges approves the request so that CCM forwards the request to Comodo CA. The status of the certificate changes to 'Applied'. Upon issuance of the certificate, CCM collects the certificates. The status of the certificate will change to 'Issued'.
- The MS Agent tracks the order. Once the certificate is issued, the Agent downloads the certificates and forwards them to NDES server. The status of the certificate is changed to 'Downloaded'
- The NDES server pushes the certificates to the target devices.

External References:

For an overview of basic deployment steps for NDES, see the page: <https://technet.microsoft.com/en-us/library/hh831498.aspx>.

For detailed explanation of deployment of NDES, see the page:

<http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx>

3.4.2.2 Issuance of Device Certificates through SCEP

CCM allows administrators to issue device certificates by creating configuration profiles which are pushed to target devices. The configuration profile can be created using software like the iOS Configuration Utility.

To issue device certificates through SCEP, administrators can create new device certificate types and enable them for SCEP enrollment. Each device certificate type is assigned with a Device Type ID to identify it in the configuration profile applied to the devices. For more details on creation and management of device certificate types, refer to the section **Device Cert Types**.

Prerequisites:

1. Private CAs must be enabled for your account in order to add device certificate types. Please contact your Comodo account manager for more details.
2. SCEP enrollment needs to be enabled for an Organization/Department and an access code specified. This can be done while adding a new Organization/Department or by editing an Organization/Department.

To enable SCEP enrollment for an Organization:

- Click the 'Settings' tab and choose 'Organizations'
- In the 'Organizations' screen, click the 'Add' button or select an organization and click the 'Edit' button
- In the 'Add New Organization' or 'Edit Organization' dialog, click the 'Device Certificate' tab.
- Check the 'SCEP Enabled' checkbox:

Edit Organization: Dithers Construction Company

General | EV Details | Client Certificate | SSL Certificate | Code Signing Certificate | **Device Certificate** | Email Template

Self Enrollment

URI Extension*
<https://cert-manager.com/customer/entsales/device/dithers>

SCEP Enabled

Access Code*

OK Cancel

The 'Access Code' field will appear.

- Type an access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.

Note: The access code for the organization should be entered as the 'challengePassword' parameter in the profile applied to devices which belong to that organization.

- Click 'OK'.

To enable SCEP enrollment for Departments:

- Click the 'Settings' tab and choose 'Organizations'
- In the 'Organizations' screen, select an organization and click the 'Departments' tab to view its departments
- In the 'Departments' dialog, click the 'Add' button, or select an existing department and click 'Edit'
- In the Add/Edit department dialog, click the 'Device Certificate' tab.
- Check the 'SCEP Enabled' checkbox.

Add New Department

General | EV Details | Client Certificate | SSL Certificate | Code Signing Certificate | **Device Certificate**

Self Enrollment

SCEP Enabled

Access Code*

OK Cancel

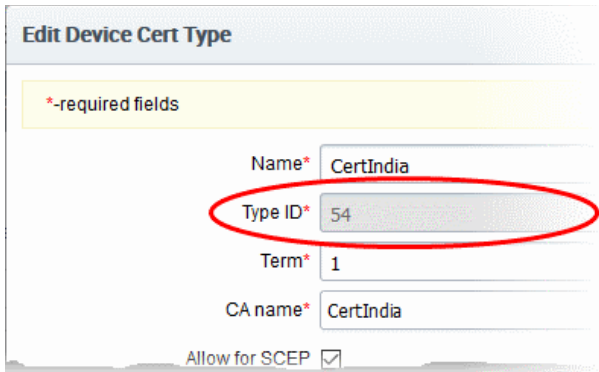
The 'Access Code' field will appear.

- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

SCEP Server URL for Device Certificate Enrollment

You need to include the URL of the SCEP server in the configuration profile for OTA enrollment. The URL should be in this format:

`http://<CCM Server>/customer/<customer name>/scep/device;deviceTypeId=<DeviceTypeId>/pkiclient.exe`

| Partner | Description |
|-----------------|--|
| <CCM Server> | The address of the CCM server you use |
| <customer name> | Your CCM company name |
| <DeviceTypeId> | <p>The identification number assigned to the type of device certificate to be enrolled. The Type ID can be viewed from the CCM interface.</p> <ul style="list-style-type: none"> • Click 'Settings' > 'Certificates' > 'Device Cert Types' • Select the device certificate type and click 'Edit' • The 'Type ID' is displayed in the Edit Device Cert Type dialog.  |

Tip: The URI protocol should be 'http' and not 'https' since the SCEP protocol relies on signed messages during a transaction.

For example: `http://cert-manager.com/customer/AcmeCorporation/scep/device;deviceTypeId=54/pkiclient.exe`

Overview of the process:

- Administrators generate a configuration profile for OTA enrollment using configuration software then apply the profile to target devices. The SCEP enrollment 'Access Code' specified for the Organization/Department is included in the profile. This means the certificate request generated by the device contains the Access Code as the challengePassword parameter.
- Once applied, the device generates the certificate request and forwards it to CCM.
- The certificate requests are added to the Certificates > Device Certificates interface for Approval. The state of the certificate is indicates as 'Requested'.
- A RAO or DRAO with appropriate privileges approves the request so that CCM forwards the request to Comodo CA. The status of the certificate changes to 'Applied'. Upon issuance of the certificate, CCM

collects the certificates. The status of the certificate will change to 'Issued'.

- The SCEP server pushes the certificates to the target devices for installation.

Note: For more details on values of parameters to be specified in the Configuration Profile, please contact your Comodo Account Manager.

3.4.2.3 Issuance of Device Certificate through Self Enrollment

The self-enrollment method allows applicants to request device certificates from Comodo as well as from Private Certificate authorities which have been added to the CCM account. Please contact your Comodo account manager to add a Private Certificate authority to your CCM account.

3.4.2.3.1 Prerequisites

- The issuance of device certificates is enabled for your account
- Device certificates are set to be available for self-enrollment in 'Settings' > 'Certificates' > 'Device Cert Types'
- The issuance of device certificate through self-enrollment is enabled for the organization/department under 'Settings' > 'Organizations' / 'Department' > 'Add' or 'Edit' button > 'Device Certificate' tab
- The RAO Device Cert or DRAO Cert administrator has been delegated control of this Organization or Department

3.4.2.3.2 Procedure Overview

- Administrator confirms completion of the **prerequisite steps**.
- Administrator sends the self-enrollment link to the applicant (see section **Initiating the enrollment process**).
- Applicant completes then submits the Self Enrollment Form (See section **The Self Enrollment Form**)
- The certificate request has to be approved by appropriate administrators.
- If the application is successful, the applicant will be able to download and install their device certificate. (See the section **Certificate Collection**)

3.4.2.3.3 Initiating the Enrollment Process

After completing the **prerequisite steps**, administrators need to communicate enrollment link details to each end-user, they wish to issue device certificates to. These details can be informed to the applicant by any preferred out-of-band communication method like email. The end-user can access the form at the given url, fill-in with the necessary details and submit it.

3.4.2.3.4 The Self Enrollment Form

Applicants need to complete the application form on the given URL, as shown below:

Please note the fields in the form above are the default fields. There may be more if custom fields have been defined for the form. See the section '[Custom Fields](#)' for more details.

| Form Element | Type | Description |
|--------------------------------------|------------|--|
| Certificate Type (required) | Drop-down | Applicant should select the device cert type from the drop-down. Only device certificate types enabled for self-enrollment will be available in the drop-down. Refer to the section Adding Device Cert Types for more details on configuring a device certificate type for availability in the self enrollment form. |
| Email Address (required) | Text Field | Applicant should enter their full email address. The device cert collection notification will be sent to this email address. |
| CSR (required) | Text Field | Applicant should paste the public key. |
| Submit | Control | Submits the application and enrolls the applicant for the device certificate. |

After clicking the 'Submit' button, a confirmation button will displayed.

3.4.2.4 Device Certificate Collection

Once the enrollment form is submitted and approved by appropriate administrators, the device certificate collection

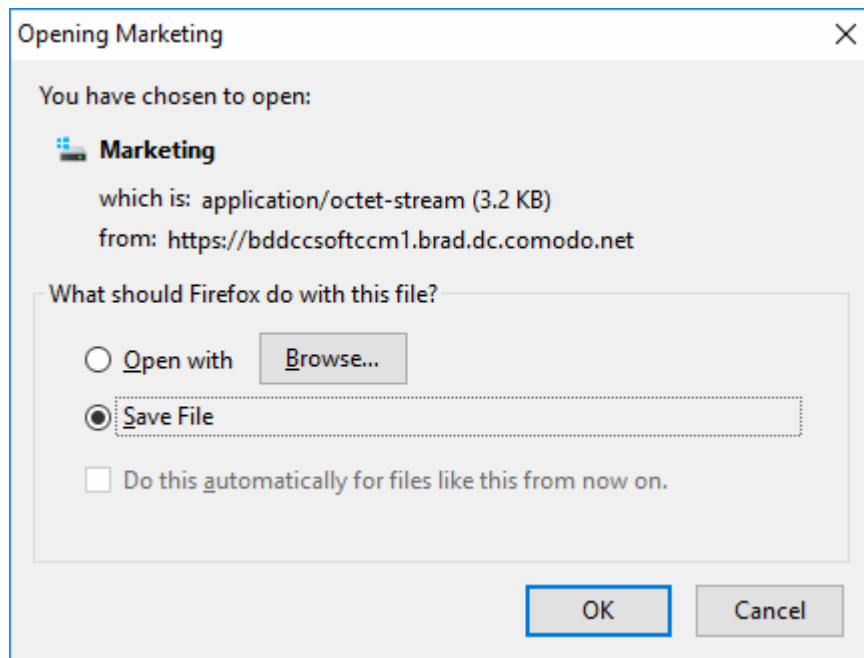
mail will be sent to the application to the email address provided in the enrollment form.

```
The Device Certificate for Marketing Device has been enrolled.

Please download it using the link:
as PKCS#7 Base64 encoded: https://bddccsoftccm1.brad.dc.comodo.net/customer/adv/device/download/61/3
as PKCS#7 Bin encoded: https://bddccsoftccm1.brad.dc.comodo.net/customer/adv/device/download/61/4
as X509, Base64 encoded: https://bddccsoftccm1.brad.dc.comodo.net/customer/adv/device/download/61/0
as X509 Certificate only, Base64 encoded: https://bddccsoftccm1.brad.dc.comodo.net/customer/adv/device/download/61/1
as X509 Intermediates/root only, Base64 encoded: https://bddccsoftccm1.brad.dc.comodo.net/customer/adv/device/download/61/2
as X509 Intermediates/root only Reverse, Base64 encoded: https://bddccsoftccm1.brad.dc.comodo.net/customer/adv/device/download/61/5

Certificate Details:
Common Name : Marketing Device
Term : 730 Days
Requested : 01/17/2017 03:28 GMT
Expires : 01/17/2019 23:59 GMT
Order Number : 1676610
```

CCM will deliver the certificate to the applicant in PKCS#7 and X509 formats. The applicant can collect the certificate by clicking the required link and saving the file in a safe location in his/her device.



3.4.2.5 Resending Device Certificate Collection Email

CCM automatically sends a collection email to end-users once a device certificate has been issued. However, if the certificate is not downloaded for a long time, then administrators may want to resend the mail. The resend dialog also allows you to change the recipient email address if the device has been registered to a different user.

To resend the certificate collection email:

- Click the 'Certificates' tab and then choose 'Device Certificates'
- Select the certificate for which you want to resend the collection mail. The certificate must have a status of 'Issued'
- Click the 'Resend Collection Link' button

The screenshot shows the 'Certificates' section of the Comodo Certificate Manager. The 'Device Certificates' tab is selected. A table lists certificates with columns for 'COMMON NAME', 'ORDER NUMBER', 'EMAIL', 'STATUS', and 'ORGANIZATION'. The first row, for 'dithers.com', is selected. A red circle highlights the 'Resend Collection Link' button in the toolbar above the table. A red arrow points from this button to a dialog box titled 'Resend Collection Link'. The dialog box contains a yellow box with the text '*-required fields', an 'Email*' field with the value 'cora@dithers.com', and 'OK' and 'Cancel' buttons.

| COMMON NAME | ORDER NUMBER | EMAIL | STATUS | ORGANIZATION |
|-------------|--------------|------------------------|------------|-------------------------------|
| dithers.com | 61025763 | cora@dithers.com | Issued | Dithers Construc Compan |
| dithers | 60316903 | dagwood@dithers.com | Downloaded | Comodo |
| dithers | 60312066 | jason.boone@comodo.com | Downloaded | Comodo |

The 'Resend Collection Link' dialog will be displayed. The recipient email address will default to the address entered during certificate enrollment.

- If you want to send the mail to a different address, enter the new address in the 'Email' field.
- Click 'OK'.

The collection mail will be sent to the specified address. Users can download and install the certificate by clicking the links in the mail (PKCS#7 and X509 formats are available).

3.4.2.6 Device Certificate Revocation

The device certificate issued to users can be revoked by appropriate administrators any time before certificate expiry date.

To revoke a device certificate go to 'Certificates' > 'Device Certificate', then select the certificate from the list and click 'Revoke' at the top.

The screenshot shows the 'Device Certificates' tab in the Comodo Certificate Manager. A table lists certificates with the following columns: COMMON NAME, ORDER NUMBER, EMAIL, STATUS, and ORGANIZATION. The first row is selected, showing 'dithers.com' with order number 61025763 and email cora@dithers.com, with a status of 'Issued'. A red circle highlights the 'Revoke' button in the toolbar above the table. A red arrow points from this button to a 'Revoke reason' dialog box. The dialog box contains a text area with the message: 'The Device Certificate is revoked for administrative reasons.' and 'OK' and 'Cancel' buttons.

| COMMON NAME | ORDER NUMBER | EMAIL | STATUS | ORGANIZATION |
|-------------|--------------|------------------------|------------|------------------------------|
| dithers.com | 61025763 | cora@dithers.com | Issued | Dithers Construction Company |
| dithers | 60316903 | dagwood@dithers.com | Downloaded | |
| | 60312066 | jason.boone@comodo.com | Downloaded | Comodo |

- In the 'Revoke reason' enter appropriate message and click 'OK'.

The certificate will be displayed as 'Revoked' under 'Status' in the interface.

4 Code Signing on Demand

Code Signing on Demand (CSD) offers customers a faster, more intuitive and highly secure way to digitally sign their software. The service is available in both hosted and cloud versions and is capable of signing EXE .DLL .CAB .MSI .OCX .SY, JAVA JAR and Android application files. The CSD service is available in two modes:

- **In-House Hosted Mode** - Developers upload software to a local portal. The code signing process is handled by a locally installed controller. After enrolling for a code signing certificate for a developer, the controller generates the certificate request for the developer and submits the request to CCM. The controller tracks the order number. Once the certificate is issued, the controller will download the certificate and store it in your local network. The developer can then upload the files to the local portal for signing. Upon approval by the administrator, the controller signs the file and notifies the developer. Private keys are generated and stored in encrypted format within the host's network. CCM also allows you to configure the controller to generate and store the code-signing certificate on a Hardware Security Module (HSM) connected to the local network.
- **Cloud Mode** - Developers upload software to Comodo Certificate Manager. The code signing process is performed within Comodo's highly secure cloud servers. After enrolling for a code signing certificate for a developer, the service generates the certificate request for the developer, submits the request to CCM, tracks the order and collects the certificate once issued. Developers can then upload files to the cloud portal for signing. Upon approval by the administrator, the service will sign the code and notify the developer to download the signed files. Private keys are generated and stored in encrypted format in

Comodo's data-center for the lifetime of the certificate, tightly protected by Comodo's military grade security infrastructure. You can also opt to store the keys on a Hardware Security Module (HSM).

Both modes require you to create a new 'Developer' role in CCM. The developer will be responsible for uploading software and collecting the signed code (after administrator approval).

Note: The CSD service will be available only if this feature is enabled for your account. If you wish to add this service, please contact your Comodo account manager.

Integration with a HSM

CCM allows you to use a HSM device to generate the keys for the CS certificates. The keys will be generated in PKCS # 11 format and saved in an unextractable format on the HSM device.

HSM integration is available for both In-House mode and Cloud Mode:

- **In-House Hosted Mode** - You can configure the controller software to generate the key pair on a HSM device on your local network for each CS certificate enrollment. Refer to the section **Installing the Controller (Hosted Mode)** for more details.
- **Cloud Mode** - Contact your Account Administrator to setup HSM integration for your account

The 'Code Signing on Demand' Interface

The 'Code Signing on Demand' area allows you to configure the service controller, add and manage 'Developers', and manage developer signing requests.

The 'Code Signing on Demand' area is divided into three main administrative areas, namely:

- The 'Configuration' tab - Allows you to download the agent required for hosted mode
- The 'Requests' tab - Allows you to view and approve/decline code signing requests from developers
- The 'Developers' tab - Allows you to add and manage 'Developer' accounts in CCM

Dashboard Certificates Discovery **Code Signing on Demand** Reports Admins Settings About

Configuration Requests Developers

Initialize Code Signing on Demand

- 1 Download and Install Controller
- 2 Start the Controller
- 3 Wait for few minutes
- 4 Check this page to finish Controller configuration

Prerequisites

Supported Linux x64 OS.

Before you start using the Controller, please make sure you have read the 'Readme' file after Controller installation

Download

Visibility of the 'Code Signing on Demand' area is restricted to:

- MRAO administrators - can configure the controller and add developers and manage code signing requests for any Organization or Department.
- RAO Code Signing administrators - can add developers and manage code signing requests only for Organizations (and any subordinate Departments) that have been delegated to them.

- DRAO Code Signing administrators - can add developers and manage code signing requests only for Departments that have been delegated to them.

This chapter contains the following sections:

- [Setting up the CSD controller](#)
- [Add Developers](#)
- [Obtain a Code Signing Certificate For CSD](#)
- [How to sign code using CSD](#)
- [Configure the CSD service](#)

4.1 Setting-up the CSD Controller

- **In-House Hosted Mode** - Download the controller software from the 'Code Signing on Demand' > 'Configuration' area and install it on a server within your local network. Once installed and connected, the service can be configured from the same interface. See [Installing the controller \(Hosted Mode\)](#) and [Configure the CSD service](#)
- **For Cloud Service Mode** - Configure the service from the 'Code Signing on Demand' > 'Configuration' area of the CCM interface. See [Configure the CSD service](#) for more details.

4.1.1 Installing the Controller (Hosted Mode)

Setting up the Code Signing on Demand (CSD) controller involves two steps:

- [Installing the CSD Controller](#)
- [Installing the Osslsigncode tool](#)

Installing the CSD Controller

You can download the setup file for the CSD controller from the CCM interface as a .bin file and install it on the Linux server through command line. The controller can be configured to generate the private and public keys for the CS certificates. You may also elect to generate the keys on a Hardware Security Module (HSM).

To download and install the controller setup file

- Click the 'Code Signing on Demand' tab then click 'Configuration'

The screenshot displays the 'Code Signing on Demand' configuration page in the Comodo Certificate Manager. The navigation bar at the top includes 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', 'Admins', 'Settings', and 'About'. The 'Code Signing on Demand' section is active, with sub-tabs for 'Configuration', 'Requests', and 'Developers'. The main content area is titled 'Initialize Code Signing on Demand' and contains a numbered list of four steps: 1. Download and Install Controller, 2. Start the Controller, 3. Wait for few minutes, and 4. Check this page to finish Controller configuration. Below the list is a 'Prerequisites' box with the text: 'Supported Linux x64 OS. Before you start using the Controller, please make sure you have read the 'Readme' file after Controller installation'. A 'Download' button is located at the bottom of the prerequisites box.

- Click the 'Download' button.
- Transfer the file to your Linux server.
- Install the CSD Controller on the Linux server from the command line.

```

3. Notice of any changes or modifications to the above files, including
THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATION
FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL BE
ABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE
The name and trademarks of copyright holders may NOT be used in advertising or promotional
d any associated documentation will at all times remain with copyright holders.

Do you agree with this license?[Y/n]: y

Are you use HSM or software version ? : [y/N] y
Enter path to HSM module:
[/usr/lib/x86_64-linux-gnu/softhsm/libsofthsm2.so]: opt/comodo
Enter path to SPKCS11engine:
[/usr/lib/engines/engine_pkcs11.so]: opt/comodo/spkcs11
Enter HSM slot number:
[0]: 0
Enter pin for slot of HSM:
[Secret1]: 111
Installation complete. CCM CS Controller started on PID: 19460.

[root@localhost opt]#

```

- After accepting to the EULA, the option for setting the HSM integration will appear.
- Enter 'Y' if you want to use a HSM or 'N' if you wish the controller to generate and store the keys in its vault
- If you elect to use a HSM, enter the following parameters one by one:
 - Network path to the HSM module
 - Path to SPKCS 11 Engine
 - HSM Slot Number to be used
 - PIN number for the HSM Slot

Upon successful connection, the controller will be installed and will connect to the CCM server. You can configure the controller from the CCM interface. Refer to the section **In-House Hosted Mode** for more details.

Note: Your HSM appliance may need some additional configuration to generate keys. Refer to the instructions in the owner's manual of your appliance.

Installation of Osslsgncode tool

- Download the tool from <http://sourceforge.net/projects/ossllsgncode/>

The tool's installation procedure depends on the distributive version and your environment.

Note: It is recommended to install the ossllsgncode tool into /usr/bin. Otherwise, the CSD Controller may not have access to it and you will need to provide it manually.

1. Latest CentOS

```

yum install gcc intltool libxml2-devel glib2-devel libcurl* openssl* bzip2* gdk*
wget http://ftp.gnome.org/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.34.tar.xz
tar -xf libgsf-1.14.30.tar.xz

```

```
cd libgsf-1.14.30
./configure --prefix=/usr
make
make install
cp /usr/lib/pkgconfig/libgsf-1.pc /usr/lib64/pkgconfig/libgsf-1.pc
pkg-config libgsf-1 --modversion
cd ..
cd osslsigncode-1.7.1
./configure
make ; make install
```

2. Latest Debian

```
apt-get install libbz2-dev libgdk-pixbuf2.0-dev glib2.0-dev libxml2-dev intltool libcurl4-openssl-dev libssl-dev
wget http://ftp.gnome.org/pub/GNOME/sources/libgsf/1.14/libgsf-1.14.34.tar.xz
tar -xf libgsf-1.14.34.tar.xz
cd libgsf-1.14.34
./configure --prefix=/usr
make
make install
cd ..
cd osslsigncode-1.7.1
./configure
make ; make install
```

3. Other Linux

- i. Download and unzip osslsigncode-1.7.1.tar.gz from <http://sourceforge.net/projects/openssl/signcode/>
- ii. See README.txt. The usual installation has 3 steps:

```
./configure
make
make install
```

Note: Usually the installation will require extra dependencies that should be previously installed.

Environment Tuning

1. Configure Controller's Web Server

The controller out of the box contains self signed certificate installed on Jetty Web Server. In case if client's browser restricts access to Sites without public trust certificates, you need to update Jetty Web Server certificate.

Please follow the instructions:

- i. Get or Enroll public trust SSL Certificate.
- ii. Put the Certificate and Private key into Java Key Store (JKS) with password. E.g. file 'cs-agent.jks' and

password '12345'

- iii. Copy the file into 'conf' directory inside the Controller. Usually: '/opt/comodo/ccmcscontroller/conf'
- iv. Update 'agent.properties' file which is located in 'conf' directory inside Agent.

Usually: '/opt/comodo/ccmcscontroller/conf/agent.properties'. Specify JKS file and password

ssl.keystore=cs-agent.jks

ssl.keystore.password=12345

- v. Restart the Controller. Usually: '/etc/init.d/ccmcscontroller stop' and '/etc/init.d/ccmcscontroller start'

2. The Controller needs to accept incoming requests. Check that the default Controller's port 9092 is open.
3. Make sure that the 'hostname' command returns a valid Hostname.

On completion of installation, the controller will automatically establish connection to CCM and start running immediately.

During the first run, the controller connects to CCM, obtains the configuration files updates its configuration and generates a password for its database.

The 'Code Signing on Demand' > 'Configuration' area will display the status as 'Connected' and shows the IP address of the server upon which the controller is installed. The controller periodically polls CCM and obtains the commands from it for execution.

The screenshot displays the 'Code Signing on Demand' configuration interface. At the top, a navigation menu includes 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', 'Admins', 'Settings', and 'About'. The 'Code Signing on Demand' section is active, showing sub-tabs for 'Configuration', 'Requests', and 'Developers'. The 'Configuration' tab is selected, revealing the following controls:

- Controller Status:** Connected (indicated by a green box).
- Last Activity:** just now.
- Activity Log:** A 'Show' button.
- Controller Hostname/IP Address:** A text input field containing '10.0.34.83'.
- Database Password:** A masked text input field with a 'Show' button.
- Number of Keys Stored:** 0.
- Auto-Approve Code Signing Requests:** An unchecked checkbox.

Below these fields is the 'Backup Configuration' section, which includes:

- SFTP location:** A text input field.
- SFTP User:** A text input field.
- SFTP Password:** A masked text input field with a 'Show' button.
- Backup File Password:** A masked text input field with a 'Show' button.
- Frequency:** Radio buttons for 'Manual' and 'Daily'.
- Next backup at (UTC):** A dropdown menu set to '12 AM'.
- Backup Now:** A button.
- Save:** A button at the bottom of the section.

The 'Restore Existing Code Signing Keys From Backup' section at the bottom contains:

- SFTP File location:** A text input field.
- SFTP User:** A text input field.
- SFTP Password:** A masked text input field with a 'Show' button.
- Backup File Password:** A masked text input field with a 'Show' button.
- Restore:** A button at the bottom of the section.

Code Signing on Demand - Configuration Interface - Table of Fields and Controls

| Field | Description |
|-----------------------|--|
| Controller Status | Indicates whether the controller is currently connected to CCM or not. |
| Last Activity | Indicates the date and time of last polling of the Controller to CCM |
| Activity Log | Clicking the 'Show' button opens the Commands dialog that displays the list of command received by the controller form the CCM and their execution status. Refer to the section View Activities of the CSD Controller for more details. |
| IP Address | Displays the IP address of the server on which the controller is installed. |
| Database Password | The password for the protecting the database. The password is used for encrypting the stored certificates and their private keys in the database. The password is auto generated and cannot be changed by the administrator. <ul style="list-style-type: none"> Clicking the 'Show' button displays the password. |
| Number of Keys Stored | Shows the number of certificates and their private keys stored and managed by the Private Key Store controller. |
| Backup Configuration | |
| SFTP location | The administrator can specify the location/URL of the SFTP server for the backup of the Code Signing certificates and their keys. Refer to the section Backup/Restore Code Sining Certificates for more details. |
| SFTP User | The username for the account in SFTP server, for access by the CSD service controller. |
| SFTP Password | The password for the account in SFTP server, for access by the CSD service controller. |
| Backup File Password | The password for encrypting the files stored in the backup server |
| Frequency | The frequency at which the database backup operations are executed. Refer to the section Backup/Restore Code Sining Certificates for more details. |
| Save | Saves the backup configuration |

4.2 Add Developers

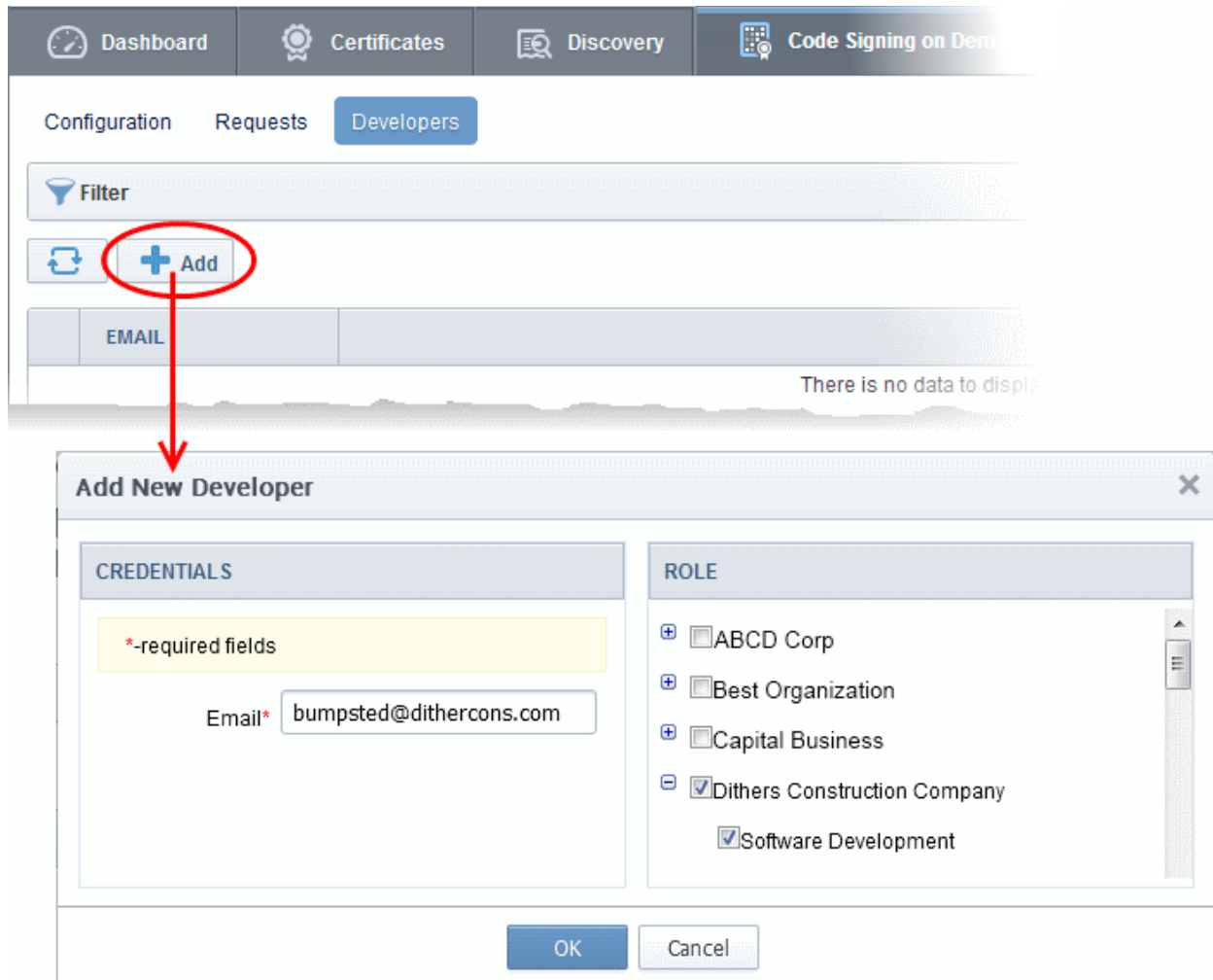
A 'Developer' is a role in CCM with permission to:

- Login to the CSD service
- Upload files for code-signing
- Download code-signed files

You can create a developer as a new user, or add developer privileges to an existing CCM user. An MRAO or RAO administrator will need to approve the developer's actual signing requests, unless you enable auto-approve in the CSD configuration screen.

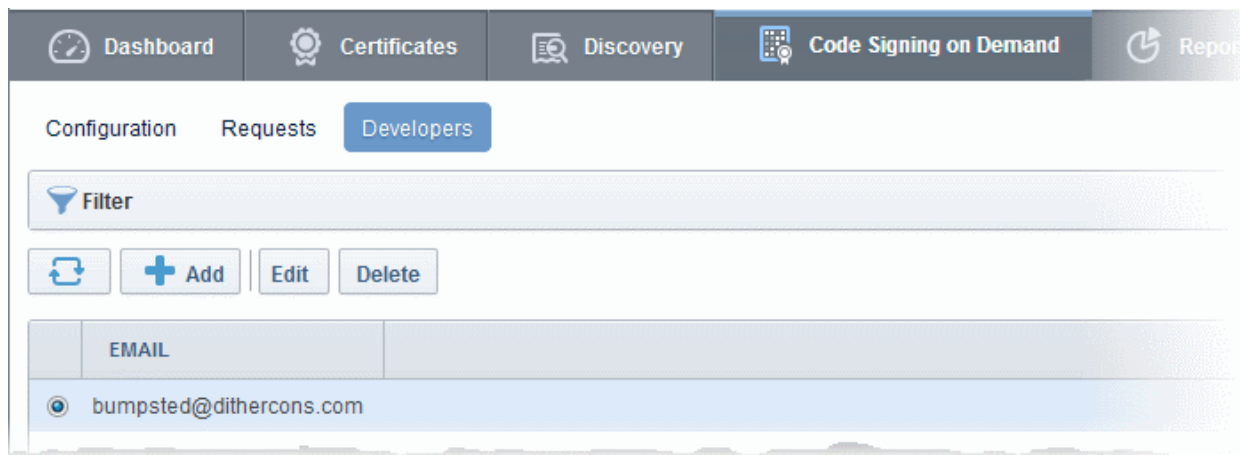
To add a developer

- Open the 'Developers' interface by clicking 'Code Signing on Demand' > 'Developers'
- Click the 'Add' button. This will open 'Add New Developer' dialog.

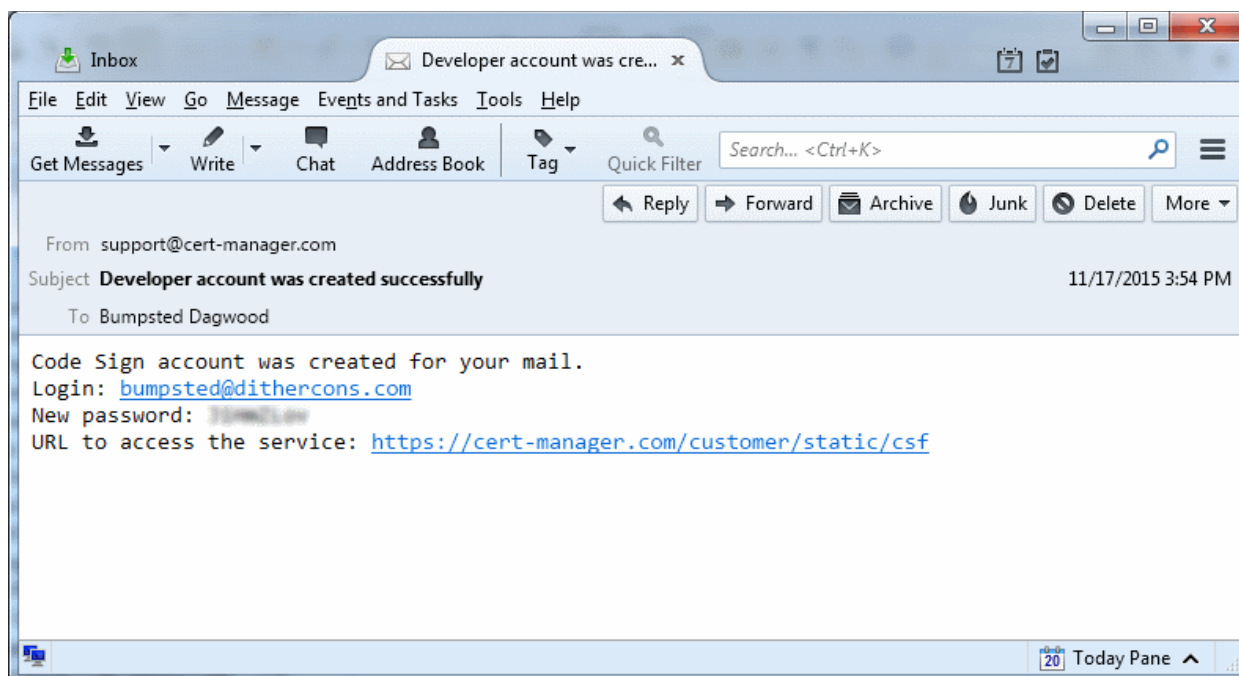


- Type the email address of the developer in the email field.
- Select the Organization(s) / Department(s) to which the developer should belong on the right
- Click 'OK' to confirm your selection.

The developer will be added to the list. You can edit the user to change their Organization/Department, reset their password or remove the developer.



A notification email will be sent to the developer with the credentials to access the CSD service. An example is shown below:

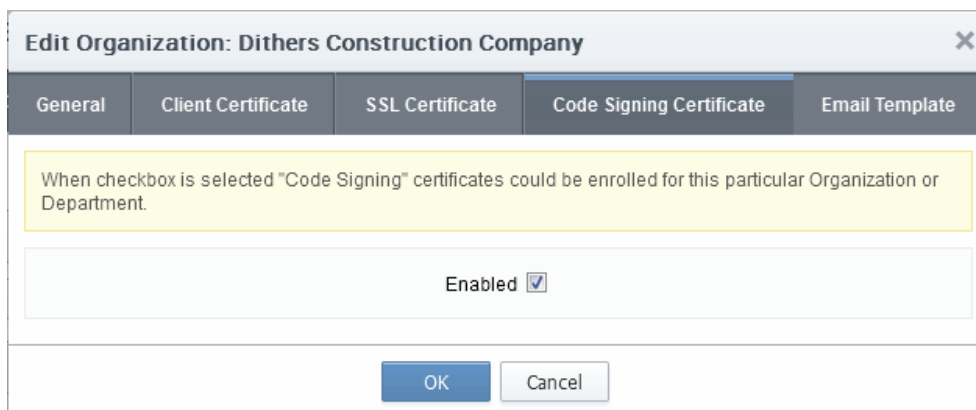


4.3 Obtain a code-signing certificate for CSD

Prerequisites:

- You have created a 'Developer' role as explained in the preceding section.
- The domain for which the code signing certificate is to be issued has been enabled for Code Signing certificates and that the domain has been made activated by your Comodo account manager. For example, if you wish to issue code signing certs to end-user@mycompany.com, then mycompany.com must have been validated by Comodo. All certificate requests made on validated domains or sub-domains are issued automatically. Certificate requests for new domains will first have to undergo validation by Comodo.
- The domain from which the code signing certificates are to be issued has been delegated to the Organization or Department. See [Creating a New Organization](#) and [Editing an Existing Organization](#) for more details on adding a domain to an Organization.
- The RAO Code Signing or DRAO Code Signing administrator has been delegated control of this Organization or Department.

- The MRAO or delegated RAO administrator has enabled Code Signing Certificates for the Organization by selecting the 'Enabled' check-box in the 'Code Signing tab' of the 'Add New/Edit' Organizations dialog box (see screen-shot below)



- For Hosted mode, the CSD service controller also needs to be installed on the local network and connected to CCM.
- Optional. The controller is configured to generate and store keys on a HSM appliance.

Procedure Overview:

1. The administrator confirms the completion of the **prerequisite steps**.
2. The administrator adds a new code-signing certificate for the Developer from the 'Certificates' > 'Code Signing Certificates' interface, with 'Code Signing on Demand' enabled for the certificate.
 - For Hosted Mode - The CSD controller generates and stores the key pair locally and submits the CSR to Comodo CA. Once the certificate is issued, the CSD controller automatically downloads the certificate and stores it in your local network. If a HSM appliance is used, the key pair is generated and stored on the HSM. On issuance of the certificate, the controller downloads the certificate and stores it on the HSM appliance.
 - For Cloud Mode - The CSD cloud service generates and stores the key pair and submits the CSR to Comodo CA. Once the certificate is issued, the service collects the certificate and stores it in Comodo data center. If the HSM service is used, the key pair is generated and stored on the HSM. On issuance of the certificate, the service collects the certificate and stores it on the HSM.

To enroll a code signing certificate for the developer

- Open the 'Code Signing Certificates' interface by clicking 'Certificates' > 'Code Signing Certificates'
- Click the 'Add' button to open the code-signing certificate application form.
- Complete all required fields on the form, making sure:
 - The correct developers email address is used.
 - The correct Organization and Department are specified for the developer.
 - The 'Code Signing on Demand' box is checked.

The screenshot shows the Comodo Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, and Code Signing on Demand. Under the Certificates tab, there are sub-tabs for SSL Certificates, Client Certificates, and Code Signing Certificates. A filter bar is present, followed by buttons for Refresh, Add, Export, and Import from CSV. Below this is a table with columns: NAME, EMAIL, ORDER NUMBER, STATE, and ORC. The 'Add' button is circled in red, and an arrow points from it to the 'Add New Code Signing Certificate' dialog box.

Add New Code Signing Certificate

*-required fields

Organization: Dithers Construction Company

Department: None

Domain: dithercons.com

Email Address*: bumpsted@dithercons.com

Term: 1 year

Full Name*: Bumpsted Dagwood

Contact email: [empty]

Code Signing on Demand: [info icon]

Signature Algorithm: RSA

Key Size: 2048

Subscriber Agreement: EULA

Print

I agree.* Scroll to bottom of the agreement to activate check box.

OK Cancel

The following table explains the fields on the form:

| Field | Description |
|------------------------|--|
| Organization | Select the Organization to which the developer belongs. |
| Department | Select the Department to which the developer belongs. |
| Domain | Select the domain pertaining to the Organization/Department |
| Term | Select the term of the certificate. |
| Email Address | Enter the email address of the developer. |
| Full Name | Full name of the applicant. |
| Contact Email | Enter the contact email address of the applicant that should be included in the certificate. The contact email address may be the customer facing email address like support@company.com, sales@company.com etc. |
| Code Signing on Demand | Enable this check-box to allow the certificate to be used by the CSD service. |
| Signature Algorithm | Choose the signature algorithm to be used by the certificate. |
| Keysize | Choose the key-size (in bits) by the certificate. |
| Subscriber Agreement | Displays the End-User License Agreement (EULA) for the certificate. Read through the EULA and accept to it by selecting the 'I agree' checkbox for the application to proceed. |

- Click 'OK' to submit the request.

The certificate will be added with the state 'init' indicating that the certificate enrollment has been initiated.

The screenshot shows the 'Code Signing Certificates' section of the Comodo Certificate Manager. A table lists certificates with columns: NAME, EMAIL, ORDER NUMBER, STATE, ORGANIZATION, DEPARTMENT, EXPIRES, and CODE SIGNING ON-THE-FLY. The first entry is 'Bumpsted Dagwood' with email 'bumpsted@dithercons.com', and its 'STATE' is 'Init', which is circled in red. The 'ORGANIZATION' is 'Dithers Construction Company' and 'CODE SIGNING ON-THE-FLY' is checked.

| NAME | EMAIL | ORDER NUMBER | STATE | ORGANIZATION | DEPARTMENT | EXPIRES | CODE SIGNING ON-THE-FLY |
|------------------|-------------------------|--------------|-------|------------------------------|------------|---------|-------------------------------------|
| Bumpsted Dagwood | bumpsted@dithercons.com | | Init | Dithers Construction Company | | | <input checked="" type="checkbox"/> |

Once issued, the state of the certificate will change to 'Issued':

The screenshot shows the 'Code Signing Certificates' section after the certificate has been issued. The 'STATE' for the 'Bumpsted Dagwood' certificate is now 'Issued', circled in red. The 'ORDER NUMBER' is now '1503301' and the 'EXPIRES' date is '11/20/2016'. The 'CODE SIGNING ON-THE-FLY' checkbox remains checked.

| NAME | EMAIL | ORDER NUMBER | STATE | ORGANIZATION | DEPARTMENT | EXPIRES | CODE SIGNING ON-THE-FLY |
|------------------|-------------------------|--------------|--------|------------------------------|------------|------------|-------------------------------------|
| Bumpsted Dagwood | bumpsted@dithercons.com | 1503301 | Issued | Dithers Construction Company | | 11/20/2016 | <input checked="" type="checkbox"/> |

The certificate can now be used to sign code submitted by your developer. Each signing action will, however, need to be approved by an administrator UNLESS you enable 'Auto-approve code signing requests' in **CSD Configuration**.

4.4 How to sign code using CSD

Once you have **created a developer** and **obtained at least one CSD enabled code-signing certificate**, your developer is ready to upload files for signing.

Checklist:

| In-House Hosted Mode | Cloud Service Mode |
|---|--|
| <ul style="list-style-type: none"> The 'Code Signing on Demand' (CSD) service is enabled in 'Hosted Mode' for your account The CSD controller is installed on your network and connected to CCM. Refer to section In-House Hosted Mode for more details. Developer accounts have been created and issued with a CSD Code Signing certificate. | <ul style="list-style-type: none"> The 'Code Signing on Demand' (CSD) service is enabled in 'Cloud Mode' for your account Developer accounts have been created and issued with a CSD Code Signing certificate. |

Overview of steps:

- Step 1 - Upload the files to be Signed** - The developer logs-in to the CSD service portal, enters the details of the file(s) to be signed, selects the signing service and uploads the files. This will create a request which can be viewed in the 'Code Signing on Demand' > 'Requests' interface. See **Step 1 - Upload the files to be Signed** for more details.
- Step 2 - Approve the Code Signing Request** (optional) - The Administrator views the request, checks the files to be signed and approves the request from the 'Code Signing on Demand' > 'Requests' interface. See **Step 2 - Approve the Code Signing Requests** for more details. Note - this step can be skipped if 'Auto-Approve Code Signing Requests' is enabled in 'Configuration'.
- Step 3 - Download Code-Signed files** - Once approved and digitally signed, the status of the request will change to 'Signed'. A notification mail is sent to the developer with a URL to download the signed files. See **Step 3 - Download Code Signed Files** for more details.

Step 1 - Upload the files to be Signed

Once a developer has been added to CCM they will be able to login to CCM using the link in their confirmation email. By default, the format of this URL is: [https://cert-manager.com/customer/\[REAL CUSTOMER URI\]/csd](https://cert-manager.com/customer/[REAL CUSTOMER URI]/csd).

- After logging in they can upload files using the following form:

COMODO
Certificate Manager

Create Code Signing request

Email: *

Password: *

Organization: *

Department: *

Version: *

Signing Service: *

test.exe **Complete**


No files selected.

- **Organization** - Displays the organization(s) to which the developer belongs. The organization selected here will be shown in the certificate as the publisher of the software.
- **Department** - Allows the developer to choose a department. If departmental information is also required in the certificate.
- **Version** - Developer should type the version number of the software they wish to sign.
- **Signing Service** - Select the signing service. Choices are 'Microsoft Authenticode', 'Java' and 'Android'.
- **Browse...** - Developer should choose the files they wish to upload and sign.

Once all fields are complete and the file has been selected, click the 'Create' button to submit the signing request to the CSD service. A confirmation dialog will be displayed:

COMODO
Certificate Manager

Info



Code Signing Request has been created. You will be notified when your files will be signed.

A code signing request will be created in the 'Code Signing on Demand' > 'Requests' interface. By default, the request needs to be approved by the appropriate MRAO, RAO or DRAO administrator before the code-signing action will take place. If 'Auto-Approval' of Code Signing Requests is enabled, the service starts the signing process immediately. See 'Configuration' to enable this feature.

Step 2 - Approve the Code Signing Request

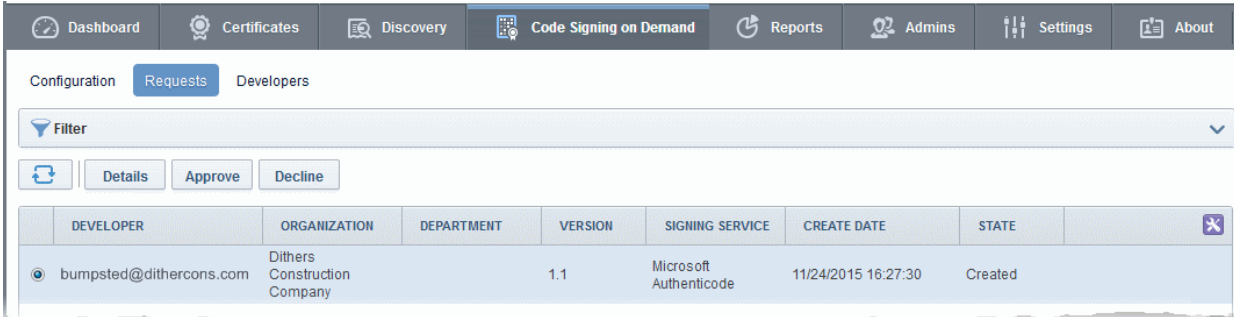
After the files have been uploaded by the developer, a code signing request will appear in the 'Code Signing on Demand' > 'Requests' area. Under the default settings, an administrator needs to review and approve the request.

before the service will actually sign the files.

To view and approve/decline the code signing requests

- Click 'Code Signing on Demand' tab and choose the 'Requests' sub tab.

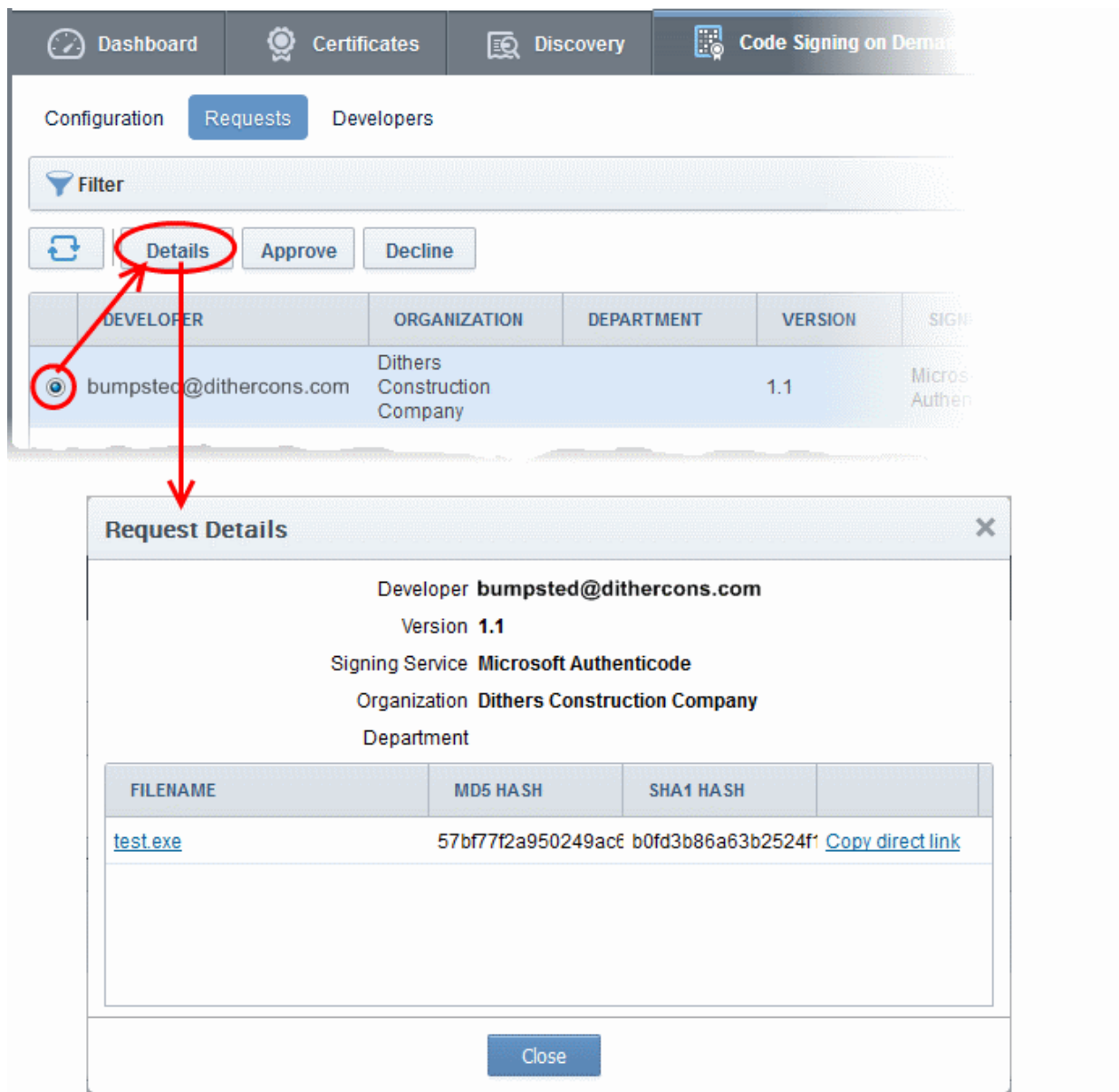
A list of requests will be displayed.



The screenshot shows the 'Code Signing on Demand' section of the Comodo Certificate Manager. The 'Requests' sub-tab is selected, and the 'Configuration' section is expanded. A table of requests is displayed with the following data:

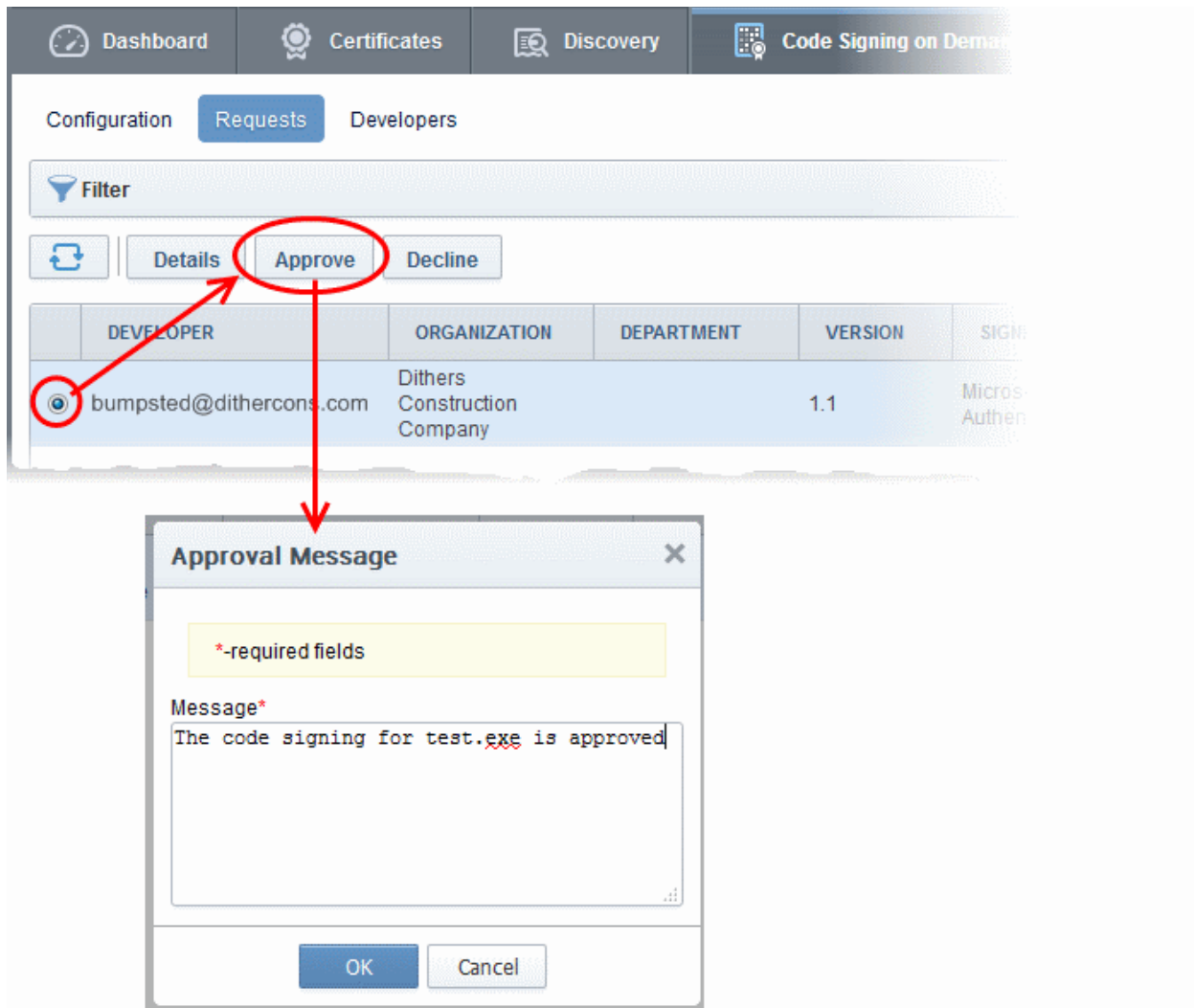
| DEVELOPER | ORGANIZATION | DEPARTMENT | VERSION | SIGNING SERVICE | CREATE DATE | STATE |
|-------------------------|------------------------------|------------|---------|------------------------|---------------------|---------|
| bumpsted@dithercons.com | Dithers Construction Company | | 1.1 | Microsoft Authenticode | 11/24/2015 16:27:30 | Created |

- To view the details of a request and check the files, choose the request and click 'Details'.



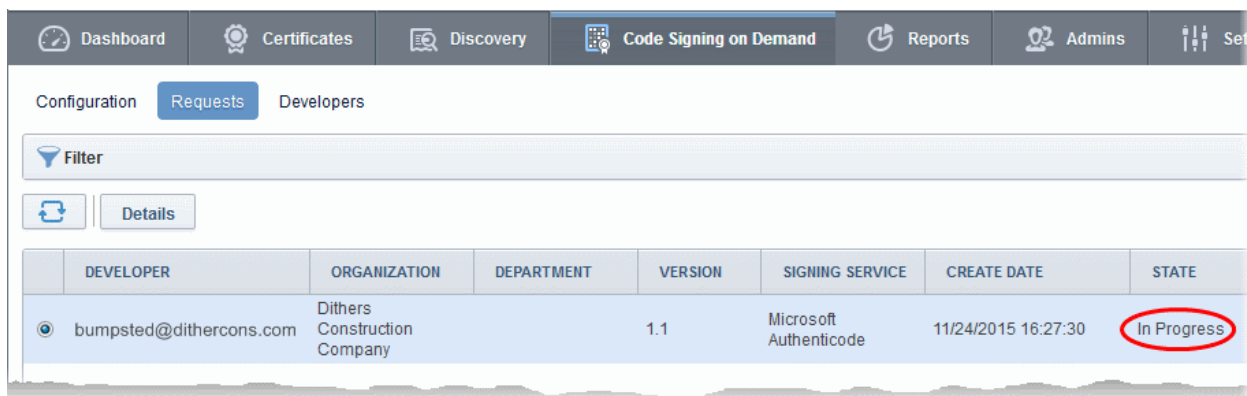
The 'Request Details' dialog displays the developer's name and the file details along with the MD5 and SHA1 hash values of the files.

- To download the file for examination, click the file name.
- To approve the code signing request, select the request and click 'Approve':



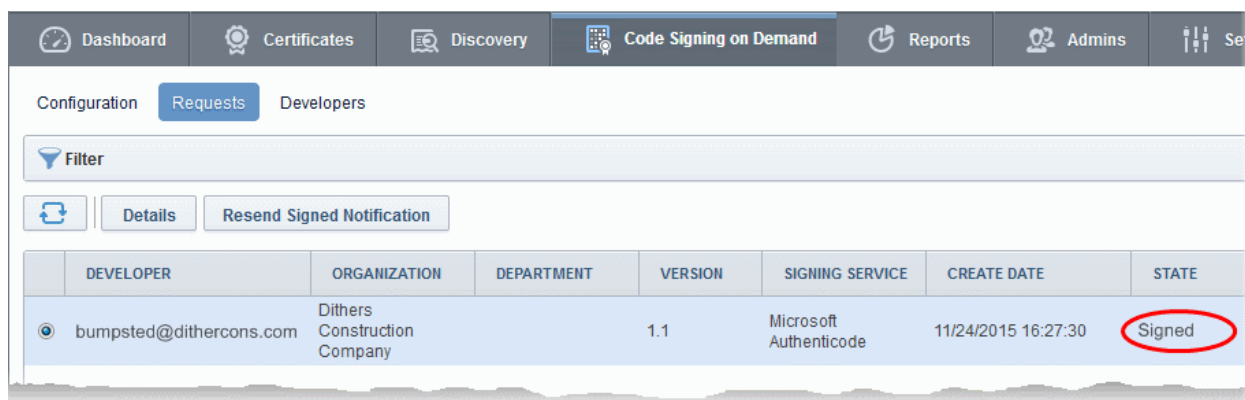
- Enter an approval message and click OK.

The request will be approved and its state will change to 'In Progress':



Once the code-signing process has completed, the request state will change to 'Signed' and a notification mail will be sent to the developer to download the signed file.

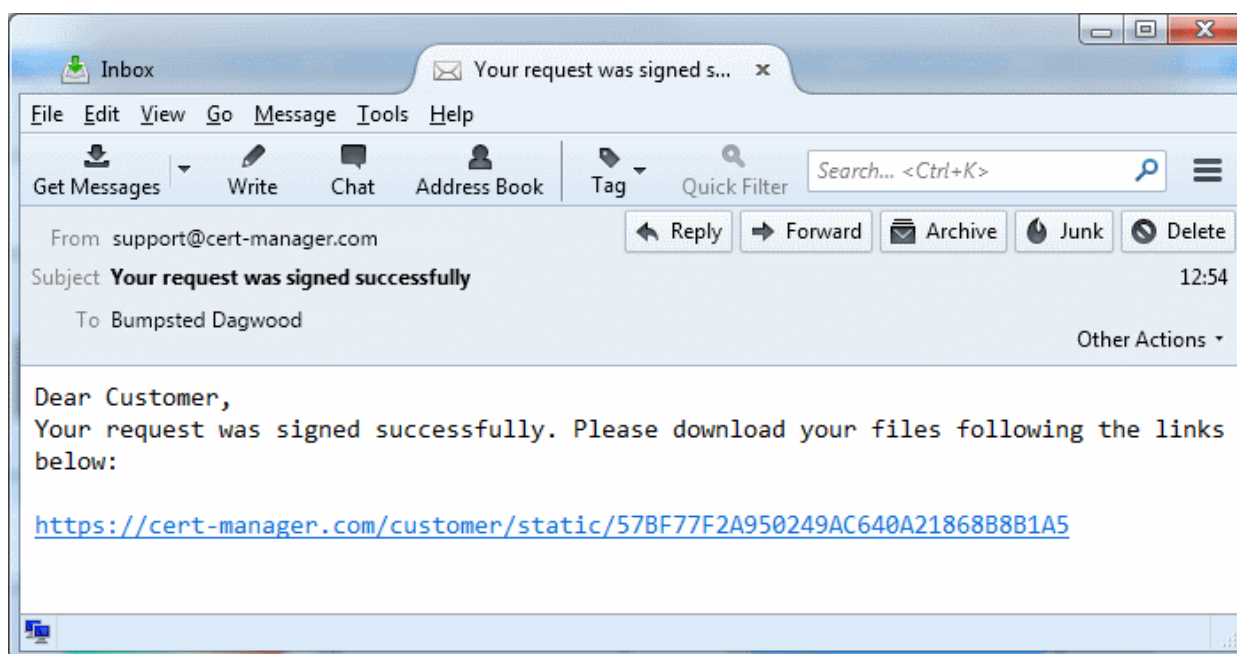
The Developer must download the signed files within three days of the notification. The files will be removed from the database after three days after signing. If required, administrators can resend this notification by clicking the 'Resend Signed Notification' button:



Note. As mentioned earlier, administrators have the option to forgo the approval process by enabling 'Auto-Approve Code Signing Requests' in the 'Configuration' interface.

Step 3 - Download Code-Signed files

On successful completion of the signing process, the developer will receive a notification email with links to download each signed file. An example is shown below.

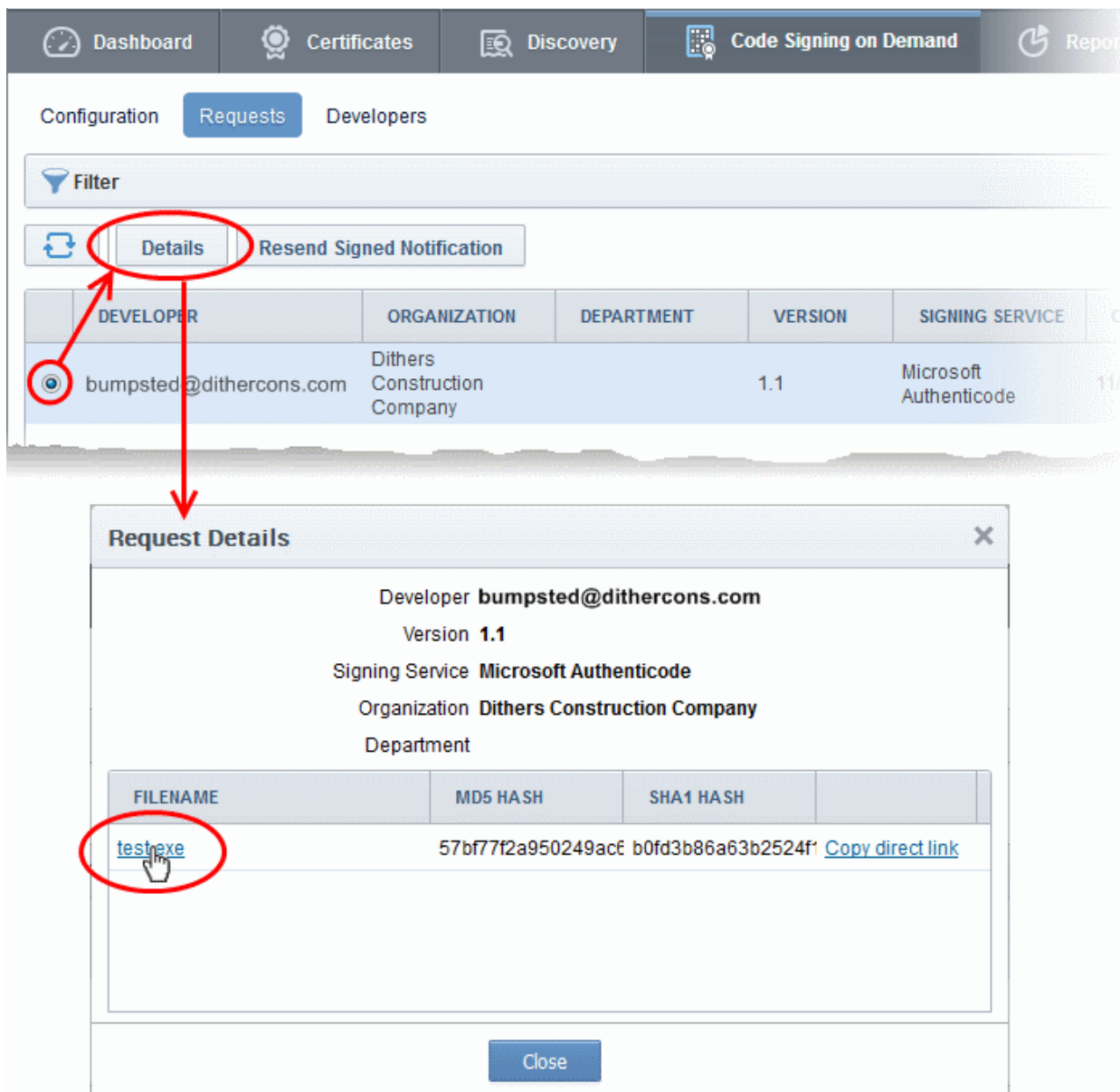


The developer can click the links and download the signed files.

Note: The Developer must download the signed files within three days of the notification. The files will be removed from the database after three days from the date of signing.

Administrators can also download signed files from the 'Details' dialog of the request.

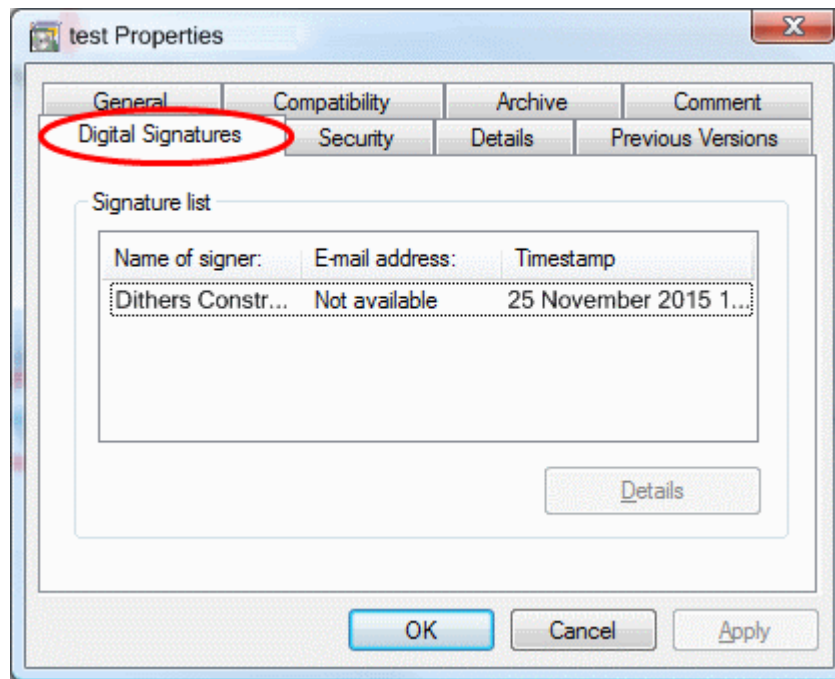
- Choose the request from the 'Code Signing on Demand' > 'Requests' interface and click 'Details'



- Click the file name in the 'Request Details' dialog to download the signed file.

To check whether the file is signed

- Right click on the file and choose 'Properties'
- Choose the 'Digital Certificates' tab



The details of the signer will be displayed.

4.5 Configure the CSD service

The CSD service can be configured for local database password protection, backup and restore operations and auto-approval of code-signing requests from the developers. The configuration parameters depend on the mode of service enabled for your account. The following sections explain the configuration on:

- **In-House Hosted Mode**
- **Cloud Service Mode**

4.5.1 In-House Hosted Mode

In Hosted mode, the CSD controller creates an encrypted database on your network which is used to store your certificates and private keys. This area allows you to configure the controller to automatically backup this database to a specified location and to enable auto-approval of certificate requests.

To configure the CSD controller, click the 'Code Signing on Demand' tab and choose 'Configuration' sub tab.

Dashboard Certificates Discovery **Code Signing on Demand** Reports Admins Settings About

Configuration Requests Developers

Controller Status **Connected**

Last Activity just now

Activity Log

Controller Hostname/IP Address* 10.0.34.83

Database Password*

Number of Keys Stored 0

Auto-Approve Code Signing Requests

Backup Configuration

SFTP location

SFTP User

SFTP Password

Backup File Password*

Frequency Manual Daily Next backup at (UTC): 12 AM

Restore Existing Code Signing Keys From Backup

SFTP File location*

SFTP User

SFTP Password

Backup File Password*

The 'Code Signing on Demand' > 'Configuration' interface allows you to:

- **View the activities of the CSD controller**
- **Configure for auto approval of code signing requests**
- **Backup/Restore Code Signing Certificates and their private keys**

View the Activities of the CSD Controller

Once the controller is installed on your local network it automatically connects with CCM. The connection status is displayed in the upper pane of the 'Code Signing on Demand' > 'Configuration' interface. You can view the list of commands received by the controller from the CCM and their execution status at any time.

- Clicking the 'Show' button beside 'Activity Log' in the 'Code Signing on Demand' > 'Configuration' interface, opens the 'Commands' dialog with the list of commands received by the controller in chronological order.

Controller Status **Connected**

Last Activity a moment ago

Activity Log **Show**

Controller Hostname/IP Address* 10.0.21.83

Database Password*

Commands

Details

| NAME | DATE | STATE |
|-------------------------------------|---------------------|------------|
| Generate CSR and Manage Private Key | 11/23/2015 16:29:34 | Successful |
| Update Configuration | 11/23/2015 16:24:11 | Successful |
| Update Configuration | 11/23/2015 16:22:24 | Successful |

15 rows/page 1 - 3 out of 3

Close

Commands Dialog - Column Descriptions

| Column Header | Description |
|---------------|---|
| Name | Shows the command received from CCM during the consecutive polls. |
| Date | Indicates the precise date and time, the command was received. |
| State | Indicates the execution state and result of the command. |

- Choosing a command and clicking the 'Details' button at the top, displays the details of the command.

The screenshot shows the 'Commands' section of the Comodo Certificate Manager interface. A table lists several commands, with the first one selected. A red circle highlights the 'Details' button in the top toolbar, and another red circle highlights the selected row in the table. A red arrow points from the 'Details' button to the 'Details' dialog box that opens below.

| NAME | DATE | STATE |
|--|---------------------|------------|
| <input checked="" type="radio"/> Generate CSR and Manage Private Key | 11/23/2015 16:29:34 | Successful |
| <input type="radio"/> Update Configuration | 11/23/2015 16:24:11 | Successful |
| <input type="radio"/> Update Configuration | 11/23/2015 16:22:24 | Successful |

Details [X]

Name **Generate CSR and Manage Private Key**

Date **11/23/2015 16:29:34**

State **Successful**

Detail Message

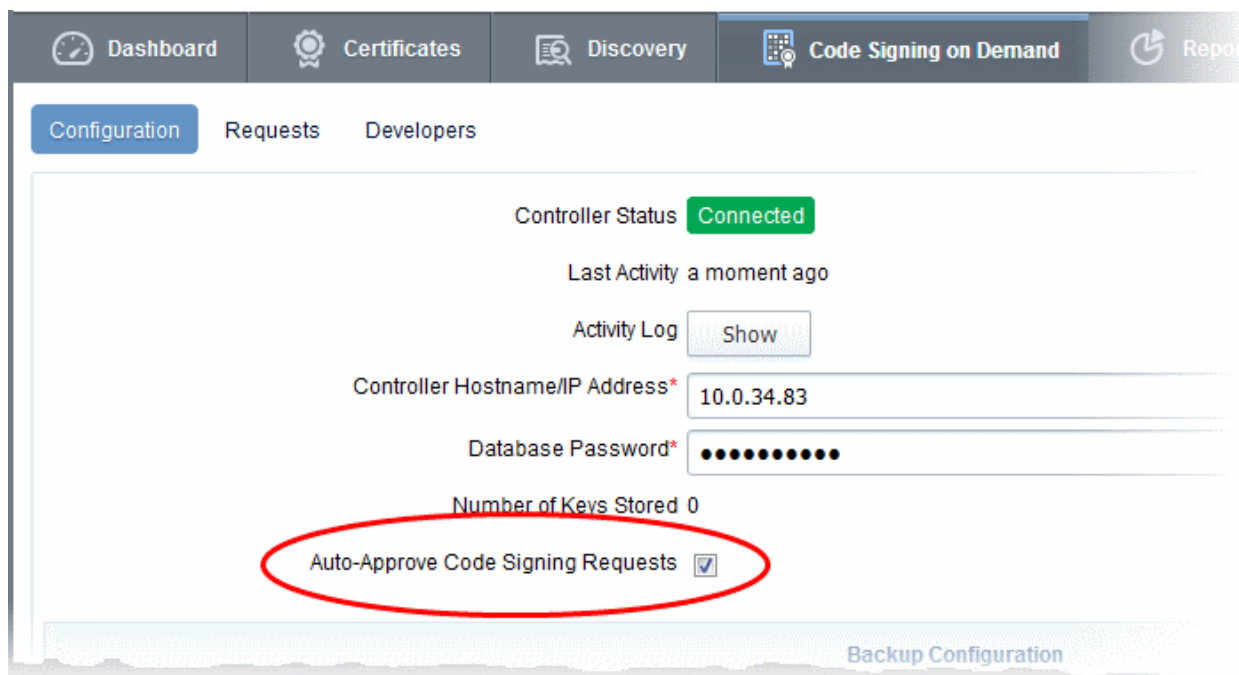
```
Common Name:  
Bumpsted Dagwood  
Key Algorithm: RSA
```

[Close]

Configure for Auto Approval of Code Signing Requests

By default, the code signing requests, generated by the developers by uploading the files to be signed, are to be approved by the MRAO, RAO or the DRAO administrator for the CSD service controller to sign the code file. The administrator can view, manage and approve the requests from the 'Code Signing on Demand' > 'Requests' interface. You can configure the controller for auto-approval, If you want the requests to be auto-approved without the manual approval of the administrator to speed up the process. The controller will start the signing processes, once the files are uploaded by the developer. Refer to the section [How to sign code using CSD](#) for more details.

- To enable auto-approval of code signing requests, select the 'Auto-Approve Code Signing Requests' checkbox in the 'Code Signing on Demand' > 'Configuration' interface.

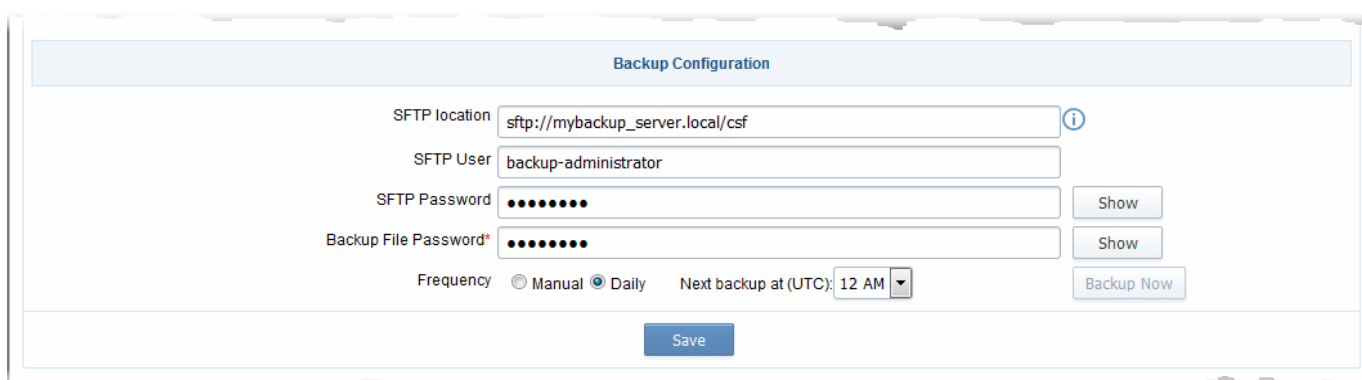


Backup/Restore Code Signing Certificates and Their Private Keys

The administrator can configure backup for the CSD database at a remote SFTP server and schedule periodic backup operations or run backups manually. In case the code signing certificates belonging to the developers and their private keys are lost, they can be restored from the backup.

To configure for backup

- Click 'Code Signing on Demand' > 'Configuration' to open the 'Configuration' interface
- Enter the details of the SFTP server to be configured as the backup location, under 'Backup Configuration'



| Backup Configuration - Table of Parameters | |
|--|--|
| Parameter | Description |
| SFTP Location | Enter the path of the backup location in the SFTP server, at which the CSD service backup is to be created. |
| SFTP User | Enter the username of your user account in the SFTP server for the CSD controller to access the SFTP server. |

| | |
|----------------------|---|
| SFTP Password | Enter the password of your user account in the SFTP server. Clicking the 'Show' button displays the password. |
| Backup File Password | Enter the password for the backup file to be created. Clicking the 'Show' button displays the password. |
| Frequency | Set the schedule at which the backup operations are to be executed. <ul style="list-style-type: none"> Manual - The Backup will be run only on clicking the 'Backup Now' button manually Daily - The Backups are created daily at the time specified in the 'Next backup at:' drop-down. Choose the time in ETC at which the backups are to be run daily. |

- Click 'Save' for your configuration to take effect.
- To run an instant backup, click the 'Backup Now' button.

The Backup is configured. You can run the backup any time you want by clicking the 'Backup Now' button from the 'Code Signing on Demand' > 'Configuration' interface or the backup operations will be executed as per the schedule.

In case the CSD controller and/or the code signing certificates with their private keys are lost from the server for some reason, you can restore them from the backup, by installing another controller in the same or a different server in your local network and configuring it from the 'Code Signing on Demand' > 'Configuration' interface

To restore the keys

- Download the setup file for the new controller, by selecting the operating system of your server from the 'Code Signing on Demand' > 'Configuration' interface and install it on your network. Refer to the section [Installing the Controller \(Hosted Mode\)](#) for more details.

Upon successful installation, the controller will connect to CCM and its state will be displayed as 'Connected' in the 'Code Signing on Demand' > 'Configuration' interface.

- Enter the SFTP details of the remote SFTP server configured as backup location under 'Restore Existing Code Signing Keys From Backup' and click 'Restore'.

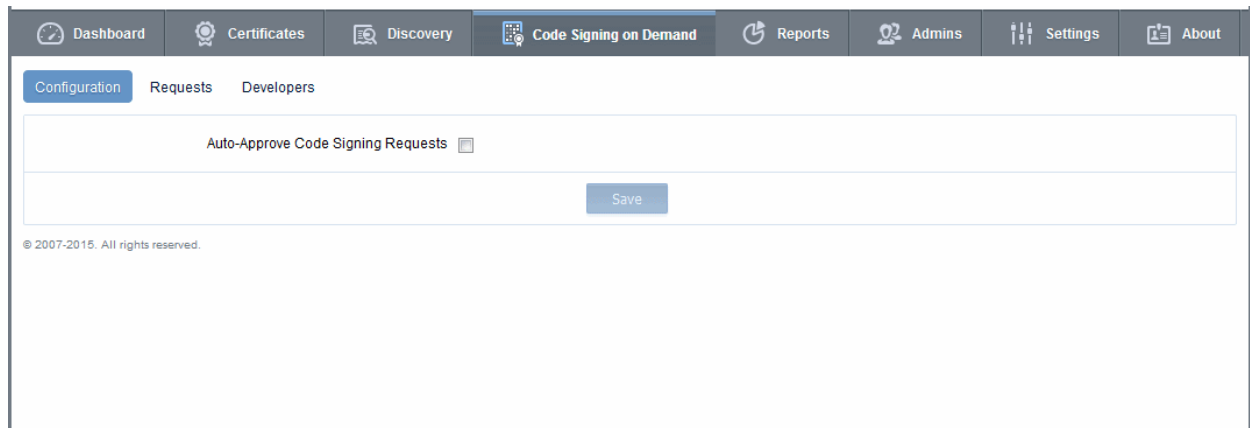
The screenshot shows a web interface titled "Restore Existing Code Signing Keys From Backup". It contains four input fields: "SFTP File location*" with the value "sftp://mybackup_server.local/csf", "SFTP User" with "backup-administrator", "SFTP Password" (masked with 10 dots), and "Backup File Password*" (masked with 10 dots). Each password field has a "Show" button to its right. An information icon (i) is next to the SFTP File location field. A blue "Restore" button is centered at the bottom of the form.

The code signing certificates and their keys will be restored to the database created by the new controller.

4.5.2 Cloud Service Mode

To configure the CSD service

- Click the 'Code Signing on Demand' tab then 'Configuration'



- Auto-Approve Code Signing Requests - By default, code signing requests from developers must be approved by an administrator before the actual signing will take place. Administrators can view, manage and approve requests from the 'Code Signing on Demand' > 'Requests' interface.

If you want signing to commence without administrator approval, enable the 'Auto-Approve Code Signing Requests' check-box. The service will start the signing processes immediately after files are uploaded by the developer. Refer to the section [How to sign code](#) using CSD for more details.

5 Admin Management

5.1 Section Overview

The 'Admins' tab allows administrators to create, manage and edit permissions for new and existing administrators. There are 9 types of administrator:

- Master Registration Authority Officer (MRAO)
- Registration Authority Officer (RAO) - SSL
- Registration Authority Officer (RAO) - S/MIME
- Registration Authority Officer (RAO) - Code Signing
- Registration Authority Officer (RAO) - Device Cert
- Department Registration Authority Officer (DRAO) - SSL
- Department Registration Authority Officer (DRAO) - S/MIME
- Department Registration Authority Officer (DRAO) - Code Signing
- Department Registration Authority Officer (DRAO) - Device Cert

Administrative Roles:

Master Registration Authority Officer (MRAO)

- The MRAO is the top level administrator and can access all areas and functionality of the CCM interface.
- MRAO admins are visible only to other MRAO Admins in the 'Admin Management' area of the CCM interface.
- The MRAO can delegate control over the certificates, domains and notifications of any Organization or Department.

- The MRAO also has full rights over the creation and privileges of Registration Authority Officers (RAOs), Department Registration Authority Officers (DRAOs) and end-users of any Organization or Department. [Click here for more details.](#)

Registration Authority Officer (RAO)

- A Registration Authority Officer (RAO) is an administrative role created by an MRAO or fellow RAO for the purposes of managing the certificates and end-users belonging to one or more CCM Organizations.
- They have control over the certificates that are ordered on behalf of their Organization(s); over Domains that have been delegated to their Organization/Dept by an MRAO; over any Departments of their Organization and over that Organization's end-user membership.
- The RAOs can create Departments and DRAO Administrators within their own Organization, but they should be approved by the MRAO.
- RAO Administrators cannot create a new Organization or edit the General settings of any Organization - even those Organizations to which they have been delegated control. [Click here for more details.](#)

Department Registration Authority Officer (DRAO)

- Department Registration Authority Officers are created by, and subordinate to, the RAO class of Administrator.
- They are assigned control over the certificates, users and domains belonging to a Department(s) of an Organization.
- DRAOs have privileges to access, manage and request certificates for Departments of a Organization that have been delegated to them by a RAO.
- DRAOs have no Admin creation rights. They can edit only self or fellow DRAO administrators of the Department(s) that they administrate.
- DRAOs have visibility of and can request certificates only for the Department(s) that have been delegated to them. They have no access to manage certificates belonging to Organizations or Departments for which they have not been granted permissions. [Click here for more details.](#)

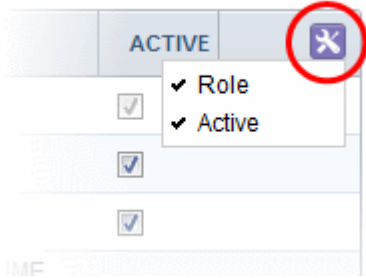
It is also possible to create an Administrator with more than one Admin privileges. Further details about the privileges and security roles of these administrator types can be found in section **1.2.3. Administrative Roles**. The remainder of this chapter contains detailed explanations of the controls available from the 'Admins' tab.

| NAME | EMAIL | LOGIN | TYPE | ROLE | ACTIVE |
|---------------------|-----------------------|----------------|----------|--|-------------------------------------|
| Muratcan Tepencelik | muratcan@comodo.com | muratcan | Standard | MRAO Admin | <input checked="" type="checkbox"/> |
| James DRAO | james@ditherscons.com | james_drao | Standard | DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> |
| George RAO | george@acme.com | george_rao_all | Standard | RAO Admin - S/MIME, RAO Admin - SSL, RAO Admin - Code Signing | <input checked="" type="checkbox"/> |
| Admin MRAO | admin@ditherscons.com | admin | Standard | MRAO Admin | <input checked="" type="checkbox"/> |
| Rufeek | a@a.a | rufeek | Standard | MRAO Admin | <input checked="" type="checkbox"/> |

Admin Management Area - Table of Parameters

| Fields | Values | Description |
|--------|--------|----------------------------|
| Name | String | Administrator's full name. |

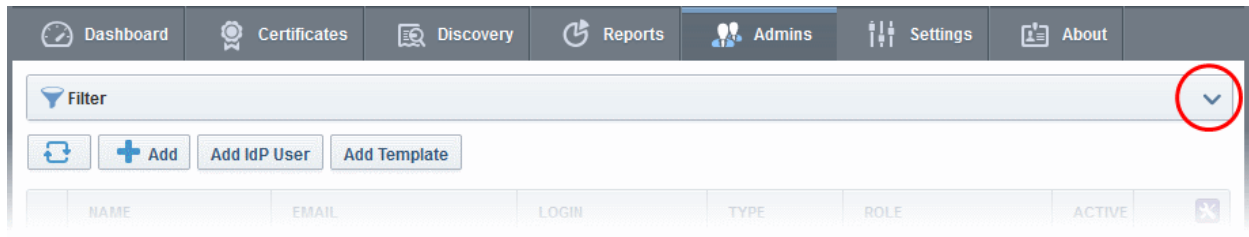
| Admin Management Area - Table of Parameters | | |
|---|-------------------------|--|
| Fields | Values | Description |
| Email | String | Administrator's Email Address (it will be used for client certificate enrollment, notifications) |
| Login | String | The login username of the administrator. |
| Type | | Shows the type of the administrators |
| | Standard | Indicates that the administrator is created in CCM |
| | IdP Template | Indicates that the administrator is added via Identity Provider (IdP) template |
| | IdP User | Indicates that the administrator is added in CCM and was authenticated by IdP |
| Role | MRAO Admin | The MRAO is the top level administrator and can access all areas and functionality of the Certificate Manager interface. (More...) |
| | RAO Admin SSL | RAO SSL administrators have privileges to access, manage, request and approve the requests of SSL certificates for Departments/domains belonging to their Organization. (More...) |
| | RAO Admin S/MIME | RAO S/MIME administrators have privileges to access, manage, request and approve the requests of Client Certificates for Departments/domains that have been delegated to their Organization. (More...) |
| | RAO Admin Code Signing | RAO Code Signing administrators have privileges to access, manage, request and issue the Code signing Certificates for end-users belonging to their Organization. (More...) |
| | RAO Admin Device Cert | RAO Device Cert administrators have privileges to access, manage, and approve Device Certificates issued for devices enrolled through AD server or through SCEP, belonging to their Organization. (More...) |
| | DRAO Admin SSL | DRAO SSL administrators have privileges to access, manage and request SSL certificates for Departments of a Organization that have been delegated to them by MRAO or a RAO Admin. (More...) |
| | DRAO Admin S/MIME | DRAO S/MIME administrators have privileges to access, manage, request Client Certificates for domains that have been delegated to their Department. (More...) |
| | DRAO Admin Code Signing | DRAO Code Signing administrators have privileges to access, manage, request and issue the Code signing Certificates for end-users belonging to their Department. (More...) |
| | DRAO Admin Device Cert | DRAO Device Cert administrators have privileges to access, manage, approve and issue the Device Certs for Devices enrolled through AD server or through SCEP, belonging to their Department. (More...) |
| Active | Checkbox | Indicates whether the administrator is active or not. Also allows the MRAO and delegated RAO admins to switch other admins between active and inactive states according to their privilege levels. |

| Admin Management Area - Table of Parameters | | |
|---|----------------------------|--|
| Fields | Values | Description |
| <p>Note: An administrator can enable or disable the columns displayed in the table, from the drop-down at the right end of the table header :</p>  | | |
| Control Buttons | Refresh | Refreshes the list |
| | Add | Enables MRAO and RAO administrators to add new administrators. |
| | Add IdP User | Enables MRAO administrators to enroll new administrators via Identity Provider (IdP) credentials. |
| | Add Template | Enables MRAO administrators to define privileges for administrators that enrolled via IdP link in the login dialog. |
| Administrator Control Buttons | Edit | Enables MRAO and RAO administrators to modify the details of the selected administrator. |
| | Delete | Deletes the administrator. Note: <i>If an Administrator is deleted, the details of that Administrator can be viewed but they will no longer be editable.</i> |
| | View | Enables MRAO admins to view the details of RAO/DRAO added by another RAO, pending approval. |
| | Approve | Enables MRAO admins to approve RAO/DRAO added by an RAO. The newly added administrator becomes active only on approval by the MRAO. |
| | Reject | Enables MRAO admins to reject RAO/DRAO added by an RAO, pending approval. |
| | Reset Lockout | Enables MRAOs to unlock the login screen that has been locked due to consecutive five wrong attempts to login. |
| | Send/Resend IdP Invitation | Enables MRAO and RAO administrators to send invitation to existing administrators to allow them to login via their IdP credentials. |

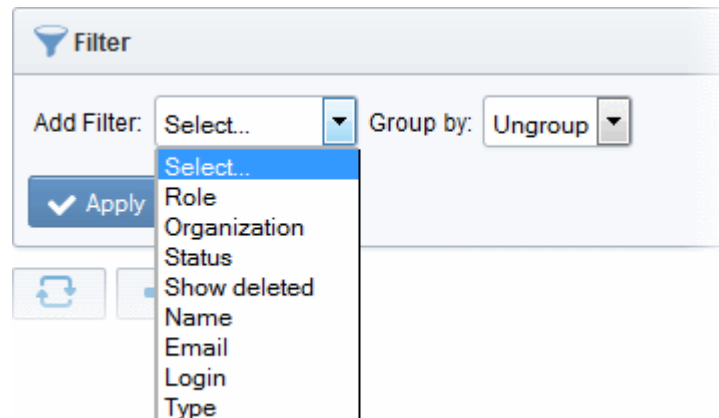
5.1.1 Sorting and Filtering Options

- Clicking on the column header 'Name', 'Email' or Type sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for particular administrator by using filters:



To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.

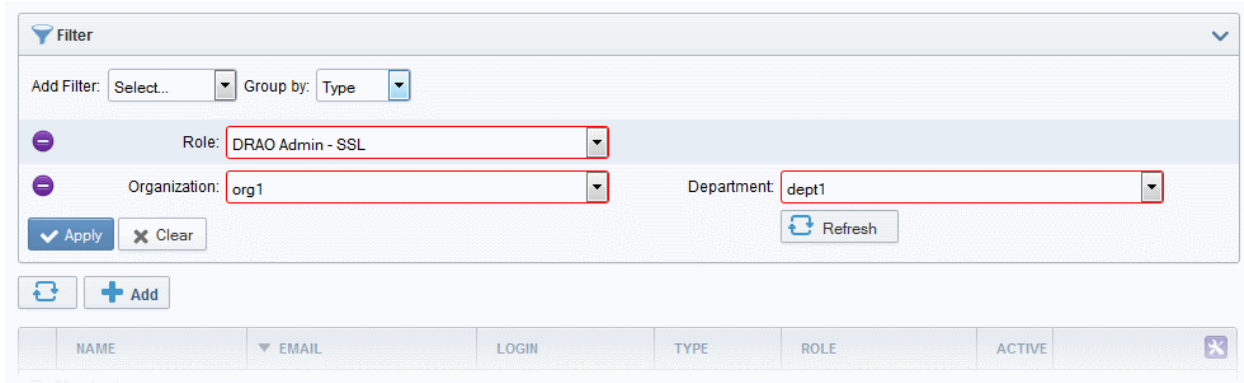


For example if you want to search for DRAO SSL administrators belonging to 'org1' Organization and 'dept1' Department and group them based on their types:

- Choose 'Role' from the 'Add Filter' drop-down
- Choose 'Organization' from the 'Add Filter' drop-down

The Organization and Department filters will be displayed.

- Choose 'org1' Organization and 'dept1' Department from the 'Organization' and 'Department' drop-downs respectively
- Choose 'Type' from the 'Group by' drop-down



- Click the 'Apply' button.

The filtered items based on the entered and selected parameters will be displayed:

| | NAME | EMAIL | LOGIN | TYPE | ROLE | ACTIVE | |
|-----------------------|-------------|------------------|--------|----------|---|-------------------------------------|--|
| Standard | | | | | | | |
| <input type="radio"/> | drao3 test | drao3@ccmqa.com | drao3 | Standard | DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> | |
| <input type="radio"/> | drao39 test | drao39@ccmqa.com | drao39 | Standard | DRAO Admin - S/MIME, DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> | |
| <input type="radio"/> | drao37 test | drao37@ccmqa.com | drao37 | Standard | DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> | |
| <input type="radio"/> | drao38 test | drao38@ccmqa.com | drao38 | Standard | DRAO Admin - SSL, DRAO Admin - Code Signing | <input checked="" type="checkbox"/> | |

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Admins' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

5.2 Adding Administrators

CCM allows administrators to add new admin users in two ways: 1. Manually adding administrators and 2. Inviting them to login via Identity Provider credentials. The IdP method is an optional feature and should be enabled for your account. Please contact your account manager to enable this option. The following method describes how to manually add administrators.

1. Click the 'Admins' tab from the top of the Certificate Manager interface
2. Click the 'Add' button to open the 'Add new Client Admin' form.
3. Complete the 'Add New Client Admin' form.

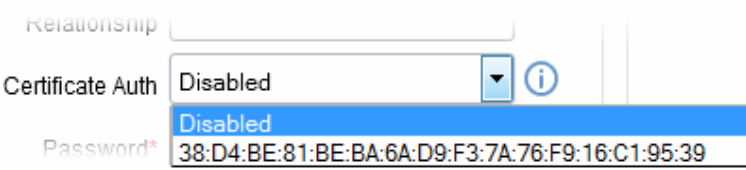
Add New Client Admin
✕

| CREDENTIALS | PRIVILEGES | ROLE |
|--|--|---|
| <div style="background-color: #ffffcc; padding: 5px; margin-bottom: 10px;">*-required fields</div> <p>Login* <input type="text" value="john_rao_ssl"/></p> <p>Email* <input type="text" value="john@dithers.com"/></p> <p>Forename* <input type="text" value="John"/></p> <p>Surname* <input type="text" value="Smith"/></p> <p>Title <input type="text" value="Mr."/></p> <p>Telephone Number <input type="text" value="+919876543210"/></p> <p>Street <input type="text" value="Mount Road"/></p> <p>Locality <input type="text" value="Riverdale"/></p> <p>State/Province <input type="text" value="Alabama"/></p> <p>Postal Code <input type="text" value="123456"/></p> <p>Country <input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="United States"/></p> <p>Relationship <input type="text" value="SSL Cert Admin"/></p> <p>Certificate Auth <input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Disabled"/> ⓘ</p> <p>Password* <input type="password" value="•••••"/></p> <p>Confirm Password* <input type="password" value="•••••"/></p> | <p><input type="checkbox"/> Allow creation of peer admin users</p> <p><input type="checkbox"/> Allow editing of peer admin users</p> <p><input type="checkbox"/> Allow deleting of peer admin users</p> <p><input checked="" type="checkbox"/> Allow DCV</p> <p><input checked="" type="checkbox"/> Allow SSL details changing</p> <p><input checked="" type="checkbox"/> Allow SSL auto approve</p> <p><input type="checkbox"/> WS API use only</p> <p><input type="checkbox"/> MS AD Discovery</p> | <p>Expand All</p> <p><input type="checkbox"/> MRAO Admin</p> <p>+ <input type="checkbox"/> RAO Admin - SSL</p> <p>+ <input type="checkbox"/> RAO Admin - S/MIME</p> <p>+ <input type="checkbox"/> RAO Admin - Code Signing</p> <p>+ <input type="checkbox"/> RAO Admin - Device cert</p> <p>- <input checked="" type="checkbox"/> DRAO Admin - SSL</p> <p style="margin-left: 20px;">- Dithers Organization</p> <p style="margin-left: 40px;"><input checked="" type="checkbox"/> Stores Department</p> <p style="margin-left: 20px;">+ SSL Support Team</p> <p>+ <input type="checkbox"/> DRAO Admin - S/MIME</p> <p>+ <input type="checkbox"/> DRAO Admin - Code Signing</p> <p>+ <input type="checkbox"/> DRAO Admin - Device cert</p> |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> | | |

4. Click 'OK' to add the administrator to the Certificate Manager.

5.2.1 'Add New Client Admin' form - Table of Parameters

| Form Element | Type | Description |
|--------------------|------------|---|
| Credentials | | |
| Login* | Text Field | Enter the login username for the new administrator. |
| Email* | Text Field | Enter full email address of the new administrator. |
| Forename* | Text Field | Enter first name of the new administrator. |
| Surname* | Text Field | Enter surname of the new administrator. |
| Title | Text Field | Enter the title for the new administrator. |
| Telephone Number | Text Field | Enter the contact phone number for the new administrator. |
| Street | Text Field | Enter the address details of the new administrator. |
| Locality | Text Field | |
| State/Province | Text Field | |
| Postal Code | Text Field | |

| Form Element | Type | Description |
|--|------------|--|
| Country | Drop-down | |
| Relationship | Text Field | The role of the new administrator, for example, RAO SSL Administrator. |
| Certificate Auth | Drop-down | <p>Enables the administrator to specify whether the new administrator must authenticate themselves to Certificate Manager with his/her client certificate over a https: connection prior to being granted login rights. The drop-down is auto-populated with the client certificate(s) issued by CCM for the new administrator, based on his/her email address in the 'Email' field.</p>  <p>If authentication is needed, the administrator can select the certificate from the drop-down. The new administrator can login to CCM, only if the specified certificate is installed on the computer from which he/she attempts to login.</p> <p>If authentication is not needed, the administrator can select 'Disabled' from the drop-down.</p> |
| Password* | Text Field | <p>Enter the password for the new administrator to access the CCM interface and reenter the same for confirmation.</p> <p>The new administrator will need to change the password upon his/her first login.</p> |
| Confirm Password* | Text Field | |
| Privileges | | |
| <p>Administrator can assign admin management privileges to the new administrator. The new administrator will be able to add, edit or remove other administrators of their own level or of lower level in the hierarchy, depending on the options selected here.</p> | | |
| Allow creation of peer admin users | Checkbox | Enables the new administrator to add new administrators from their management interface. |
| Allow editing of peer admin users | Checkbox | Enables the new administrator to edit roles of existing administrators from their management interface. |
| Allow deleting of peer admin users | Checkbox | Enables the new administrator to remove existing administrators from their management interface. |
| <p>Note: The new administrator can create, edit or delete the other administrators of their own tier and administrators of the lower tier. Refer to the descriptions under Administrative Roles in the section 4.1 Section Overview for more details.</p> | | |
| Allow domain validation without Dual Approval | Checkbox | The new administrator will be privileged so that the domain creation/delegation approved by the administrator will be activated immediately, without the requirement of approval by a second MRAO. This checkbox will be active only for Administrators with MRAO role. Refer to the section Domains for more details. |

| Form Element | Type | Description |
|--|------------|--|
| Allow DCV | Checkbox | Enables the new administrator to initiate Domain Control Validation (DCV) process for newly created domains. The privilege is available only for MRAO and RAO/DRAO SSL Administrators. |
| Allow SSL Details changing | Checkbox | Enables the new MRAO or RAO/DRAO SSL administrator to change the details of SSL certificates from the Certificates > SSL Certificates interface. |
| Allow SSL auto approve | Checkbox | The SSL certificates requested by the MRAO administrator is automatically approved and those by RAO/DRAO SSL administrators are automatically approved by the administrator of same level and await approval from higher level administrator. |
| WS API use only | Checkbox | The administrator account can only be used for API integration. CCM GUI access will not be allowed for this account. |
| MS AD Discovery | Checkbox | Enables the new administrator to access the Settings > MS Agents interface, integrate an AD server to CCM by downloading and installing the MS agent and view the certificates/web servers discovered by the MS agents by scanning respective AD servers. |
| <p>Note: 'Allow domain validation without Dual Approval' and 'Allow DCV' fields will only be visible if the features are enabled for your account.</p> | | |
| Role | | |
| <p>Administrator can assign the role to the new administrator. For more details on the roles, refer to the section Administrative Roles.</p> | | |
| <ul style="list-style-type: none"> MRAO Admin RAO Admin SSL RAO Admin S/MIME RAO Admin Code Signing RAO Device Cert DRAO Admin SSL DRAO Admin S/MIME DRAO Admin Code Signing DRAO Device Cert | Checkboxes | <p>The new Administrator can be assigned to a particular Organization/Department by selecting the appropriate Organization/Department from the list that appears after selecting a role. All Organizations are listed by default. Clicking the '+' button beside the Organization name expands the tree structure to display the Departments associated with the Organization.</p> <ul style="list-style-type: none"> Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization. |

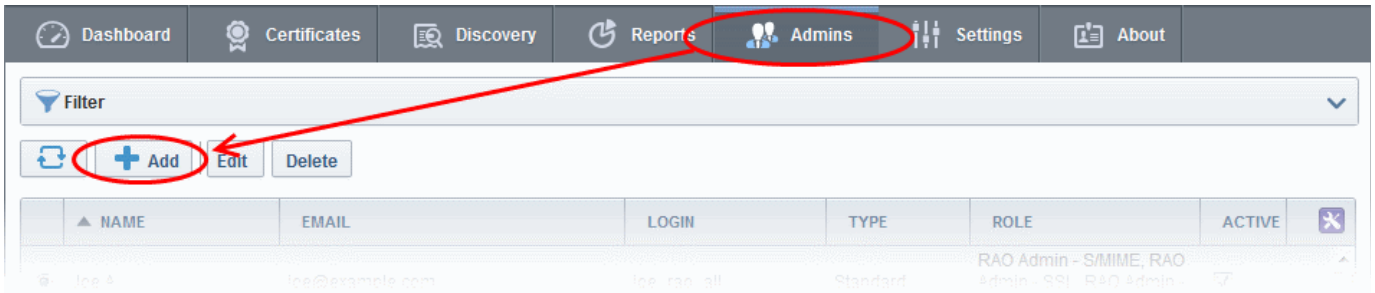
Note: Fields marked with * are mandatory.

Important Note: The administrators created by the MRAOs and RAOs with the Admin Creation Privileges are immediately added to the CCM. But the administrators created by other RAOs will await approval from the MRAO. The new administrators will be added to CCM only if the MRAO approves them by selecting the administrator and

clicking the 'Approve' button at the top in the Admin Management area of the CCM interface. The details of the new administrator created by an MRAO can be modified at any time by selecting the administrator and clicking the 'Edit' button at the top. The details of the new administrator created by an RAO can be edited at any time after the new administrator has been approved by the MRAO.

5.2.2 Example: Adding a New Administrator with Multiple Roles

1. Click the 'Admin Management' tab at the top left of the Certificate Manager interface.
2. Click the 'Add' button to open the 'Add new Client Admin' form (as shown below).



3. Complete the 'Add New Client Admin' form.

Add New Client Admin

| CREDENTIALS | PRIVILEGES | ROLE |
|--|---|--|
| <p>*-required fields</p> <p>Login* <input type="text" value="joe_rao_all"/></p> <p>Email* <input type="text" value="joe@dithers.com"/></p> <p>Forename* <input type="text" value="Joe"/></p> <p>Surname* <input type="text" value="A"/></p> <p>Title <input type="text" value="Mr"/></p> <p>Telephone Number <input type="text" value="+919000012345"/></p> <p>Street <input type="text" value="Mount Road"/></p> <p>Locality <input type="text" value="Riverdale"/></p> <p>State/Province <input type="text" value="Alabama"/></p> <p>Postal Code <input type="text" value="123456"/></p> <p>Country <input type="text" value="United States"/></p> <p>Relationship <input type="text" value="Certificate Admin"/></p> <p>Certificate Auth <input type="text" value="Disabled"/></p> <p>Password* <input type="password" value="•••••"/></p> <p>Confirm Password* <input type="password" value="•••••"/></p> | <p><input type="checkbox"/> Allow creation of peer admin users</p> <p><input type="checkbox"/> Allow editing of peer admin users</p> <p><input type="checkbox"/> Allow deleting of peer admin users</p> <p><input checked="" type="checkbox"/> Allow DCV</p> <p><input checked="" type="checkbox"/> Allow SSL details changing</p> <p><input checked="" type="checkbox"/> Allow SSL auto approve</p> <p><input type="checkbox"/> WS API use only</p> <p><input checked="" type="checkbox"/> MS AD Discovery</p> | <p>Expand All</p> <p><input type="checkbox"/> MRAO Admin</p> <p><input checked="" type="checkbox"/> RAO Admin - SSL</p> <p style="margin-left: 20px;"><input type="checkbox"/> Comodo SE</p> <p style="margin-left: 20px;"><input type="checkbox"/> Device Org</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> Dithers Organization</p> <p style="margin-left: 20px;"><input type="checkbox"/> SSL Support Team</p> <p><input checked="" type="checkbox"/> RAO Admin - S/MIME</p> <p style="margin-left: 20px;"><input type="checkbox"/> Comodo SE</p> <p style="margin-left: 20px;"><input type="checkbox"/> Device Org</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> Dithers Organization</p> <p style="margin-left: 20px;"><input type="checkbox"/> SSL Support Team</p> <p><input checked="" type="checkbox"/> RAO Admin - Code Signing</p> <p><input checked="" type="checkbox"/> RAO Admin - Device cert</p> <p style="margin-left: 20px;"><input type="checkbox"/> Comodo SE</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> Device Org</p> <p style="margin-left: 20px;"><input type="checkbox"/> Dithers Organization</p> <p style="margin-left: 20px;"><input type="checkbox"/> SSL Support Team</p> <p><input type="checkbox"/> DRAO Admin - SSL</p> <p><input type="checkbox"/> DRAO Admin - S/MIME</p> <p><input type="checkbox"/> DRAO Admin - Code Signing</p> <p><input type="checkbox"/> DRAO Admin - Device cert</p> |
| <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> | | |

- Fill out the contact, login details and password and select the privileges that should apply to the new administrator
- Next, you should specify the new administrator's security role:

A new administrator can be:

- MRAO Admin - Will be able to manage ALL certificates for ALL listed Organizations, (this is disables the Organization selection checkboxes.)
- RAO Admin SSL - Will be able to manage ONLY SSL certificates and ONLY for selected Organization(s).
- RAO Admin S/MIME - Will be able to manage ONLY client certificates and ONLY for selected Organization(s).
- RAO Admin Code Signing - Will be able to manage ONLY the code signing certificates issued to end-users belonging to the selected Organization(s).
- RAO Admin Device Cert - Will be able to manage ONLY the device authentication certificates issued to devices belonging to the selected Organization(s).
- DRAO Admin SSL - Will be able to manage ONLY SSL certificates and ONLY for selected Departments(s).
- DRAO Admin S/MIME - Will be able to manage ONLY client certificates and ONLY for selected Departments(s).
- DRAO Admin Code Signing - Will be able to manage ONLY the code signing certificates issued to end-users belonging to the selected Department(s).
- DRAO Admin Device Cert - Will be able to manage ONLY the device authentication certificates issued to devices belonging to the selected Department(s).

The same RAO can be assigned as RAO SSL, RAO S/MIME and RAO Code Signing as required. Similarly, same DRAO can be assigned as RAO SSL, RAO S/MIME and RAO Code Signing as required. Further details about the privileges and security roles of these administrator types can be found in section **1.2.3. Administrative Roles**

4. Select the Organization/Department to which the new administrator will have access as shown above.

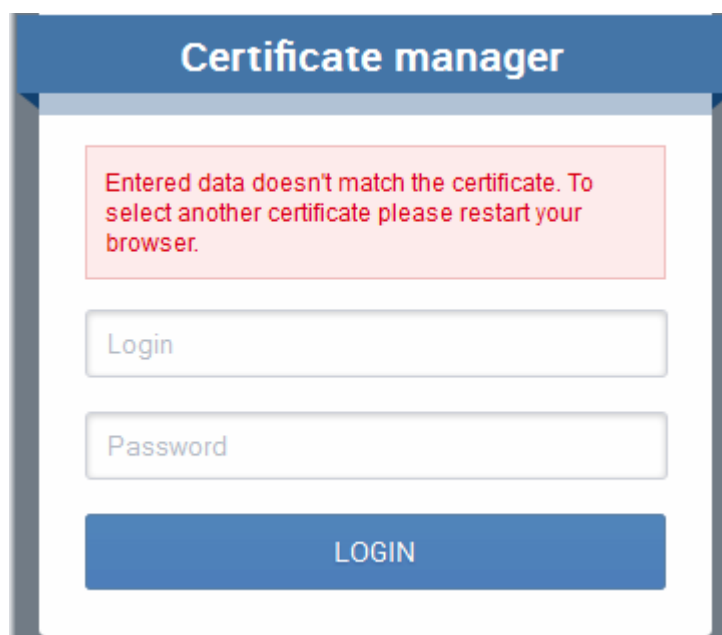
If the single RAO is chosen as RAO SSL, RAO S/MIME and/or RAO Code Signing, he or she can have the multiple privileges only for a particular Organization. Similarly, If the single DRAO is chosen as DRAO SSL, DRAO S/MIME and/or DRAO Code Signing, he or she can have the multiple privileges only for a particular Department.

5. Click 'OK' to save all changes and finish the process.

5.2.2.1 The 'Certificate auth' Field

If enabled, the administrators currently being created will only be able to login to Certificate Manager after authenticating themselves with an certificate. This means, that the Certificate Manager Server will request the certificate specified during creation of the administrator in addition to their login and password details.

If Certificate Manager does not detect the authentication certificate specified during adding an admin, an error will be displayed and the administrator will not be able to login.



The screenshot shows a web interface titled "Certificate manager". At the top, there is a blue header with the title. Below the header, a red-bordered box contains the following error message: "Entered data doesn't match the certificate. To select another certificate please restart your browser." Below this message are two input fields: "Login" and "Password". At the bottom of the form is a blue button labeled "LOGIN".

Note: In the event that an administrator has replaced their certificate used for 'Certificate Auth', Certificate Manager needs to re-sync their certificate information. You will need to re-select the appropriate certificate. To do this:

- Open the Admins interface by clicking the 'Admins' tab
- Click 'Edit' button at the top after selecting the radio button next to the administrator's name to re-open the administrator configuration dialog
- Select the new authentication certificate from the 'Certificate Auth' drop down.
- Save by clicking 'OK'.

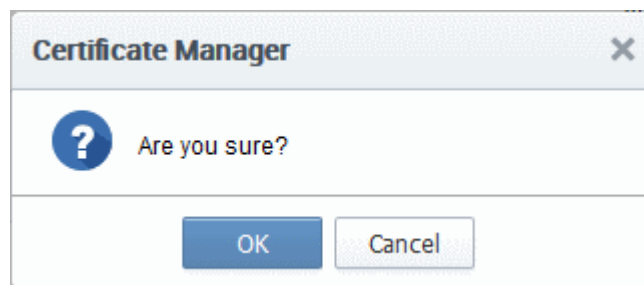
5.3 Editing Administrators

All parameters of any administrator can be modified at any time by selecting the administrator under the 'Admins' tab and clicking the 'Edit' button at the top.

Full details of the options available when editing an existing administrator are available in the section '**Add New Client Admin**' form - [table of parameters](#)'.

5.4 Deleting an Administrator

Master administrator can delete any administrator by selecting the administrator and clicking the 'Delete' button at the top.



- Click OK to delete the Administrator.

Note: There must always be at least one MRAO Administrator. It is not possible to delete the 'last' Master Administrator.

6 Settings

6.1 Overview

The 'Settings' tab contains a maximum of eleven sub-tabs. The number of tabs available depends on the privilege level of the currently logged-in Administrator.

| | NAME | CITY | STATE | COUNTRY | VALIDATION STATUS |
|----------------------------------|----------------------|-------------|-------------------------------|---------|-------------------|
| <input type="radio"/> | docs[50] | Chennai | TN | IN | Not Validated |
| <input type="radio"/> | XYZ Organization[55] | City Name | Name of the state or province | US | Not Validated |
| <input type="radio"/> | Dithers Company[51] | Kanchipuram | TN | IN | Not Validated |
| <input checked="" type="radio"/> | acme corp[54] | Chennai | TN | IN | Validated |

- **Organizations** - Enables MRAO and RAO administrators to view the list of Organizations, add/edit/delete Organizations and assign Departments and Domains to the Organizations. MRAOs can initiate the process of validating Organizations for the purpose of requesting and issuance of OV SSL certificates to Organizations and Departments under them.
- **Departments** - Visible only to DRAO class administrators (DRAO's see a 'Departments' tab instead of the 'Organizations' tab). Allows DRAOs to view all Departments that have been delegated to them and to request new domains for those Departments.
- **Domains** - Contains a list of all domains that have been created in CCM. This interface allows administrators to add new domains, edit domain details, activate or deactivate a domain, delegate the domain to a particular Organization or Department of an Organization, select the validation type and to filter viewed domains using a range of parameters.
- **Notifications** - Allows administrators to precisely define email notifications to various personnel based on a range of parameters - including notifications triggered by SSL certificate status, notifications triggered by Client Certificate status and notifications triggered by Discovery Scan Summaries.
- **Encryption and Key Escrow** - Overview of key escrow processes.

Note: MRAO and RAO/DRAO S/MIME Administrators are strongly advised to familiarize themselves with the information in this section before creating their first Organization or Department. Once key escrow options have been set they cannot be reversed.

- **Access Control** - Enables administrator to grant access only for specified IP range.
- **Email Template** - Allows MRAO and RAO administrators to directly edit the content of the automated notification emails issued by CCM. DRAO administrators can edit templates for their Department via the 'Edit Department' dialog (Settings > Departments > Edit)
- **Private Key Store** - Allows the MRAO to configure the controller software which manages the private keys

and their backups.

- **Certificates** - Enables MRAO admins to select the types and term length of certificates which will be available through the built-in application form and/or Self Enrollment form. MRAO admins can also add additional custom fields to these forms. **Note:** The custom fields can be added only if this feature is enabled for your account. Please contact your Comodo account manager for enabling this feature.
- **MS Agents** - Enables MRAO admins download the agent, view existing agents and modify agent settings. Once installed, MS agents fetch details about the network and all types of certificates installed on all servers, devices and AD objects in the network.
- **Assignment Rules** - Allows MRAO admins to create rules which will assign certificates found during a discovery scan to a specific organization or department.

6.2 Organizations

6.2.1 Section Overview

The creation of Organizations and Departments and the association of these entities with a domain is an important step towards the issuance and effective management of SSL, code signing, S/MIME and device authentication certificates via the CCM interface.

- Organizations are umbrella entities created by administrators for the purposes of requesting, issuing and managing certificates for domains and employees.
- Organizations can be sub-divided into Departments for the purpose of certificate and end-user management.
- Each Organization can have multiple Departments. Furthermore, each Organization and each Department can have multiple domains delegated to it.
- It is possible to assign Organization level administrators (RAO Admins) and Department level administrators (DRAO Admins).
- Depending on their roles, Organization level administrators can manage certificates, domains and users belonging to their Organization *and* any of its sub-Departments. They are also able to create new Departments and appoint Department administrators.
- Depending on their roles, Department level administrators can view and manage only those certificates, domains and users belonging to the Department for which they have been delegated responsibility.

Comodo Certificate Manager uses the following naming conventions for Organizations and Administrators:

| CCM Entity | Administrator Types |
|---|--|
| Organization | RAO - SSL Admin RAO - S/MIME Admin RAO - Code Signing Admin RAO - Device cert |
| Department | DRAO - SSL Admin DRAO - S/MIME Admin DRAO - Code Signing Admin DRAO - Device cert |
| Master Registration Authority Officers (MRAOs) have complete visibility of and control over all Organizations and | |

Departments.

Although we strongly advise Administrators to plan any Organizational and administrative structure beforehand, it is, of course, possible to rearrange and tweak it later. Organizations, Departments, Domains and Administrators are each created and configured as independent entities in CCM. It is the association and delegation of these entities into a coherent superstructure which forms the key to an effective certificate management hierarchy for your enterprise. If you would like further advice on setting up an Organizational structure and administrative chains-of-command then please contact your Comodo account manager. Our representatives have years of experience in PKI management infrastructures and will be pleased to help you find the correct deployment strategy for your company.

6.2.1.1 Example Scenarios

In order to maximize the effectiveness of your CCM implementation, it is important that you first decide the structure of your Organizational and administrative hierarchy. CCM's flexibility allows you to create and delegate hierarchies that are as simple or sophisticated as you require.

The examples listed below are merely workable suggestions for reasonably straightforward situations. Administrators should, of course, follow their own policies when determining how to setup and manage domains between Organizations and Departments. Each example outlines a hypothetical issuance scenario followed by two or three alternative solutions that are possible through CCM:

Example 1:

Scenario: You wish to issue only SSL certificates for a single first level domain and two sub-domains.

Solution 1 - Simple:

- Create a single Organization
- No Departments
- Delegate all the domain and the sub-domains to this single Organization
- The MRAO manages all SSL certificates for all domains

| Organization Name | Department Name | Administrator | Could be used to manage certificates for: |
|-------------------|-----------------|---------------|---|
| Organization 1 | - | MRAO | http://website_1.com |
| | | | http://payments.website_1.com |
| | | | http://mail.website_1.com |

Solution 2 - Intermediate:

- Create three Organizations
- No Departments
- Delegate each domain to a separate Organization
- Create three RAO SSL Admins
- Delegate one RAO SSL Admin to each of the Organizations

| Organization Name | Department Name | Administrator | Could be used to manage certificates for: |
|-------------------|-----------------|-----------------|---|
| Organization 1 | - | RAO SSL ADMIN 1 | http://website_1.com |

| | | | |
|----------------|---|-----------------|-------------------------------|
| Organization 2 | - | RAO SSL ADMIN 2 | http://payments.website_1.com |
| Organization 3 | - | RAO SSL ADMIN 3 | http://mail.website_1.com |

Solution 3 - Intermediate:

- Create a single Organization
- Create three Departments under this Organization
- Delegate each Domain to one of these Departments
- Create one RAO SSL Admin
- Delegate the RAO SSL to control the Organization (and therefore also its Departments)
- Create three DRAO SSL Admins
- Delegate one DRAO SSL Admin to each of the Departments

| Organization Name | Department Name | Administrator | Could be used to manage certificates for: |
|-------------------|-----------------|------------------|---|
| Organization 1 | Department 1 | DRAO SSL ADMIN 1 | http://website_1.com |
| | Department 2 | DRAO SSL ADMIN 2 | http://payments.website_1.com |
| | Department 3 | DRAO SSL ADMIN 3 | http://mail.website_1.com |

Example 2:

Scenario: Your company issues both SSL certificates and S/MIME certificates. Your company operates 2 distinct websites, each with it's own unique first level domain name and two sub-domains.

Solution 1 - Very Simple:

- Create a single Organization
- No Departments
- Delegate both first level domains and all sub-domains to this single Organization
- The MRAO manages all SSL certificates and all S/MIME certificates for all domains

| Organization Name | Department Name | Administrator | Could be used to manage certificates for: |
|-------------------|-----------------|---------------|---|
| Organization 1 | - | MRAO | http://website_1.com |
| | | | http://payments.website_1.com |
| | | | http://mail.website_1.com |
| | | | http://website_2.com |
| | | | http://payments.website_2.com |
| | | | http://mail.website_2.com |

Solution 2 - Sophisticated:

- Create two Organizations
- Create three Departments in each Organization

- Delegate one first level Domain and it's sub domains to each of the three Departments in an Organization
- Create one RAO Admin. Assign this single RAO with SSL and S/MIME Administrative roles
- Delegate the RAO to control both Organizations (and therefore all Departments, domains and sub-domains)
- Create three DRAO SSL Admins
- Create six DRAO S/MIME Admins
- Delegate one DRAO Admin per certificate type to each of the three Departments

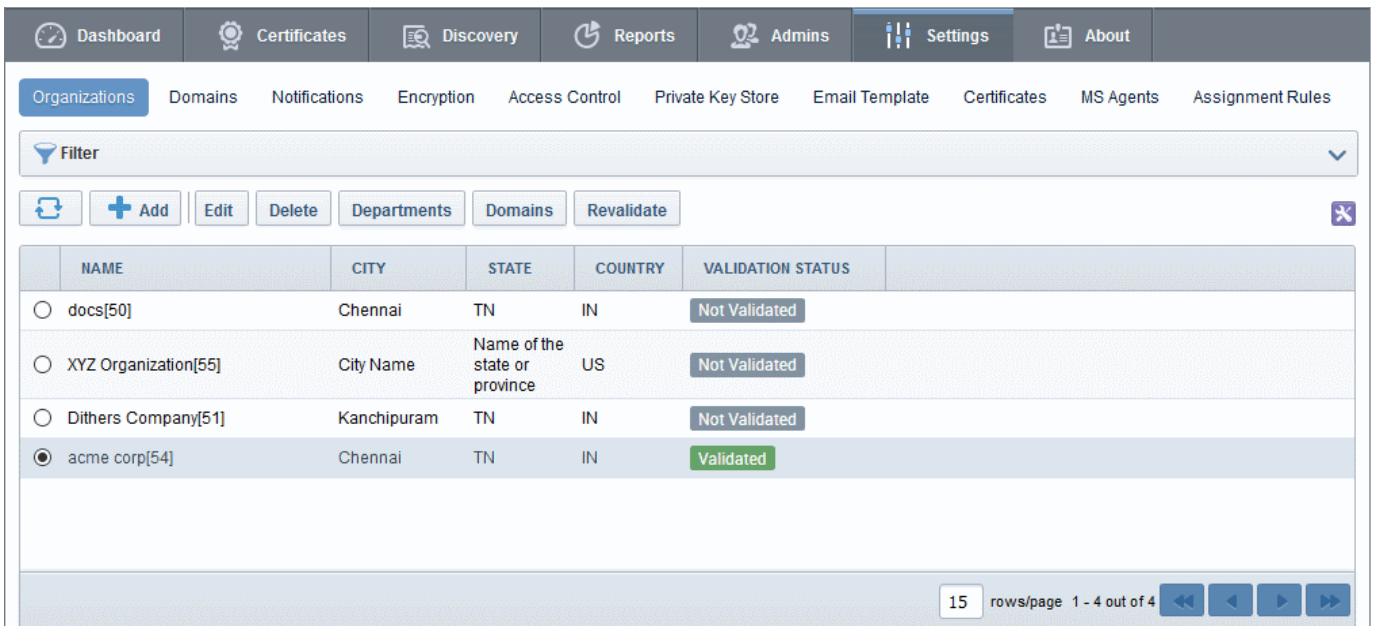
This means that you will have 2 Organizations, each with three Departments. Each of these Departments is associated with a distinct first level domain or sub-domain. Each Department has *two* Departmental Administrators - each responsible for a particular certificate type. All of these Department Administrators (DRAOs) are sub-ordinate to the Organization Admin (RAO) who is, in turn, sub-ordinate to the MRAO.

| Organization Name | Department Name | Administrator | Could be used to manage certificates for: |
|-------------------|-------------------------------|---------------------|---|
| Organization 1 | Organization 1 - Department 1 | DRAO SSL ADMIN 1 | http://website_1.com |
| | | DRAO S/MIME ADMIN 1 | http://website_1.com |
| | Organization 1 - Department 2 | DRAO SSL ADMIN 2 | http://payments.website_1.com |
| | | DRAO S/MIME ADMIN 2 | http://payments.website_1.com |
| | Organization 1 - Department 3 | DRAO SSL ADMIN 3 | http://mail.website_1.com |
| | | DRAO S/MIME ADMIN 3 | http://mail.website_1.com |
| Organization 2 | Organization 2 - Department 1 | DRAO SSL ADMIN 1 | http://website_2.com |
| | | DRAO S/MIME ADMIN 4 | http://website_2.com |
| | Organization 2 - Department 2 | DRAO SSL ADMIN 2 | http://payments.website_2.com |
| | | DRAO S/MIME ADMIN 5 | http://payments.website_2.com |
| | Organization 2 - Department 3 | DRAO SSL ADMIN 3 | http://mail.website_2.com |
| | | DRAO S/MIME ADMIN 6 | http://mail.website_2.com |

6.2.2 Organization Management

6.2.2.1 Organizations Area Overview

To open the 'Organizations' management area, click the 'Organizations' sub-tab under the 'Settings' tab. The 'Organizations' tab is not visible to a DRAO (they see the 'Departments' tab instead).



This area :

- Lists all Organizations available to an Administrator as per their privilege level
- Facilitates the creation and deletion of Organizations and Departments
- Facilitates the modification of settings for any existing Organization or Department
- Allows Administrators to delegate Domains to an Organization or Department
- Allows Administrators to initiate the Organization validation process
- Allows Administrators to search and filter Organizations by Name and Department.

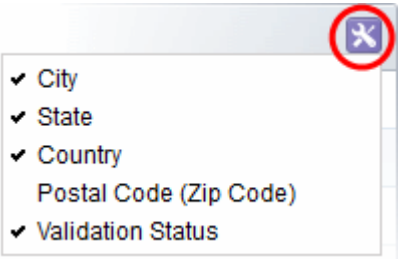
Administrative Roles:

- MRAO Administrators - Can see a list of all the Organizations and their Departments in the Organizations area. They can create new Organizations and Departments and have full control over the management of all the Organizations and Departments. They can initiate the process of validating Organizations for the purpose of requesting and issuance of OV SSL certificates to Organizations and Departments.
- RAO Administrators - Can only see their own Organization(s) in the 'Organizations' area. They cannot create new Organizations but can manage and create Departments for the Organization(s) that has/have been delegated to them.
- DRAO Administrators cannot view the 'Organizations' area. They have visibility only of the 'Departments' tab. They have the rights to manage only the Department(s) that has/have been delegated to them.

The following table provides a summary of the ability of Administrator types to manage Organizations and Departments:

| MRAO | RAO | DRAO |
|---|--|---|
| Can create and manage: <ul style="list-style-type: none"> • Any Organization • Any Department | <ul style="list-style-type: none"> • Can Manage the Delegated Organization • Can create and manage Subordinate Department(s) | Can manage Delegated Department (s) (via the 'Departments' sub-tab) |

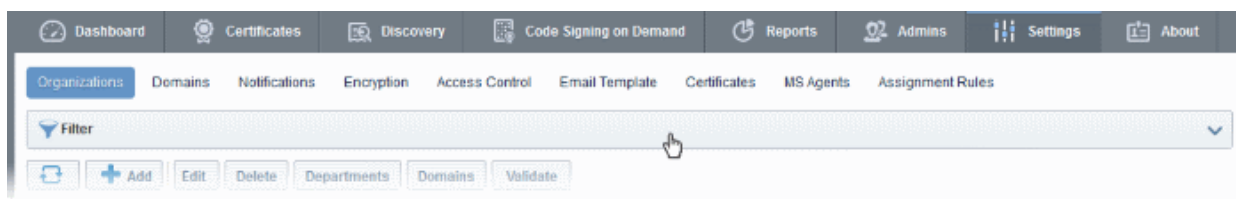
6.2.2.2 Summary of Fields and Controls

| Organizations Area - Table of Parameters | | |
|--|-------------|---|
| Fields | Values | Description |
| Name | String | Name of the Organization |
| City | String | Name of the City where the Organization is located |
| State | String | Name of the State or province |
| Country | String | Two character country code |
| Postal Code | Numeric | The postal code or zip code of the city |
| Validation Status | String | Displays whether the Organization is validated for the request and issuance of OV SSL certificates. For more details refer to the section Validating an Organization . |
| <p>Note: An administrator can select the columns to be displayed in the table from the drop-down at the right end of the table header:</p> <div style="text-align: center;">  </div> | | |
| Control Buttons | Add | Enables MRAO Administrators to create a new Organization for the purposes of issuing certificates to end-users and domains. The button is not visible to RAO and DRAO Admins. |
| | Refresh | Refreshes the list |
| Organization Control Buttons Note: The Organization control buttons appear only on selecting an Organization | Edit | Enables administrators to modify General, Client, SSL and Code Signing Certificate settings pertaining to an existing Organization. |
| | Delete | Deletes the Organization. The button is not visible to RAO and DRAO Administrators. |
| | Departments | Enables administrators to view and manage Departments that belong to that Organization. |
| | Domains | Enables administrators to view, edit and delegate domains to the Organization and the Departments within the Organization. |
| | Validate | Enables administrators to initiate the Organization validation process. |

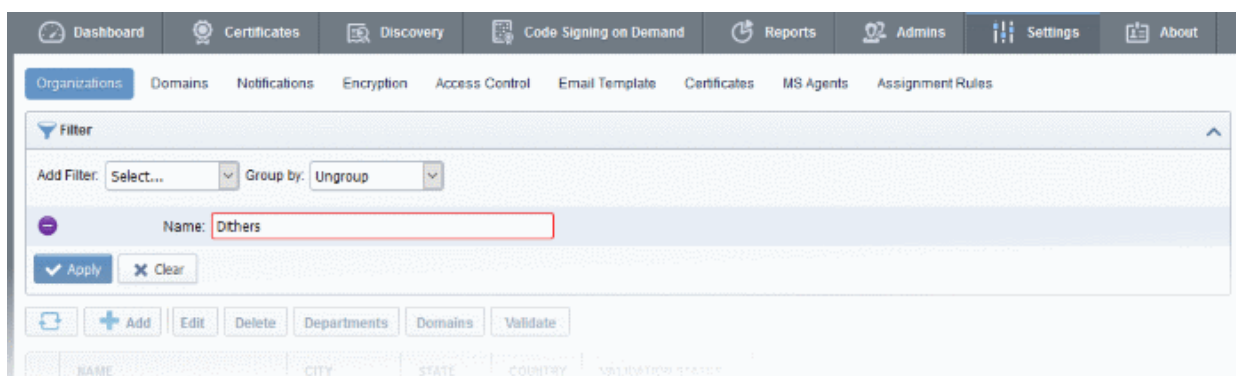
6.2.2.3 Sorting and Filtering Options

- Clicking on the column header 'Name' sorts the items in the alphabetical order of the names of the Organizations.

Administrators can search for particular Organization by using the filters.

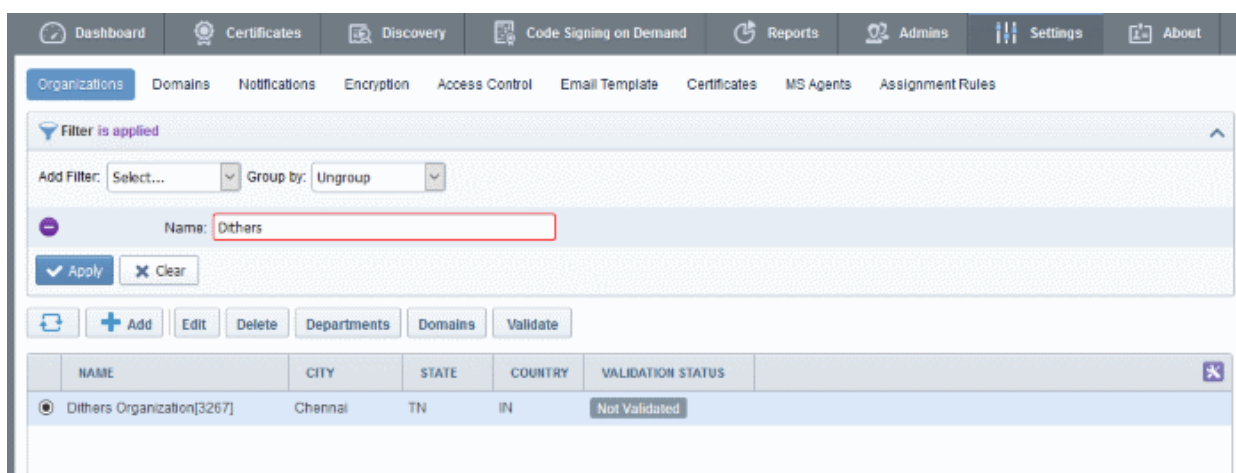


To apply filters, click anywhere on the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



- Enter part of or full name in the 'Name' field and click the Apply button.

The filtered items based on the entered parameters will be displayed.



- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Organizations' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.2.2.4 Creating a New Organization

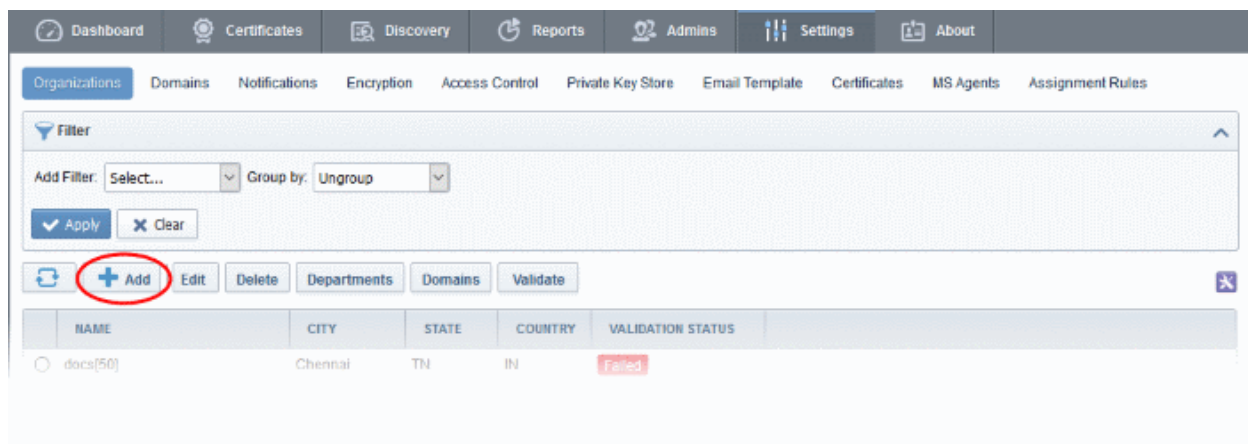
In order to provide certificates to employees, for websites, for code signing or for devices, the MRAO should first create an 'Organization'. Organizations are uniquely identified by combination of the Organization's 'Access Code' and the Common Name specified in 'General' properties. More than one Organization can share either the same Access Code or the same Common Name but no two Organizations can share both.

If OV certificates are enabled for the CCM account, the Organizations for which OV certificates are requested, need to be validated by Comodo. For more details on Organization Validation please refer to the section [Validating an Organization](#).

Once an Organization is created, an appropriately privileged Administrator can:

- Request SSL certificates using the CCM interface for the domain that is associated with that Organization and can approve or reject certificate requests
- Create multiple Departments within an Organization and associate each Department with a distinct domain(s). (See '**Organizations / Section Overview**' for more details)
- Assign membership of that Organization to end-users and provision them with client certificates for the Common Name (domain) that is associated with that Organization. (List of end-users is viewable in the 'Client Certificates' area of 'Certificates Management' section)
- Manage the client certificates of end-users belonging to that Organization via the 'Client Certificates' sub-tab of CCM interface
- Manage SSL certificates for the Organization via the 'SSL certificates' area
- Manage Code Signing certificates for the Organization via the 'Code Signing' area
- Manage device certificates for the Organization via the 'Device Certificates' area
- Edit the General, Client Certificate and SSL Certificate parameters that apply to that Organization by clicking the 'Edit' button at the top after selecting the checkbox next to its name in the 'Organizations' sub area of 'Settings'
- Utilize the **Certificate Discovery** feature to audit, then monitor all certificates on the network
- Configure a wide range of email notifications for that Organization
- View, filter and export a variety of reports and activity logs for that Organization

The MRAO admin can add a new Organization at any time by clicking the 'Add' button located at the top of the 'Organizations' area:



This will open the 'Add New Organization' dialog.

The dialog contains a maximum of six tabs:

- **General**
- **EV Details**
- **Client Cert**
- **SSL**
- **Code Signing**
- **Device Certificate**

The next six sections of this guide will explain these tabs in more detail.

6.2.2.4.1 General Settings

'General' settings allows the MRAO to configure high level details relating to the new Organization:

Add New Organization [X]

General | Client Certificate | SSL Certificate | Code Signing Certificate | Device Certificate

*-required fields

Organization Name*

Address1*

Address2

Address3

City*

State/Province*

Postal Code*

Country*

Validation Status

Anchor certificate

OK Cancel

- The 'Organization Name' and 'Address' information specified for an Organization will be used to populate the 'Subject' field of any SSL certificates requested and issued for this Organization.
- It is important that Administrators make sure that the details above match those used when generating their CSR.
- Fields marked with "*" are mandatory and an Organization cannot be created without filling them out.
- The details entered in the 'General' section are used for Client, SSL and Code Signing Certificates requested on behalf of that Organization.
- In order to issue Organization Validated (OV) SSL certificates for Organizations and Departments under them your CCM should have been enabled for OV certificates and the Organization should be validated by Comodo. The validation process for newly created Organizations can be initiated by MRAOs and when the process is completed successfully, the 'Validation Status' field will display 'Validated'. The Anchor Certificate will display as ON and this will be used for OV reference by CCM whenever an Organization Validated SSL certificate is requested for an Organization or Departments under it.

The various stages of validation status are:

- Not Validated - The validation process not started.
- Validated - The Organization is validated and anchor certificate issued.
- Pending - Validation process started and not completed.
- Failed - The validation process failed for the Organization.
- Expired - The validation period of 36 months is expired for the Organization.

For more details on Organization Validation, refer to the section [Validating an Organization](#).

- Client and SSL certificates may only be automatically issued to common names of domains (and sub-domains) delegated to the Organization which Comodo CA has pre-validated that you have the right to use. If you apply for certificates on a new domain, then Comodo CA will first need to validate your ownership of the domain before the certificate can be issued for it. See [Delegating Domains to Organizations](#) for more details.
- For more details on these fields, see '[General Settings](#)' - [table of parameters](#)'
- For background information on Organizations and Departments, see '[Organizations / Section Overview](#)'

6.2.2.4.2 General Settings - Table of Parameters

| Field Name | Values | Description |
|--------------------|---------------------------|---|
| Organization Name | <i>Textbox (required)</i> | The name of the Organization to be created. |
| Address 1 | Textbox (required) | Organization's address (used for issuing SSL and S/MIME certificates) |
| Address 2 | Textbox | Organization's address (used for issuing SSL and S/MIME certificates) |
| Address 3 | Textbox | Organization's address (used for issuing SSL and S/MIME certificates) |
| City | Textbox (required) | City where the Organization is located (used for issuing SSL and S/MIME certificates) |
| State/Province | Textbox (required) | State or province (used for issuing SSL and S/MIME certificates) |
| Postal Code | Textbox (required) | Postal code (used for issuing SSL and S/MIME certificates) |
| Country | Textbox (required) | Two characters country code (used for issuing SSL and S/MIME certificates) |
| Validation Status | | Indicates the progress of Organizational Validation (OV) on the 'Organization' in question. States can be 'Not validated', 'Validated', 'Pending', 'Failed', 'Expired'. The Validation Status will be displayed only if OV certificates are enabled for the CCM account. |
| Anchor Certificate | | Indicates the status of Anchor certificate. The Anchor Certificate is issued after the Organization Validation is completed. This is used as a reference for Organization Validation status by CCM whenever an OV SSL certificate is requested for the Organization or Departments under it. The Anchor Certificate field will be displayed only if OV certificates are enabled for the CCM account. |

6.2.2.4.3 EV Details Tab

The EV Details tab allows appropriately privileged administrators to enter the details of the Organization that are required for validation purpose before the issuance of EV SSL certificates for the Organization and / or Departments under it. The details provided in these fields will be auto populated in the EV SSL certificate request form. The administrator can also leave these fields blank and the details will be fetched from the EV SSL certificate request form and automatically filled when the request is submitted.

Note: The EV details tab is displayed only if Extended Validation Registration Authority (EVRA) feature is enabled for your CCM account. Contact your CCM account manager for enabling this feature.

Add New Organization
✕

General
EV Details
Client Certificate
SSL Certificate
Code Signing Certificate
Device Certificate

Incorporation or Registration Agency

Incorporating Agency

Main Telephone Number

DUN and Bradstreet Number

Company Registration Number

Jurisdiction of Incorporation City or Town

State or Province of Incorporation

Country of Incorporation

Date of Incorporation

Business Category

Contract Signer

Title

Forename

Surname

Email

Telephone Number

Street

Locality

State/Province

Postal Code

Country

Relationship

6.2.2.4.4 EV Details - Table of Parameters

| Field Name | Type | Description |
|---|------------|--|
| Incorporating Agency | Textbox | Name of the Incorporating Agency in whose records the name of the Organization exists as a legal entity. |
| Main Telephone Number | Textbox | The primary telephone number of the Incorporating Agency. |
| DUN and Bradstreet Number | Textbox | The nine digit number issued by D&B to the Organization. |
| Company Registration Number | Textbox | The registration number issued to the Organization. |
| Locality | Textbox | The locality where the Organization is established. |
| State or Province of Incorporation | Textbox | The State or Province where the Organization is located. |
| Country of Incorporation | Drop-downs | The country where the Organization is established. |
| Date of Incorporation | Selection | The date on which the Organization was registered. |
| Business Category | Drop-down | The business category of the Organization. The options are: Private Organization Government Entity Business Entity Non-Commercial Entity |
| Contract Signer - The person representing the Organization that has signed the EV SSL contract with Comodo. | | |
| Title | Textbox | Title of the contract signer |
| Forename | Textbox | First name of the contract signer |
| Surname | Textbox | Last name of the contract signer |
| Email | Textbox | Email address of the contract signer |
| Telephone | Textbox | Primary telephone number of the contract signer |
| Street | Textbox | Name of the street where the contract signer is located. |
| Locality | Textbox | Name of the locality where the contract signer is located. |
| State/Province | Textbox | Name of the state or province where the contract signer is located. |
| Postal Code | Textbox | Postal code of the area where the contract signer is located. |
| Country | Drop-downs | Name of the country where the contract signer is located. |
| Relationship | Textbox | The relationship of the contract signer with the Organization. |

6.2.2.4.5 Client Cert Settings Tab

The Client Cert tab allows appropriately privileged administrators to configure enrollment and term settings relating to S/MIME (email and client) certificates issued to end-users. The settings chosen in this section relate only to those

client certificates issued to the domain associated with the currently selected Organization.

Add New Organization
✕

General

Client Certificate

SSL Certificate

Code Signing Certificate

Device Certificate

Self Enrollment

Access Code*

Web API

Secret Key*

Allow Key Recovery by Master Administrators

Allow Key Recovery by Organization Administrators

Allow Principal Name

Allow Principal Name Customization

Client Cert Types

6.2.2.4.6 Client Certificate tab - Table of Parameters

| Field Name | Type | Description |
|--|---|---|
| Self Enrollment | Checkbox Default state - not checked | <p>Checking this box will allow the end-users that belong to the Organization to apply for a personal certificate using the enrollment form hosted (by default) at: https://CCM/customer/customer_uri/S/MIME. The Administrator can communicate the self-enrollment URL and the Access Code specified for the Organization to an end-user, enabling the end-user for self enrollment.</p> <ul style="list-style-type: none"> Users that apply for a client certificate using the enrollment form will also be automatically created as a new 'End-User' in this Organization/Department if they do not already exist. (List of end-users is viewable in the 'Client Certificates' area of 'Certificates Management' section). It is possible for Certificate Manager Account holders to use their own custom form templates rather than the default form supplied by Comodo. See your account manager for more details on enabling this functionality. |
| Access Code (Appears only if the 'Self Enrollment' checkbox is selected) | Textbox (required) | <p>An Access Code identifies a particular Organization or Department and is used to authenticate certificate requests that are made using the Self-Enrollment form.</p> <p>Organizations and Departments are uniquely identified by combination of the Organization's 'Access Code' and the 'Common Name' (domain) specified in 'General' properties. Multiple Organizations or Departments can have the same Access</p> |

| Field Name | Type | Description |
|--|---|--|
| | | <p>Code OR the same Common Name - but no single entity can share both.</p> <p>Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form.</p> <p>Applicants that request a certificate using the Self Enrollment Form will need to enter this code.</p> |
| Web API | Checkbox Default state - not checked | <ul style="list-style-type: none"> Checking this box allows applicants to enroll for certificates through the Web Service API. This requires special agreement with Comodo CA. For detailed instructions please refer to Web API documentation. |
| Secret Key (Appears only if the 'Web API' checkbox is selected) | String | <p>Secret key is a phrase that is unique for all Organizations. This phrase restricts access for enrolling certificates for that Organization.</p> <ul style="list-style-type: none"> Used in pair with 'Organization ID' (visible only for already created Organizations). |
| Allow Key Recovery by Master Administrators | Checkbox Default state - checked | <p>If selected, the MRAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the MRAO has initialized their master key pair in the Encryption tab.</p> <p>See 'Encryption and Key Escrow' for a more complete explanation of key recovery processes.</p> |
| Allow Key Recovery by Organization Administrators | Checkbox Default state - checked | <p>If selected, the RAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the Encryption tab.</p> <p>See 'Encryption and Key Escrow' for a more complete explanation of key recovery processes.</p> |
| Allow Principal Name | Checkbox Default state - not checked | <p>Checking this box enables Principal Name support to the Organization. If enabled, the client certificates issued to the end-users of the Organization will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Name(SAN) field. If included, the Principal Name will be the primary email address of the end-user to whom the certificate is issued. But this can be customized at a later time by editing the end-user if Principal Name Customization is enabled for the Organization/Department.</p> |
| Allow Principal Name Customization | Checkbox Activated only on selecting 'Allow Principal Name' checkbox | <p>Checking this box enables customization of the Principal Names by the Administrator.</p> |

| Field Name | Type | Description |
|-------------------|-----------------------|---|
| Client Cert Types | Button 'customize' | <p>The Client Cert types customization options allow the administrator to specify the Client Certificate types and term lengths that will be available for this Organization through the Self Enrollment Forms. Refer to the section Customize an Organization's Client Certificate Types for more details.</p> <ul style="list-style-type: none"> Clicking the 'customize' button will open the 'Bind Client Cert Types' interface. All choices made in the 'Bind Client Cert Types' interface will apply only to this specific Organization. The more powerful 'Client Cert Types' area contains a very similar interface that allows MRAO Administrators to determine universal certificate type and term lengths that apply to ALL Organizations If a particular certificate type or term is not visible in the 'Bind Client Cert Types' area then it may need enabling in the 'Client Cert Types' area. |

6.2.2.4.6.1 Customize an Organization's Client Certificate Types

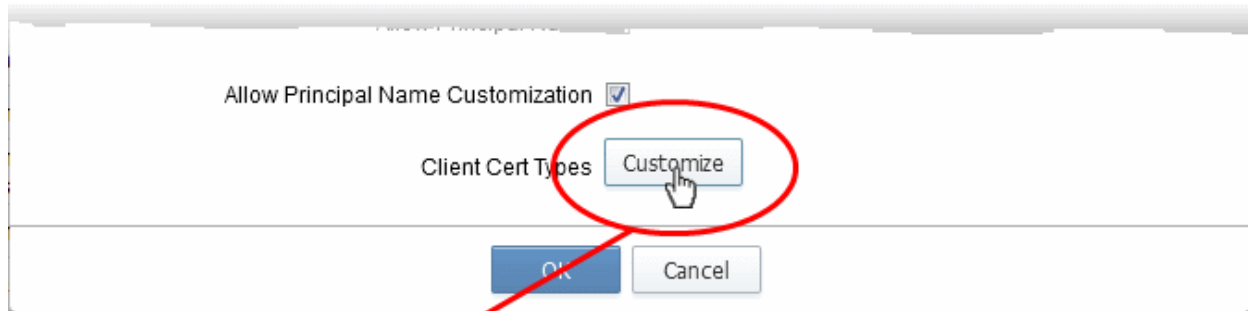
Security Roles:

- MRAO - can customize client certificate type availability for all Organizations and Departments
- RAO S/MIME - can customize client certificate type availability only for the Organizations and Departments belonging to the Organizations that are delegated to them.
- DRAO S/MIME - cannot customize client certificate type availability.

The types and term lengths of client certificates that are available to any particular Organization can be customized using the 'Customize Client Cert Types' interface. Creating a targeted 'certificate roster' simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate for that Organization.

Comodo offers different types of Client certificates depending on their purpose. For example, 'Signing Only', 'Encryption Only', 'Dual Use' (Signing + Encryption), 'Smart Card Logon and Authentication' and more. MRAO administrators can request their Comodo Account Manager to enable multiple types of client certificates for their account. It also possible to create custom client certificate types with combinations of capabilities depending on the requirements of your organization. Administrators can view the list of client certificate types enabled for their account, and restrict their availability on global basis, from the Settings > Certificates > 'Client Cert Types' interface. Refer to the section **Client Cert Types** for more details.

To access the 'Customize Client Cert Types' interface, click the 'Customize' button under the 'Client Cert' tab of the Add New/Edit Organization interface:



Customize Client Cert Types

Enrollment Form

Customized

| Name* | Terms* | Validation Type |
|---|-----------|-----------------|
| <input checked="" type="checkbox"/> Primary Client Certificate (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Signing Only (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Dual Use (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Encryption Only (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Smart Card Client Cert (531) | Select... | HIGH |
| <input type="checkbox"/> Standard Assurance Client Certificate (SHA-2) (531) | | |
| <input type="checkbox"/> Standard Assurance Client Certificate - Dual Use (362) | | |

This will open the 'Customize Client Cert Types' interface for that Organization, that enables to restrict the Client Cert types that will be available to applicants using the **Self Enrollment Form** for that Organization.

By default, the 'Customized' option is left unchecked so that all the certificate types are available through the self enrollment forms (both Access Code and Secret ID based application forms).

Prior to customization, MRAO Administrators can also view the Client Cert Type customization as imposed by the RAO Administrator of an Organization and can modify the same. Refer to **Viewing Pre-imposed Client Certificate Type Customization for an Organization** for more details.

To restrict the Client Cert types and their term lengths:

1. Select the 'Customized' checkbox.
2. Check the names of the certificates you wish to be available for the Organization leave the others unchecked.
3. Click the 'Select' button next to the certificate name to choose which terms will be available. If you want to set the selected term as default term for the selected certificate type, select 'Default' radio button.

The Validation types for each cert type is shown in the 'Validation Type' column. The two types of validation are 'Standard' and 'High'.

Customize Client Cert Types
✕

Enrollment Form

Customized

| Name* | Terms* | Validation Type |
|---|--|-----------------|
| <input checked="" type="checkbox"/> Primary Client Certificate (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Signing Only (1) | <div style="border: 1px solid gray; padding: 2px; display: inline-block;"> Terms Default <input checked="" type="checkbox"/> 1 year <input checked="" type="radio"/> <input checked="" type="checkbox"/> 2 years <input type="radio"/> </div> | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Dual Use (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Encryption Only (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Smart Card Client Cert (531) | Select... | HIGH |
| <input type="checkbox"/> Standard Assurance Client Certificate (SHA-2) (531) | | |
| <input type="checkbox"/> Standard Assurance Client Certificate - Dual Use (362) | | |

OK
Cancel

View
i

Note: The validation type for each client cert type are as configured by the MRAO in 'Settings' > 'Certificates' > 'Client Cert Types' and apply to all Organizations. The type cannot be changed for each Organization. Refer to the section **Client Cert Types** for more details.

"Standard" validation type can be completed quickly and takes advantage of the user authentication mechanisms that are built into CCM.

Under 'Standard Personal Validation' type, the user is authenticated using the following criteria:

- User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization
- The Organization has been independently validated by a web-trust accredited Certificate Authority as the owner of that domain
- User must know either a unique Access Code or Secret ID that should be entered at the certificate enrollment form. These will have been communicated by the administrator to the user via out-of-band communication.
- User must be able to receive an automated confirmation email sent to the email address of the certificate that they are applying for. The email will contain a validation code that the user will need to enter at the certificate collection web page.

'High Personal Validation' type requires that the user undergo the validation steps listed above AND

- Face-to-Face meeting with the issuing Organization

Note: The additional validation steps must be completed PRIOR to the administrator selecting 'High Personal Validation' type.

4. Click 'OK'.

The administrator needs to log out then back in again for the customization options to take effect.

Only the types and terms of client certificates that are selected in the 'Bind Client Cert Types' interface will now be available in the 'Type' drop-down field of the Self Enrollment form.

Viewing Pre-imposed Client Certificate Type Customization for an Organization

While editing an existing Organization, MRAO Administrators can view the Client Cert Type customization imposed by the RAO Administrator of the Organization, before imposing his/her own customization, by clicking the 'View' button at the bottom right of the 'Bind Client Cert Types' interface.

Note: The 'View' button will be active only when the 'Customized' checkbox is not selected in the 'Customize Client Cert Types' interface.

Clicking the 'View' button will display the 'Bind Client Cert Types' dialog as displayed to the RAO Administrator of the respective Organization.

| Enrollment Form | | |
|--|-----------|-----------------|
| <input type="checkbox"/> Customized | | |
| Name* | Terms* | Validation Type |
| <input checked="" type="checkbox"/> Client Certificate (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Signing Only (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Dual Use (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Client Certificate - Encryption Only (1) | Select... | STANDARD |
| <input checked="" type="checkbox"/> Smart Card Client Cert (531) | Select... | HIGH |

This interface also allows the MRAO Administrator to modify the customization of client certificate type availability for the Organization by the RAO Administrator.

Notes:

- All choices made in the 'Bind Client Cert Types' interface will apply only to this specific Organization.
- The more powerful '**Client Cert Types**' area contains a very similar interface that allows MRAO to determine universal certificate type and term lengths that apply to ALL Organizations.

6.2.2.4.7 SSL Certificates Settings Tab

The 'SSL' tab allows the MRAO to specify Self Enrollment, certificate types and term lengths, Web API capabilities and expiry synchronization settings relating to the SSL certificates issued to the domain associated with the Organization (or Department of the Organization). The settings chosen in this section relate only to those certificates

issued to the domain associated with the currently selected Organization.

Add New Organization
✕

General

Client Certificate

SSL Certificate

Code Signing Certificate

Device Certificate

Self Enrollment

Access Code*

Sync. Expiration Date

Sync. Month

Sync. Day (1 - 31)

Web API

Secret Key*

SSL Types

Server Software

6.2.2.4.8 SSL Certificate tab - Table of Parameters

| Field Name | Type | Description |
|-----------------|---|--|
| Self Enrollment | <i>Checkbox</i> <i>Default state - not checked</i> | <p>Checking this box will enable external requests for SSL certificates to be made by using the Self Enrollment Form hosted (by default) at: https://cert-manager.com/customer/customer_uri/ssl?action=enroll</p> <ul style="list-style-type: none"> Certificates requested using the Self Enrollment Form will appear in the 'SSL Certificates' sub-tab of 'Certificates Management' section of Comodo Certificate Manager before they are submitted to Comodo CA for validation. It is the responsibility of the administrator to review then approve or decline the request. If the request is approved it will then be forwarded to Comodo CA for processing. If the application is made for a domain that has been pre-validated for your account then certificate will be issued immediately. If the application is made for a new domain, then Comodo will first need to validate your company's ownership of that domain prior to issuing the certificate. After successful validation, the new domain will be added to your list of 'pre-validated' domains and future certificates will be processed immediately. To successfully complete the SSL request, the applicant must supply the correct Access Code for the Organization at the Self Enrollment Form. This Access Code should be communicated to the applicant using any out-of-bands methods like email. Provided that the Access Code matches the Organization being applied for AND the email address that the applicant entered at the enrollment form is from the same domain as that Organization's |

| Field Name | Type | Description |
|---|---|---|
| | | 'Common Name' then SSL certificates can be requested by individuals that do not yet exist in Comodo Certificate Manager. In such circumstances, a new end-user will be automatically created under the 'SSL Certificates' sub-tab of CCM interface with the end-user name 'requesterSSL <DOMAIN.com>' (where DOMAIN.com = the domain name for which the application is being made). This End-User will automatically be assigned membership of the Organization that the SSL Certificate was ordered for but will not own a Client Certificate. |
| Access Code (Appears only if the 'Self Enrollment' checkbox is selected) | <i>String</i> | <ul style="list-style-type: none"> An Access Code identifies a particular Organization or Department and is used to authenticate certificate requests that are made using the Self-Enrollment form. Organizations and Departments are uniquely identified by combination of the Organization's 'Access Code' and the 'Common Name' (domain) specified in 'General' properties. Multiple Organizations or Departments can have the same Access Code OR the same Common Name - but no single entity can share both. Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form. Applicants that request a certificate using the Self Enrollment Form will need to enter this code. |
| Sync. Expiration Date | <i>Checkbox</i> | <p>Checking this box will enable the ability to modify and synchronize the expiration month and day of all certificates issued to the Organization.</p> <ul style="list-style-type: none"> It is possible to select only a specific day of the month for expiry (simply select 'Not Used' for 'Sync. Month') It is possible to select both a specific day and a specific month for expiry. It is not possible to specify just a month of expiry. |
| Sync. Month: | <i>Drop-down Selection</i> | Allows Administrators to choose a specific month of the year during which all certificates issued to the Organization will expire. Administrators will also need to choose a specific day of expiration. |
| Sync. Day: | <i>String Numeric character. Between 1-31 if no specific month is chosen. Between 1-31 ; 1-30 or 1-28 if a specific month is also chosen.</i> | <p>The Organization's Administrators can specify the day of the month on which certificates issued to the domain will expire.</p> <p>Specifying a certain day of the month for expiry for all SSL certificates issued to an Organization(s) can greatly simplify the certificate management process - especially in enterprises with large volumes of certificates.</p> <p>Note 1: Certificate terms cannot exceed the duration selected at the SSL certificate application form. This means:</p> <ul style="list-style-type: none"> If a specific Month is ALSO selected at the 'Sync. Month' drop down THEN the certificate will expire on the occurrence of that precise date that is closest to the certificate term selected on the SSL Certificates Self Enrollment Form or the Built In Application Form If a specific Month is NOT selected at the 'Sync. Month' drop down |

| Field Name | Type | Description |
|--|--|--|
| | | <p>THEN the certificate will expire on the numbered day of the month that is nearest to the certificate term <i>selected on the SSL Certificates Self Enrollment Form or the Built In Application Form</i></p> <p>Example: Ordinarily, a 2 year certificate issued on the 12th of August 2014 would expire 730 days later on the 12th August 2016.</p> <p>However:</p> <ul style="list-style-type: none"> • If the administrator has ONLY specified day 16 as the 'sync expiry day' then the certificate will expire on the 16th of July 2016 • If the administrator has ONLY specified day 5 as the 'sync expiry day', then the certificate will expire on the 5th August 2016 • If the administrator has specified 14th of June as the sync expiry 'day' and 'month', then the certificate will expire on the 14th June 2016 • If the administrator has specified 14th of August as the sync expiry 'day' and 'month', then the certificate will expire on the 14th August 2015 <p>Note 2: <i>Specifying a sync expiry day only affects certificates issued from that point forward. The expiry date of certificates that have already been issued will not change. The sync expiry day will, however, apply to all renewals of existing certificates.</i></p> |
| Web API | Checkbox <i>Default state - not checked</i> | Checking this box allows to open access for enrolling certificates through Web Service API. This requires special agreement with Comodo CA. For detailed instructions please refer to Web API documentation. |
| Secret Key (Appears only if the 'Web API' checkbox is selected) | String | <p>The Secret key is a phrase that is unique for all Organizations. This phrase restricts access for enrolling certificates for that Organization.</p> <ul style="list-style-type: none"> • Used in pair with 'Organization ID' (visible only for already created Organizations). |
| SSL Types | Button <i>'Customize'</i> | <p>The SSL types customization options allow the administrator to specify the SSL Certificate types and term lengths that will be available for this Organization for new certificate applications.</p> <ul style="list-style-type: none"> • Clicking the 'Customize' button will open the 'Bind SSL Types' interface. • All choices made in the 'Bind SSL Types' interface will apply only to this specific Organization. • It is possible to make different certificate types and terms available to the applicant depending on whether the application is made using the Built-in application form (Admin UI) or the (Self) Enrollment form. See section Customize an Organization's SSL Certificate Types for more details on this and the other options available through the 'Bind SSL Types' interface. • The more powerful 'SSL Types' area contains a very similar interface that allows Master Administrators to determine universal certificate type and term lengths that apply to ALL Organizations • If a particular certificate type or term is not visible in the 'Bind SSL Types' area then it may need enabling in the 'SSL Types' area. SSL |

| Field Name | Type | Description |
|-----------------|-----------------------|--|
| | | Administrators should seek the advice of the Master Administrator. |
| Server Software | Button 'Customize' | <p>The Server Software customization options allow the administrator to specify the types of server software that are allowed for this Organization.</p> <ul style="list-style-type: none"> Clicking the 'Customize' button will open the 'Server Software' interface, with a list of server software The administrator can select the server software that can be used for the Organization All choices made in the 'Server Software' interface will apply only to this specific Organization. The server software selected in this field will be available in the 'Server Software' drop-down of both the Built-in application form (Admin UI) or the (Self) Enrollment form. See section Customize an Organization's Server Software Types for more details on this. |

6.2.2.4.8.1 Customize an Organization's SSL Certificate Types

Security Roles:

- MRAO - can customize SSL certificate type availability for all Organizations and Departments
- RAO SSL - can customize SSL certificate type availability only for Organizations (and any subordinate Departments) that are delegated to them.
- DRAO - cannot customize SSL certificate type availability.

(i.e. RAO/DRAO SSL Admins cannot change which SSL certificates are available to Organizations or Departments that they control).

The types and term lengths of SSL certificates that are available to any particular Organization can be customized using the 'Bind SSL Types' interface. Creating a targeted 'certificate roster' simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate for that Organization.

To access the 'Bind SSL Types' interface, click the 'Customize' button beside SSL Types under the SSL tab of the Add New/Edit Organization interface. This will open the 'Bind SSL Types' for that Organization.

Add New Organization

General Client Certificate **SSL Certificate** Code Signing Certificate Device Certificate

Self Enrollment

Access Code* 123456

Sync. Expiration Date

Sync. Month Not used

Sync. Day 1 (1 - 31)

Web API

Secret Key* 123456

SSL Types **Customize**

Server Software Customize

OK Cancel

Bind SSL Types

Admin UI

Customized

| Name | Terms |
|--|-----------|
| <input checked="" type="checkbox"/> Instant SSL | Select... |
| <input checked="" type="checkbox"/> Multi-Domain Instant SSL Certificate | Select... |
| <input checked="" type="checkbox"/> PremiumSSL Wildcard Certificate | Select... |
| <input checked="" type="checkbox"/> SSL EV Certificate | Select... |
| <input checked="" type="checkbox"/> Private UCC | Select... |

Enrollment Form

Customized

| Name | Terms |
|--|-----------|
| <input checked="" type="checkbox"/> Instant SSL | Select... |
| <input checked="" type="checkbox"/> Multi-Domain Instant SSL Certificate | Select... |
| <input checked="" type="checkbox"/> PremiumSSL Wildcard Certificate | Select... |
| <input checked="" type="checkbox"/> SSL EV Certificate | Select... |
| <input checked="" type="checkbox"/> Private UCC | Select... |

OK Cancel

- **Admin UI** - Determines the SSL certificate types that will be available to applicants using the **Built-In Application form** for that Organization.
- **Enrollment Form** - Determines the SSL certificate types that will be available to applicants using the **Self Enrollment Form** for that Organization.
- It is therefore possible to choose a different selection of certificate availabilities for an Organization depending on whether the Built-in or Self-Enrollment form is to be used.

By default, the 'Customized' option is left unchecked so that all the certificate types are available through both types of application form.

To restrict the SSL types and their terms

1. Select the 'Customized' option below either or both 'Admin UI' or 'Enrollment Form'.
2. Check the names of the certificates you wish to be available to that Organization and leave the others unchecked.

- Click the 'Select' button next to the certificate name to choose which terms will be available.

- Click 'OK'.

The MRAO needs to log out then back in again for the customization options to take effect.

The types and terms of SSL certificates that are selected in the 'Bind SSL Types' interface will now be available in the 'Type' and 'Term' drop-down fields of this Organization's application forms.

Notes:

- All choices made in the 'Bind SSL Types' interface will apply only to this specific Organization.
- The more powerful '**SSL Types**' area contains a very similar interface that allows MRAO to determine universal certificate type and term lengths that apply to ALL Organizations.

6.2.2.4.8.2 Customize an Organization's Server Software Types

Security Roles:

- MRAO - can customize server software types that can be used for all Organizations and Departments
- RAO SSL - can customize server software types that can be used for only for Organizations (and any subordinate Departments) that are delegated to them.
- DRAO - cannot customize server software types.

The types of server software that can be used to any particular Organization can be customized using the 'Server Software' interface. Only those allowed server software will be listed in the Server Software drop down of both the **Self Enrollment** and the **Built-in Application** forms for adding new SSL certificate for that Organization.

To access the 'Server Software' interface, click the 'Customize' button beside 'Server Software', under the SSL tab of the Add New/Edit Organization interface. This will open the 'Server Software' for that Organization.

✕
Add New Organization

General

Client Certificate

SSL Certificate

Code Signing Certificate

Device Certificate

Self Enrollment

Access Code*

Sync. Expiration Date

Sync. Month ▼

Sync. Day (1 - 31)

Web API

Secret Key*

SSL Types

Server Software

✕
Server Software

| | |
|--|--|
| <input checked="" type="checkbox"/> AOL <input checked="" type="checkbox"/> Apache/ModSSL <input checked="" type="checkbox"/> Apache-SSL (Ben-SSL, not Stronghold) <input type="checkbox"/> C2Net Stronghold <input type="checkbox"/> Cisco 3000 Series VPN Concentrator <input checked="" type="checkbox"/> Citrix <input type="checkbox"/> Cobalt Raq <input type="checkbox"/> Covalent Server Software <input type="checkbox"/> IBM HTTP Server <input type="checkbox"/> IBM Internet Connection Server <input type="checkbox"/> iPlanet <input type="checkbox"/> Java Web Server (Javasoft / Sun) <input type="checkbox"/> Lotus Domino <input type="checkbox"/> Lotus Domino Go! <input checked="" type="checkbox"/> Microsoft IIS 1.x to 4.x <input checked="" type="checkbox"/> Microsoft IIS 5.x and later <input checked="" type="checkbox"/> Netscape Enterprise Server <input type="checkbox"/> Netscape FastTrack | <input type="checkbox"/> Novell Web Server <input type="checkbox"/> Oracle <input type="checkbox"/> Quid Pro Quo <input type="checkbox"/> R3 SSL Server <input type="checkbox"/> Raven SSL <input type="checkbox"/> RedHat Linux <input type="checkbox"/> SAP Web Application Server <input type="checkbox"/> Tomcat <input type="checkbox"/> Website Professional <input type="checkbox"/> WebStar 4.x and later <input type="checkbox"/> WebTen (from Tenon) <input type="checkbox"/> Zeus Web Server <input type="checkbox"/> Ensim <input type="checkbox"/> Plesk <input type="checkbox"/> WHM/cPanel <input type="checkbox"/> H-Sphere <input type="checkbox"/> OTHER |
|--|--|

By default, no server software will be selected.

- To restrict the Server Software types select the names of the server software you wish to allow for that Organization and leave the others unchecked. Click OK to save the selection.

The MRAO needs to log out then back in again for the customization options to take effect.

Note: All choices made in the 'Server Software' interface will apply only to this specific Organization.

6.2.2.4.9 'Code Signing Certificates' Settings tab

The 'Code Signing' tab allows the Administrators to enable request/issuance of Code Signing Certificates for the Organization. The setting in this section relate only to those certificates issued to the domain associated with the currently selected Organization.

Add New Organization [Close]

General | Client Certificate | SSL Certificate | **Code Signing Certificate** | Device Certificate

When checkbox is selected "Code Signing" certificates could be enrolled for this particular Organization or Department.

Enabled

OK Cancel

6.2.2.4.10 Code signing Certificates - Table of Parameters

| Field Name | Type | Description |
|------------|---|---|
| Enabled | Checkbox Default state - not checked | Checking this box will enable the request and issuance of Code Signing Certificates to end-users that are members of this Organization. |

6.2.2.4.11 Device Certificate Settings Tab

The 'Device Certificate' tab allows admins to enable device certificates for an organization. Devices certs can be obtained using the self-enrollment forms or via SCEP.

Add New Organization [Close]

General | EV Details | Client Certificate | SSL Certificate | Code Signing Certificate | **Device Certificate**

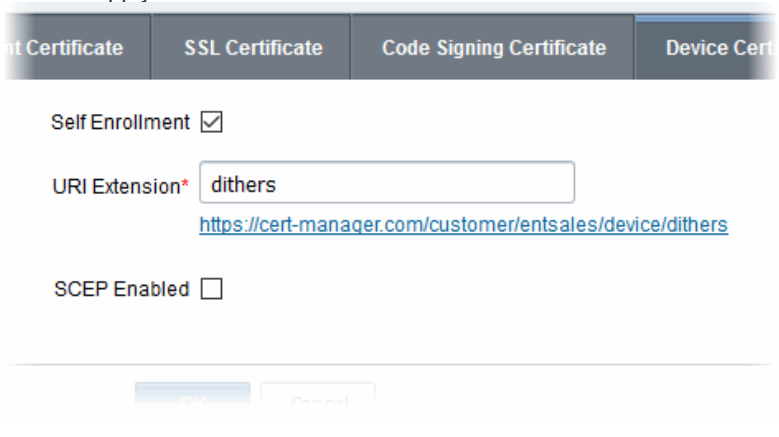
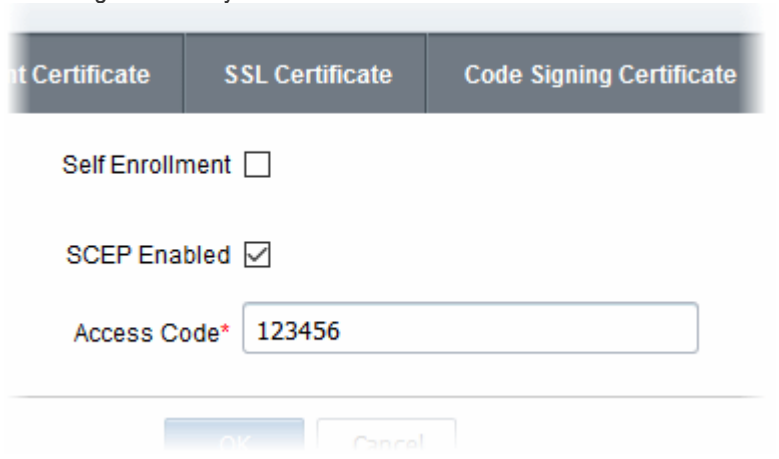
Self Enrollment

SCEP Enabled

OK Cancel

- Self Enrollment – Users can request device certificates via the self-enrollment application forms. If enabled, you need to specify the URI extension
- SCEP Enabled – Apply for device certificates for an organization using SCEP. An access code is required.

6.2.2.4.12 Device Certificates - Table of Parameters

| Field Name | Type | Description |
|-----------------|---|---|
| Self Enrollment | Checkbox Default state - not checked | <ul style="list-style-type: none"> Enabling this box allows end-users to request device certificates by completing the self-enrollment form. You can specify a URL extension if one is not already set. The URL of the form is automatically shown below the extension field. This URL should be passed to applicants so they can apply for device certificates:  |
| SCEP Enabled | Checkbox Default state - not checked | <ul style="list-style-type: none"> Select this box to enable enrollment of device certificates via SCEP for an organization. Administrators need to specify an access code after enabling this option. The code should included in the configuration profile for OTA enrollment of device certificates. The code is to be included in the profile, as the 'challengePassword' parameter in the certificate request generated by the device.  |

6.2.2.5 Editing an Existing Organization

Selecting an Organization and clicking the 'Edit' button at the top will open the Edit Organization dialog.

Edit Organization: org1 [X]

General | EV Details | Client Certificate | SSL Certificate | Code Signing Certificate | Device Certificate | Email Template

*-required fields

Organization Name*

Address1*

Address2

Address3

City*

State/Province*

Postal Code*

Country*

Validation Status

Anchor certificate

OrgID 52

Access Control List

The 'Edit' Organization dialog enables administrators to view/modify the 'General', 'EV Details', 'Client Cert', 'SSL' and Code Signing Certificate details pertaining to an existing Organization at any time.

- MRAO Administrators - can view and edit details under all the tabs
- RAO Administrators - can view and edit details under all the tabs except 'General Settings'. The details under General Settings tab are visible to the RAO but cannot be edited.

Full details of the options available when editing an existing Organization are available in the previous section, '[Creating a new Organization](#)'. Additionally the 'Email Template' tab allows the Administrator to directly edit the content of the automated notification emails as set by him/her in the Notifications area. For more details, refer to the [Email Templates](#) section of this guide.

General Settings

The General Settings area under Edit Organization dialog is similar to that in the '[Create New Organization](#)' dialog except for an additional Access Control List option.

- **Access Control List:** Enables the administrator to configure and limit incoming access to the CCM interface to certain IP addresses and ranges. This is very useful if they want to grant access only to certain IP addresses and so prevent unauthorized or unsecured access to the CCM interface. After specifying one or more IP addresses or ranges in CIDR notation, only administrators attempting to login from these specified addresses will be allowed access.
- The MRAO can access a more powerful **Access Control** area by clicking Settings > Access Control, which has a similar interface and allows to limit incoming access to the CCM interface. The Access Control settings made by the MRAO through 'Settings' > 'Access Control' will over-rule any settings made through 'Edit Organization' area. Also RAO/DRAO can restrict access only to IP ranges that fall within the range that the MRAO has set in the 'Settings' > 'Access Control' area.
- For details on other options in the General Settings Area, see [General Settings](#)
- For details on the EV Details tab, see [EV Details Tab](#)
- For details on the Client certificate tab, see [Client Cert Settings Tab](#)

- For details on the SSL certificate tab, see [SSL Certificates Settings Tab](#)
- For details on the Code Signing certificate tab, see [Code Signing Certificates Settings tab](#)
- For details on the Device certificate tab, see [Device Certificate Settings Tab](#)
- For details on the Email Template, see [Customizing Notification Email Templates](#)

Note: Any changes you make to the settings of an existing Organization will NOT affect certificates that have already been issued to domains belonging to that Organization.

6.2.2.5.1 Imposing Access Restrictions to CCM interface

Security Roles:

- MRAO - Access restrictions imposed by MRAO will apply for the management of the certificates, administrators, end-users and settings for all the Organizations and Departments.
- RAO - Access restrictions imposed by RAOs will apply for the management of the certificates, administrators, end-users and settings for the Organizations (and any subordinate Departments) that have been delegated to them.
- DRAO - Access restrictions imposed by DRAOs will apply for the management of the certificates, end-users and settings for the Departments that have been delegated to them.

To limit incoming access to the CCM interface

- Click the Edit button beside 'Access Control List' from the 'Settings' > 'Organizations' > 'Edit Organization' dialog. The 'Access Control' dialog will appear.

Country* United States

Validation Status Not Validated

Anchor certificate

OrgID 52

Access Control List **Edit**

OK Cancel

Access Control for: org1 X

Filter

Refresh + Add

| CIDR | DESCRIPTION |
|---------|-------------|
| No data | |

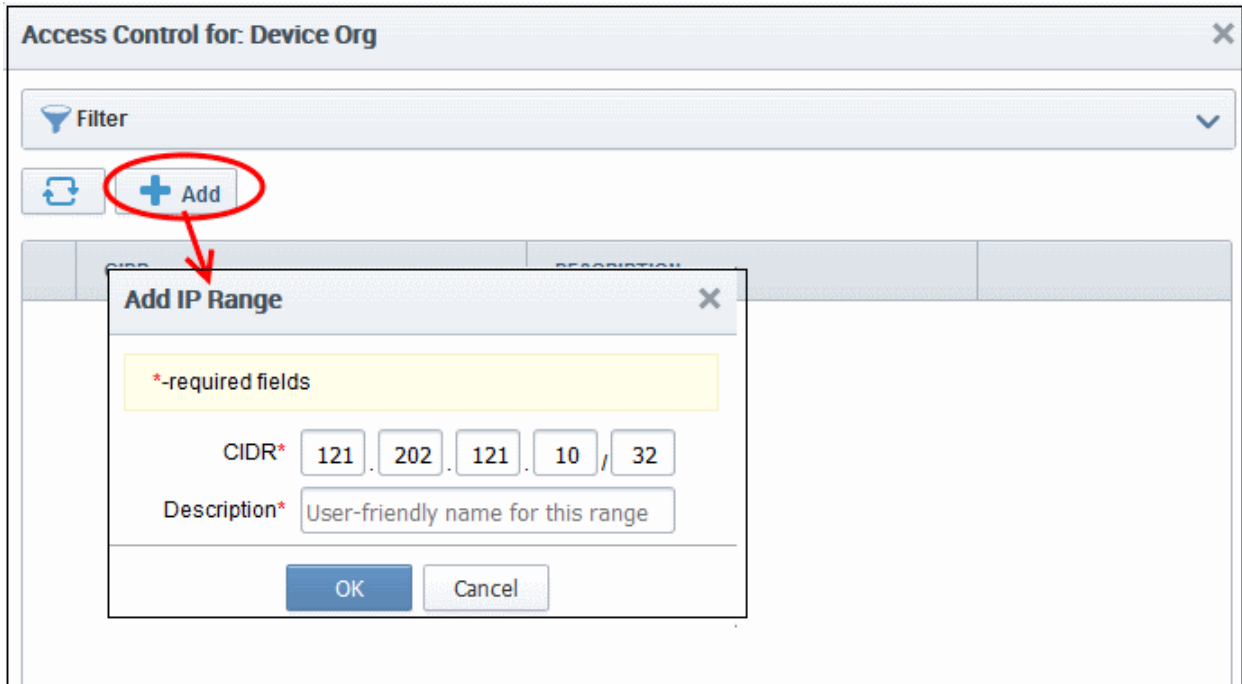
15 rows/page No Cidr Found! << < > >>

Close

| Column Display | Description |
|-----------------|--|
| CIDR | Short for Classless Internet DOMAIN Routing. Administrator should specify IP range: it should be IP address followed by network prefix, e.g. 123.456.78.91/16. |
| Description | Contains a short description for the IP range as entered by the administrator while creating the CIDR. |
| Control Buttons | Description |
| Edit | Enables administrator to edit CIDR's details. |
| Delete | Enables administrator to delete the CIDR. |
| Add | Opens 'Add IP Range' dialog. |
| Refresh | Updates the list of IP ranges |

To add a new IP Range

- Click 'Add'. The 'Add IP Range' dialog will appear.



- Enter the IP range, followed by network prefix, e.g. 123.456.78.91/16.
- Enter a short description for the IP range
- Click 'OK'.

The IP range will be added as a new CIDR and the access to CCM from the new IP range will be allowed.

6.2.2.5.2 Customizing Notification Email Templates

- CCM can send automatic email notifications to certificate applicants, administrators and end-users after events like certificate approval, collection and revocation.
- Notifications are set by administrators in the **Notifications** area.
- While **global email templates** are configured in Settings > Email Template, this interface allows you to customize email templates for a particular Organization / Department.
- If no custom email template is configured for an Org/Dept, then the global email template will apply.

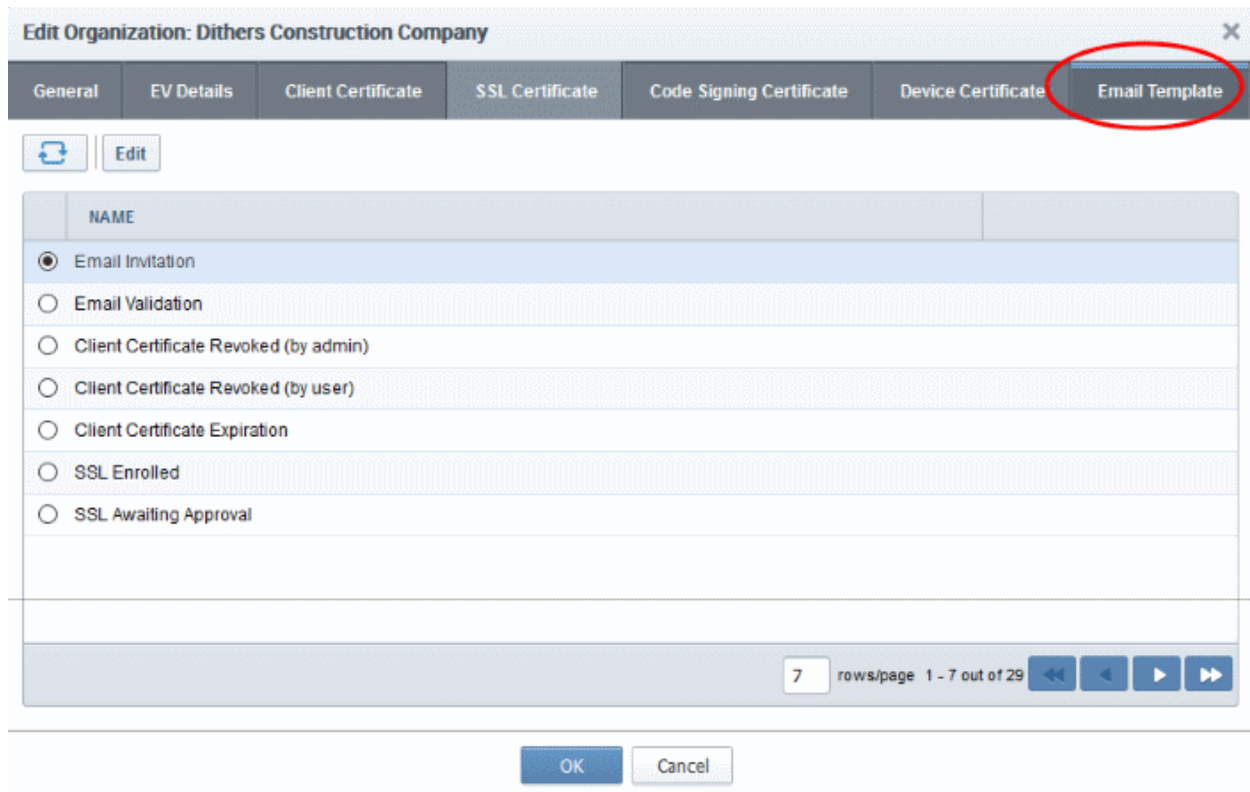
To customize the email template for an Organization:

- Go to Settings > Organizations
- Select an organization

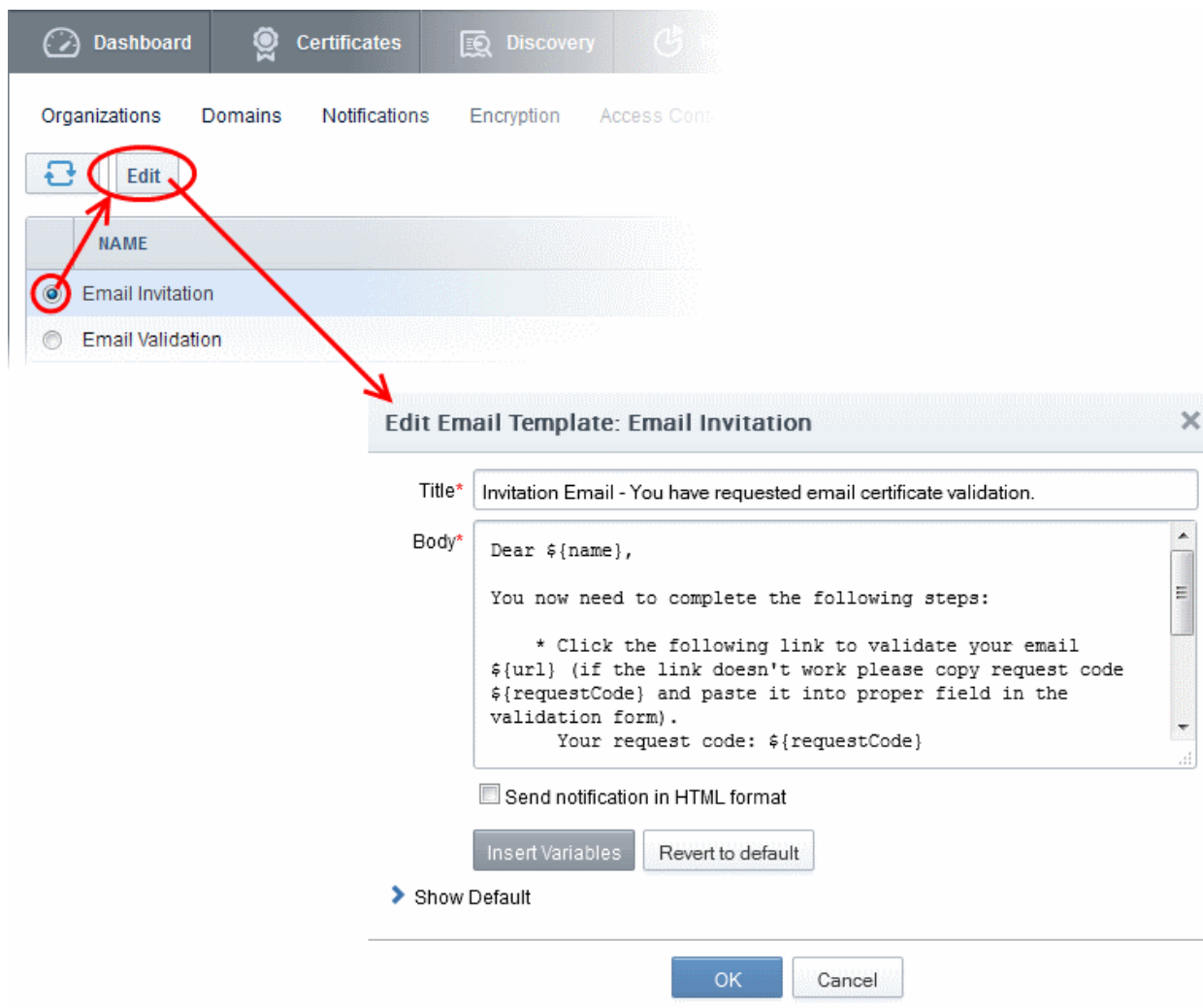
OR

- Select an organization then click 'Departments' and select a department
- Click 'Edit'

The procedure for editing mail templates is the same for both organizations and departments. Click the 'Email Template' tab.



Select the email template and click the 'Edit' button at the top. An example is shown below:



The 'Title' field displays the subject line of the email. The 'Body' section contains the message and variables which will be replaced with the exact values of the certificate/domain concerned. You can customize the content as required.

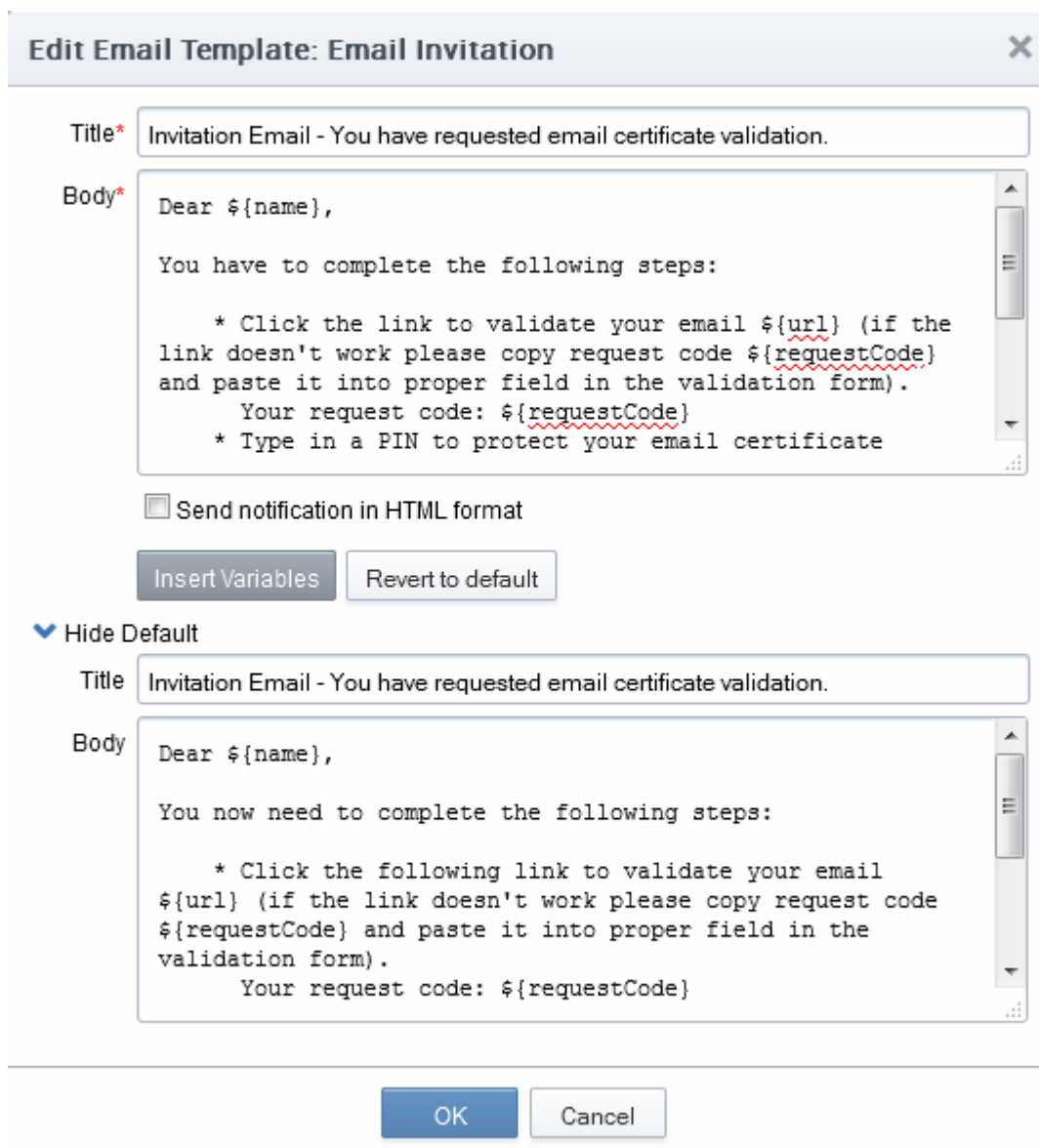
- Selecting the checkbox 'Send notification in HTML format' will send automated email notifications to administrators, applicants and end-users in HTML format.
- Clicking 'Insert Variables' will display a list of the variables used in the specific template. The administrator can select the variable to be inserted into the content from the list. This is useful if the administrator has accidentally deleted variable(s) which are essentially required in the template.



- Clicking 'Revert to default' enables the administrator to reset to the default content as shipped with CCM.



- Clicking 'Show Default' will display the default content for administrator to refer.



- Click 'OK' for your changes to take effect.

6.2.2.6 Validating an Organization

Before you can issue Organization Validated (OV) SSL certificates for an Organization (or Department), the

Organization must first be validated by Comodo.

Note: The request and issuance of OV certificates for Organizations or Departments require OV certificates enabled for your CCM account. If not enabled previously, contact your CCM account manager for enabling this feature.

The 'Validation Status' of new Organizations will initially be 'Not Validated' and the 'Anchor Certificate' field will be blank. MRAOs can initiate the validation process by selecting the Organization and clicking the 'Validate' button. Validation Status will change to 'Validated' after successful validation and the 'Anchor Certificate' status will be 'ON'. This certificate will be used as a reference by CM whenever an OV SSL certificate is requested for the Organization or any Department under it. Address details entered in the 'General' tab of 'Add or Edit Organization' are used for the validation process and they cannot be edited while the validation status is 'Pending'. Details can be edited again only when the validation status is 'Validated', 'Expired' or 'Failed'.

When a new Department is added under a validated Organization, its address details will be fetched from the Organization's anchor certificate and these will auto-populate the Department's 'General' tab. The Department name will be blank for the administrator to complete and this will be shown as the 'Organizational Unit' (OU) in the final certificate. If a Department was added with different address details before the parent Organization was validated, then these details will be replaced with those in the anchor certificate the next time an OV certificate is ordered for the Department.

To validate an Organization, select it and click the 'Validate' button:

The screenshot shows the 'Organizations' section of the Comodo Certificate Manager. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Reports, Admins, Settings, and About. Below these are sub-tabs: Organizations, Domains, Notifications, Encryption, Access Control, Private Key Store, Email Template, Certificates, MS Agents, and Assignment Rules. A 'Filter' section is present, followed by action buttons: Add, Edit, Delete, Departments, Domains, and Validate. The 'Validate' button is circled in red. Below the buttons is a table with columns: NAME, CITY, STATE, COUNTRY, and VALIDATION STATUS. The table contains five rows of organizations. The 'org1[52]' row is selected, and a red arrow points from the 'Validate' button to a 'Certificate Manager' dialog box. The dialog box contains a question mark icon and the text: 'Please confirm that you want to start the Validation process for this organization.' with 'OK' and 'Cancel' buttons.

| NAME | CITY | STATE | COUNTRY | VALIDATION STATUS |
|-------------|----------|-------|---------|-------------------|
| Bar[9] | BarCity | CT | US | Not Validated |
| Football[7] | SkyCity | AL | US | Not Validated |
| org2[53] | ODS | ods | US | Not Validated |
| Advanced[2] | Sky-City | AL | US | Validated |
| org1[52] | Ods | ods | US | Not Validated |

- Click 'OK' to confirm starting the validation process.

The validation process will begin and when completed successfully, 'Validation Status' will display 'Validated' in the 'Edit' > 'General' tab for the Organization.

The various stages of validation status are:

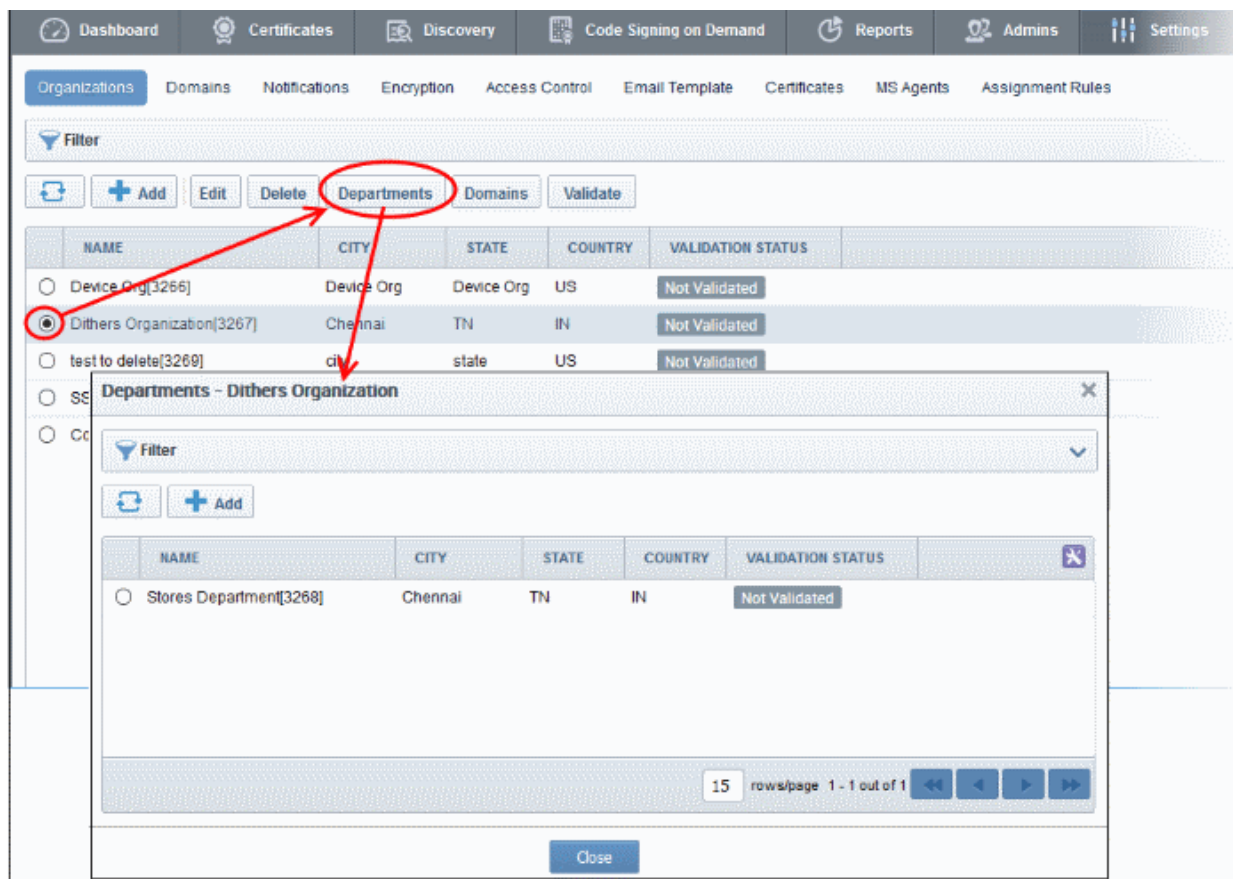
- **Not Validated** - The validation process not started. MRAOs can start the process of validation by selecting an Organization and clicking the 'Validate' button at the top.
- **Validated** - The Organization is validated and anchor certificate issued. The Organization and Departments under it can request for OV SSL certificates.
- **Pending** - Validation process started and not completed. The address details of the Organization in the 'General' tab is locked and non-editable.
- **Failed** - The validation process failed for the Organization. MRAOs can initiate the validation process again

by clicking the 'Validate' button.

- **Expired** - The validation period of 36 months is expired for the Organization. MRAOs can initiate the validation process by clicking the 'Validate' button.

6.2.2.7 Managing the Departments of an Organization

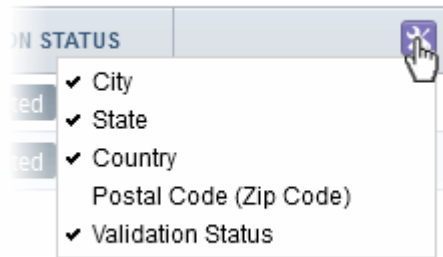
MRAO and RAO Administrators can view and edit Departments belonging to an Organization by selecting it and clicking the 'Departments' button at the top. This will open a dialog that lists all Departments belonging to the Organization and controls to Edit, Delete, Add and manage Domains.



6.2.2.7.1 Departments Dialog - Table of Parameters

| Column Display | Description |
|------------------------|---|
| Name | A list of all Departments that have been delegated to the Administrator that is currently logged in. |
| City | Displays the name of the city entered at the time of creating the Department |
| State | Displays the name of the State entered at the time of creating the Department |
| Country | Displays the name of the Country entered at the time of creating the Department |
| Postal Code (Zip Code) | Displays the postal code entered at the time of creating the Department |
| Validation Status | Displays whether the Department is validated for the request and issuance of OV SSL certificates. For more details refer to the section Validating an Organization . |

Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:

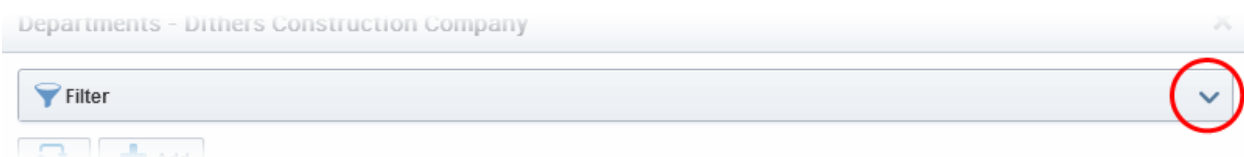


| | | |
|---|---------|--|
| Controls Buttons | Add | Enables Administrators to modify General, Client, SSL and Code Signing Certificate settings pertaining to an existing Department. |
| | Refresh | Updates the list of Departments. |
| Department Control Buttons Note: The Department control buttons appear only on selecting a Department | Edit | Enables Administrators to modify General, Client, SSL, Code Signing Certificate and E-mail Template settings pertaining to an existing Department. |
| | Delete | Deletes the Department. The Control is not visible to DRAO Administrators. |
| | Domains | Enables Administrators to view, edit and delegate domains to the Departments. |

6.2.2.7.2 Sorting and Filtering Options

- Clicking on the column header 'Name' sorts the items in the alphabetical order of the names of the Departments.

Administrators can search for particular Department by using filters.



To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down. For example, if you want to filter the Department by 'Name':

The screenshot shows the 'Departments - org1' window. At the top, there is a 'Filter' section with a dropdown menu open. The dropdown menu lists 'Name', 'Validation Status', and 'Show deleted'. The 'Name' option is selected. Below the dropdown, there is an 'Apply' button. To the right of the dropdown, there is a 'Group by:' dropdown menu set to 'Ungroup'. Below the filter section, there are 'Refresh' and 'Add' buttons. At the bottom, there is a table with the following data:

| | NAME | CITY | STATE | COUNTRY | VALIDATION STATUS |
|-----------------------|-----------------------|------|-------|---------|-------------------|
| <input type="radio"/> | Stores Department[56] | Ods | ods | US | Pending |

- Enter the name of the Department in part or full in the 'Name' field.

The screenshot shows the 'Departments - org1' window. The 'Filter' section is now a search bar with 'Name:' and a text input field containing 'Stores'. Below the search bar, there are 'Apply' and 'Clear' buttons. The 'Apply' button is highlighted. Below the search bar, there are 'Refresh' and 'Add' buttons.

- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Departments' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.2.2.7.3 Creating Departments

An Organization may consist of sub-ordinate Departments, managed by DRAO Administrators. In order to provide certificates to the employees, end-users or websites pertaining to the Departments, the MRAO or the RAO Administrators can should first create the Departments under the Organization and associate domains to the Departments.

MRAO and RAO Administrators can add a new Department at any time by clicking the 'Add' button located at the top of the 'Departments' dialog:

Add New Department

General | EV Details | Client Certificate | SSL Certificate | Code Signing Certificate | Device Certificate

*-required fields

Department Name* Security Department

Address1* Ms

Address2

Address3

City* Ods

State/Province* ods

Postal Code* 600000

Country* United States

Validation Status Pending

Anchor certificate 1676691

OK Cancel

The dialog contains five tabs - General, EV Details, Client Cert, SSL and Code Signing. Apart from 'Client Certificates', these tabs are the same as those in the 'Add New Organization' dialog. If the parent Organization is already validated by Comodo for the request and issuance of OV SSL certificates, the address details except the Department Name will be auto populated with the parent Organization's address. Refer to the section [Validating an Organization](#) for more details.

- The 'General' tab - see [General Settings](#) for more details
- The 'EV Details' tab - see [EV Details Tab](#) for more details.
- The 'SSL Certificate' tab - see [SSL Certificate Settings tab](#) for more details
- The 'Code Signing' tab - see [Code Signing Certificates Settings tab](#) for more details
- The 'Device Certificate' tab – see [Device Certificate Settings Tab](#) for more details.

Client Certs tab

The Client Certificate tab is the same as that explained in [Client Certificate Settings Tab](#) but contains an additional setting related to key recovery:

Add New Department
✕

General

EV Details

Client Certificate

SSL Certificate

Code Signing Certificate

Device Certificate

Self Enrollment

Access Code*

Web API

Secret Key*

Allow Key Recovery by Master Administrators

Allow Key Recovery by Organization Administrators

Allow Key Recovery by Department Administrators

Allow Principal Name

Allow Principal Name Customization

Client Cert Types

| | | |
|---|---|---|
| Allow Key Recovery by Master Administrators | Checkbox Default state - checked if pre-enabled by MRAO* | If selected, the MRAO Administrator will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificates UNTIL the MRAO has initialized their master key pair in the 'Encryption' tab. See 'Encryption and Key Escrow' for a more complete explanation of key recovery processes. |
| Allow Key Recovery by Organization Administrators | Checkbox Default state - checked if pre-enabled by MRAO* | If selected, the RAO Administrator will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the 'Encryption' tab. See 'Encryption and Key Escrow' for a more complete explanation of key recovery processes. |
| Allow Key Recovery by Department administrators | Checkbox Default state - checked if pre-enabled by MRAO* | If selected, the DRAO Administrator will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted |

| | | |
|--|--|---|
| | | <p>with the DRAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificate UNTIL the DRAO has initialized their master key pair in the 'Encryption' tab.</p> <p>See 'Encryption and Key Escrow' for a more complete explanation of key recovery processes.</p> |
|--|--|---|

- The settings outlined above will be active ONLY IF the MRAO has enabled the appropriate key recovery options when [configuring Client Certificate options](#) for the Organization.

6.2.2.7.4 Editing Departments belonging to an Organization

The existing Departments under any Organization can be edited by the appropriately privileged administrator at any time by selecting the Department and clicking the Edit button at the top in the 'Departments' interface.

The Edit Department dialog will appear.

Edit Department: Stores Department ✕

General
EV Details
Client Certificate
SSL Certificate
Code Signing Certificate
Device Certificate
Email Template

*-required fields

Department Name*

Address1*

Address2

Address3

City*

State/Province*

Postal Code*

Country*

Validation Status Pending

Validator Admin MRAO

Anchor certificate 1676691

OrgID 56

Access Control List

General Tab

The 'General' settings area is similar to general settings in the [Create New Department](#) dialog except for an additional option - 'Access Control List'.

- For details on other options, see [General Settings - Table of Parameters](#)
- For more details on ACL, see [Imposing Access Restrictions to CCM interface](#)
- For more details on the 'EV Details' tab, see [EV Details Tab](#)
- For more details on the 'Client Certs' tab, see [Client Certs tab](#) under [Creating Departments](#)
- For more details on the 'SSL Certificate' tab, see [SSL Certificate Settings tab](#)

- For more details on the 'Code Signing Certificate' tab, see [Code Signing Certificates Settings tab](#)
- For more details on the 'Device Certificate' tab, see [Device Certificate Settings Tab](#)
- For more details on the 'Email Template' tab, see [Customizing Notification Email Template](#)

6.2.2.7.5 Managing Domains Belonging to a Department

The domains delegated to a Department can be viewed and managed by selecting the Department and clicking the 'Domains' button from the top. The 'Domains' dialog enables appropriately privileged Administrators to view, edit and delegate any Domains attached to the Department.

| | NAME | DELEGATION STATUS | DATE REQUESTED | DCV EXPIRATION |
|-----------------------|---------------|-------------------|----------------|----------------|
| <input type="radio"/> | corp1.net[58] | Approved | 01/17/2017 | |
| <input type="radio"/> | corp1.com[57] | Approved | 01/17/2017 | |

A detailed explanation on this area is available in section: [5.4.2.1 Domains Area Overview](#)

6.2.2.7.6 Deleting an Existing Department

The Administrator can remove a Department if he/she no longer wishes to issue certificates from it, by selecting it and clicking the 'Delete' button from the top.

Note: Deleting an Organization will automatically revoke any certificates issued to that Department and will delete any end-users that are members of it. For this reason, CCM will prompt for confirmation:

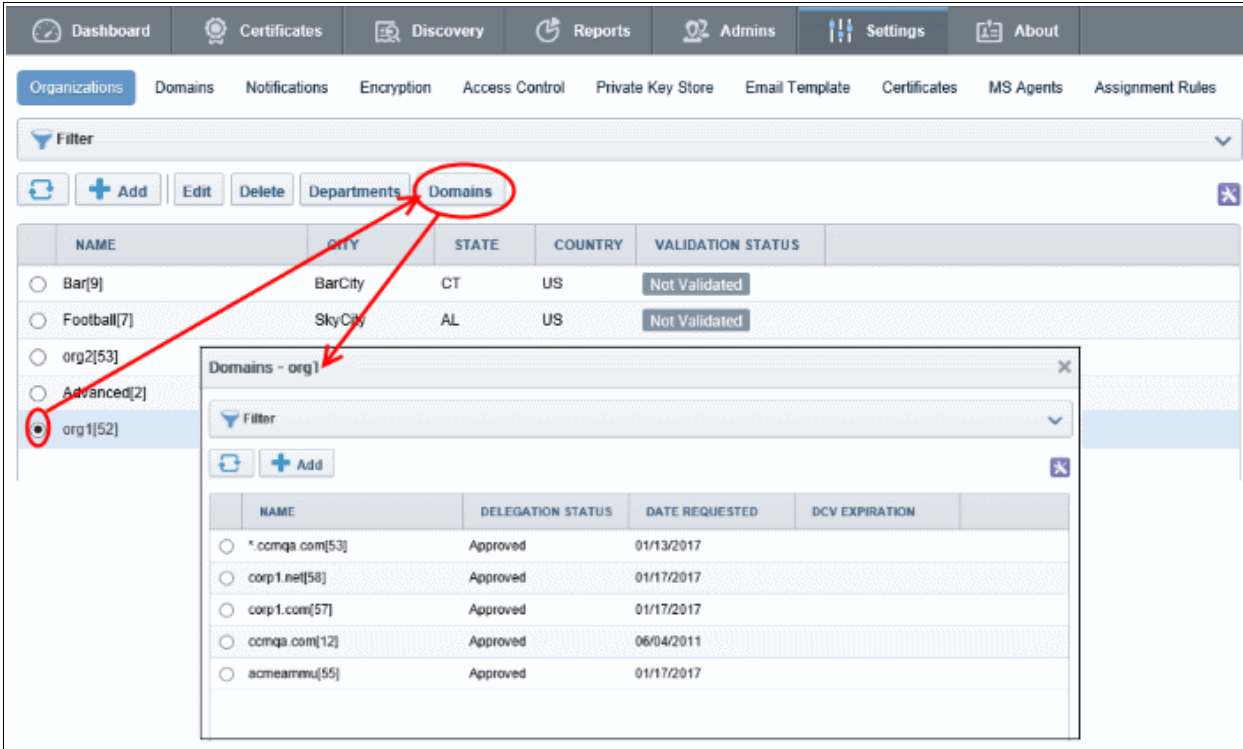
Delete Organization

Are you sure you want to delete this organization/department?
Deleting the organization/department will cause all users under that organization/department to be deleted, and all certificates revoked

OK Cancel

6.2.2.8 Managing the Domains of an Organization

The Administrators can view and manage the domains delegated to an Organization by selecting it and clicking the 'Domains' button at the top. The 'Domains' dialog displays a list of Domains attached to the Organization and the Departments under that Organization.



| NAME | CITY | STATE | COUNTRY | VALIDATION STATUS |
|-------------|---------|-------|---------|-------------------|
| Bar[9] | BarCity | CT | US | Not Validated |
| Football[7] | SkyCity | AL | US | Not Validated |
| org2[53] | | | | |
| Advanced[2] | | | | |
| org1[52] | | | | |

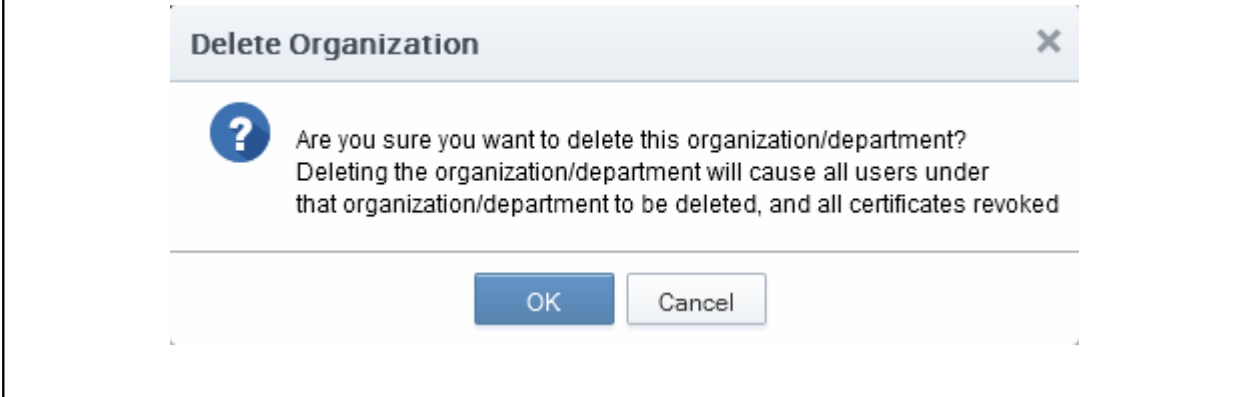
| NAME | DELEGATION STATUS | DATE REQUESTED | DCV EXPIRATION |
|-----------------|-------------------|----------------|----------------|
| *.comqa.com[53] | Approved | 01/13/2017 | |
| corp1.net[58] | Approved | 01/17/2017 | |
| corp1.com[57] | Approved | 01/17/2017 | |
| comqa.com[12] | Approved | 06/04/2011 | |
| acmeammu[55] | Approved | 01/17/2017 | |

A detailed explanation of the controls available in this area is available in section [5.4.Domains](#)

6.2.2.9 Deleting an Existing Organization

The Administrator can remove an Organization, if he/she no longer wishes to issue certificates from it, by selecting it and clicking the 'Delete' button from the top.

Note: Deleting an Organization will automatically revoke any certificates issued to that Organization and will delete any end-users that are members of it. For this reason, CCM will prompt for confirmation:



Delete Organization

Are you sure you want to delete this organization/department?
Deleting the organization/department will cause all users under that organization/department to be deleted, and all certificates revoked

OK Cancel

Note: The Delete control will not be visible for RAOs and DRAOs.

6.3 Departments

The Departments tab allows DRAO Administrators to manage existing domains and add new domains to the Departments that are delegated to them. Clicking the 'Edit' button at the top after selecting a Department will allow the DRAO Administrator to alter the general and email template settings for the Department for which they have been delegated control.

Important Note: The 'Departments' area is visible only to DRAO Administrators. MRAOs and RAOs will instead see the 'Organizations' tab and can manage the Departments associated with any specific Organization (for which they are assigned rights to) by clicking the Departments button after selecting it beside the Organization name from the Organizations interface. Refer to [5.2.2.7 Managing Departments of an Organization](#) for more details. The 'Departments' area is, in effect, a limited view of the information available in 'Organizations' area - containing data and controls relating to the Department that the DRAO is responsible for.

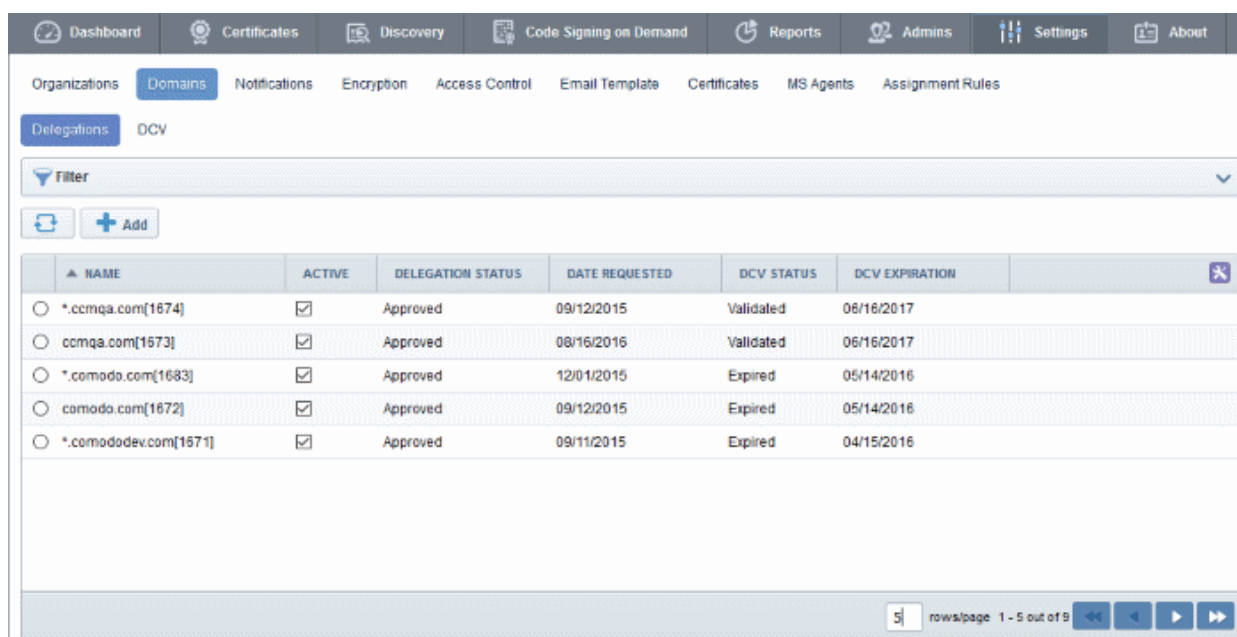
| NAME | ORGANIZATION | CITY | STATE | COUNTRY | VALIDATION STATUS |
|---|----------------------|---------|-------|---------|-------------------|
| <input type="radio"/> dome[3265] | SSL Support Team | Clifton | NJ | US | Not Validated |
| <input type="radio"/> Stores Department[3268] | Ditlers Organization | Chennai | TN | IN | Not Validated |

The 'Departments' area is similar to the 'Departments' dialog that appears on clicking the Departments button for a selected Organization from the 'Organizations' interface. Detailed explanations on the options and controls in this area are available at [4.2.2.7 Managing Departments of an Organization](#).

6.4 Domains

6.4.1 Section Overview

The 'Domains' tab allows Administrators to view the list of domains associated with the Organizations that are enrolled with CCM and the Departments within the Organizations. The Administrators can also create new domains, initiate Domain Control Validation (DCV) and delegate/re-delegate existing domains to the required Organizations/Departments and restrict the certificate types that can be offered for the domains, depending on the purpose(s) for which its use is authorized, from this interface.



- MRAO Administrator - Can create, edit and delegate a domain to any Organization or Department. They can also request, approve and manage certificates for any domain. The domains created by MRAO are automatically approved.
- RAO Administrator - Can create, edit and delegate domains to Organizations (and any subordinate Departments) that have been delegated to them. Can also initiate DCV, request, approve and manage certificates for such domains. The domains created or approved by RAO are to be validated and approved by two MRAOs with appropriate privileges. The delegation can also be approved by a single MRAO with 'Domain validation without Dual Approval' privileges.
- DRAO Administrator - Can create, edit and delegate domains to the Department that have been delegated to them. Can initiate DCV, request, approve and manage certificates for such domains. The domains created by DRAO are to be validated and approved first by the RAO of the Organization to which the Department belongs and then by two MRAOs with appropriate privileges. The delegation can also be approved by a single MRAO with 'Domain validation without Dual Approval' privileges. The 'Domain Awaiting Approval' notification will be sent to MRAO only after the domain created by DRAO is first approved by RAO.

Note: Dual MRAO Approval for created Domains and Domain Control Validation (DCV) options will be visible only if the respective features are enabled for your account.

The following table provides a summary of the ability of Administrator types to manage Domains:

| Action | MRAO Administrator | RAO Administrator | DRAO Administrator |
|--|---|---|---|
| Creating Domains | ✓ | ✓ | ✓ |
| Initiate Domain Control Validation (DCV) | ✓ | ✓ | ✓ |
| Delegating Domains | Can delegate domains to any Organization/Department | Can delegate domains only to those Organizations/Departments that have been delegated to them | Can delegate domains only to those Departments that have been delegated to them |
| Validating and Approving | ✓ | ✓ | ✗ |

| | | | |
|-----------------|--|--|--|
| created Domains | | Can approve domains created by DRAO Administrators of the Departments under the Organization, prior to approval by the MRAO. | |
|-----------------|--|--|--|

Note: A single domain can be delegated to more than one Organization/Department as per requirements.

6.4.1.1 Wildcard Domains

When a wildcard domain is created and delegated to an Organization or a Department, and is validated by MRAO, then the primary domain and all the sub-domains belonging to it are automatically validated only for the same Organization or the Department. For example, if *.example.com is delegated and validated for a specific Organization 'Test Organization', then all the sub-domains such as anything.example.com and something.example.com are automatically validated and approved for the 'Test Organization'.

If the sub-domains of a primary domain delegated to an Organization or Department are to be delegated to other Organizations or Departments, they need to be validated and approved by the MRAO. For example, if *.example.com is delegated and validated for a specific Organization 'Test Organization' and:

- If an RAO wants to re-delegate the sub-domain(s) such as anything.example.com and something.example.com to other Organization 'Demo Organization' then the re-delegation needs to be validated and approved by the MRAO.
- If a DRAO wants to re-delegate the sub domain(s) such as anything.example.com and something.example.com to a Department 'Test Department' (a Department that belongs to the same Organization) then the re-delegation needs to be validated and approved by the RAO.

6.4.2 Domain Management

6.4.2.1 The Domains Area

To open the Domain management area click the 'Domains' sub-tab under the 'Settings' tab.

| NAME | ACTIVE | DELEGATION STATUS | DATE REQUESTED | DCV STATUS | DCV EXPIRATION |
|-----------------------|-------------------------------------|-------------------|----------------|------------|----------------|
| *.ccmq.com[1674] | <input checked="" type="checkbox"/> | Approved | 09/12/2015 | Validated | 06/16/2017 |
| ccmq.com[1673] | <input checked="" type="checkbox"/> | Approved | 08/16/2016 | Validated | 06/16/2017 |
| *.comodo.com[1683] | <input checked="" type="checkbox"/> | Approved | 12/01/2015 | Expired | 05/14/2016 |
| comodo.com[1672] | <input checked="" type="checkbox"/> | Approved | 09/12/2015 | Expired | 05/14/2016 |
| *.comododev.com[1671] | <input checked="" type="checkbox"/> | Approved | 09/11/2015 | Expired | 04/15/2016 |

The Domain management area is divided into two areas accessible by clicking the respective tabs at the top left:

- **Delegations** - Displays a list of all enrolled domains with their delegation status and controls to approve delegate/re-delegate them.
- **DCV** - Displays list of enrolled domains as a tree structure with their Domain Control Validation (DCV) status and controls to initiate the DCV process.

Note: Domain Control Validation (DCV) tab will be visible only if the DCV feature is enabled for your account.

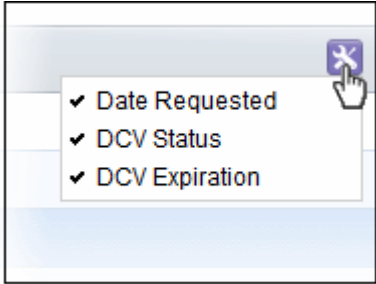
6.4.2.1.1 Domain Delegations

The Domain Delegations area is displayed by default under 'Domains' > 'Settings' and displays a list of requested and approved domains.

- **MRAO Administrator** - Can add new domains, view all the requested and approved domains with their delegation and DCV status. The MRAO Administrator can also view the full details of a domain, delegate/re-delegate domains to required Organizations/Departments and approve domains requested by RAO and DRAO Administrators. Domains added by MRAO Administrators are automatically approved. MRAO administrators can also view domains without delegation that were added by RAO and DRAO administrators and delegate to required Organizations/Departments.
- **RAO Administrator** - Can add new domains to the Organizations that have been delegated to them, view the requested and approved domains delegated to their Organizations with their delegation and DCV status. The RAO Administrator can also view the full details of a domain, delegate/re-delegate domains to their Organizations/Departments and approve domains requested by DRAO Administrators. The domains created or approved by RAO are to be approved by two MRAOs with appropriate privileges. If '**Allow domain validation without Dual Approval**' was selected during the MRAO creation process, then requests can be approved by just a single MRAO'.
- **DRAO Administrator** - Can add new domains to the Departments that have been delegated to them, view the requested and approved domains delegated to their Departments with their delegation and DCV status. The DRAO Administrator can also view the full details of a domain and delegate/re-delegate domains to their Departments. The domains created by DRAO are to be validated and approved first by the RAO of the Organization to which the Department belongs and then by two MRAOs with appropriate privileges. If 'Allow domain validation without Dual Approval' was selected during the MRAO creation process, then requests can be approved by just a single MRAO'. The 'Domain Awaiting Approval' notification will be sent to MRAO only after the domain created by DRAO is first approved by RAO.

6.4.2.1.1.1 Summary of Fields and Controls

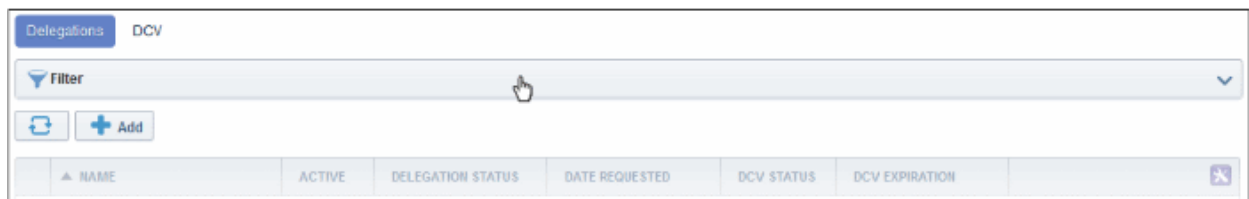
| Column Display | | Description |
|-------------------|--|---|
| Name | | A list of all available Domains created for this account. List is displayed in ascending alphabetical order. The domains which are awaiting approval are displayed in red. |
| Active | | The checkbox allows the administrator to toggle the domain between the active and inactive states. If this is made inactive, the status of the domain will be shown as suspended. |
| Delegation Status | | Indicates the request/approval status of the domain. |
| Date Requested | | Indicates the date on which the domain was requested. |
| DCV Status | | Indicates the validation status of the domain. Note: DCV Status column will be visible only if the respective feature is enabled for |

| | | |
|--|----------|--|
| | | your account. |
| DCV Expiration | | Indicates the date on which the DCV for the domain will expire. |
| <p>Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:</p> | | |
|  | | |
| Controls | | Contains controls that allow MRAO and RAO administrators to add new domains, delegate any existing domain to an Organization/Department and MRAO Administrators to validate and approve the newly created Domains. DRAO Administrators can only create Domains and associate it to the Departments that have been delegated to them. |
| | Add | Enables administrators to create a new Domains to be associated with the existing Organizations and Departments, for the purposes of issuing certificates to end-users |
| | Refresh | Updates the list of displayed Domains. |
| Domain Control Buttons | View | Enables administrators to view details of the domains. The MRAO can also validate and approve the Domains created by self or other administrators using this control. |
| | Delegate | Enables administrators to associate or delegate an existing domain to Organizations and Departments as required. Note: This control is not visible to DRAO Administrators. |
| | Delete | Deletes the domain. This control is available only for domains yet to be approved. |

6.4.2.1.1.2 Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective column

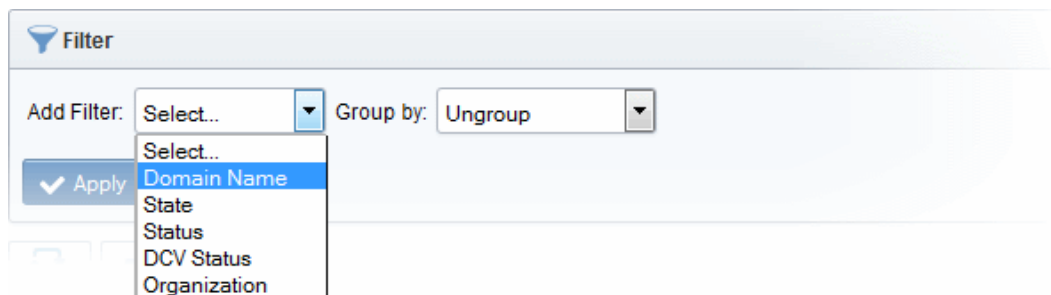
Administrators can search for particular domain by using filters:



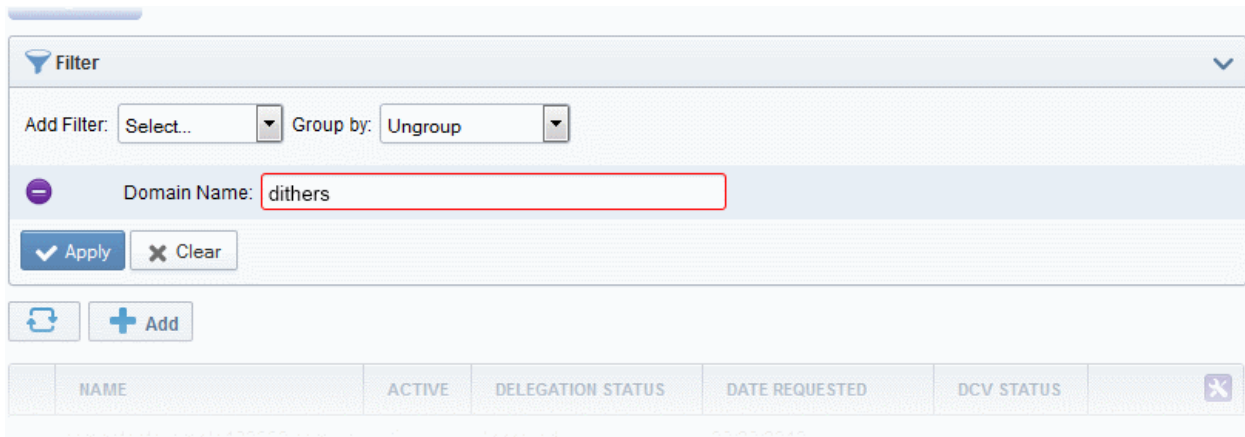
| Filter Options | Description |
|----------------|---|
| Domain Name | Enables Administrators to filter the list of Domains by name. |
| State | Enables Administrators to filter the list of Domains based on their active state: |

| | |
|--------------|--|
| | <p>ANY - Displays the list of all the domains;</p> <p>Active - Displays the list of Domains which are currently active, as set by the administrator.</p> <p>Inactive - Displays the list of Domains which are currently inactive, as set by the administrator.</p> |
| Status | <p>Enables Administrators to filter the list of Domains based on their delegation status:</p> <p>ANY - Displays the list of all the domains;</p> <p>Requested - Displays the list the domains which are requested and awaiting for approval by MRAO.</p> <p>Approved - Displays the list of Domains which are already approved by the MRAO.</p> |
| DCV Status | <p>Enables Administrators to filter the list of Domains based on their DCV status:</p> <p>ANY - Displays the list of all domains</p> <p>Not Started - Displays the list of domains for which the validation process is not started.</p> <p>Awaiting Submittal - Displays the list of domains for which the DCV process has been initiated but the request has not yet been submitted to the Domain Administrator.</p> <p>Submitted - Displays the list of domains for which the DCV request has been submitted to the Domain Administrator.</p> <p>Validated - Displays the list of domains for which the domain control is validated.</p> <p>Expired - Displays the list of domains for which DCV is expired.</p> |
| Organization | <p>Enables to filter only the domains associated with the Organization selected from the drop-down menu.</p> <p>Note: This Field is not visible to RAO and DRAO Administrators.</p> |

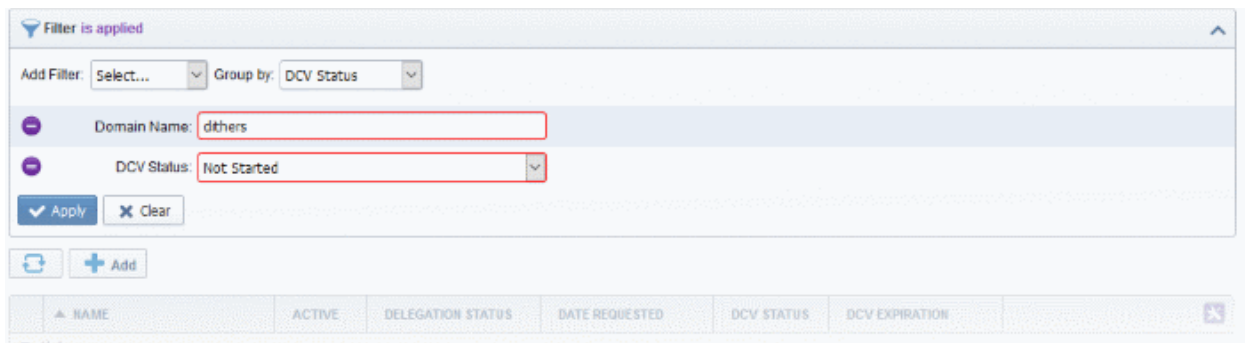
You can add filters by selecting from the options in the 'Add Filter' drop-down. For example, if you want to filter the domain with the domain name, select 'Domain Name':



- Enter the domain name in part or full in the 'Name' field.

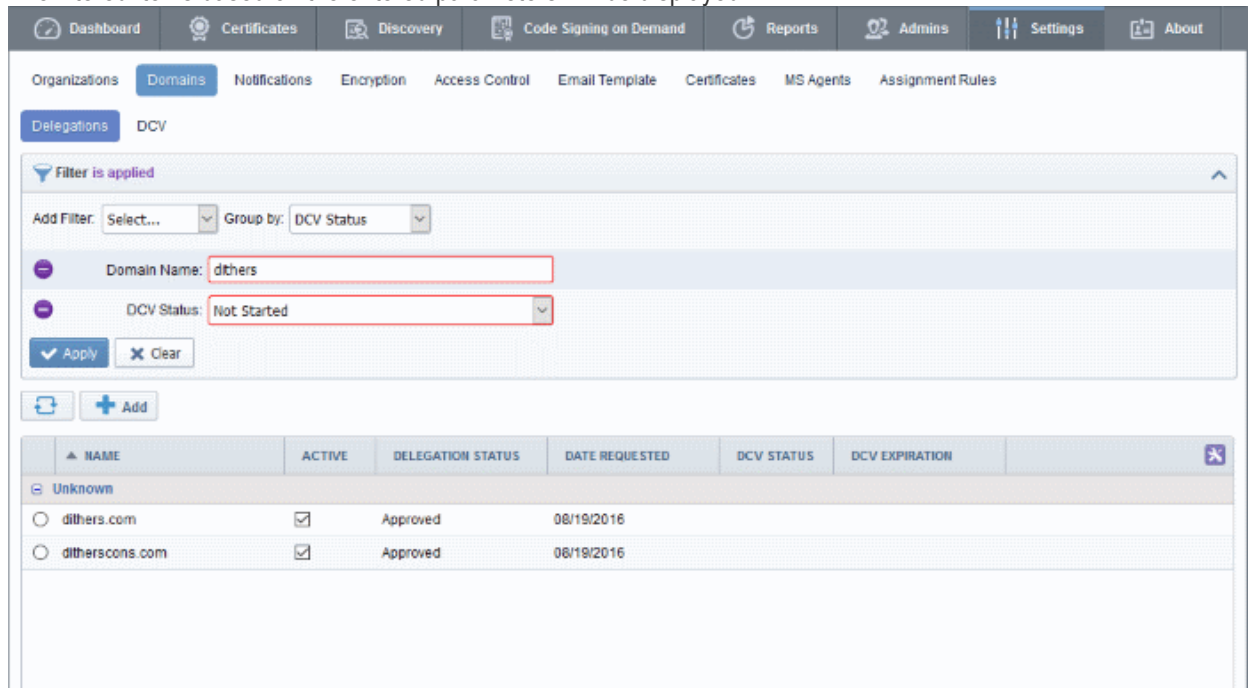


- If you want to group the results based on their delegation status or their DCV status, select the option from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:



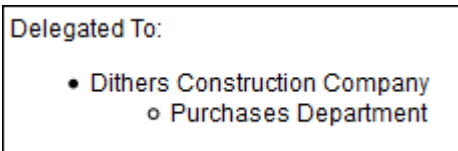
- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the

'Domains' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.4.2.1.1.3 Tool Tip

On pointing the mouse cursor over a domain, the Organizations/Departments to which the domain is delegated is displayed as a tool tip. Also if the domain is re-delegated to another Organization/Department, and awaits approval from the MRAO, the awaiting status is also displayed.



6.4.2.1.2 DCV

The DCV area of the Domains interface displays a list of registered domains along with their DCV status and expiration dates. From this interface, MRAOs can initiate the DCV process on any domain. Domains enrolled by RAO/DRAO SSL Administrators are to be approved by MRAO Administrators before being subject to validation.

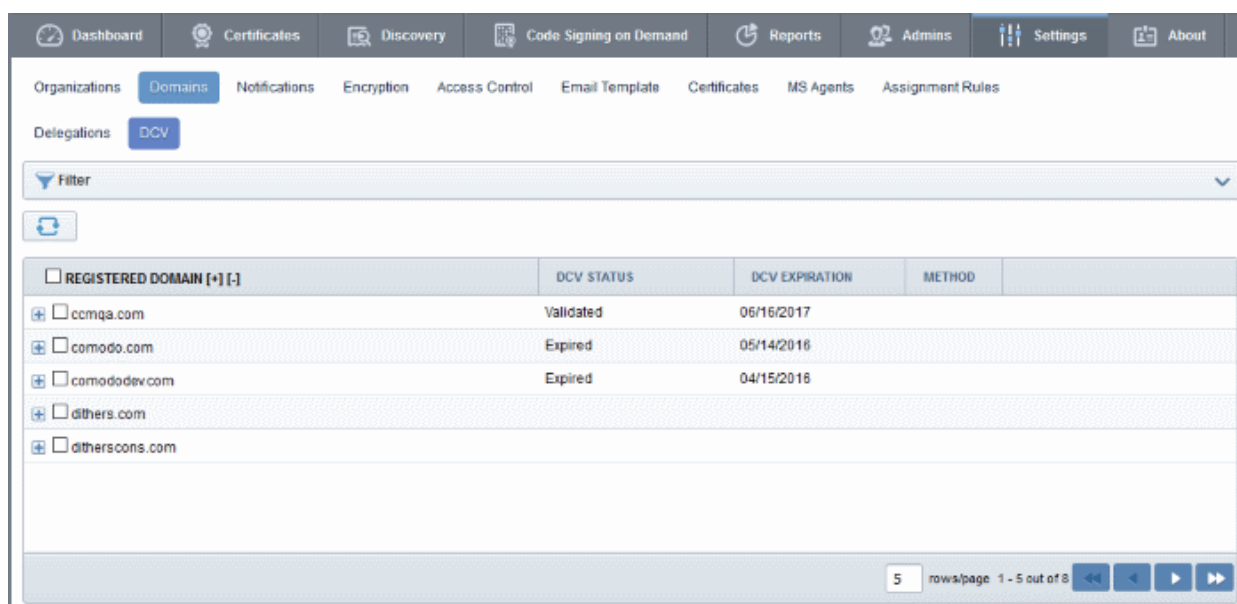
- MRAO Administrator - Can initiate DCV process for all registered Domains.
- RAO Administrator - Can initiate DCV process for the domains delegated to the Organizations that are administrated by them.
- DRAO Administrator - Can initiate DCV process for domains delegated to the Departments that are administrated by them.

The Administrator can choose anyone from the three methods to initiate DCV process for a domain:

- Email - CCM will send an automated email with a validation link to the email address of the domain administrator. The domain will be validated on the domain administrator visiting the validation link in the mail.
- DNS CNAME - CCM will send a hash value that must be entered as DNC CNAME for the domain. CCM will validate by checking the DNS CNAME of the domain
- HTTP/HTTPS File - CCM will send a .txt file which is to be placed at the root of the web server. CCM will validate the domain based on the presence of the sent file

If a wildcard domain is created and delegated to an Organization or a Department, CCM will validate only the registered High Level Domain (HLD). If the HLD is successfully validated, all the sub domains within the name space of the HLD will be considered validated.

For more details on initiating DCV process, refer to the section [Validating the Domain](#).



6.4.2.1.2.1 Summary of Fields and Controls

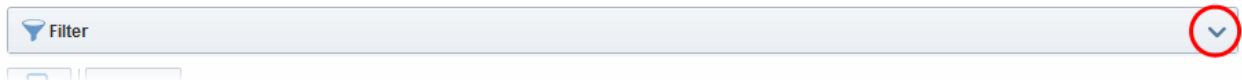
| Column Display | Description |
|---|---|
| Registered Domain | A list of all available Domains created for this account. Clicking the '+' beside a domain name displays the sub-domains of the registered domain. |
| DCV Status | Indicates the validation status of the domain. The status can be one of the following: <ul style="list-style-type: none"> Not Started or blank - The DCV process has not been initiated for the registered high level domain (HLD). Awaiting Submittal - The DCV process has been initiated but the request has not yet been submitted to the Domain Administrator. This status will be available only for the following DCV methods: <ul style="list-style-type: none"> HTTP / HTTPS CNAME Submitted - The DCV request has been submitted to the domain administrator. Validated - The registered high level domain (HLD) has been successfully validated Expired - Displays the list of domains on which DCV has expired. |
| DCV Expiration | Indicates the date when Domain Control Validation for the domain expires. The DCV has to be done again after the expiry period. |
| Method | Indicates the DCV method chosen by the administrator for validating the domain. |
| DCV Control Button Note: The DCV Control button appears only on selecting a domain. | Enables the MRAO and RAO/DRAO SSL Administrators to initiate or restart the DCV process for the selected Domain. |

6.4.2.1.2.2 Sorting and Filtering Options

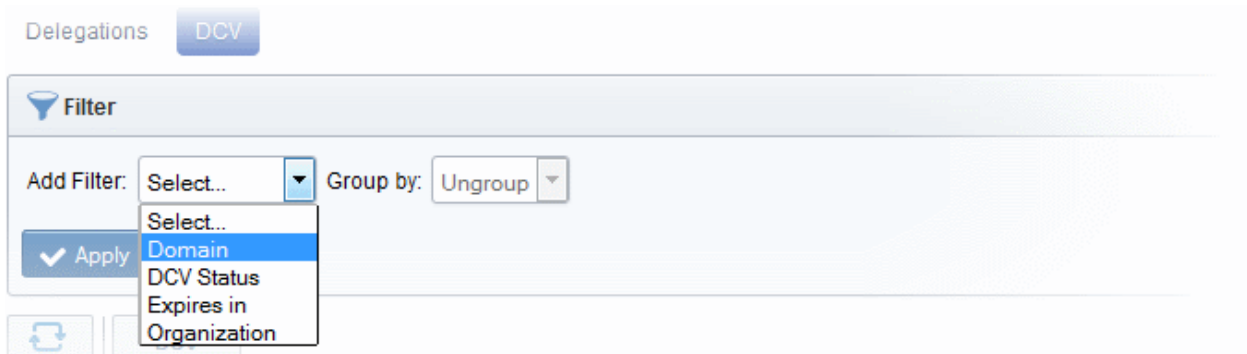
- Clicking on a column header sorts the items in the alphabetical order of the entries in the respective

column

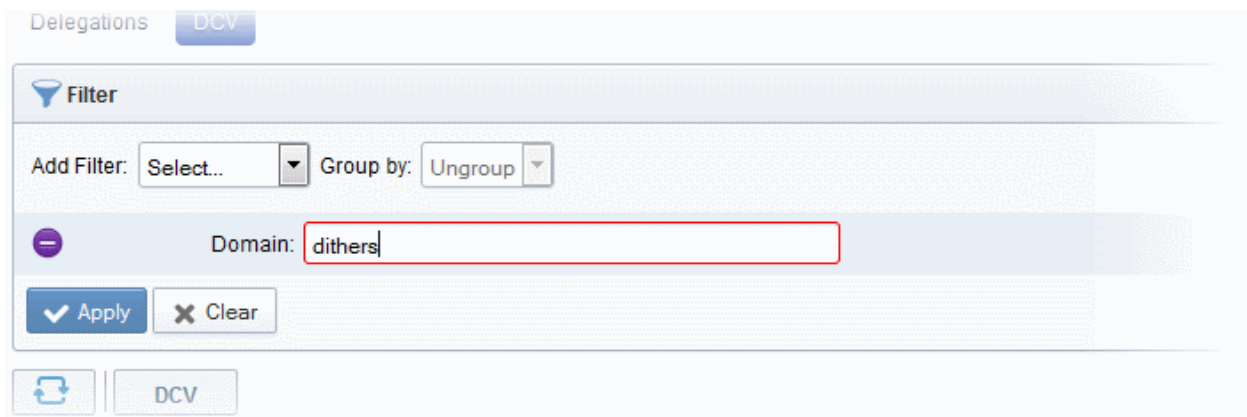
Administrators can search for particular domain by using filters:



To apply filters, click on the down arrow at the right end of the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



- Enter name of the domain in part or full in the Name field.



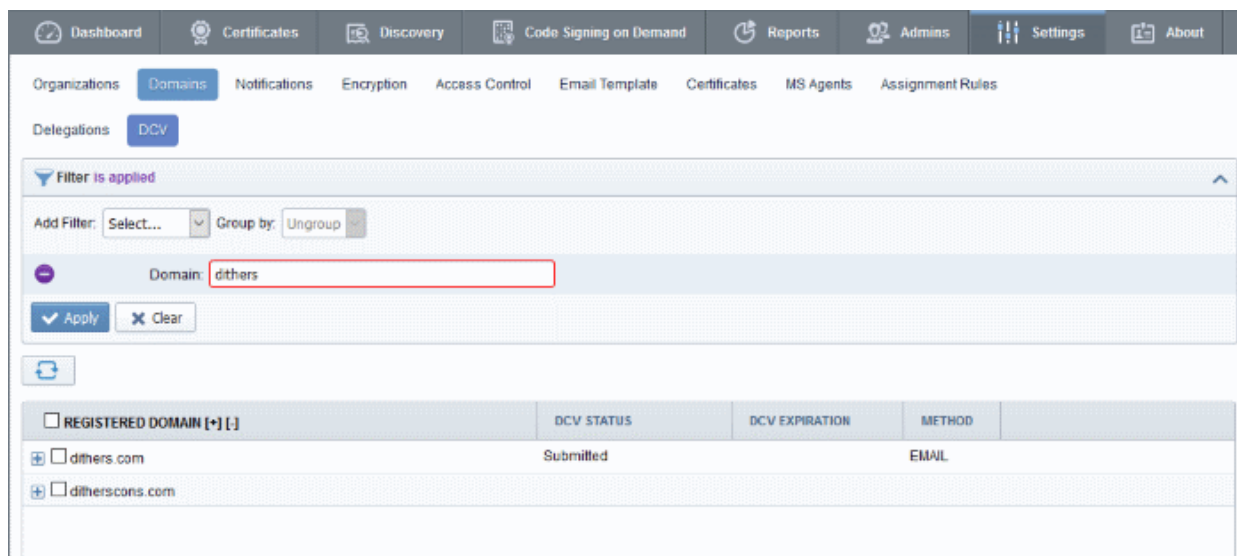
The available filter criteria and their filter parameters are given in the following table:

| Filter Options | Description |
|----------------|---|
| Domain | Enables Administrators to filter the list of Domains by name. |
| DCV Status | Enables Administrators to filter the list of Domains based on their DCV status: <ul style="list-style-type: none"> • ANY - Displays the list of all the domains; • Not Started - Displays only the Domains for which the DCV process has not yet been started. • Awaiting Submittal - Displays only the Domains for which the DCV process has started but the request has not yet been submitted to the Domain Administrator. • Submitted - Displays only the Domains for which the DCV request has been submitted to the domain administrator. • Validated - Displays only the Domains for which the validation has been successfully completed • Expired - Displays a list of domains on which DCV has expired. |

| | |
|--------------|--|
| Expires in | <p>Enables Administrators to filter the list of Domains based on the remaining days for their DCV expiry. The administrator can choose the domains to be listed, whose DCV request expires in:</p> <ul style="list-style-type: none"> • Any • Next 3 days • Next 7 days • Next 14 days • Next 30 days • Next 60 days • Next 90 days |
| Organization | <p>Enables to filter only the domains associated with the Organization selected from the drop-down menu.</p> <p>Note: This Field is not visible to RAO and DRAO Administrators.</p> |

- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:



- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Domains' > 'DCV' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.4.2.2 Creating a New Domain

In order to request, approve and manage all the company's certificates, the administrator should first create domains corresponding to different Organizations/Departments of the company. These domains are to be delegated to respective Departments and/or Organizations delegated to them. The delegated domains are to be validated through Domain Control Validation (DCV) process, which is to be initiated by MRAO or an RAO/DRAO SSL with the sufficient privileges. Only approved and validated domains are facilitated for the request and approval of the SSL certificates and the issuance of client certificates to the end-users falling within the domain. The administrator can also restrict the certificate types that can be requested for the domain depending on the purpose for which its use is authorized.

To create a new domain click the 'Add' button located at the top of the 'Domains' area. This will open the 'Create domain' dialog.

✕
Create Domain

Domain*

Description

Active

| Organizations/Departments | SSL | S/MIME | Code Signing |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> abcdcomp.com | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> Dithers Construction Company | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Purchases Department | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Stores Department | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Elegant | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Elite | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Good Organization | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

[Expand All](#)

6.4.2.2.1 Create Domain - Table of Parameters

| Field Name | Values | Description |
|---------------------------|-------------------|---|
| Domain | String (required) | The name of the Domain |
| Description | String | A short description of the domain. |
| Organizations/Departments | Checkboxes | Enables the administrator to delegate the currently created domain to an Organization/Department. All Organizations are listed by default. Clicking the '+' button beside the Organization name expands the tree structure to display the Departments associated with the Organization. The created domain can be associated to the Organization(s) and/or the Department(s) by selecting the respective checkbox(es). A single domain can be delegated to more than one Organization/Department. Clicking on 'Expand All' expands the tree structure to display all the Departments under each Organization. Clicking on 'Collapse All' in the expanded view collapses the tree structure of all the Organizations and hides the Departments under each Organization. |
| SSL, S/MIME, Code Signing | Checkboxes | Enables the administrator to allow or restrict the types of certificates that can be requested for the created domain, by checking or unchecking the respective checkboxes. The certificate types can be restricted according to the purpose of the domain created. |
| Active | Checkbox | Enables the administrator to toggle the status of the domain between |

| Field Name | Values | Description |
|------------|--------|---|
| | | active and inactive states. Default = Active state. |

6.4.2.2.2 Validating Domains

All new domains added to CCM must pass Domain Control Validation (DCV) before Comodo can issue them with certificates. Administrators can initiate DCV on an individual basis or, if all domains share a common 'Whols' email record, may initiate DCV on multiple domains at once.

- MRAO Administrator - Can initiate DCV process for all registered Domains.
- RAO Administrator - Can initiate DCV process for the domains delegated to the Organizations that are administrated by them.
- DRAO Administrator - Can initiate DCV process for domains delegated to the Departments that are administrated by them.

CCM enables the Administrator to initiate DCV process by three methods:

- Email - CCM will send an automated email with a validation link to the selected email address of the domain administrator. The domain will be validated on the domain administrator visiting the validation URL in the mail. The Email method can be used for both validating a single domain and multiple domains at a time.
- DNS CNAME - CCM will send a hash value that must be entered as DNC CNAME for the domain. CCM will validate by checking the DNS CNAME of the domain.
- HTTP/HTTPS File - CCM will send a .txt file which is to be placed at the root of the web server. CCM will validate the domain based on the presence of the sent file.

If a wildcard domain is created and delegated to an Organization or a Department, CCM will validate only the registered High Level Domain (HLD). If the HLD is successfully validated, all the sub domains within the name space of the HLD will be considered validated.

The following sections explain on:

- **Validating a single domain**
- **Validating multiple domains at a time**

Validating a Single Domain

To initiate DCV for a Domain

1. Open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV'.
2. Next, initiate DCV by selecting the domain and clicking the 'DCV' button that appears at the top. This will open the DCV wizard:

The screenshot shows the Comodo Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Code Signing on Demand, and Report. Below these are sub-tabs: Organizations, Domains, Notifications, Encryption, Access Control, Email Template, and Certificates. Under Domains, there are sub-tabs: Delegations and DCV. A 'Filter' box is present. Below the filter, there is a 'DCV' button circled in red. A table lists domains with columns for 'REGISTERED DOMAIN [+]', 'DCV STATUS', and 'DCV E...'. The domain 'dithersprojects.com' is selected, with its checkbox also circled in red. A red arrow points from the 'DCV' button to a modal window titled 'Domain - dithersprojects.com'. The modal window shows the 'Requested Domain Name' as 'dithersprojects.com', 'DCV Status' as 'Not Started', and 'DCV Method' as empty. Below this, it says 'Select a Domain Control Validation method you want to use:' with four radio button options: 'Email' (selected), 'HTTP', 'HTTPS', and 'CNAME'. At the bottom of the modal, there are 'Cancel', 'Back', and 'Next' buttons.

Select the DCV method from:

- **Email**
- **HTTP/HTTPS**
- **CNAME**

... and click 'Next'.

Email

On selection of EMAIL method, the next step allows you to select the email address of the Domain Administrator for sending the validation email.

✕
Domain - dithersprojects.com

1 Email Selection
2 Awaiting Validation

| | |
|-----------------------|----------------------------|
| Requested Domain Name | dithersprojects.com |
| DCV Status | Not Started |
| DCV Method | Email |

Select an email address that will be used for validation:

▼
 ...

...

admin@dithersprojects.com

administrator@dithersprojects.com

hostmaster@dithersprojects.com

postmaster@dithersprojects.com

webmaster@dithersprojects.com

Cancel

Back

Validate

3. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'Validate'.

An automated email will be sent to the selected Domain Administrator email address. The DCV status of the Domain will change to 'Submitted'.

✕
Domain - dithersprojects.com

1 Email Selection
2 Awaiting Validation

| | |
|-----------------------|----------------------------|
| Requested Domain Name | dithersprojects.com |
| DCV Status | Submitted |
| DCV Method | Email |

A validation letter was sent to **admin@dithersprojects.com**.
Please follow the instructions it contains.

Cancel

Back

Reset

On receiving the email, the domain administrator should click the validation link in it and enter the validation code in

the validation from that appears on clicking the validation link in order to complete the validation process. Once completed, the DCV status of the Domain will change to 'Validated'

HTTP/HTTPS

On selection of HTTP or HTTPS method, the next step allows you to download the .txt file for sending to the Domain Administrator. CCM creates a Hash value for the .txt file and stores it for future reference on validating the domain. The DCV status of the Domain will be changed to 'Awaiting Submittal'.

Domain - dithersprojects.com ✕

1 Get Validation Info
 2 Preliminary Test
 3 Awaiting Validation

| | |
|-----------------------|----------------------------|
| Requested Domain Name | dithersprojects.com |
| DCV Status | Awaiting Submittal |
| DCV Method | HTTPS_CSR_Hash |

SHA1 Hash **72B21EEE5B37D791308461F4BB041A1845F87DC8**

MD5 Hash **CC5412BF14B25A69F0D3A571C2426767**

Instructions for HTTPS DCV:

1. Create a text file containing the following two lines:

```
72B21EEE5B37D791308461F4BB041A1845F87DC8
comodoca.com
```

or get it from here: [Download](#)

2. Save the file with the following name (case sensitive):

```
CC5412BF14B25A69F0D3A571C2426767.txt
```

Cancel

Back

Test

3. Click 'Download' and save the .txt file or create a new notepad file, copy and paste the string given in item 1 and save the file with the name given in item 2.
4. Click Close. CCM will save the hash value generated for future comparison.
5. Send the .txt file to the Domain Administrator through any out-of-band communication method like email and request the domain administrator to place the file in the root of the HTTP/HTTPS server, so that the file is accessible by one of the paths specified in item 3.
6. Once the Domain Administrator has placed the .txt file on the HTTP/HTTPS server, open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV' tab
7. Resume the DCV process by clicking the DCV button in the row of the Domain
8. Click 'Test' to check whether the file has been placed in the web server root. If the file is present, the 'DCV Submission dialog' will appear. Click 'Submit'. The DCV status of the domain will change to 'Submitted'.
9. CCM will validate the Domain on successful submission and the DCV status of the domain will change to 'Validated'.

DNS CName

On selection of CNAME method, CCM creates a DNS CNAME record for the requested domain and stores its hash value for future reference. The next step allows you to get the DNS CNAME record for the requested domain. The DCV status of the Domain will be changed to 'Awaiting Submittal'.

Domain - dithersprojects.com ✕

1 Get Validation Info
2 Preliminary Test
3 Awaiting Validation

| | |
|-----------------------|----------------------------|
| Requested Domain Name | dithersprojects.com |
| DCV Status | Awaiting Submittal |
| DCV Method | CNAME_CSR_Hash |

| | |
|-----------|---|
| SHA1 Hash | 72B21EEE5B37D791308461F4BB041A1845F87DC8 |
| MD5 Hash | CC5412BF14B25A69F0D3A571C2426767 |

Instructions for CNAME DCV:

1. Create a CNAME DNS record for **dithersprojects.com** as follows

CC5412BF14B25A69F0D3A571C2426767.dithersprojects.com. CNAME
 72B21EEE5B37D791308461F4BB041A1845F87DC8.comodoca.com.
2. After you have created the CNAME record, click the **Test** button below.

Cancel
Back
Test

3. Copy the CNAME DNS record given in item no. 1 and pass it to the domain administrator through any out-of-band communication method like email and request the domain administrator to create the record for the domain.
4. Click Close. CCM will save the hash value generated for future comparison.
5. After the Domain Administrator has created the record, open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV' tab
6. Resume the DCV process by clicking the 'DCV' button in the row of the Domain.
7. Click 'Test' to check whether the record has been created. If it is created, the 'DCV Submission' dialog will appear. Click 'Submit'. The DCV status of the domain will change to 'Submitted'.
8. CCM will validate the Domain on successful submission and the DCV status of the domain will change to 'Validated'.

Validating Multiple Domains at a time

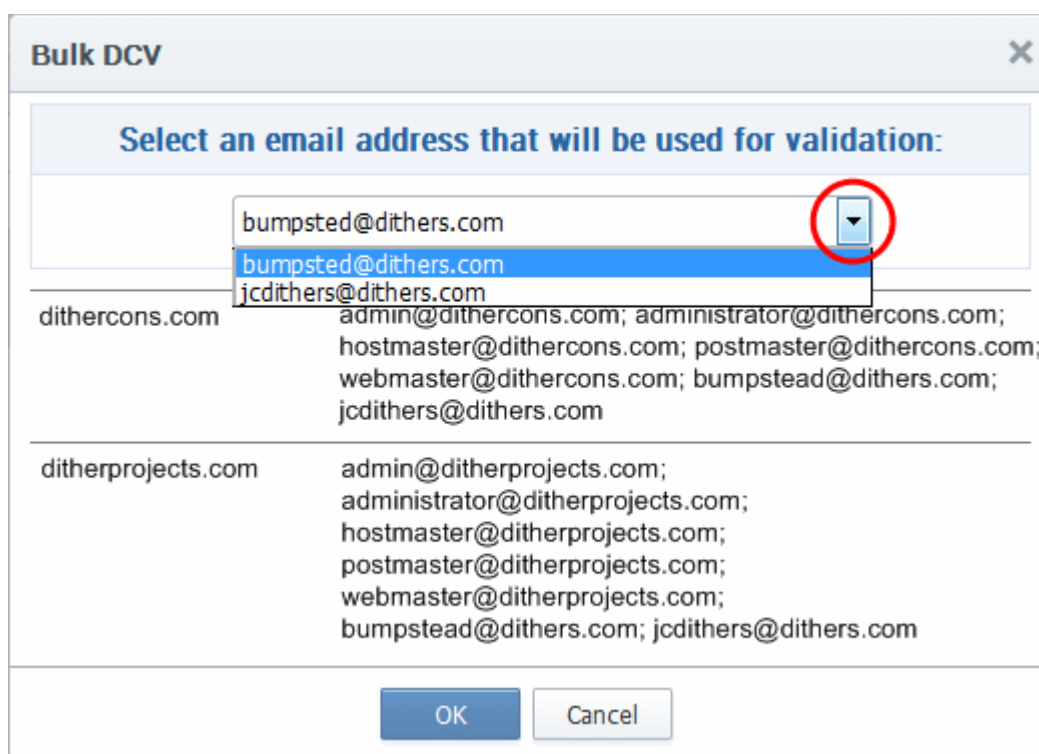
Domain Control Validation (DCV) can be initiated for multiple domains that share a common domain administrative email account in the WhoIs database, at once.

To initiate Bulk DCV for multiple domains

1. Open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV'.
2. Select the domains that share common domain administrator email address
3. Click the 'DCV' button

The screenshot shows the Comodo Certificate Manager interface. The top navigation bar includes 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', and 'Reports'. Below this, there are tabs for 'Organizations', 'Domains', 'Notifications', 'Encryption', 'Access Control', 'Email Template', and 'Certificates'. Under the 'Domains' tab, there are sub-tabs for 'Delegations' and 'DCV'. A 'Filter is applied' message is visible. A 'DCV' button is circled in red, with an arrow pointing to the 'Bulk DCV' dialog box. The dialog box has a title bar 'Bulk DCV' and a close button. It contains the instruction 'Select an email address that will be used for validation:' followed by a dropdown menu showing 'bumpsted@dithers.com'. Below this, there are two lists of email addresses for 'dithercons.com' and 'ditherprojects.com'. The 'dithercons.com' list includes: admin@dithercons.com; administrator@dithercons.com; hostmaster@dithercons.com; postmaster@dithercons.com; webmaster@dithercons.com; bumpstead@dithers.com; jcdithers@dithers.com. The 'ditherprojects.com' list includes: admin@ditherprojects.com; administrator@ditherprojects.com; hostmaster@ditherprojects.com; postmaster@ditherprojects.com; webmaster@ditherprojects.com; bumpstead@dithers.com; jcdithers@dithers.com. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

The Bulk DCV dialog will open. The dialog contains lists of possible domain administrator email addresses and the email addresses fetched from the Whois database for each domain. Common email addresses identified from the lists are displayed in the drop-down at the top.



4. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'OK'.

An automated email will be sent to the selected Domain Administrator email address. The DCV status of the Domain will change to 'Submitted'.

On receiving the email, the domain administrator should click the validation link in it to open the validation form and enter the validation code contained in the email, in order to complete the validation process. Once completed, the DCV status of the Domains will change to 'Validated'.

6.4.2.2.1 Changing DCV method for Validation Pending Domains

The MRAO or RAO/DRAO SSL Administrator with appropriate privileges can change the DCV method for the domains whose validation is pending, from the DCV interface.

To change the validation method

1. Open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV'.
2. Click the 'DCV' button in the row of the domain with DCV status is 'Awaiting Submittal' or 'Submitted'. The DCV wizard will start.
3. Click 'Back' The wizard will move to the previous step of selecting the DCV method
4. Select the new DCV method and continue the process as explained in the section [Validating the Domain](#).

6.4.2.3 Delegating/Re-delegating an Existing Domain

The administrator can delegate or re-delegate the domain to Organizations/Departments according to the requirement from the 'Domains' > 'Delegate' area. Selecting the domain and clicking 'Delegate' button from the top opens the 'Delegate Domain' interface that allows the administrator to delegate or re-delegate the domain. The screen also displays domains that were added by RAO and DRAO administrators without delegating them to any Organizations/Departments. The administrator can delegate these domains to the required Organizations/Departments. The administrator can also select the certificates to be made available for the domain on delegation to the specific Organization/Department based on purpose of delegating the domain to the Organization/Department.

The screenshot displays the 'Delegations' page in the Comodo Certificate Manager. The 'Delegate' button is highlighted with a red circle, and a red arrow points to the 'Delegate Domain' dialog box. The dialog box shows the domain 'dithersprojects.com' and a list of organizations/departments with checkboxes for SSL, S/MIME, and Code Signing.

| NAME | ACTIVE | DELEGATION STATUS | DATE REQUESTED | DCV STATUS |
|---------------------|-------------------------------------|-------------------|----------------|-------------------|
| coradithers.com | <input checked="" type="checkbox"/> | Approved | 03/23/2015 | Submitted |
| dithersprojects.com | <input type="checkbox"/> | Approved | 03/23/2015 | Awaiting Submitte |
| ditherscons.com | <input checked="" type="checkbox"/> | Approved | 03/18/2015 | Submitted |

| Organizations/Departments | SSL | S/MIME | Code Signing |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> AAA Organization | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> ABCD Company | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Cora Company | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Dithers Construction Company | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Elegant | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Elite | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> Good Organization | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

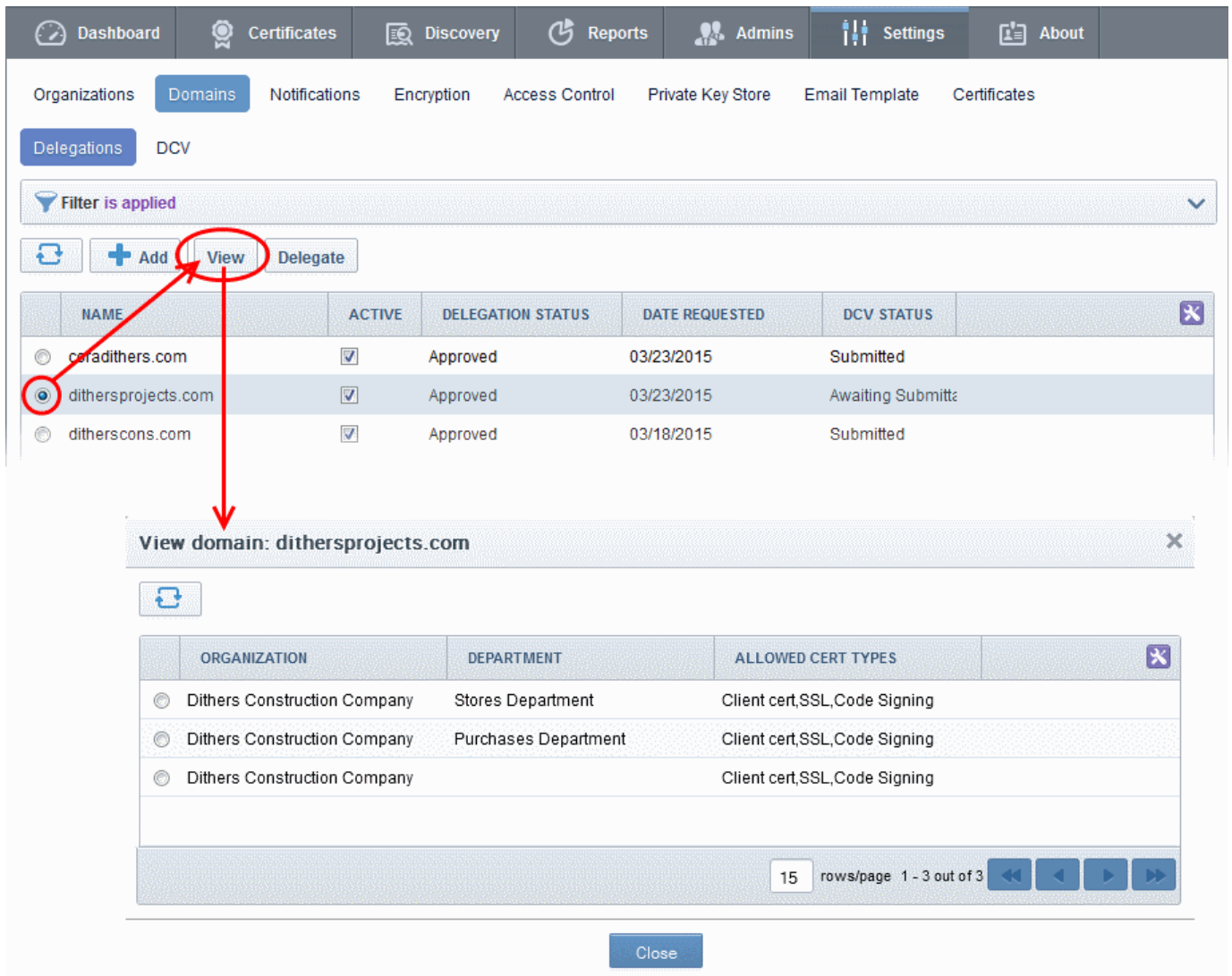
Also the administrator can validate the domain before delegating/re-delegating it specific Organization/Department by clicking the 'Validate' link. Clicking the link enables the administrator to send an automated email to the domain control administrator to check the domain control authority. See [Validating the Domain](#) for more details.

The domains delegated/re-delegated by the MRAO is activated immediately, but the domains delegated by other administrators are to be approved by the MRAO to become active.

Full details on delegating a domain are available in the previous section, '[Create Domain - Table of Parameters](#)'

6.4.2.4 Viewing, Validating and Approving Newly Created Domains

The list of the Organization(s) and Department(s) to which a domain has been delegated and the certificate types enabled for them can be viewed by the appropriately privileged administrator by selecting the domain and clicking the 'View' button from the top. The view dialog also enables the administrators to view the requisition details of the domain and MRAO to validate and approve the domains created by other administrators. The domain becomes active only after the MRAO approves it and only then it enables for request and issuance of SSL certificates, Client certificates and Code Signing certificates.



6.4.2.4.1 View Domain - Summary of Fields and Controls

| Column Display | Description |
|--------------------|--|
| Organization | The Organization(s) to which the domain has been delegated. The delegations which are pending approval by the MRAO are displayed in red. |
| Department | The Department(s) to which the domain has been delegated. The delegations which are pending approval by the MRAO are displayed in red. |
| Description | Provides a short description of the domain as entered during creation of the domain by the administrator. |
| Requested by | Displays the name of the administrator who has created the domain. |
| Date Requested | The date at which the domain was added to CCM. |
| MRAO Approver | Displays the name of the MRAO administrator who has approved the creation/delegation of the domain. |
| Date Approved | The date at which the domain was approved by MRAO. |
| Allowed Cert Types | The Certificate types that are enabled and available for the domain |

Note: The administrator can enable or disable the columns from the drop-down button beside the last item in the

table header:



| | | |
|--|---------|---|
| Controls | Refresh | Updates the list of displayed Organizations and Departments and their details. |
| Delegation Control Buttons Note: The Delegation control buttons are visible only on selecting a domain | Details | Enables the administrator to view the requisition details of the domain. |
| | Approve | Enables MRAO administrator to approve the creation and delegation of the domain by RAO and DRAO administrators. Note: This control button is visible only for Domains with 'Requested' status and only to MRAO and RAO administrators. |
| | Reject | Enables MRAO administrator to decline the creation and delegation of the domain by RAO and DRAO administrators. Note: This control button is visible only for Domains with 'Requested' status and only to MRAO and RAO administrators. |

6.4.2.4.2 Approval of Creation and Delegation of Domains

Domains that are created and delegated by:

- MRAO Administrators are automatically validated and approved;
- RAO Administrators are to be validated by the MRAO to become active;
- DRAO Administrators are to be first validated and approved by the RAO Administrator of the Organization to which the Department delegated with the domain belongs and then by the MRAO to become active.

Domains which are awaiting approval are displayed in red color in the Domains area of the CCM interface.

The MRAO and RAO Administrator can check the validity of the Domain and approve/reject the request for the Domain.

To approve or reject a domain delegation

- Open the 'View Domain' dialog
- Select the Organization/Department for which the domain delegation has been requested
- Click 'Approve' or 'Reject' button from the top

View domain: ditherspayers.com ✕

| | ORGANIZATION | DEPARTMENT | ALLOWED CERT TYPES | ✕ |
|----------------------------------|------------------------------|----------------------|------------------------------|----------------|
| <input checked="" type="radio"/> | Dithers Construction Company | Purchases Department | Client cert,SSL,Code Signing | |
| <input type="radio"/> | Dithers Construction Company | Stores Department | Client cert,SSL,Code Signing | |
| <input type="radio"/> | Dithers Construction Company | | Client cert,SSL,Code Signing | |

15 rows/page 1 - 3 out of 3 ◀◀ ▶▶ ▶▶

If a domain is created/delegated by a DRAO Administrator, it will be displayed in red only to the RAO Administrator of the Organization to which the Department belongs, indicating it is awaiting approval, in the 'Domains' area of the CCM interface. Once it is validated and approved by the RAO Administrator, it becomes visible to the MRAOs for validation/approval.

If a domain is created by an RAO Administrator, it will be displayed in red to the MRAO Administrators indicating that it is awaiting validation/approval.

Once a requested domain is validated and approved by the MRAO a domain approval notification will be sent and the domain will be enabled for request and issuance of SSL certificates, client certificates and Code Signing certificates.

6.4.2.4.3 Viewing Requisition and Approval Details of a Domain

The administrator can view the request and approval details of the domain delegation by selecting an Organization or a Department and clicking the 'Details' button from the 'View Domain' interface.

Request Details
✕

Organization **Dithers Construction Company**

Department **Purchases Department**

Domain **ditherspayments.com**

Requested by **Joe D**

Date Requested **03/25/2015**

RAO Approver **Joe A**

Date RAO Approved **03/25/2015**

MRAO Approver 1 **John Smith**

Date MRAO Approved **03/25/2015**

Status **Approved**

Description **For receiving payments**

Email Address **joed@example.com**

Allowed Cert Types **Client cert,SSL**

Close

6.4.2.4.4 Request Details - Table of Parameters

| Field | Description |
|--------------------|---|
| Organization | Indicates the name of the Organization to which the domain is delegated. |
| Department | Indicates the name of the Department to which the domain is delegated. |
| Domain | Indicates the name of the selected Domain. |
| Requested by | The name of the Administrator who has requested for the approval of the delegation of the domain to the Organization/Department . |
| Date Requested | Date of requisition for delegation of the domain. |
| RAO Approver | The name of the RAO SSL administrator who approved the domain, if the domain was requested by a DRAO SSL administrator. |
| Date RAO Approved | The date on which the domain was approved by the RAO SSL administrator. |
| MRAO Approver | The name of the MRAO administrator who approved the domain. |
| Date MRAO Approved | The date on which the domain was approved by the MRAO |
| Status | Indicates whether the domain has been approved or awaiting approval for delegation. |
| State | Indicates whether the domain is active or inactive as set by the administrator. |
| Description | A short description for the domain as entered by the administrator while creating it. |
| E-mail Address | Email address of the administrator who requested for the delegation of the |

| Field | Description |
|--------------------|---|
| | domain. |
| Allowed Cert Types | Indicates the Certificate types which could be requested/issued for the domain. |

6.5 Notifications

The 'Notifications' interface enables MRAO, RAO and DRAO Administrators to set up and manage email notifications to various personnel - including notifications triggered by events like requisition, issuance, download, installation, expiry of certificates, requisition, approval and validation of domains and their delegations, creation of administrators, certificate discovery scan reports and more.

Tip: CCM also enables the Administrators to customize the email templates of the notifications as required. Refer to **Email Templates** for more details.

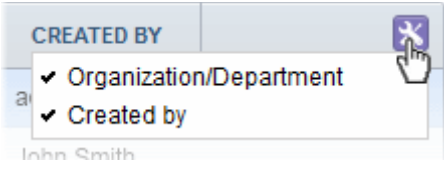
Administrative Roles:

- MRAO - Can see a list of all the notification types set by them, RAO Administrators and DRAO Administrators. They can create new notification types and can edit settings for notification for any Organization and any Department.
- RAO - Can only view the notification set by them for the users belonging the Organizations (and any subordinate Departments) that have been delegated to them. They can create and manage notifications only for the notification types on which they have authority AND only for the Organization (and any subordinate Departments) that have been delegated to them.
- DRAO - Can only view the notifications setup for the users belonging to Department(s) delegated to them. They can create and manage notifications only for the notification types on which they have authority AND only for the Departments that have been delegated to them.

| DESCRIPTION | ORGANIZATION/DEPARTMENT | DAYS | CREATED BY |
|--|-------------------------|------|--------------------|
| <input type="radio"/> Device cert expiration | Device Org | 7 | Administrator MRAO |
| <input type="radio"/> Device cert revoked | ANY | | Administrator MRAO |
| <input type="radio"/> Client cert expiration | ANY | 7 | Administrator MRAO |

Notifications - Summary of Fields and Controls

| Column Display | Description |
|-------------------------|---|
| Description | Provides a short description for the notification, as entered by the administrator during creation. |
| Organization/Department | The Organization(s)/Department(s) for which the notification was created. The |

| | | |
|---|---------|---|
| | | notification mails will be sent to the only to Administrators of these Organization(s)/Department(s). |
| Days | | Number of days in advance of the event, the notification will be sent. |
| Created by | | Displays the name of the administrator who has created the notification. |
| <p>Note: An administrator can enable or disable the columns from the drop-down button beside the last item in the table header:</p>  | | |
| Control Buttons | Add | Enables the Administrator to add a new notification. |
| | Refresh | Updates the list of displayed Notifications. |
| Notification Control Buttons | Edit | Enables the administrator to edit the notification. See note below. |
| | Delete | Enables the Administrator to delete the notification. See note below. |
| <p>Note: The Notification control buttons are visible only on selecting a Notification</p> | | |

Important Notes:

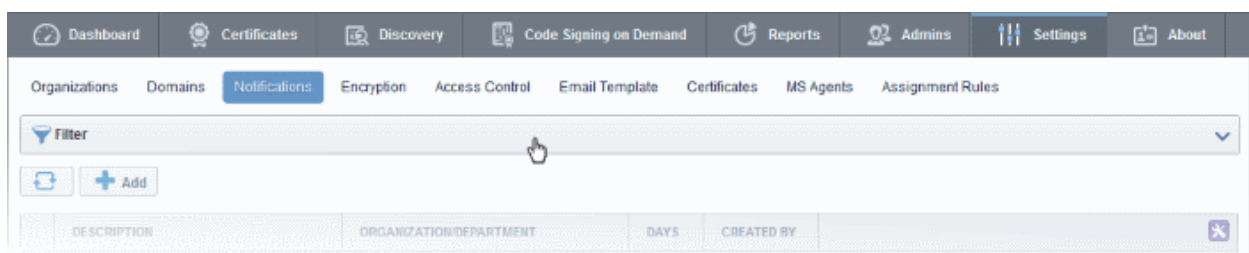
An administrator can either edit or delete an existing notification when all the following conditions are true:

- The administrator has authority for all of the Organizations and Departments contained within the scope of the notification.
- The administrator has authority for the notification type.
- The creator of the notification is of the same or lower administrative level than that of the administrator.

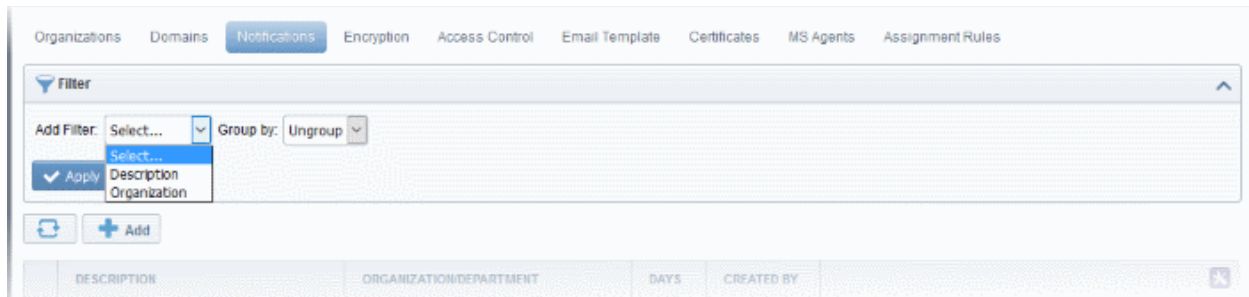
Sorting and Filtering Options

- Clicking on a column headers 'Description' and 'Days' sorts the items in the alphabetical order of the entries in the respective column.

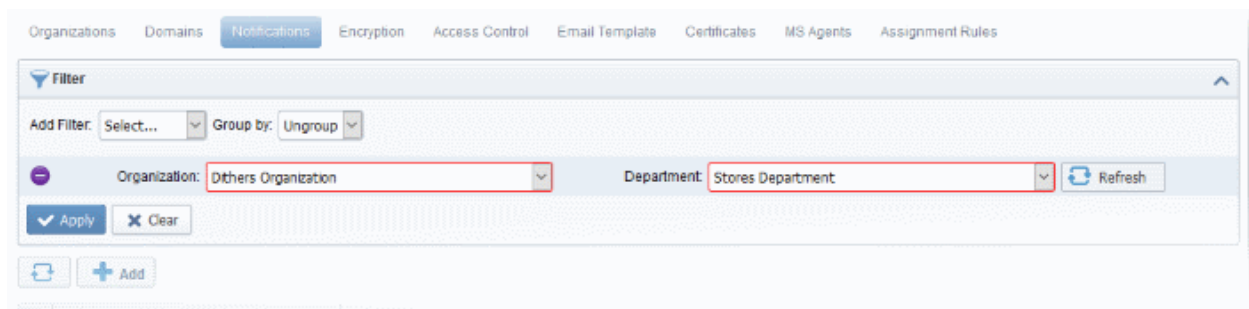
Administrators can search for a particular notification from the list by using the filters:



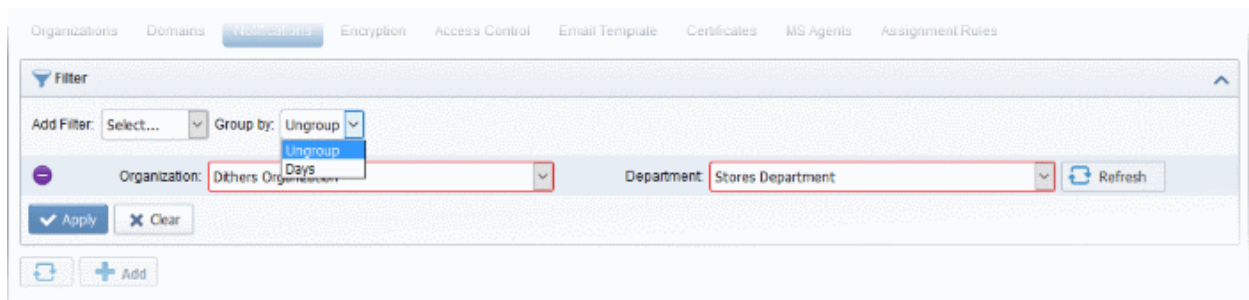
To apply filters, click anywhere on the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down. For example, if you want to filter the notification type set for an Organization/Department, select 'Organization' from the 'Add Filter' drop-down:



- Select the Organization and the Department from the 'Organization' and 'Department' drop-downs.



To group the results based on the days parameter, select 'Days' from the 'Group by' drop-down.



- Click the 'Apply' button.

The filtered items based on the selected parameters will be displayed:

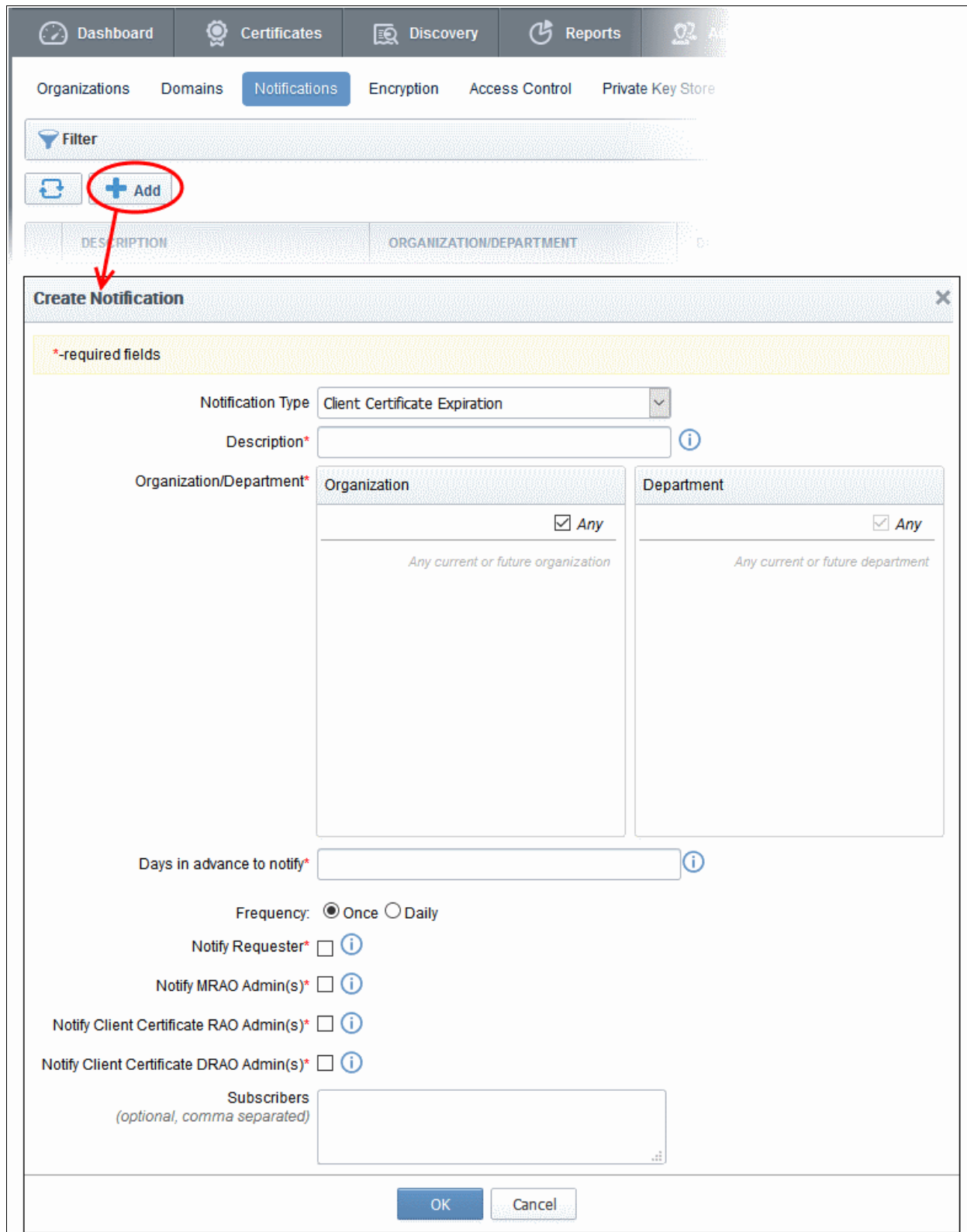
| DESCRIPTION | ORGANIZATION/DEPARTMENT | DAYS | CREATED BY |
|--|-------------------------|------|--------------------|
| <input type="radio"/> Device cert revoked | ANY | | Administrator MRAO |
| <input type="radio"/> Client cert expiration | ANY | 7 | Administrator MRAO |

- To remove the filters, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Notifications' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.5.1 Adding a Notification

Administrators can add a new notification by clicking the 'Add' button under the 'Notifications' sub-tab and filling out the form that appears.



When adding a notification administrator should first select a Notification Type.

There are several types of notifications available for selection. The list of notification types in the drop-down is dependent on the role of the administrator. For example, RAO SSL and DRAO SSL administrators will see the options corresponding only to SSL certificates and so on.

An administrator can create notifications when he/she has authority for *all* of the Organizations and Departments contained within the scope of the notification *and* the administrator has authority for the notification type.

Similarly, an administrator can view existing notifications when he/she has authority for *any* of the Organizations or Departments contained within scope of the notification *and* the administrator has authority for the notification type.

The screenshot shows the 'Create Notification' dialog box. At the top, there is a yellow banner indicating '*-required fields'. Below this, the 'Notification Type' dropdown is open, showing a list of notification types. The 'Description*' field is empty. The 'Organization/Department*' field is also empty, with a dropdown menu showing 'Any' selected. Below these fields, there is a 'Days in advance to notify*' input field. At the bottom, there are radio buttons for 'Frequency' (Once and Daily) and a checkbox for 'Notify Requester*'. Information icons (i) are present next to several fields.

The following table explains the notification types that are available for administrators according to their administrative roles.

| Notification | Notification Type | Administrator Type |
|-------------------------------------|--------------------------|--|
| Client Certificate Expiration | Client Certificate | MRAO, RAO S/MIME admins, DRAO S/MIME admins. |
| Client Certificate Revoked | Client Certificate | MRAO, RAO S/MIME admins, DRAO S/MIME admins. |
| Code Signing Certificate Downloaded | Code Signing Certificate | MRAO, RAO Code Signing admins, MRAO Code Signing admins. |
| Code Signing Certificate Revoked | Code Signing Certificate | MRAO, RAO Code Signing admins, MRAO Code Signing admins. |
| Code Signing Certificate Expiration | Code Signing Certificate | MRAO, RAO Code Signing admins, MRAO Code Signing admins. |
| Code Signing Certificate Requested | Code Signing Certificate | MRAO, RAO Code Signing admins, MRAO Code Signing admins. |
| SSL Approved | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin. |

| Notification | Notification Type | Administrator Type |
|--|-----------------------------------|--|
| SSL Awaiting Approval | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin. |
| SSL Declined | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin. |
| SSL Expiration | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin. |
| SSL Issuance Failed | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin. |
| SSL Revoked | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin. |
| Discovery Scan Summary | Other | All administrators. |
| Remote SSL Certificate Installed | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin |
| Remote SSL Certificate Installation Failed | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin |
| Auto-Installation/Renewal Failed | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin |
| Certificate Ready for Manual Installation | SSL Certificate | MRAO, RAO SSL admin, DRAO SSL admin |
| Device Certificate Expiration | Device Authentication Certificate | MRAO, RAO Device Certificate admins, DRAO Device Certificate admins. |
| Device Certificate Revoked | Device Authentication Certificate | MRAO, RAO Device Certificate admins, DRAO Device Certificate admins. |
| Device Certificate Awaiting Approval | Device Authentication Certificate | MRAO, RAO Device Certificate admins, DRAO Device Certificate admins. |
| Client Admin Creation | Other | All administrators. |
| Domain Awaiting Approval | Other | All administrators. |
| Domain Approved | Other | All administrators. |
| DCV Expiration | Domain Control Validation | MRAO, RAO SSL admin, DRAO SSL admin |
| DCV Validated | Domain Control Validation | MRAO, RAO SSL admin, DRAO SSL admin |
| DCV Needed-New Domain | Domain Control Validation | MRAO, RAO SSL admin, DRAO SSL admin |
| Code Sign Request Created | Code Signing Certificate | MRAO, RAO Code Signing admins, DRAO Code Signing admins. |

| Notification | Notification Type | Administrator Type |
|---------------------------|--------------------------|--|
| Code Signing CSoD Revoked | Code Signing Certificate | MRAO, RAO Code Signing admins, DRAO Code Signing admins. |

Note: The Notification Types related to DCV will be available only if the DCV feature is enabled for your account.

Detailed description of each type of form is given below. The 'Create Notification' form varies pursuant to the selected 'Notification Type'.

6.5.2 Notification Types

6.5.2.1 'Client Certificate Expiration' Create Notification Form

Enables administrator to set notification about terms of expiration of client certificates.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Days in advance to notify*

Frequency: Once Daily

Notify Requester*

Notify MRAO Admin(s)*

Notify Client Certificate RAO Admin(s)*

Notify Client Certificate DRAO Admin(s)*

Subscribers
(optional, comma separated)

6.5.2.1.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|---|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator can select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Days in advance to notify (required) | Text Field | Enables the administrator to send number of days the end-user will be informed about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent to the member(s) only once or daily till the expiration date by selecting the respective radio button. |

| Form Element | Type | Description |
|---|------------|---|
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for person that requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify Client Certificate RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO S/MIME Admin(s) of the Organization(s). |
| Notify Client Certificate DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO S/MIME Admin(s) of the Departments(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.2 'Client Certificate Revoked' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon revocation of a client certificate.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department
- Purchases Department
- Stores Department

For Certificates Revoked by* User Administrator

Notify Requester* (i)

Notify MRAO Admin(s)* (i)

Notify Client Certificate RAO Admin(s)* (i)

Notify Client Certificate DRAO Admin(s)* (i)

Subscribers
(optional, comma separated)

6.5.2.2.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| For Certificates Revoked by: (required) | Checkbox | Administrator should select a person (administrator or user) after whose revoke action, the notification will be send. |
| Notify Requester (required) | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |

| | | |
|---|------------|---|
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify Client Certificate RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO S/MIME Admin(s) of the Organization(s). |
| Notify Client Certificate DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO S/MIME Admin(s) of the Departments(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.3 'Code Signing Certificate Downloaded' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate was downloaded by the Administrator.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

▼ Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

▼ Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify Code Signing RAO Admin(s)* ⓘ

Notify Code Signing DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.3.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify Code Signing RAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s). |
| Notify Code Signing DRAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO Code Signing Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.4 'Code Signing Certificate Revoked' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate was revoked.

Create Notification
✕

*-required fields

Notification Type ▾

Description* ⓘ

Organization/Department*

Organization

▾ Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

▾ Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify Code Signing RAO Admin(s)* ⓘ

Notify Code Signing DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.4.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Requester (required) | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |
| Notify MRAO Admin(s) (required) | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |

| Form Element | Type | Description |
|--|------------|---|
| Notify Code Signing RAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s). |
| Notify Code Signing DRAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO Code Signing Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.5 'Code Signing Certificate Expiration' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate is due to expire.

Create Notification
✕

*-required fields

Notification Type: Code Signing Certificate Expiration ▼

Description*: ⓘ

Organization/Department*: **Organization**

☐ ▼
☐ Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

☐ ▼
☐ Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Days in advance to notify*: ⓘ

Frequency: Once Daily

Notify Requester*: ⓘ

Notify MRAO Admin(s)*: ⓘ

Notify Code Signing RAO Admin(s)*: ⓘ

Notify Code Signing DRAO Admin(s)*: ⓘ

Subscribers
(optional, comma separated)

OK
Cancel

6.5.2.5.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Days in advance to notify <i>(required)</i> | Text Field | Enables the administrator to send number of days the end-user will be informed about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent to the member(s) only once or daily till the expiration date by selecting the respective radio button. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify Code Signing RAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s). |
| Notify Code Signing DRAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO Code Signing Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.6 'Code Signing Certificate Requested' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose Code Signing Certificate is been requested by the Administrator to the CA.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Best Organization
 - None

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify Code Signing RAO Admin(s)* ⓘ

Notify Code Signing DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.6.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Requester (required) | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |
| Notify MRAO Admin(s) (required) | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |

| Form Element | Type | Description |
|--|------------|---|
| Notify Code Signing RAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO Code Signing Admin(s) of the selected Organization(s)/Department(s). |
| Notify Code Signing DRAO Admins(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO Code Signing Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.7 'SSL Approved' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon Approval of an SSL certificate request by an Administrator.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department* **Organization**

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Certificate Type

Notify Owner* ⓘ

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.7.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: <i>(required)</i> | Drop-down | Administrator should choose the type of SSL certificate for which the notification is to be set. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. The Owner of the certificate is the Administrator that first approved the request for the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.8 'SSL Awaiting Approval' Create Notification Form

Enables the administrator to send a notification about an SSL certificate state after the certificate was requested. An SSL certificate request must be approved by the administrator. Before the request is approved, its state is 'Awaiting Approval'.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Certificate Type

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.8.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the notification is to be set. |
| Notify Requester (required) | Checkbox | Enables the administrator to send the notification for person, who requested the certificate. |

| Form Element | Type | Description |
|---|------------|--|
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.9 'SSL Declined' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose SSL Certificate request was declined by the Administrator.

Create Notification ✕

***-required fields**

Notification Type:

Description*:

Organization/Department*

| Organization | Department |
|--|--|
| <input type="checkbox"/> Any | <input type="checkbox"/> Any |
| <input type="checkbox"/> AAA Organization | <input checked="" type="checkbox"/> Dithers Construction Company |
| <input type="checkbox"/> ABCD Company | <input checked="" type="checkbox"/> None |
| <input type="checkbox"/> Best Organization | <input type="checkbox"/> Purchases Department |
| <input checked="" type="checkbox"/> Dithers Construction Company | <input type="checkbox"/> Stores Department |
| <input type="checkbox"/> Elegant | |

Certificate Type:

Notify Owner* ⓘ

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.9.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the notification will be set. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. The Owner of the certificate is the Administrator that first approved the request for the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for a person, who requested the certificate. |
| Notify Master Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.10 'SSL Expiration' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose SSL Certificates are due to expire, in advance.

Create Notification ✕

**-required fields*

Notification Type:

Description*:

Organization/Department*

| Organization | Department |
|--|--|
| <input type="checkbox"/> Any | <input type="checkbox"/> Any |
| <input type="checkbox"/> AAA Organization | <input checked="" type="checkbox"/> Dithers Construction Company |
| <input type="checkbox"/> ABCD Company | <input checked="" type="checkbox"/> None |
| <input type="checkbox"/> Best Organization | <input type="checkbox"/> Purchases Department |
| <input checked="" type="checkbox"/> Dithers Construction Company | <input type="checkbox"/> Stores Department |
| <input type="checkbox"/> Elegant | |

Certificate Type:

Days in advance to notify*:

Frequency: Once Daily

Notify Owner*:

Notify Requester*:

Notify MRAO Admin(s)*:

Notify SSL DRAO Admin(s)*:

Subscribers
(optional, comma separated)

6.5.2.10.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|---|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Department(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the notification will be set. |
| Days in advance to notify <i>(required)</i> | Text Field | Enables the administrator to send number of days the notification will be sent about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent only once or daily till the expiration date by selecting the respective radio button. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for a person, who owns the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for a person, who requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.11 'SSL Issuance Failed' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel for whom the SSL Certificate issuance has failed.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Certificate Type

Notify Owner*

Notify Requester*

Notify MRAO Admin(s)*

Notify SSL RAO Admin(s)*

Notify SSL DRAO Admin(s)*

Subscribers
(optional, comma separated)

6.5.2.11.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the notification will be set. |

| Form Element | Type | Description |
|--|------------|---|
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for a person, who requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.12 'SSL Revoked' Create Notification Form

Enables the administrator to set the notification about SSL certificates 'Revoke' action (the certificate could be revoked by the administrator or by the end-user).

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization Any

AAA Organization

ABCD Company

Best Organization

Dithers Construction Company

Elegant

Department Any

Dithers Construction Company

None

Purchases Department

Stores Department

Certificate Type

For Certificates Revoked by* User Administrator

Notify Owner* ⓘ

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.12.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the |

| Form Element | Type | Description |
|--|------------|---|
| | | notification will be set. |
| For Certificates Revoked by: <i>(required)</i> | Checkbox | Administrator should select a person (administrator or user) after whose revocation action, the notification is to be sent. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification for a person, who requested the certificate. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.13 'Discovery Scan Summary' Create Notification Form

Enables the Administrator to create a notification with a summary of certificate discovery scan results, for sending to selected personnel.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Certificate Type

Notify Requester*

Notify MRAO Admin(s)*

Notify SSL RAO Admin(s)*

Notify SSL DRAO Admin(s)*

Subscribers
(optional, comma separated)

6.5.2.13.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the discovery scan summary notification will be set. |
| Notify MRAO Admin(s) | Checkbox | Enables the administrator to send the notification for the MRAO |

| Form Element | Type | Description |
|---|------------|--|
| <i>(required)</i> | | Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.14 'Remote SSL Certificate Installed ' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose SSL Certificate was remotely installed by the Administrator.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department* i

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Certificate Type

Notify Owner* i

Notify Requester* i

Notify MRAO Admin(s)* i

Notify SSL RAO Admin(s)* i

Notify SSL DRAO Admin(s)* i

Subscribers
(optional, comma separated)

6.5.2.14.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the SSL certificate was installed remotely notification will be set. |

| Form Element | Type | Description |
|--|------------|--|
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the Admin status. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.15 'Remote SSL Certificate Installation Failed' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel whose remote SSL Certificate installation failed.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department* **Organization**

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Certificate Type

Notify Owner* ⓘ

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.15.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (required) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (required) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the remote installation failed notification will be sent. |
| Notify Owner (required) | Checkbox | Enables the administrator to send the notification for the Owner of the |

| Form Element | Type | Description |
|--|------------|--|
| | | certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the Admin status. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.16 'Auto Installation/Renewal Failed' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel for whom auto installation/renewal has failed.

*-required fields

Notification Type: Auto Installation/Renewal Failed ▼

Description*: ⓘ

Organization/Department*

Organization

▼ Any

- docs
- Dithers Company
- acme corp
- XYZ Organization

Department

▼ Any

- Dithers Company
 - None
 - Purchase department
 - Stores Department

Certificate Type: ANY ▼

Notify Owner* ⓘ

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.16.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |

| Form Element | Type | Description |
|--|------------|---|
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the remote installation failed notification will be sent. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the Admin status. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.17 'Certificate Ready for Manual Installation' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel for whom certificate is ready for manual installation.

6.5.2.17.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|---|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments |

| Form Element | Type | Description |
|--|------------|---|
| | | will be displayed. Choose the Organizations/Departments from the tree structure. |
| Certificate Type: (required) | Drop-down | Administrator should choose the type of SSL certificate for which the remote installation failed notification will be sent. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the Admin status. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for RAO SSL Admin(s) of the selected Organization(s)/Department(s). |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification for DRAO SSL Admin(s) of the selected Department(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.18 'Device Certificate Expiration' Create Notification Form

Enables administrator to set notifications about expiring device certificates.

The screenshot shows a 'Create Notification' dialog box with the following fields and options:

- Notification Type:** Device Certificate Expiration (dropdown menu)
- Description*:** Text input field with an information icon.
- Organization/Department*:** Two side-by-side panels.
 - Organization:** Includes checkboxes for 'Any', 'Comodo SE', 'Device Org', 'Dithers Organization' (checked), and 'SSL Support Team'.
 - Department:** Includes checkboxes for 'Any' and 'None' (checked).
- Days in advance to notify*:** Text input field with an information icon.
- Frequency:** Radio buttons for 'Once' (selected) and 'Daily'.
- Notify MRAO Admin(s)*:** Checkbox with an information icon.
- Notify Device Certificate RAO Admin(s)*:** Checkbox with an information icon.
- Notify Device Certificate DRAO Admin(s)*:** Checkbox with an information icon.
- Subscribers (optional, comma separated):** Text input field.

Buttons for 'OK' and 'Cancel' are located at the bottom of the dialog.

6.5.2.18.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|---|
| Description (<i>required</i>) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (<i>required</i>) | Checkboxes | Select Organization(s)/Departments(s) whose members should receive notifications. Selecting 'Any' (checked by default) enables notifications for members of all Organizations. To choose recipient Organizations, select the check-box on the left. |
| Days in advance to notify (<i>required</i>) | Text Field | Set the number of days before expiry that the notification should be sent. Administrators can also specify whether the notification should be sent once or daily till the expiration date. |
| Notify Requester (<i>required</i>) | Checkbox | Add the certificate requester to the list of recipients. |

| Form Element | Type | Description |
|---|------------|---|
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Send the notification to the MRAO Admin(s). |
| Notify Device Certificate RAO Admin(s) <i>(required)</i> | Checkbox | Send the notification to the RAO Device Cert Admin(s) of the Organization(s). |
| Notify Device Certificate DRAO Admin(s) <i>(required)</i> | Checkbox | Send the notification to the DRAO Device Cert Admin(s) of the Departments(s). |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.19 'Device Certificate Revoked' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon revocation of a device certificate.

Create Notification ✕

**-required fields*

Notification Type: Device Certificate Revoked

Description*: i

Organization/Department* **Organization**

▼ Any

- Comodo SE
- Device Org
- Dithers Organization
- SSL Support Team

Department

▼ Any

- Dithers Organization
- None

Notify MRAO Admin(s)* i

Notify Device Certificate RAO Admin(s)* i

Notify Device Certificate DRAO Admin(s)* i

Subscribers *(optional, comma separated)*

6.5.2.19.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|---|
| Description (<i>required</i>) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (<i>required</i>) | Checkboxes | Select Organization(s)/Departments(s) whose members should receive notifications. Selecting 'Any' (checked by default) enables notifications for members of all Organizations. To choose recipient Organizations, select the check-box on the left. |
| For Certificates Revoked by: (<i>required</i>) | Checkbox | Select a person (administrator or user) after whose revoke action, the notification will be sent. |
| Notify Requester (<i>required</i>) | Checkbox | Add the certificate requester to the list of recipients. |
| Notify MRAO Admin(s) (<i>required</i>) | Checkbox | Send the notification to the MRAO Admin(s). |
| Notify Device Certificate RAO Admin(s) (<i>required</i>) | Checkbox | Send the notification to the RAO Device Cert Admin(s) of the Organization(s). |
| Notify Device Certificate DRAO Admin(s) (<i>required</i>) | Checkbox | Send the notification to the DRAO Device Cert Admin(s) of the Departments(s). |
| Subscribers (<i>optional</i>) | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.20 'Device Certificate Awaiting Approval' Create Notification form

Enables the Administrator to set a notification about a request of a device certificate to selected personnel. The device certificate request must be approved by the MRAO/RAO Administrator. Before the request is approved, its state is 'Awaiting Approval'.

6.5.2.20.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|---|
| Description (<i>required</i>) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (<i>required</i>) | Checkboxes | Select Organization(s)/Departments(s) whose members should receive notifications. Selecting 'Any' (checked by default) enables notifications for members of all Organizations. To choose recipient Organizations, select the check-box on the left. |
| Notify MRAO Admin(s) (<i>required</i>) | Checkbox | Send the notification to the MRAO Admin(s). |
| Notify Device Certificate RAO Admin(s) (<i>required</i>) | Checkbox | Send the notification to the RAO Device Cert Admin(s) of the Organization(s). |

| | | |
|---|------------|---|
| Notify Device Certificate DRAO Admin(s) (<i>required</i>) | Checkbox | Send the notification to the DRAO Device Cert Admin(s) of the Departments(s). |
| Subscribers (<i>optional</i>) | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.21 'Client Admin Creation' Create Notification Form

Enables the Administrator to create a notification to selected personnel upon creation of new MRAO, RAO or DRAO Administrators.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Notify Client Certificate RAO Admin(s)* ⓘ

Notify Client Certificate DRAO Admin(s)* ⓘ

Notify Code Signing RAO Admin(s)* ⓘ

Notify Code Signing DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.21.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the Admin status. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments. |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO SSL Admin(s) of the selected Departments. |
| Notify Client Certificate RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO S/MIME Admin(s) of the selected Organization(s)/Departments. |
| Notify Client Certificate DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO S/MIME Admin(s) of the selected Departments. |
| Notify Code Signing RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments. |
| Notify Code Signing DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO Code Signing Admin(s) of the selected Departments. |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.22 'Domain Awaiting Approval' Create Notification Form

Enables the administrator to set a notification about a request of a domain delegation to an Organization/Department. The Domain delegation request must be approved by the MRAO/RAO Administrator. Before the request is approved, its state is 'Awaiting Approval'.

Create Notification ✕

***-required fields**

Notification Type:

Description*:

Organization/Department*

| Organization | Department |
|--|--|
| <input type="checkbox"/> Any | <input type="checkbox"/> Any |
| <input type="checkbox"/> AAA Organization | <input checked="" type="checkbox"/> Dithers Construction Company |
| <input type="checkbox"/> ABCD Company | <input checked="" type="checkbox"/> None |
| <input type="checkbox"/> Best Organization | <input type="checkbox"/> Purchases Department |
| <input checked="" type="checkbox"/> Dithers Construction Company | <input type="checkbox"/> Stores Department |
| <input type="checkbox"/> Elegant | |

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Notify Client Certificate RAO Admin(s)* ⓘ

Notify Client Certificate DRAO Admin(s)* ⓘ

Notify Code Signing RAO Admin(s)* ⓘ

Notify Code Signing DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.22.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the delegation of a created domain to an Organization/Department. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments. |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO SSL Admin(s) of the selected Departments. |
| Notify Client Certificate RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO S/MIME Admin(s) of the selected Organization(s)/Departments. |
| Notify Client Certificate DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO S/MIME Admin(s) of the selected Departments. |
| Notify Code Signing RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments. |
| Notify Code Signing DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO Code Signing Admin(s) of the selected Departments. |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

Important Note: The 'Domain Awaiting Approval' notification will be sent to MRAO only after the requested domain requested by a DRAO is approved by RAO.

6.5.2.23 'Domain Approved' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel upon Approval of creation and delegation of a domain to an Organization/Department.

Important Note: The 'Domain Approved' notification will be sent only after the request has been approved by two MRAOs with appropriate privileges. If 'Allow domain validation without Dual Approval' was selected during the MRAO creation process, then requests can be approved by just a single MRAO'

Create Notification ✕

***-required fields**

Notification Type:

Description*:

Organization/Department*

| Organization | Department |
|--|--|
| <input type="checkbox"/> Any | <input type="checkbox"/> Any |
| <input type="checkbox"/> AAA Organization | <input checked="" type="checkbox"/> Dithers Construction Company |
| <input type="checkbox"/> ABCD Company | <input checked="" type="checkbox"/> None |
| <input type="checkbox"/> Best Organization | <input type="checkbox"/> Purchases Department |
| <input checked="" type="checkbox"/> Dithers Construction Company | <input type="checkbox"/> Stores Department |
| <input type="checkbox"/> Elegant | |

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Notify Client Certificate RAO Admin(s)* ⓘ

Notify Client Certificate DRAO Admin(s)* ⓘ

Notify Code Signing RAO Admin(s)* ⓘ

Notify Code Signing DRAO Admin(s)* ⓘ

Subscribers
(optional, comma separated)

6.5.2.23.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the delegation of a created domain to an Organization/Department. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments. |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO SSL Admin(s) of the selected Departments. |
| Notify Client Certificate RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO S/MIME Admin(s) of the selected Organization(s)/Departments. |
| Notify Client Certificate DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO S/MIME Admin(s) of the selected Departments. |
| Notify Code Signing RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments. |
| Notify Code Signing DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO Code Signing Admin(s) of the selected Departments. |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.24 'DCV Expiration' Create Notification Form

Enables administrator to set notification about expiration of domain control validation if it is due to expire.

Create Notification
✕

*-required fields

Notification Type:

Description*:

Organization/Department*: **Organization**

Any
 AAA Organization
 ABCD Company
 Best Organization
 Dithers Construction Company
 Elegant

Department

Any
 Dithers Construction Company
 None
 Purchases Department
 Stores Department

Days in advance to notify*:

Frequency: Once Daily

Notify Owner*:

Notify Requester*:

Notify MRAO Admin(s)*:

Notify SSL RAO Admin(s)*:

Notify SSL DRAO Admin(s)*:

Subscribers (optional, comma separated):

6.5.2.24.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Days in advance to notify <i>(required)</i> | Text Field | Enables the administrator to set number of days the end-user will be informed about expiration of the certificate before the event. Administrator can also specify whether the notification has to be sent to |

| | | |
|--|------------|--|
| | | the member(s) only once or daily till the expiration date by selecting the respective radio button. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the delegation of a created domain to an Organization/Department. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments. |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO SSL Admin(s) of the selected Departments. |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.25 'DCV Validated' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel on successful completion of Domain Control Validation (DCV).

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

- AAA Organization
- ABCD Company
- Best Organization
- Dithers Construction Company
- Elegant

Department

Any

- Dithers Construction Company
 - None
 - Purchases Department
 - Stores Department

Notify Owner*

Notify Requester*

Notify MRAO Admin(s)*

Notify SSL RAO Admin(s)*

Notify SSL DRAO Admin(s)*

Subscribers
(optional, comma separated)

6.5.2.25.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who |

| | | |
|--|------------|--|
| | | requested the delegation of a created domain to an Organization/Department. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments. |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO SSL Admin(s) of the selected Departments. |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.26 'DCV Needed-New Domain' Create Notification Form

Enables the Administrator to create a notification that will be sent to those personnel selected when a new domain is created and awaiting validation.

Create Notification
✕

*-required fields

Notification Type

Description*

Organization/Department*

Organization

Any

Any current or future organization

Department

Any

Any current or future department

Notify Owner* ⓘ

Notify Requester* ⓘ

Notify MRAO Admin(s)* ⓘ

Notify SSL RAO Admin(s)* ⓘ

Notify SSL DRAO Admin(s)* ⓘ

Subscribers *(optional, comma separated)*

6.5.2.26.1 Table of Parameters

| Form Element | Type | Description |
|--|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify Owner <i>(required)</i> | Checkbox | Enables the administrator to send the notification for the Owner of the certificate. |
| Notify Requester <i>(required)</i> | Checkbox | Enables the administrator to send the notification to the person who requested the delegation of a created domain to an Organization/Department. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify SSL RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO SSL Admin(s) of the selected Organization(s)/Departments. |
| Notify SSL DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO SSL Admin(s) of the selected Departments. |
| Subscribers <i>(optional)</i> | Text Field | Administrator can specify email address(es) of other people to whom the notifications are to be sent. |

6.5.2.27 'Code Sign Request Created' Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel when a 'Code Signing on Demand' request has been created by a developer for a software.

Create Notification
✕

*-required fields

Notification Type

Description* i

Organization/Department*

Organization Any

DCV_check_org
 Deployment
 dithercons.com
 Dithers Construction Company
 forSmime
 Mcan Co.
 ooooo
 org1

Department Any

Mcan Co.

- None
- Development-Mcan Co.
- IT-Mcan Co.

Notify MRAO Admin(s)* i

Notify Code Signing RAO Admin(s)* i

Notify Code Signing DRAO Admin(s)* i

6.5.2.27.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description <i>(required)</i> | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department <i>(required)</i> | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify MRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify Code Signing RAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the RAO Code Signing Admin(s) of the selected Organization(s)/Departments. |
| Notify Code Signing DRAO Admin(s) <i>(required)</i> | Checkbox | Enables the administrator to send the notification all the DRAO Code Signing Admin(s) of the selected Departments. |

6.5.2.28 Code Signing CSoD Revoked Create Notification Form

Enables the Administrator to create a notification that will be sent to selected personnel when a 'Code Signing on Demand' request has been revoked by an administrator.

6.5.2.28.1 Table of Parameters

| Form Element | Type | Description |
|---|------------|--|
| Description (<i>required</i>) | Text Field | Administrator should enter text of the notification in this field. |
| Organization/Department (<i>required</i>) | Checkboxes | Administrator should select Organization(s)/Departments(s), to the members of which this notification has to be sent. Selecting 'Any' (checked by default) enables the notification to the members of all the Organizations. If the notification is to be sent only to members of certain Organizations/Departments, then select the checkbox with the drop-down arrow. The tree structure of Organizations and Departments will be displayed. Choose the Organizations/Departments from the tree structure. |
| Notify MRAO Admin(s) (<i>required</i>) | Checkbox | Enables the administrator to send the notification all the MRAO Admin(s). |
| Notify Code Signing RAO | Checkbox | Enables the administrator to send the notification all the RAO Code |

| | | |
|---|----------|--|
| Admin(s) (<i>required</i>) | | Signing Admin(s) of the selected Organization(s)/Departments. |
| Notify Code Signing DRAO Admin(s) (<i>required</i>) | Checkbox | Enables the administrator to send the notification all the DRAO Code Signing Admin(s) of the selected Departments. |

6.6 Encryption and Key Escrow

6.6.1 Introduction and Basic Concepts

Comodo Certificate Manager can store the individual private keys of end-user's client certificates so that they can be recovered at a later date by appropriately privileged Administrators. Due to the highly sensitive and confidential nature of this feature, all end-user client certificates are stored in encrypted form so that they cannot be easily stolen or compromised.

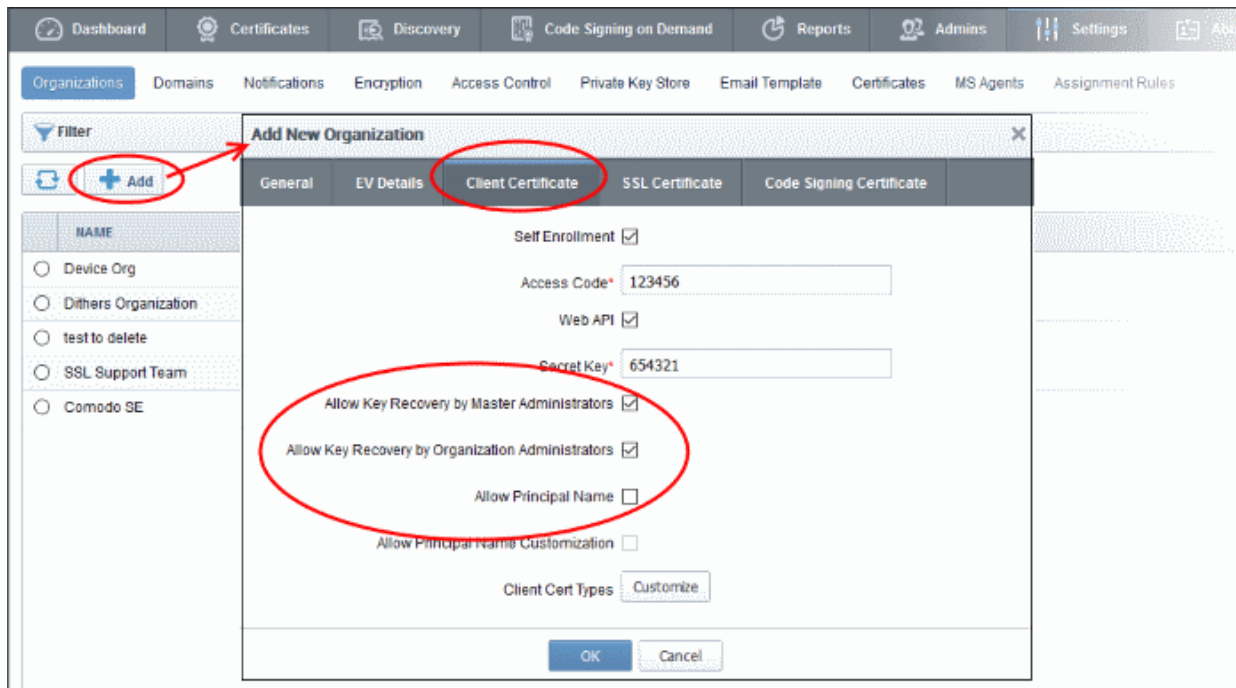
- It is possible to specify that keys in escrow be independently retrieved by any of the three levels of Administrator - MRAO and/or RAO S/MIME and/or DRAO S/MIME Administrators.
- Therefore, it is possible for CCM to store up to 2 encrypted versions of the private keys of client certificates of an Organization and up to 3 versions for a Department. Each version will be separately encrypted by three different 'master' public keys - the MRAO master key, the Organization master key and the Departmental master key.
- These master public keys are stored by CCM. The corresponding master private keys are not stored in CCM (the master 'private' key is required for decryption/retrieval). These keys must be saved in a secure location by the Administrator that is creating the Organization/Department.
- There is one master key pair per Organizational tier and these are generated (if required) during the creation of that Organizational tier (e.g. during Organization creation or during Department creation). Therefore, one master key pair will be used by all RAO S/MIME Administrators of a particular Organization - the Organization Master Key. Similarly, if key retrieval is required at the Departmental level then one pair of master keys will be used by all DRAO S/MIME Admins of a particular Department - the Department Master Key.
- IF 'Allow key recovery by MRAO/RAO/DRAO' is enabled at the point of Organization/Department creation THEN these master key pairs **must be initialized** prior to issuing client certificates. It is not possible to issue client certificates UNTIL the master private keys have been initialized. See '**Master Keys Required Prior to Client Cert Issuance**' for more details.
- Retrieving the private key of a user's client certificate from escrow will cause the revocation of that certificate. This is true if any one of the aforementioned administrative types chooses to retrieve from escrow. A private key can be retrieved from escrow by clicking the 'Download' button next to the chosen certificate. See **Recovering a User's Private Key from Escrow** for more details.

6.6.2 Setting up Key Escrow for an Organization

- Key recovery options are chosen during the creation of an Organization. Once chosen, these settings cannot be reversed.
- This section will deal purely with the key recovery elements of Organization creation. The key recovery settings are just one part of the overall Organization creation process. Administrators are therefore advised to treat this section as an information gathering exercise on key escrow prior to creating a new Organization. For a full outline of all steps and options involved in the creation of an Organization, please see **Creating a New Organization**.
- Only an MRAO Administrator is able to specify key recovery settings for an Organization. This is because only an MRAO is able to create an Organization.

To set key recovery options:

- Select 'Settings' > 'Organizations' > 'Add'. This will open the 'Add New Organization' dialog box.
- Click the 'Client Cert' tab to view and configure key recovery options:



| | | |
|--|---------------------------------------|---|
| Allow Key Recovery by Master Administrators | Checkbox Default state - checked | If selected, the MRAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the MRAO has initialized their master key pair in the Encryption tab. |
| Allow Key Recovery by Organization Administrators | Checkbox Default state - checked | If selected, the RAO will have the ability to recover the private keys of client certificates issued by this Organization. At the point of creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Organization will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the Encryption tab. |
| Allow Principal Name | Checkbox Default state - unchecked | Checking this box enables Principal Name support to the Organization. If enabled, the client certificates issued to the end-users of the Organization will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Names (SAN) field. If included, the Principal Name will be the primary email address of the end-user to whom the certificate is issued. But this can be customized at a later time by editing the end-user if Principal Name Customization is enabled for the Organization/Department. |
| Allow Principal Name Customization | Checkbox Default state - unchecked | Checking this box enables customization of the Principal Names by the Administrator. |
| The other settings in the 'Client Cert' tab are explained here . | | |

- Fill out the 'General Information' tab (and optionally the 'SSL' / 'Code Signing Certificate' tabs if those cert

types are required). See [Creating a New Organization](#) for full details concerning the creation of a new Organization.

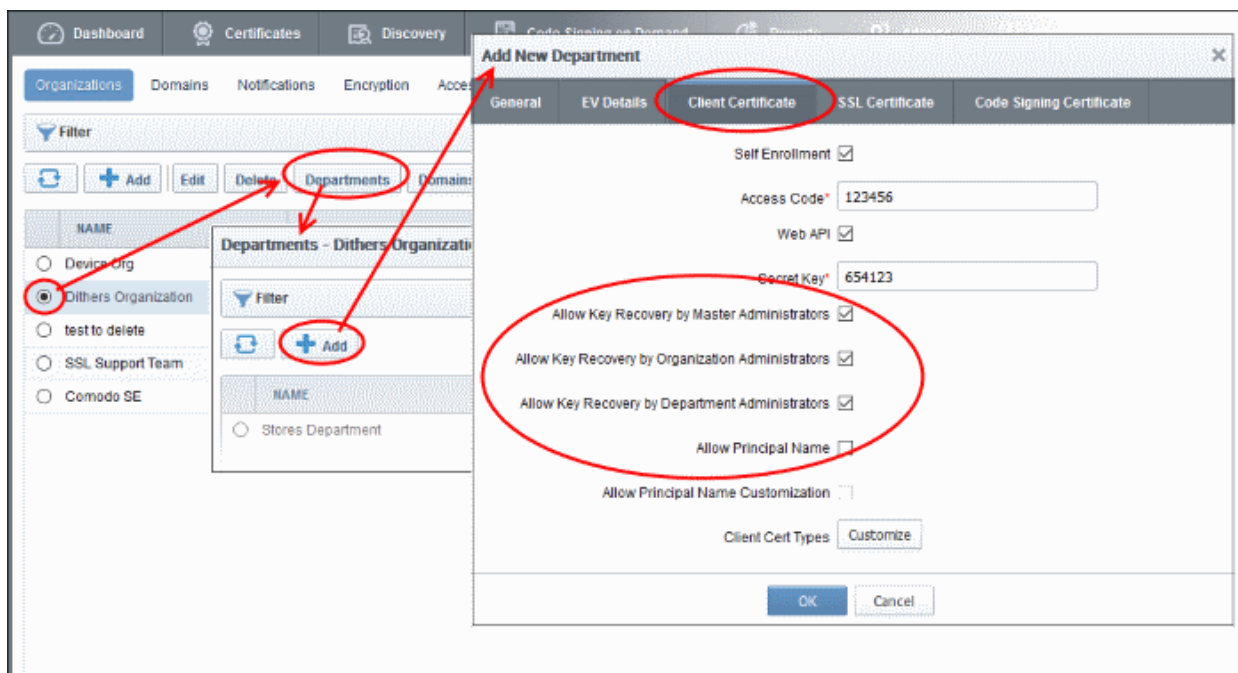
- Once you are satisfied with all settings, click 'OK' to add the Organization

6.6.3 Setting up Key Escrow for a Department

- Key recovery options are chosen during the creation of a Department. Once chosen, these settings cannot be reversed.
- This section will deal purely with the key recovery elements of Department creation. The key recovery settings are just one part of the overall Departmental creation process. Administrators are therefore advised to treat this section as an information gathering exercise on key escrow prior to creating a new Department. For a full outline of all steps and options involved in the creation a Department, please see [Managing the Departments of an Organization](#)
- Only MRAO Administrators and RAO S/MIME Administrators are able to specify key recovery settings for an Organization. This is because only those types of Administrator are able to create a Department.

To set key recovery options:

- Select 'Settings' > 'Organizations'.
- Select the 'Organization' and click 'Departments' from the top to open the 'Departments' interface
- Click 'Add' from the 'Departments' interface to open 'Add New Department' interface
- Click the 'Client Cert' tab to view and configure key recovery options:



| | | |
|---|---|--|
| Allow Key Recovery by Master Administrators | Checkbox Default state - checked if pre-enabled by MRAO* | If selected, the MRAO will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted with the MRAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificate UNTIL the MRAO has initialized their master key pair in the Encryption tab |
| Allow Key Recovery by Organization Administrators | Checkbox | If selected, the RAO will have the ability to recover the private keys of client certificates issued by this Department. At the point of |

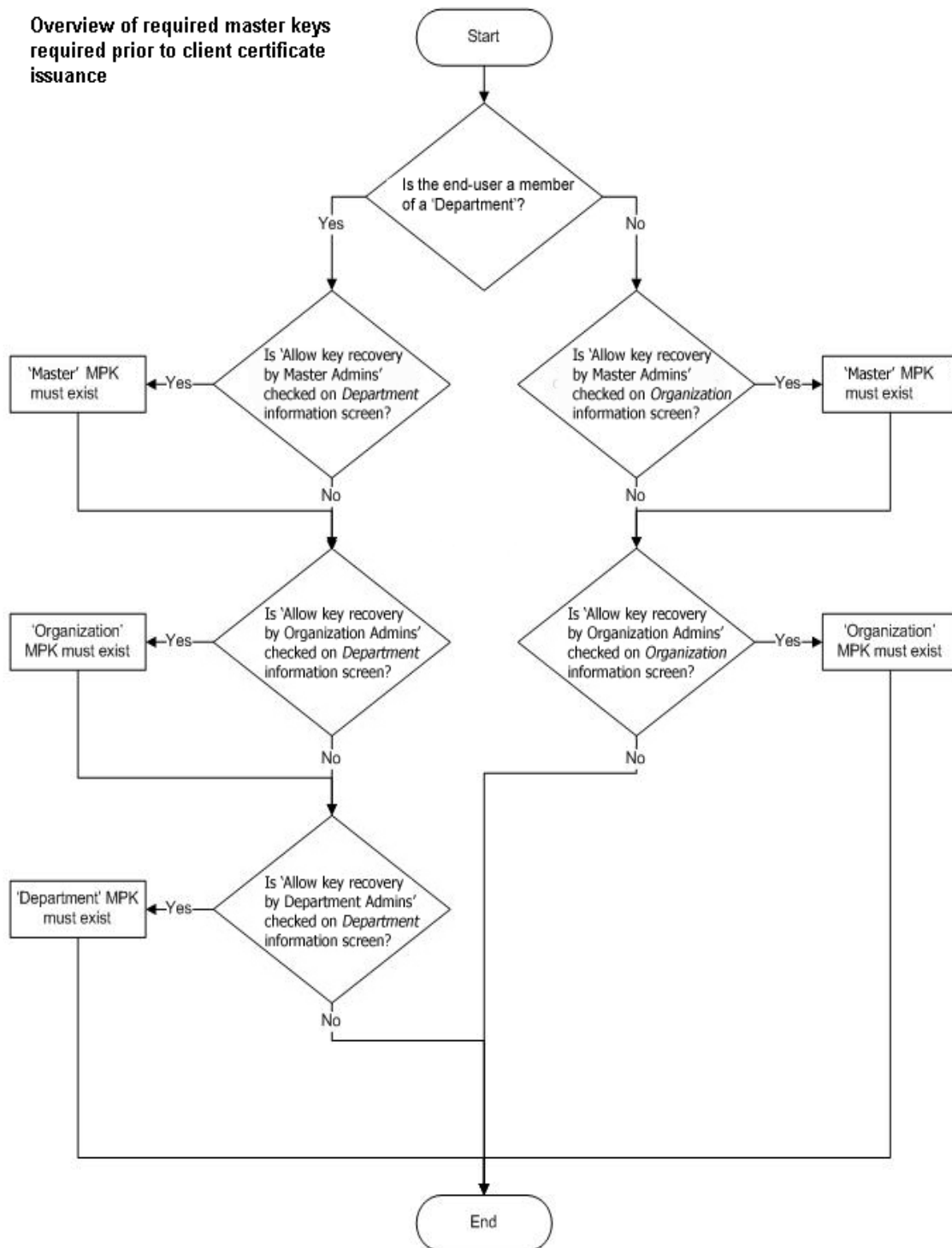
| | | |
|---|---|---|
| | Default state - checked if pre-enabled by MRAO* | creation, each client certificate will be encrypted with the RAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificate UNTIL the RAO has initialized their master key pair in the Encryption tab. |
| Allow Key Recovery by Department Administrators | Checkbox Default state - checked if pre-enabled by MRAO* | If selected, the DRAO S/MIME Administrator will have the ability to recover the private keys of client certificates issued by this Department. At the point of creation, each client certificate will be encrypted with the DRAOs master public key before being placed into escrow. If this box is selected then the Department will not be able to issue client certificates UNTIL the DRAO has initialized their master key pair in the Encryption tab. |
| Allow Principal Name | Checkbox Default state - unchecked if pre-enabled by MRAO* | Checking this box enables Principal Name support to the Department. If enabled, the client certificates issued to the end-users of the Department will include an additional name - Principal Name, in addition to the RFC822 name in the Subject Alternative Names (SAN) field. If included, the Principal Name will be the primary email address of the end-user to whom the certificate is issued. But this can be customized at a later time by editing the end-user if Principal Name Customization is enabled for the Organization/Department. |
| Allow Principal Name Customization | Checkbox Default state - unchecked if pre-enabled by MRAO* | Checking this box enables customization of the Principal Names by the Administrator. |
| <p>* The checkboxes will only be active IF the MRAO has enabled the appropriate key recovery options when configuring client certificate options for the Organization.</p> <p>The other settings in the 'Client Cert' tab are explained here.</p> | | |

- Fill out the 'General Information' tab (and optionally the 'SSL' / 'Code Signing Certificate' tabs if those cert types are required). See **Creating a New Organization** for full details concerning the creation of a new Organization.
- Once you are satisfied with all settings, click 'OK' to add the Department

6.6.4 Master Keys Required Prior to Client Cert Issuance

The diagram below is an overview of the master keys necessary per recovery requirements for the successful issuance of client certificates:

Overview of required master keys required prior to client certificate issuance



Notes:

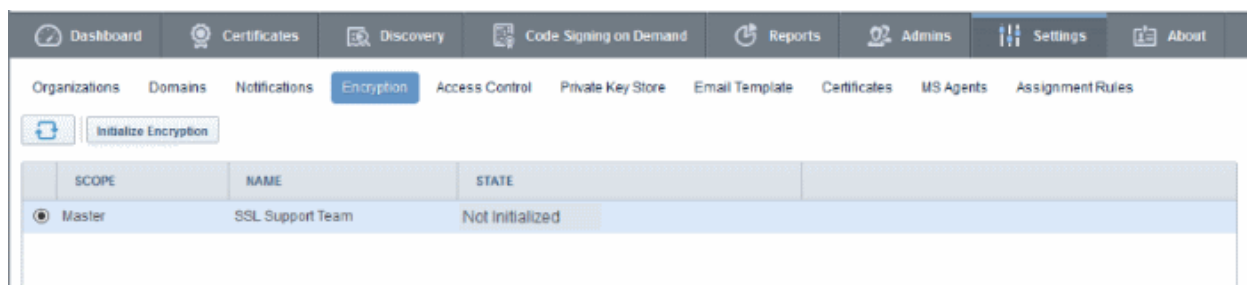
- Administrators can find out whether recovery is checked for an Organization by clicking 'Settings' > 'Organizations', clicking the 'Edit' button of the Organization in question then selecting the 'Client Cert' tab.
- MRAO and RAO S/MIME Administrators can find whether recovery is checked for a Department by clicking 'Settings' > 'Organizations', then clicking the 'Departments' button of the Organization in question. Next, select the Department in question and click 'Edit' button, then select the 'Client Cert' tab.
- 'MPK must exist' means that the key must have been initialized. If the key has not been initialized then

the Organization or Department in question will not be able to issue client certificates. If key escrow is required through all tiers (MRAO + Organization + Department) then this means that 3 master private keys will need to be initialized. To check initialization status, the currently logged in administrator should click the 'Encryption' tab

6.6.5 Encryption

This area allows administrators to encrypt the private keys of users' client certificates. If key recovery was specified during the creation of an Organization or Department, then this step is essential. No client certificates can be issued until the master key pairs have been initialized.

Note: This area is visible and accessible by the MRAO and by RAO/DRAO S/MIME Admins if key recovery has been enabled for their specific Organization/Department.

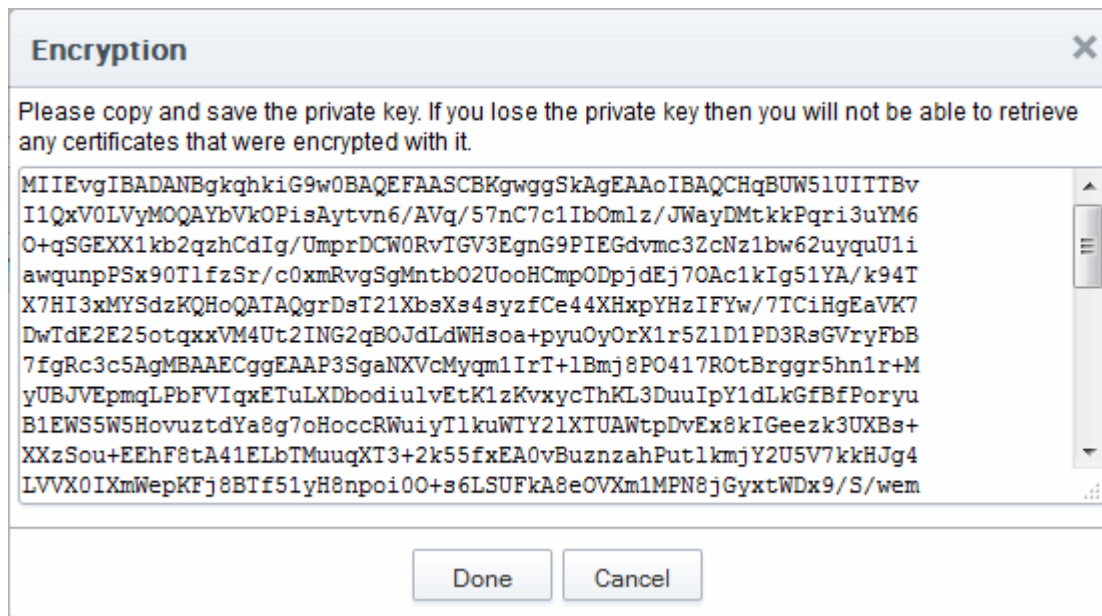


6.6.5.1 Summary of Fields and Controls

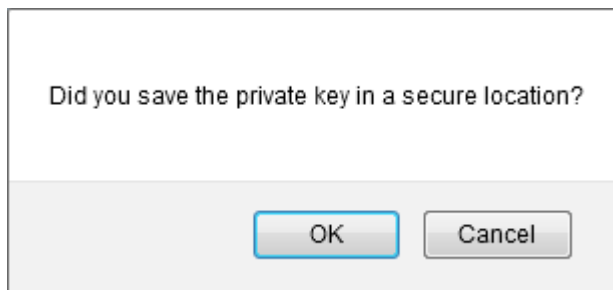
| Column Display | | Description |
|---|-----------------------|---|
| Scope | | The Hierarchy level of the Organization/Department. It can be the Master, Organization or Department. |
| Name | | The name of the Organization/Department. |
| State | | Indicates the status of private key encryption. |
| Controls | | |
| | Refresh | Reloads the list. |
| Encryption Controls Note: The Encryption control buttons will appear only on selecting the scope and depending on the state of private key encryption | Initialize Encryption | Starts the initial encryption process. This control is available only when the private key encryption has not been done earlier and the status is Not Initialized, for and Organization/Department. |
| | Reencrypt | Starts the re-encryption process of the private keys of the certificates of the end-users of belonging to an Organization/Department. This control is available only if the private keys are already encrypted. |

6.6.6 Encrypting the Private Keys

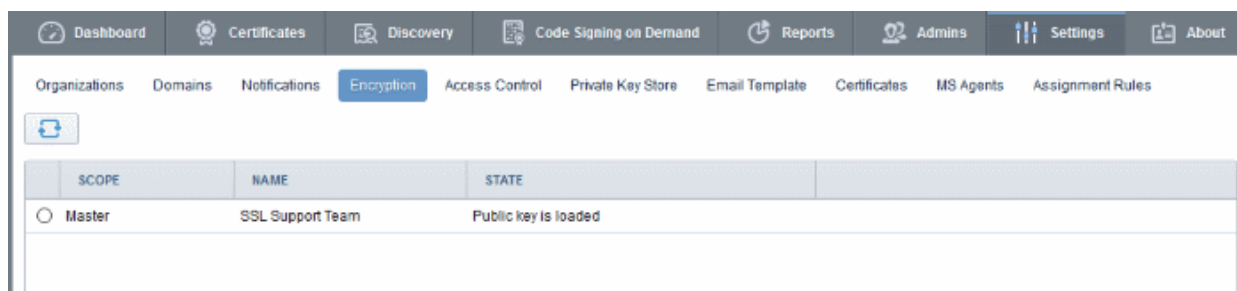
To use this feature the administrator needs to initialize private key encryption by clicking 'Initialize Encryption' button. The process will be started and a master private key will be generated. The administrators need to copy the private key and paste it in a .txt file and store in a secure location.



Note: This 'master' private key is not stored within Comodo Certificate Manager. We advise administrators to save the private key in a secure, password protected, location. It will be required should the administrator wish to either re-encrypt the keys or download a user's client certificate.



On clicking 'Done', the state is changed to 'Public key is loaded'.



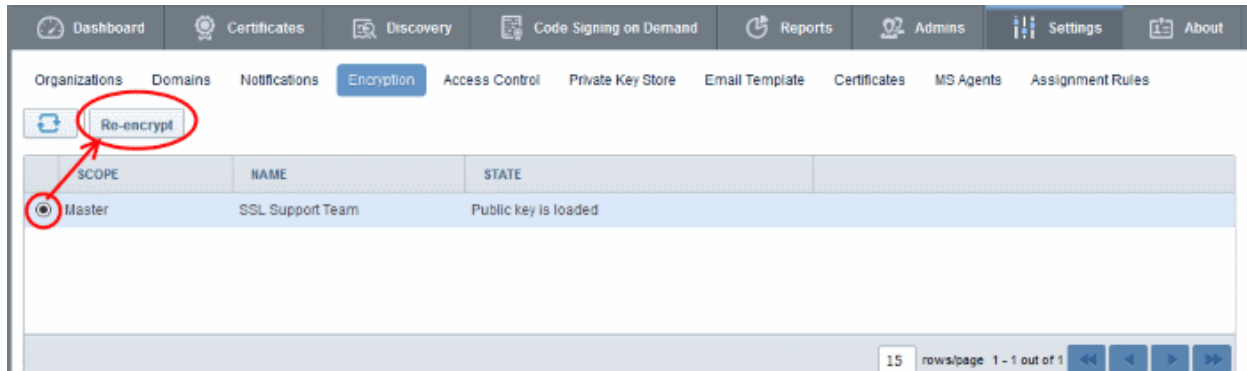
All the private keys of user client certificates are now encrypted using the master public key of the administrator that began this process. Decryption will require the private key that was saved earlier.

6.6.7 Re-encryption

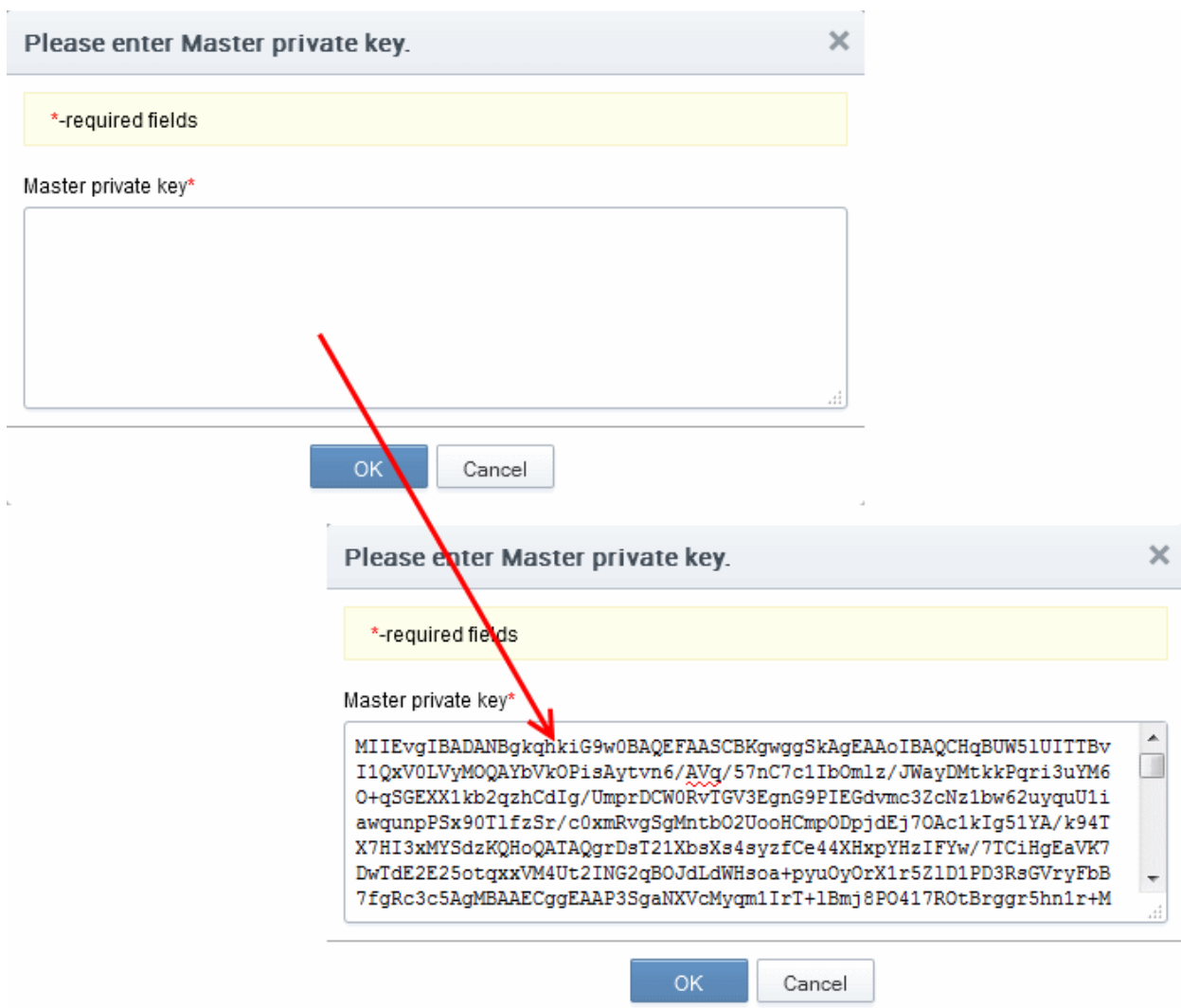
The re-encryption functionality allows MRAO, RAO S/MIME and DRAO S/MIME Administrators to change the master key pair and then automatically re-encrypt existing end-users key pairs with the new master public key. This may be necessary if the original private key becomes compromised or administrative personnel leave the company.

To start the Re-encryption process

- Select the scope and click the 'Reencrypt' button alongside the Organization/Department in the Controls column.

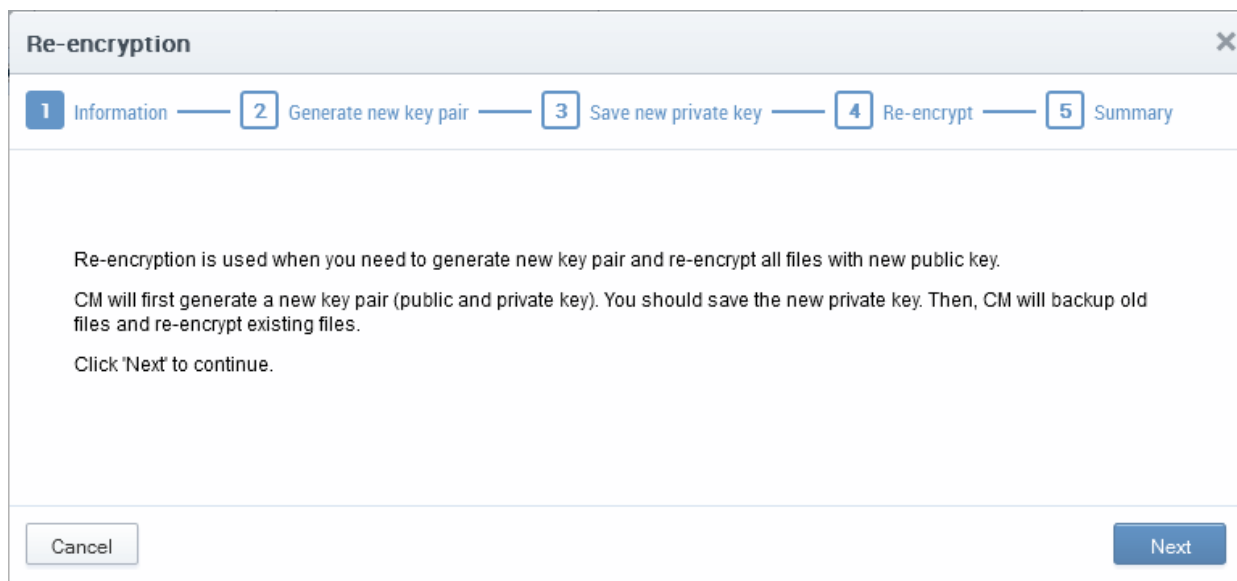


The Administrator will be prompted to paste the existing master private key to start the process:

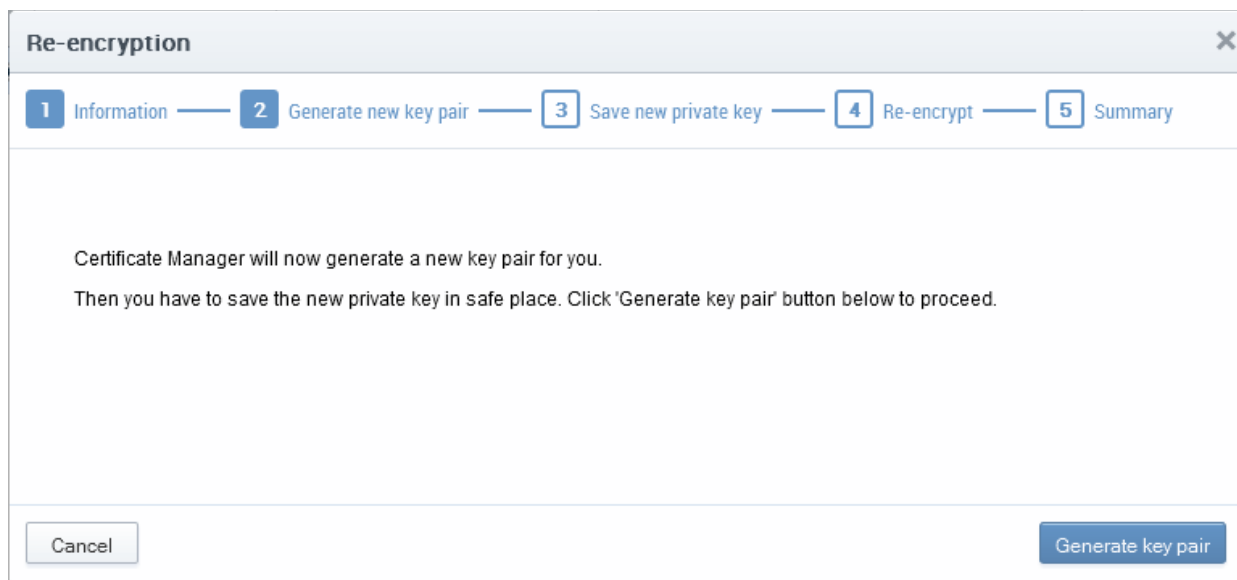


- Paste the Master key and click 'OK'.

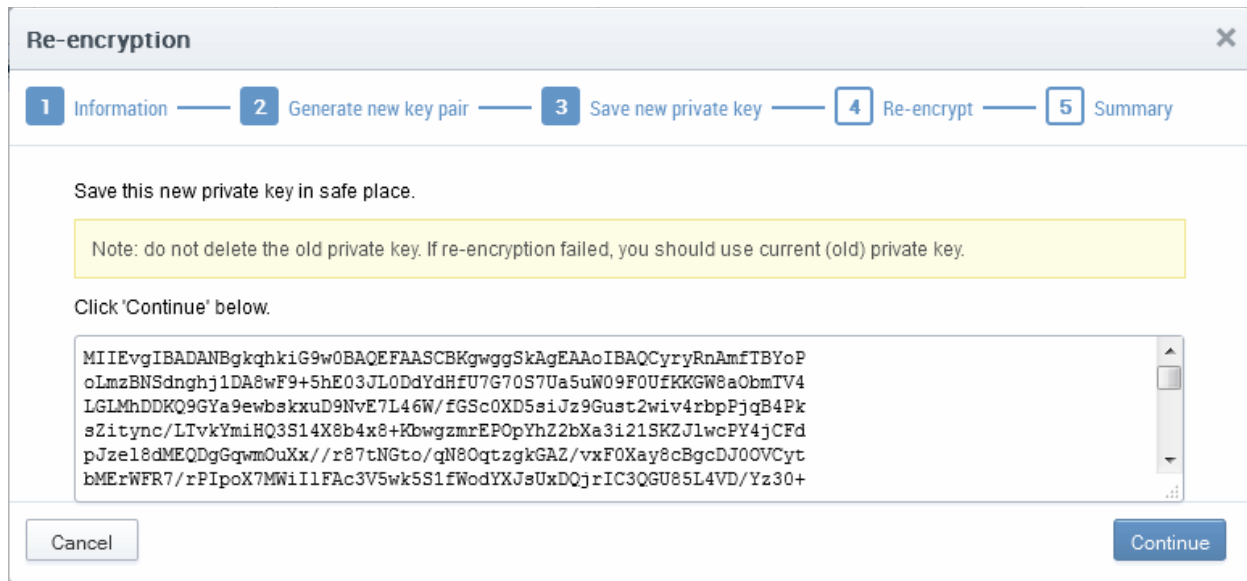
The re-encryption dialog will appear. This will provide a brief summary of the forthcoming process.



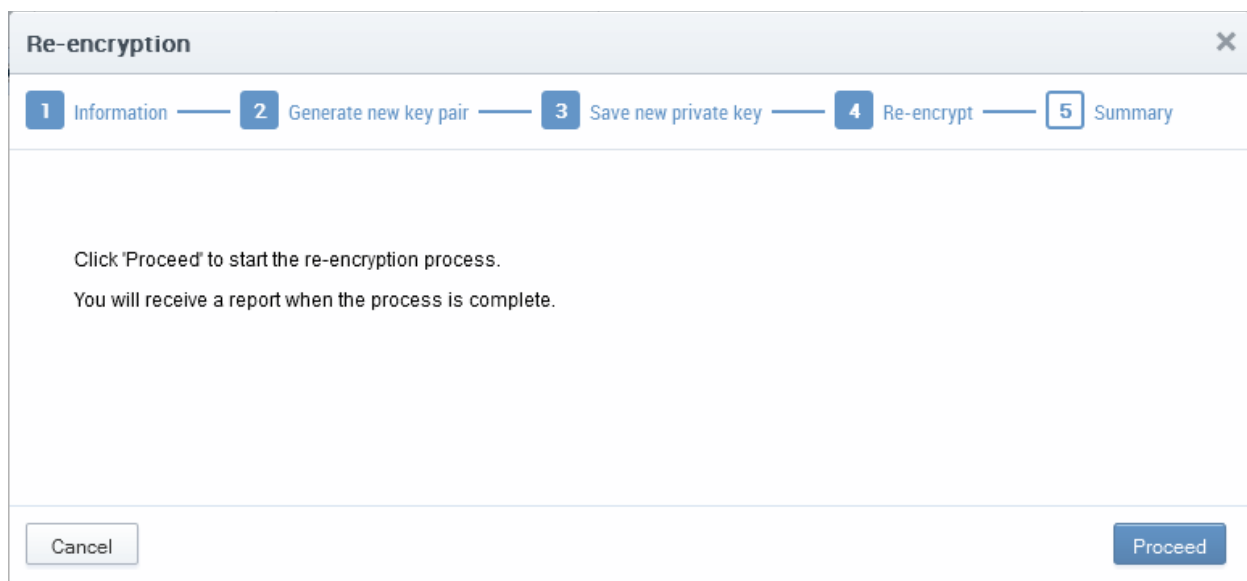
- Click 'Next' to continue:



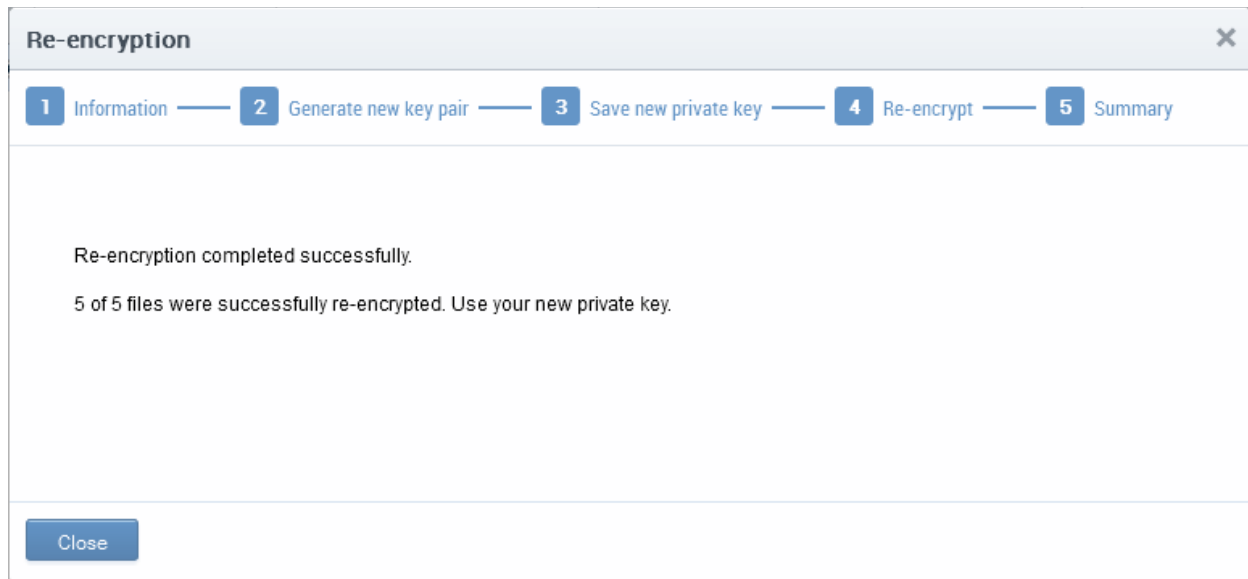
- Click the 'Generate Key Pair' to generate the new keys:



- Copy and paste the private key into a .txt file then save it in a secure, password protected location. Click 'Continue'. The re-encryption of the private keys will be started.



- Click 'Proceed' to begin re-encrypting the private keys of client certificates. Upon successful re-encryption, a summary screen will be displayed.

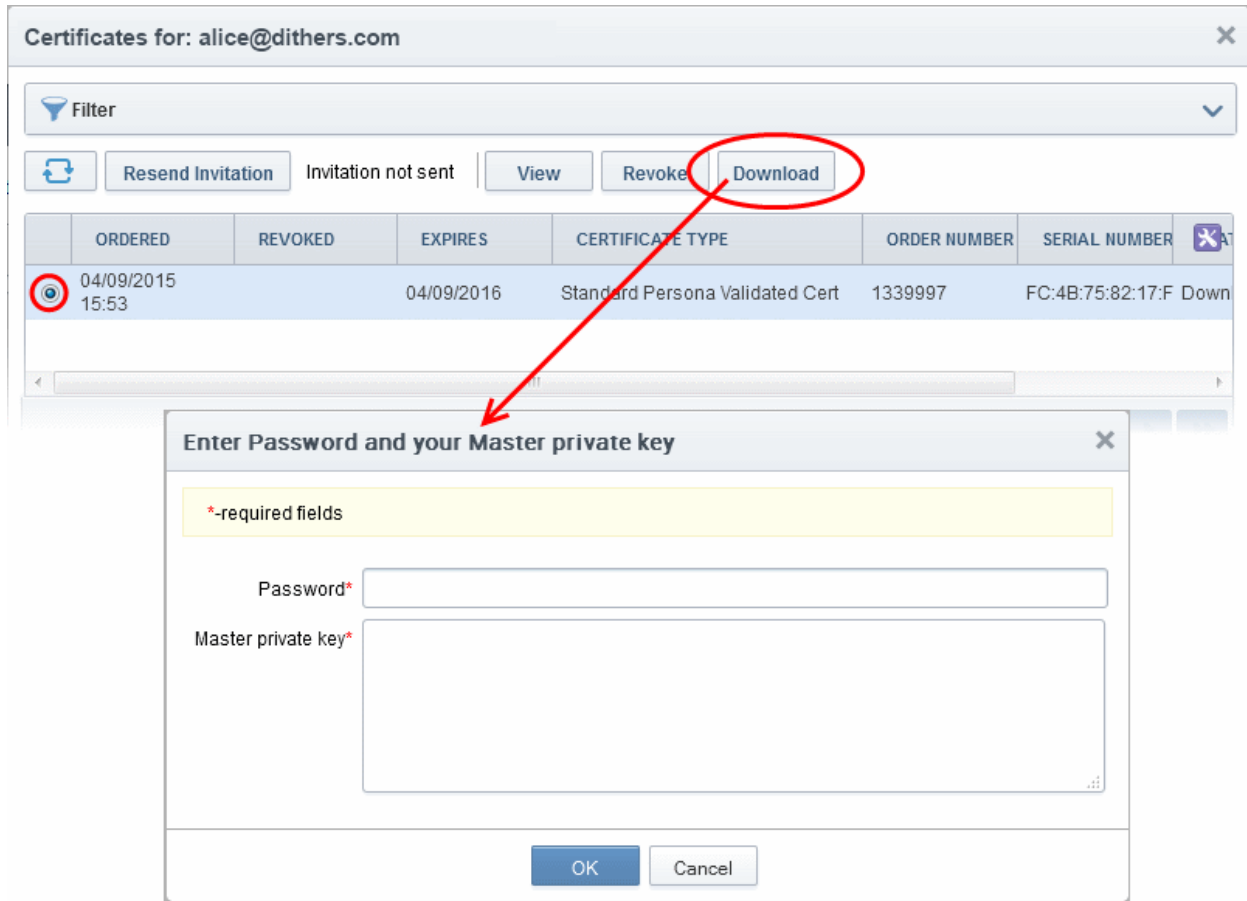


6.6.8 Recovering a User's Private Key from Escrow

The administrator may need to recover a user's private key in order to decrypt data if, for example, the original client certificate belonging to an end-user was lost or if the user left the company. The end-user's private key can be downloaded from the 'Certificates' > 'Client Certificates' interface.

- Open the 'Client Certificates' interface by clicking 'Certificates' > 'Client Certificates'.
- Select the end-user and click the 'Certs' button from the top. The 'Certificates for' interface will open with the list of all the certificates belonging to the end-user in chronological order (newest first).
- Select the certificate and click 'Download'

Note: Administrators should have their master private key ready - it will be required to complete this process.



In order to decrypt this end-user's key pair the administrator must paste the corresponding 'master' private key into the space provided in order to download any end-user's client certificates. The administrator can also set a password to protect access to private key in .p12 file as well.

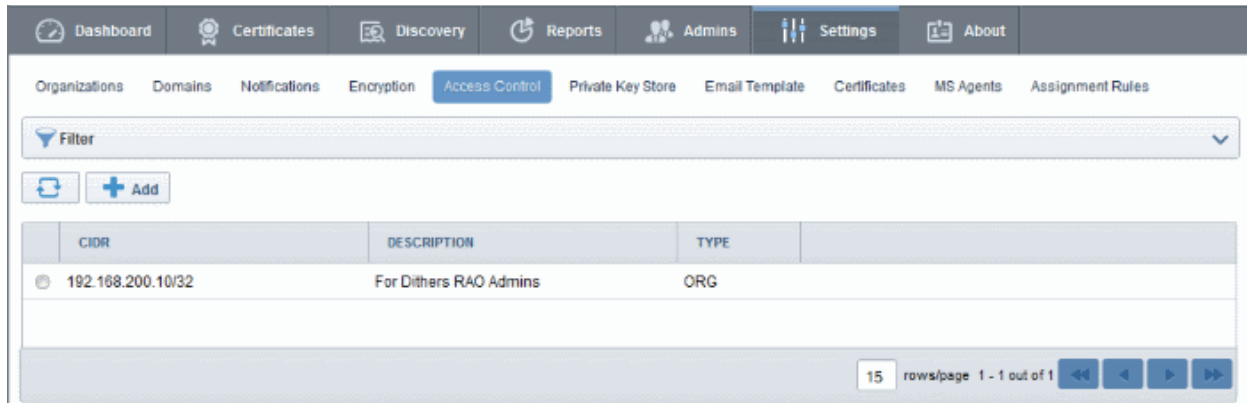
Note: Successfully downloading the private key of a client certificate will revoke that certificate.

6.7 Access Control

6.7.1 Overview

The 'Access Control' area is visible only to the MRAO. The MRAO can configure and limit incoming access to the CCM interface to certain IP addresses and ranges. This is very useful if they want to grant access only to certain IP addresses and so prevent unauthorized or unsecured access to the CCM interface.

- After specifying one or more IP addresses or ranges in CIDR notation, only administrators attempting to login from these specified addresses will be allowed access.
- Any user who is blocked from accessing CCM interface because of restriction will be provided a generic '403 Access Denied' error.
- The Access Restrictions can be applied for all the administrators, or selectively for MRAO administrator only or for RAO/DRAO administrators only.



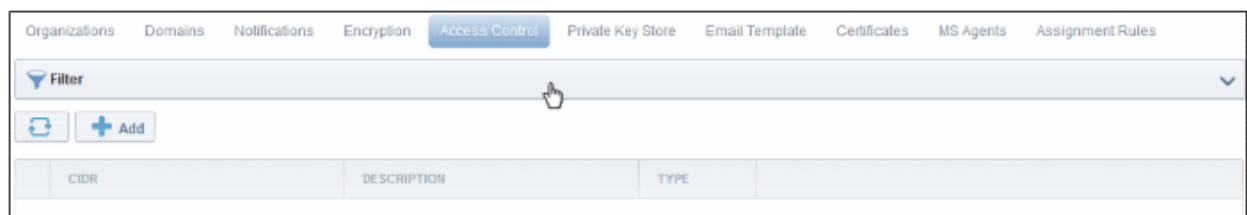
6.7.1.1 Access Control Options - Table of Parameters

| Form Element | | Description |
|----------------------|---------|--|
| CIDR | | Short for Classless Internet DOMAIN Routing. Administrator should specify IP range: it should be IP address followed by network prefix, e.g. 123.456.78.91/16. |
| Description | | Contains a short description for the allowed CIDR. |
| Type | | Displays the administrative role, like All, MRAO and ORG (RAO) for which the CIDR is defined |
| Control Buttons | Add | Allows the administrator to add a new IP Range to allow access. |
| | Refresh | Updates the list of IP ranges. |
| CIDR Control Buttons | Edit | Enables administrator to edit CIDR's details. |
| | Delete | Enables administrator to delete the CIDR. |

Note: The CIDR control buttons are visible only on selecting a CIDR entry

6.7.1.2 Filtering Options

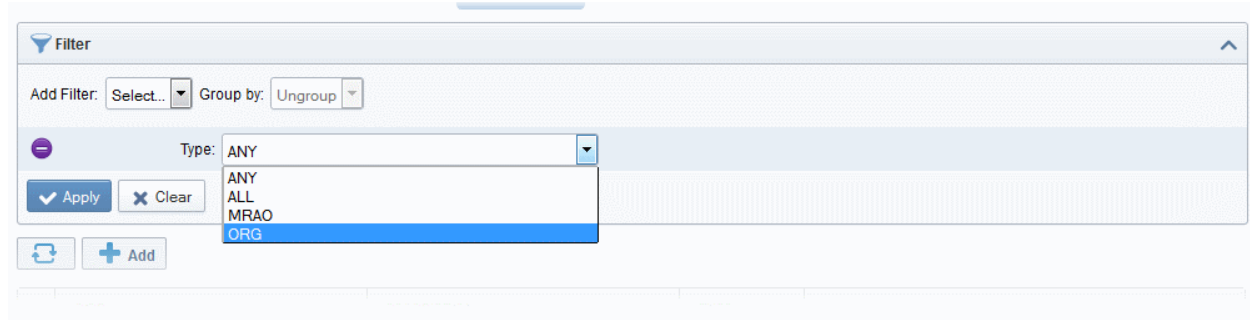
Administrators can search for CIDR entries by using filters:



To apply filters, click anywhere on the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down.

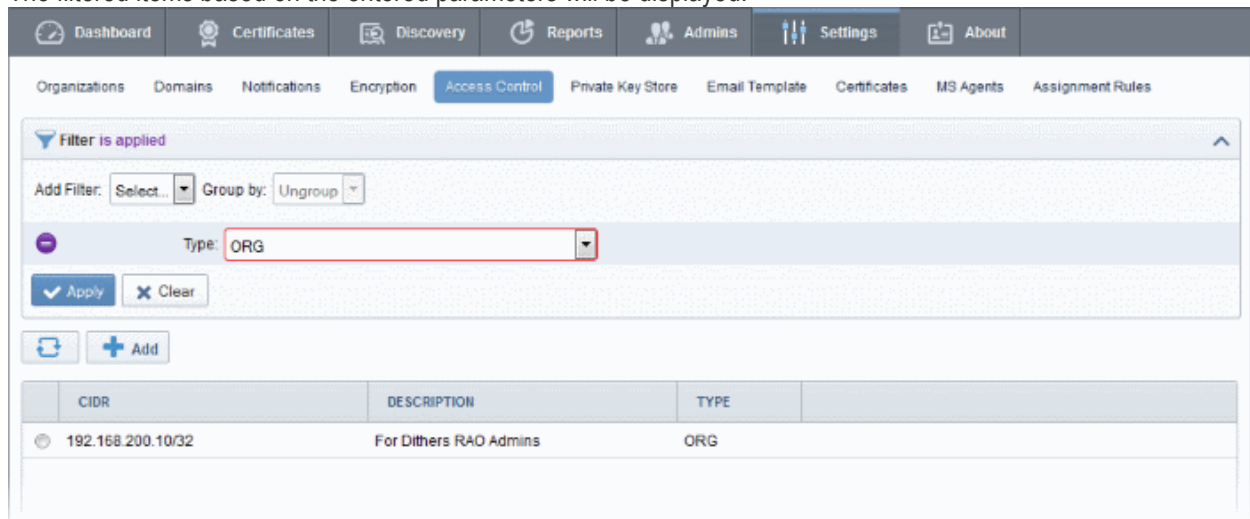
| Filter Options | Description |
|----------------|---|
| Type | <p>Enables the administrator to filter the CIDR details based on administrative roles:</p> <ul style="list-style-type: none"> • All • MRAO • ORG |

For example, if you want to filter the CIDR entries based on a specific type, select 'Type' from the 'Add Filter' drop-down and the type of administrative role from the 'Type' drop-down:



- Click the 'Apply' button.

The filtered items based on the entered parameters will be displayed:

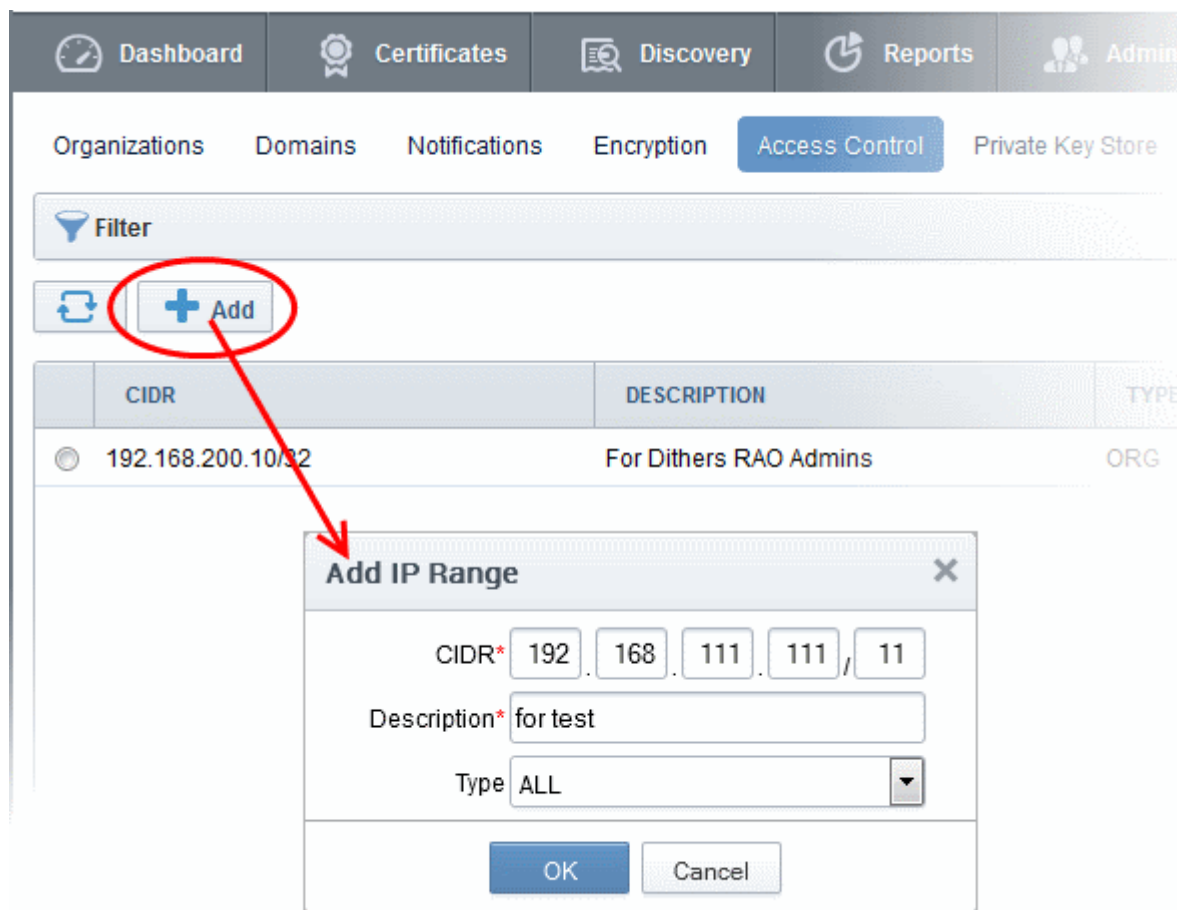


- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Access Control' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.7.2 Adding a New IP Range

New IP range can be added by clicking on 'Add' button at the top left of the interface as shown below:



6.7.2.1 Add IP Range - Table of Parameters

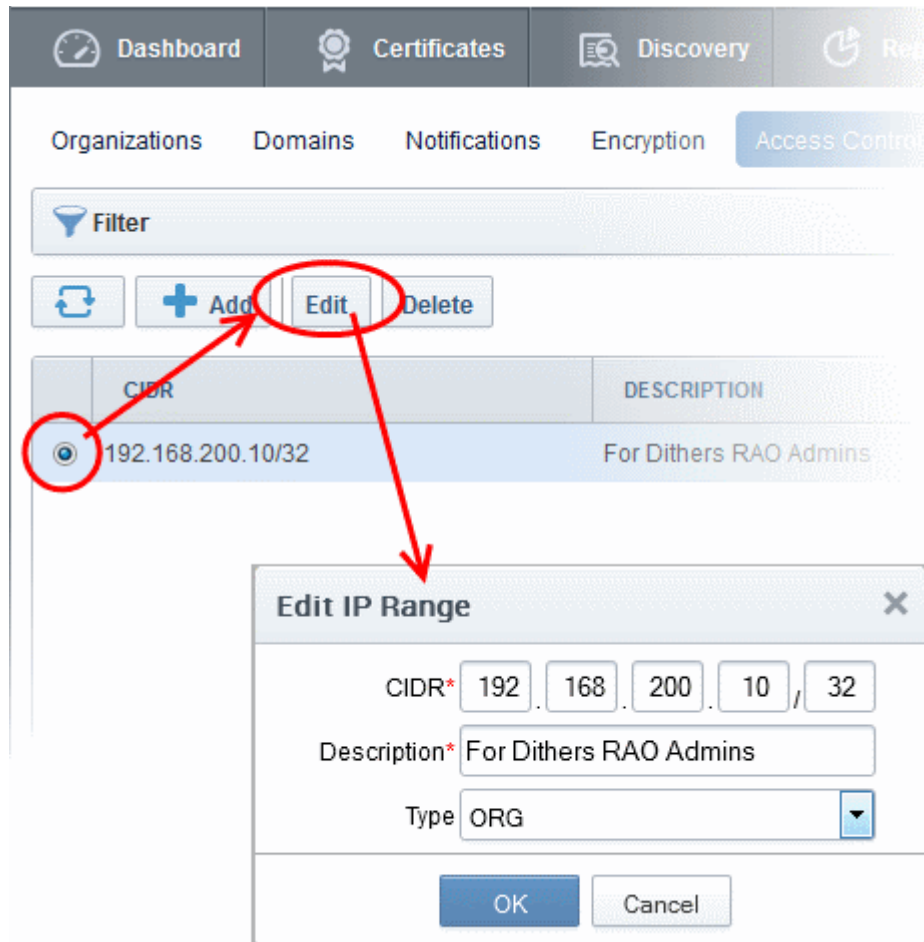
| Field Name | Values | Description |
|------------------------|-----------|--|
| CIDR (Required) | Numeric | The administrator should type the incoming IP ranges followed by network prefix, from which the access to the CCM interface has to be granted. All other IP addresses will be blocked. If no IP range is specified in Access Control then the default setting is to allow access from any IP: |
| Description (Required) | String | A short description of the IP range added. |
| Type | drop-down | Enables the administrator to select on whether the IP address restriction has to be imposed to all the administrators, MRAO administrator or the RAO administrators. All - The IP address based access restriction is imposed for all the administrators including the MRAO administrator. MRAO - The IP address based access restriction is imposed only for the MRAO administrator. ORG - The IP address based access restriction is imposed only all the RAO/DRAO administrators and not the MRAO administrator. |

Additions and changes to the access control list will not take effect for the administrator's current session, they will take effect only on the administrator's next login.

Tip: The administrator can also configure and limit incoming access to the CCM interface to certain IP addresses and ranges for the Organizations individually. Refer to the section [Editing an Existing Organization](#) for more details.

6.7.3 Editing an IP Range

An existing IP range can be edited by selecting the entry and clicking the 'Edit' button the as shown below:



The administrator can edit the values and click OK for the changes to be saved. The changes to the access control list will not take effect for the administrator's current session, they will take effect only on the administrator's next login.

- To remove a CIDR entry, select it and click 'Delete' from the top.

6.8 Private Key Store

Comodo Certificate Manager allows MRAO Administrators to create and maintain a secure Private Key Store on their local network. This can store private keys associated with certificates managed by CCM which were generated by CCM's auto CSR feature and also allows administrators to upload private keys for existing certificates. Administrators then have the option to download certificates in .pfx/.p12 format containing the public/private key pair so, for example, it may be exported to another web server.

Setting-up a Private Key Store requires controller software installed on a server in your local network. This controller can be configured from the 'Settings' > 'Private Key Store'. Once connected, the controller receives commands from CCM for CSR generation and for storing private keys. The MRAO can configure a backup of the private keys on a

remote SFTP server to restore keys in case they are lost.

Private keys can be uploaded to the keystore in the following ways:

1. **By selecting 'Autogenerate CSR and Manage Private Key' on the built-in certificate order form** - When enrolling for a certificate using the built-in enrollment form, administrators have the option to choose 'Autogenerate CSR and Manage Private Key'. If selected, CCM will send a command to the private key store controller to generate a CSR and key pair with the signature algorithm and key size chosen by the administrator. The controller stores the Private Key and uploads only the CSR to CCM. After certificate issuance, the administrator can download the certificate, including private and public keys, in .pfx/.p12 format. At the time of the download request, the private key store will retrieve a copy of the certificate from CCM over an encrypted connection, merge it with the private key and provision the certificate to the requestor. This ensures the private key does not pass outside your network. Refer to the section **Method 3 - Built-in Enrollment Form - Auto CSR Generation** for more details on applying for an SSL certificate with Auto-CSR generation.
2. **Manually upload a private key** - For CCM managed certificates which do not have a corresponding private key in the Private Key Store, administrators can manually upload the private key through the **'Certificate Details' dialog**. Once uploaded, CCM will instruct the key store controller to save a copy of the key and, once this operation is complete, will delete its own copy. After placing the private key in the store, administrators will be able to download the certificate, including private key, in .pfx/.p12 format. Refer to the section **Uploading Private Keys** for more details

Note: The Private Key Store is accessible only by the MRAO administrators.

Renewal of a Certificate

The Private Key Store eases the renewal process of SSL certificate. On renewal of a certificate whose private key is stored and managed by the Private Key Store, CCM automatically retrieves the existing CSR from the store and issues the renewal certificate, without the need for the administrator to generate a new CSR and upload it to CCM. A new private key will be generated for the new certificate and will be retained in the Private Key Store.

The following sections explain in detail on:

- **Setting-up the Private Key Store**
- **Uploading Private Keys**
- **Downloading Private Key of a Certificate**
- **Backup/Restore of the Private Key Store**
- **Removing Keys from Key Store**
- **Viewing Activities of the Controller**

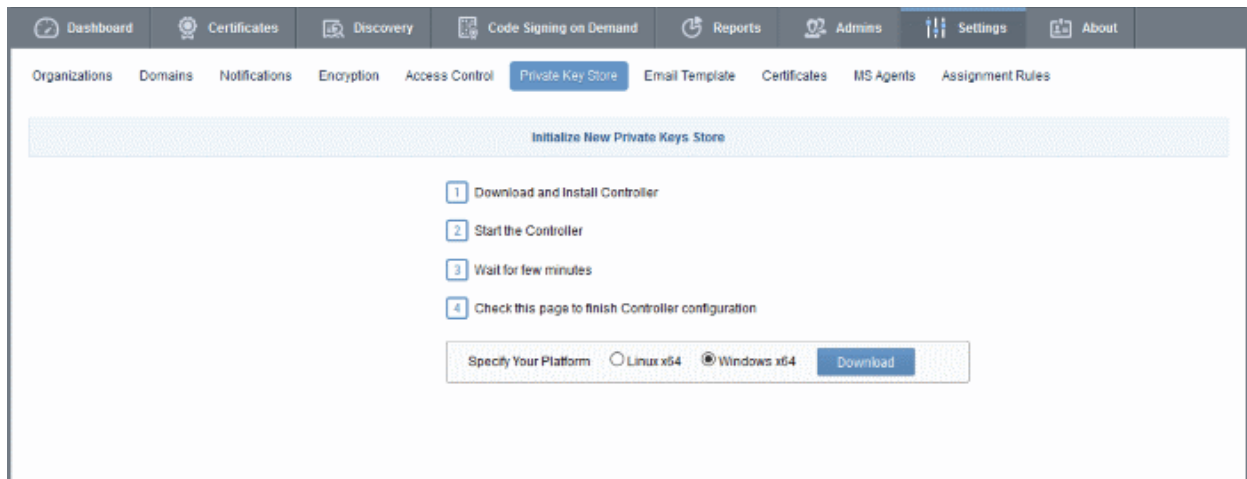
6.8.1 Setting-up the Private Key Store

The Private Key Store can be setup at your local network by installing a controller software on a server and configuring it from the 'Settings' > 'Private Key Store' area of the CCM interface.

Downloading and Installing the Controller

The controller software installation file is available from the CCM interface.

- Click 'Settings' tab and choose the 'Private Key Store' sub tab.

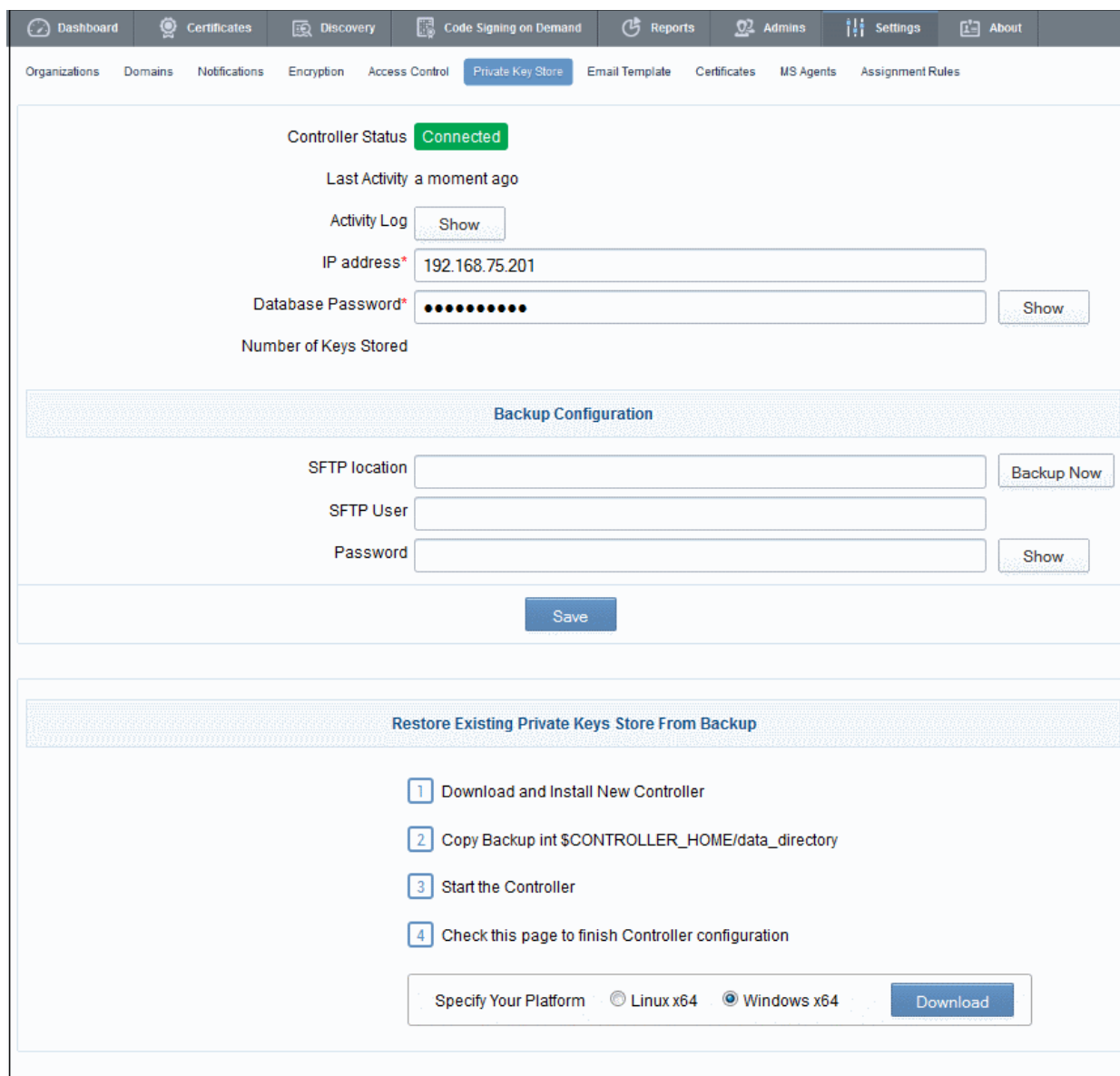


- Choose the operating system of the server on which the controller is to be installed and click the 'Download' button to download the installation file for the controller.
- Transfer the file to your server and install it.

On successful installation the controller will start to run immediately.

During the first run, the controller connects to CCM, obtains the configuration files updates its configuration and generates a password for its database.

The 'Settings' > 'Private Key Store' area will display the status as 'Connected' and shows the IP address of the server upon which the controller is installed. The controller periodically polls CCM and obtains the commands from it for execution.



| Private Key Store Interface - Table of Fields and Controls | | |
|--|------------|---|
| Field | Type | Description |
| Controller Status | Text field | Indicates whether the controller is currently connected to CCM or not. |
| Last Activity | Text field | Indicates the date and time of last polling of the Controller to CCM |
| Activity Log | Control | Clicking the 'Show' button opens the Commands dialog that displays the list of command received by the controller from the CCM and their execution status. Refer to the section Viewing Activities of the Controller for more details. |
| IP Address | Text field | Displays the IP address of the server on which the controller is installed. |
| Database Password | Text field | The password for accessing the local database created by the controller at the server. The password is auto generated and cannot be changed by the administrator. <ul style="list-style-type: none"> Clicking the 'Show' button displays the password. |

| | | |
|-----------------------------|------------|---|
| | | This password is required for downloading the private keys through the CCM. |
| Number of Keys Stored | Text field | Shows the number of private keys stored and managed by the Private Key Store controller. |
| Backup Configuration | | |
| SFTP location | Text field | The administrator can specify the location/URL of the SFTP server for the backup of the Private Key Store. Refer to the section Backup/Restore of the Private Key Store for more details. |
| SFTP User | Text field | Enter the username for the account in SFTP server, for access by the private key store controller. |
| Password | Text field | Enter the password for the account in SFTP server, for access by the private key store controller. |
| Save | Control | Saves the backup configuration |

6.8.2 Uploading Private Keys

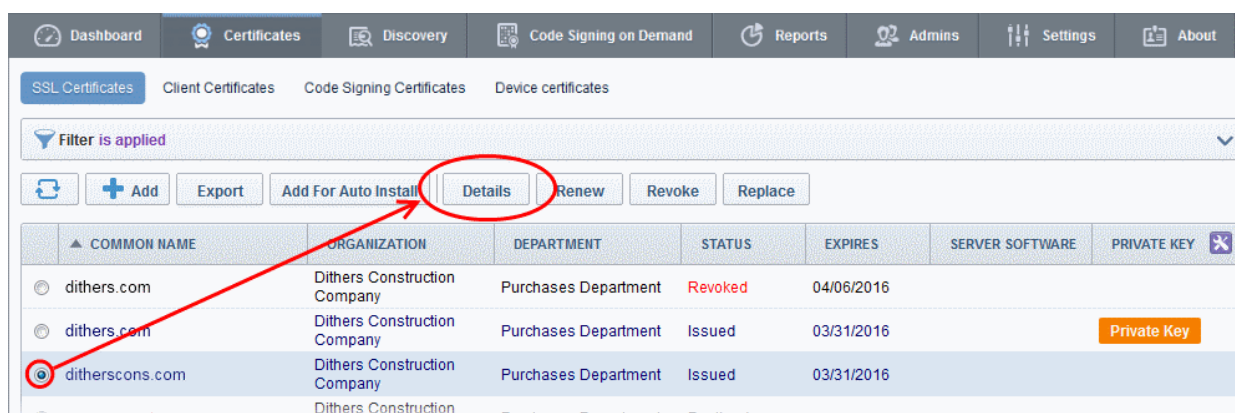
Administrators can upload, store and manage the private keys of existing, CCM-managed certificates to the key store. Using the key store to manage the private key facilitates:

- Downloading the certificate in .pfx/.p12 format for importing to another server
- Auto-upload of the CSR during the certificate renewal process

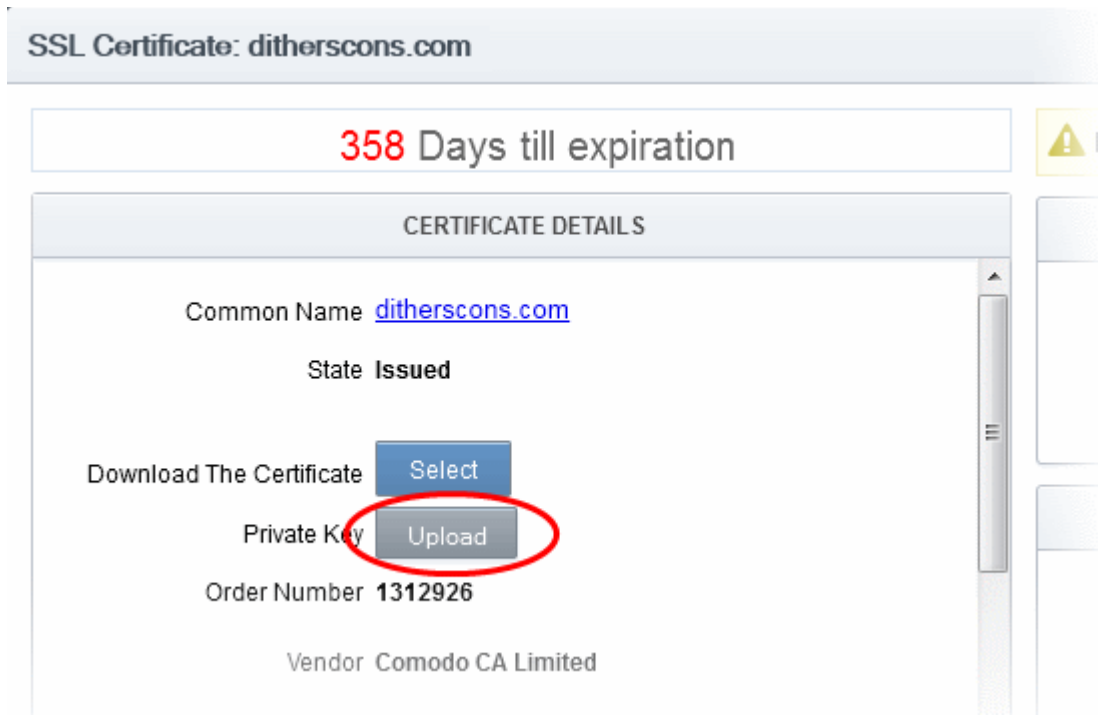
To upload the private key

- Click the Certificates Tab and choose SSL Certificates sub tab to open the SSL Certificates area
- Select the certificate for uploading the private key

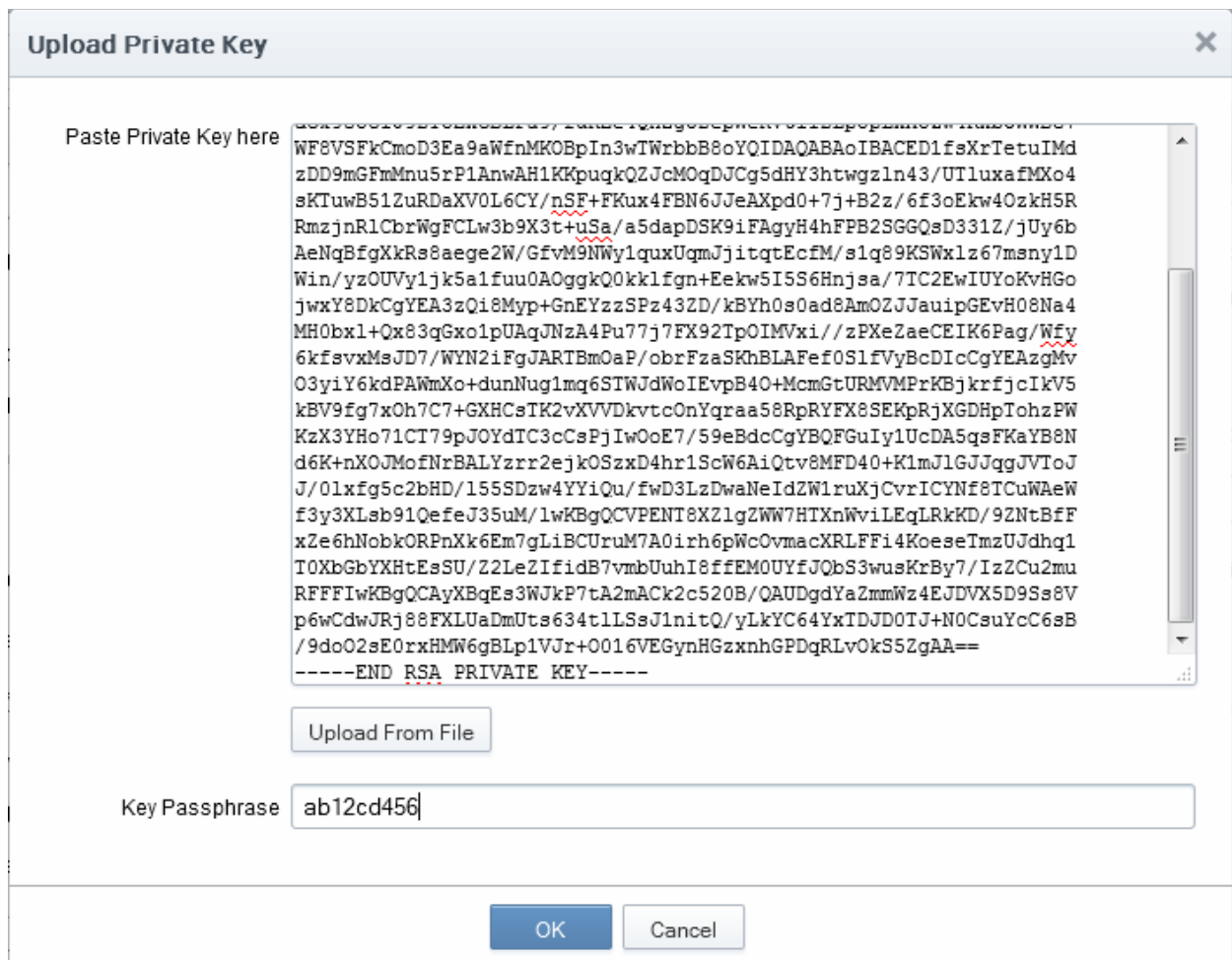
Tip: You can use the Filter options to search for the certificate. Refer to the section **Sorting and Filtering Options** under **SSL Certificates Area** for more details.



- Click the 'Details' button to open the 'Certificate Details' dialog
- Click the 'Upload' button beside 'Private Key' as shown in the figure



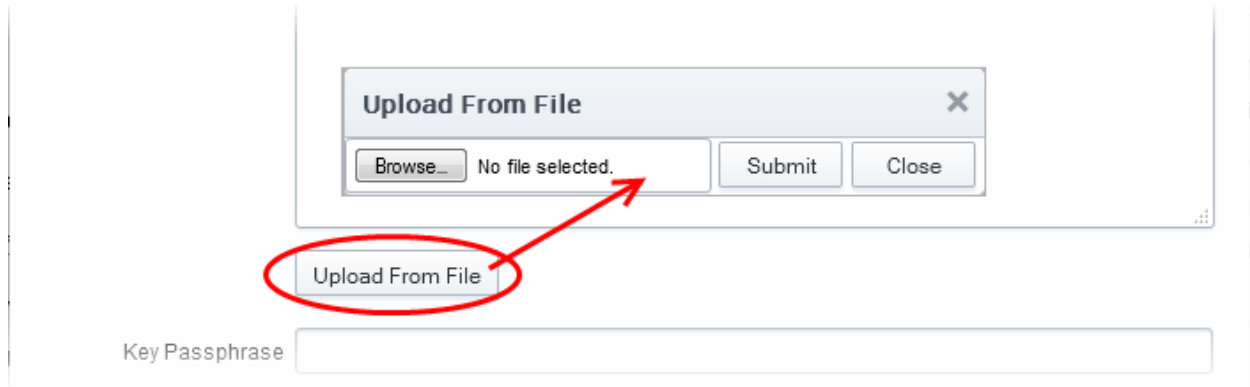
The Upload Private Key dialog will open.



- Enter the Private Key corresponding to the certificate

You can enter the private key associated with the certificate in two ways:

1. Directly paste the private key in the 'Paste Private Key here' text box
2. Save the private key as a text file and upload the file by clicking the 'Upload From File' button



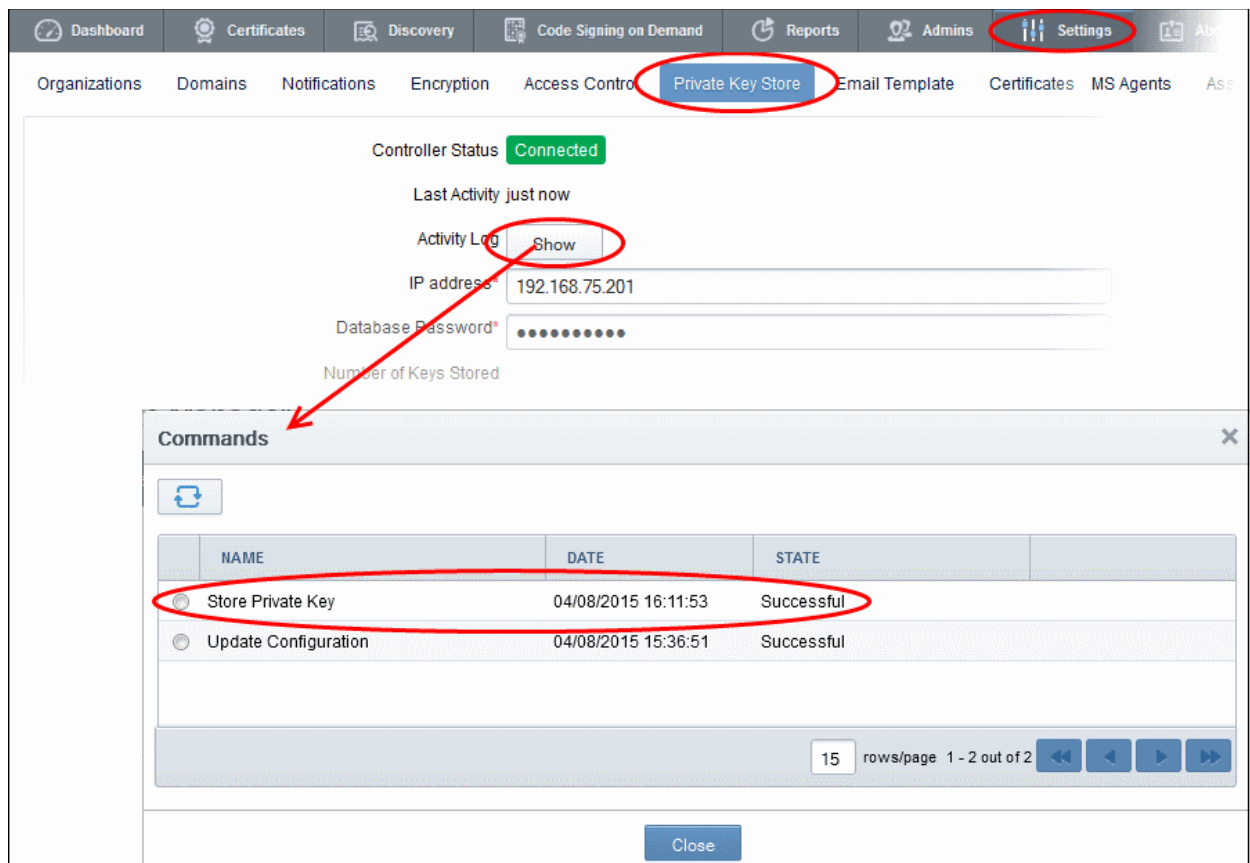
- Enter a passphrase for the key

The passphrase is required when importing the certificate with the key pair on to a server.

- Click 'OK'
- Close the 'Certificate Details' dialog

CCM will send a command to the controller to store the Private Key. You can confirm the execution of the Store Command, by viewing the activity log of the controller.

- Click 'Settings' > 'Private Key Store' to open the Private Key Store interface and click the 'Show' button beside 'Activity Log'



The private key is now stored and managed by the Private Key Store. It's availability will be indicated under the 'Private Key' column in the 'SSL Certificates' area:

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | SERVER SOFTWARE | PRIVATE KEY |
|-----------------|------------------------------|----------------------|---------|------------|-----------------|-------------|
| dithers.com | Dithers Construction Company | Purchases Department | Revoked | 04/06/2016 | | |
| dithers.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | Private Key |
| ditherscons.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | Private Key |

You can download the private key from the 'Certificate Details' dialog.

SSL Certificate: ditherscons.com

358 Days till expiration

CERTIFICATE DETAILS

Common Name [ditherscons.com](#)

State **Issued**

Download The Certificate

Private Key

Order Number **1312926**

Vendor **Comodo CA Limited**

Discovery Status: Not deployed

6.8.3 Downloading the Private Key of a Certificate

Administrators can download the private key associated with a managed certificate from the Private Key Store.

Limitations - The private key can be downloaded only for certificates whose private keys are managed by the private key store. This includes certificates applied using auto-CSR generation feature in CCM and certificates for which the private keys are manually uploaded to the Private Key Store.

The administrator should have been logged-in to CCM through a computer in the same local network on which the Private Key Store controller is installed and should have a personal authentication certificate installed on their computer.

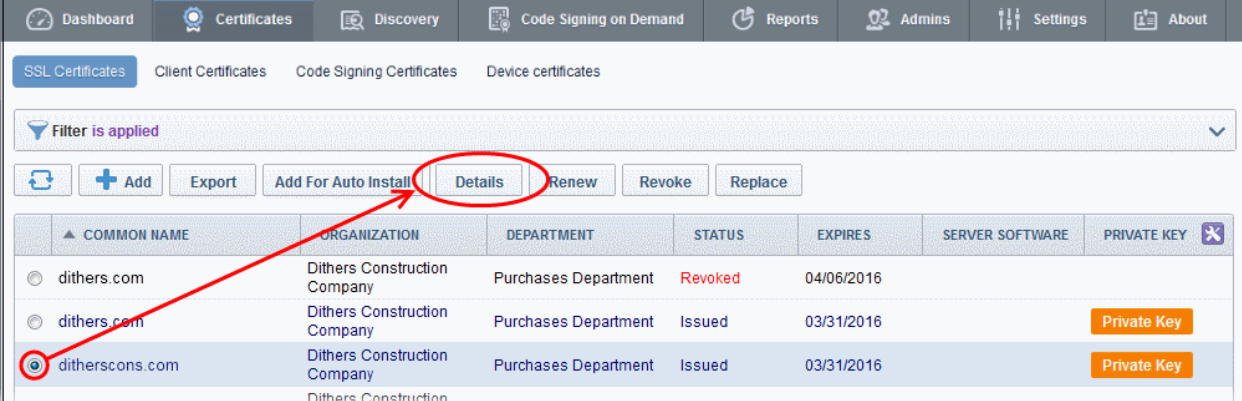
During the download process, CCM sends a download command to the controller. The controller requests for authentication of the administrator and checks for their authentication certificate. Once authenticated, the private key controller enables the administrator to download the private key in .key format. To reiterate, the key is not sent

to the CCM servers at any time. This ensures that, although the download was initiated via the CCM interface, the private key never passes outside your network.

To download the private key

- Click the 'Certificates' tab and choose 'SSL Certificates' sub tab to open the SSL Certificates area
- Select the certificate for downloading the private key

Tip: You can use the Filter options to search for the certificate. Refer to the section [Sorting and Filtering Options](#) under [SSL Certificates Area](#) for more details.



The screenshot displays the 'SSL Certificates' section of the Comodo Certificate Manager. The interface includes a navigation bar with tabs for 'Dashboard', 'Certificates', 'Discovery', 'Code Signing on Demand', 'Reports', 'Admins', 'Settings', and 'About'. Below the navigation bar, there are sub-tabs for 'SSL Certificates', 'Client Certificates', 'Code Signing Certificates', and 'Device certificates'. A filter bar indicates 'Filter is applied'. Action buttons include '+ Add', 'Export', 'Add For Auto Install', 'Details', 'Renew', 'Revoke', and 'Replace'. The 'Details' button is circled in red. Below the buttons is a table with columns: COMMON NAME, ORGANIZATION, DEPARTMENT, STATUS, EXPIRES, SERVER SOFTWARE, and PRIVATE KEY. The table contains three rows of certificates. The first row has a common name of 'dithers.com', organization 'Dithers Construction Company', department 'Purchases Department', status 'Revoked', and expires '04/06/2016'. The second row has a common name of 'dithers.com', organization 'Dithers Construction Company', department 'Purchases Department', status 'Issued', expires '03/31/2016', and a 'Private Key' button. The third row has a common name of 'ditherscons.com', organization 'Dithers Construction Company', department 'Purchases Department', status 'Issued', expires '03/31/2016', and a 'Private Key' button. A red arrow points from the 'Details' button to the 'Private Key' button in the third row.

| COMMON NAME | ORGANIZATION | DEPARTMENT | STATUS | EXPIRES | SERVER SOFTWARE | PRIVATE KEY |
|-----------------|------------------------------|----------------------|---------|------------|-----------------|-------------|
| dithers.com | Dithers Construction Company | Purchases Department | Revoked | 04/06/2016 | | |
| dithers.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | Private Key |
| ditherscons.com | Dithers Construction Company | Purchases Department | Issued | 03/31/2016 | | Private Key |

- Click the 'Details' button to open the 'Certificate Details' dialog
- Click the 'Download' button beside 'Private Key' as shown in the figure

SSL Certificate: ditherscons.com

357 Days till expiration

CERTIFICATE DETAILS Private Key

Common Name ditherscons.com

State **Issued**

Download The Certificate Select

Private Key Download Remove

Passphrase

Show Pass-phrase

Order Number **1312926**

Vendor **Comodo CA Limited**

Discovery Status **Not deployed**

Self-Enrollment Certificate ID **77881**

Type **Instant SSL**

Server Software **Apache/Mod SSL** Edit

The private key storage controller will request for authentication and search for the personal authentication certificate of the administrator in the computer from which the administrator has logged-in. If more than one certificate is found, the Select Certificate dialog will be displayed for the administrator to choose the certificate.

Select a certificate

Select a certificate to authenticate yourself to 192.168.75.201:9090

- John Smith (COMODO RSA Client Authentication and Secure Email CA)
- John Smith (COMODO Client Authentication and Secure Email CA)

Certificate information OK Cancel

- Choose the certificate for authentication and click OK.

Upon authentication verification, the download dialog will be displayed, enabling the administrator to download the private key in .key format.

6.8.4 Backup/Restore for the Private Key Store

The administrator can configure backup for the Private Key Store at a remote SFTP server and run periodic backups manually. In case the private keys store is lost, the keys can be restored from the backup.

To configure for backup

- Click 'Settings' > 'Private Key Store' to open the 'Private Key Store' interface
- Enter the details of the SFTP server to be configured as the backup location, under 'Backup Configuration'

Backup Configuration - Table of Parameters

| Parameter | Description |
|---------------|---|
| SFTP Location | Enter the path of the backup location in the SFTP server, at which the private key storage backup is to be created. |
| SFTP User | Enter the username of your user account in the SFTP server |
| Password | Enter the password of your user account in the SFTP server |

- Click 'Save' for your configuration to take effect.
- To run an instant backup, click the 'Backup Now' button.

The Backup is configured. You can run the backup any time you want by clicking the 'Backup Now' button from the 'Private Key Store' interface. It is recommend to run the backup every time a new private key is uploaded to the Private Key Store or a new certificate is enrolled with auto-CSR generation feature.

In case the the Private Key Store controller is lost in the server for some reason, you can restore the keys from the backup, by creating another Private Key Store in the same or a different server in your local network and configuring it from the 'Settings' > 'Private Key Store' interface.

To restore the keys

- Download the setup file for the new controller, by selecting the operating system of your server and clicking the Download button under 'Restore Existing Private Keys Store From Backup'
- Install the controller on your server

Upon successful installation, the controller will connect to CCM and its state will be displayed as 'Connected' in the 'Settings' > 'Private Key Store' interface.

- Enter the SFTP details of the remote SFTP server configured as backup location and click 'Save'.

The Private Keys will be restored to the Private Key Store.

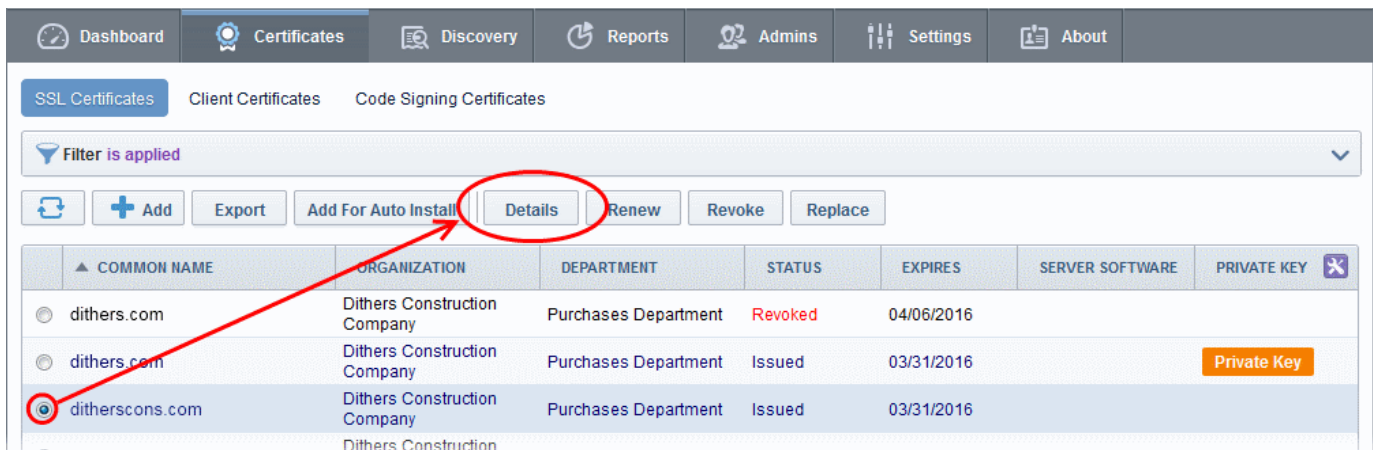
6.8.5 Removing Keys from Key Store

The administrator can remove the private keys that no longer require to be managed by the Private Key Store from the Certificate Details dialog.

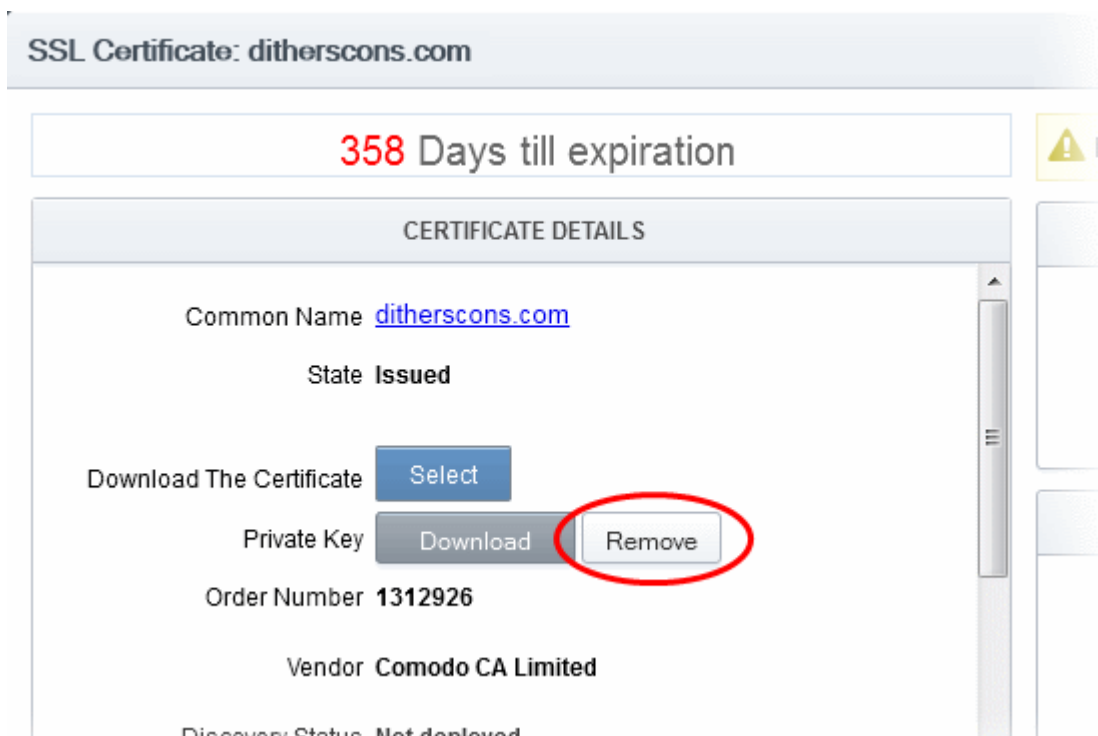
To remove a private key

- Click the Certificates Tab and choose SSL Certificates sub tab to open the SSL Certificates area
- Select the certificate whose key is to be removed

Tip: You can use the Filter options to search for the certificate. Refer to the section **Sorting and Filtering Options** under **SSL Certificates Area** for more details.



- Click the 'Details' button to open the 'Certificate Details' dialog
- Click the 'Remove' button beside 'Private Key' as shown in the figure



CCM will send a command to remove the key from the Private Key Store.

6.8.6 Viewing Activities of the Controller

The administrator can view the list of commands received by the controller from the CCM and their execution status.

- Clicking the 'Show' button beside 'Activity Log' in the 'Settings' > 'Private Key Store' interface opens the Commands dialog with the list of commands received by the controller in chronological order.

The screenshot shows the 'Private Key Store' settings page. The 'Settings' and 'Private Key Store' tabs are circled in red. The 'Activity Log' section has a 'Show' button circled in red, with a red arrow pointing to the 'Commands' dialog box. The dialog box displays a table of commands:

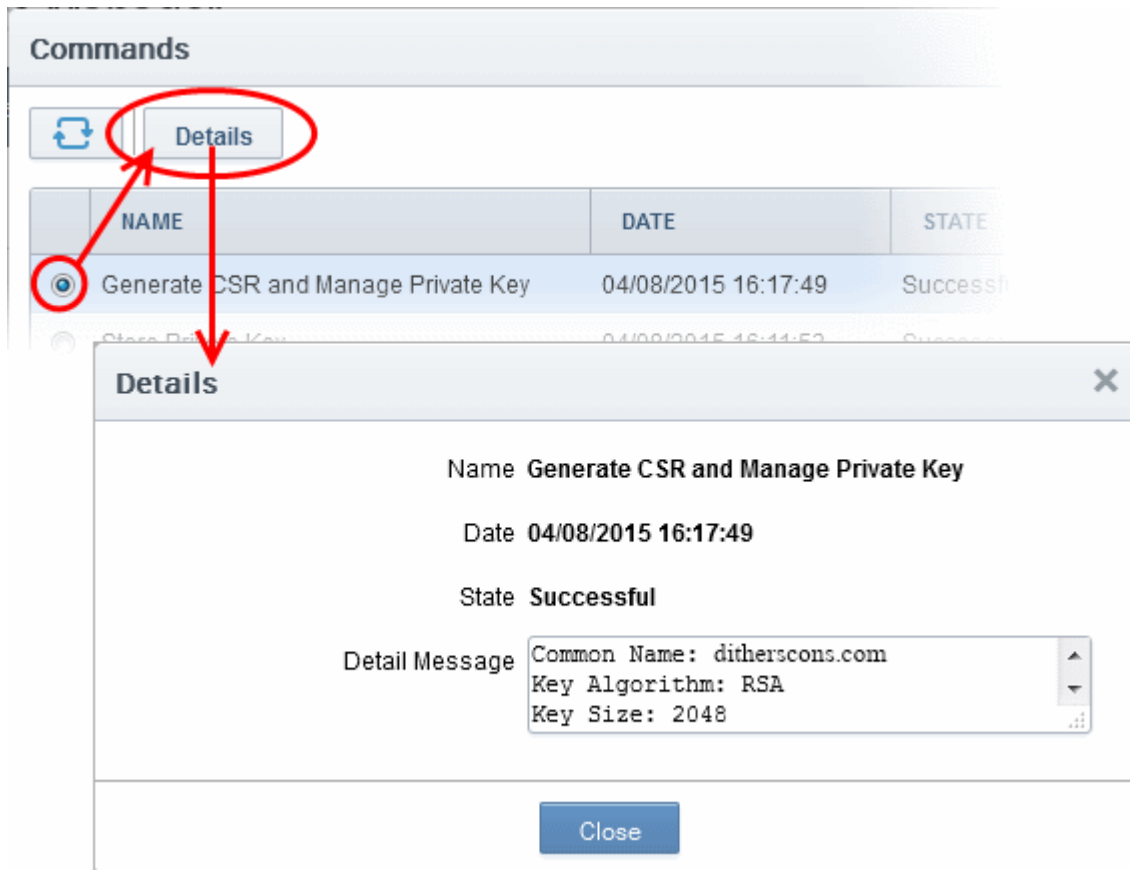
| NAME | DATE | STATE |
|-------------------------------------|---------------------|------------|
| Generate CSR and Manage Private Key | 04/08/2015 16:17:49 | Successful |
| Store Private Key | 04/08/2015 16:11:53 | Successful |
| Update Configuration | 04/08/2015 15:36:51 | Successful |

Commands Dialog - Column Descriptions

| Column Header | Description |
|---------------|--|
| Name | Shows the command received from CCM during the consecutive polls. The possible commands are: <ul style="list-style-type: none"> • No Command - Default command with indicates that there is no pending tasks for the controller. • Update Configuration - Received if configuration synchronization is required, example, during first start of the controller or controller configuration changed on CCM side by the administrator. • Generate CSR and Manage Private Key - Received on enrollment for a new certificate with auto-CSR generation feature at the CCM. The Controller generates key pair and CSR. The private key is stored in the database and CSR will be transferred to CCM side for further certificate enrollment. • Store PrivateKey - Received when an administrator manually uploads a private key associated with a managed certificate for storage and |

| | |
|-------|--|
| | management by the Private Key Store. |
| Date | Indicates the precise date and time, the command was received. |
| State | Indicates the execution state and result of the command. |

- Choosing a command and clicking the 'Details' button at the top, displays the details of the command.

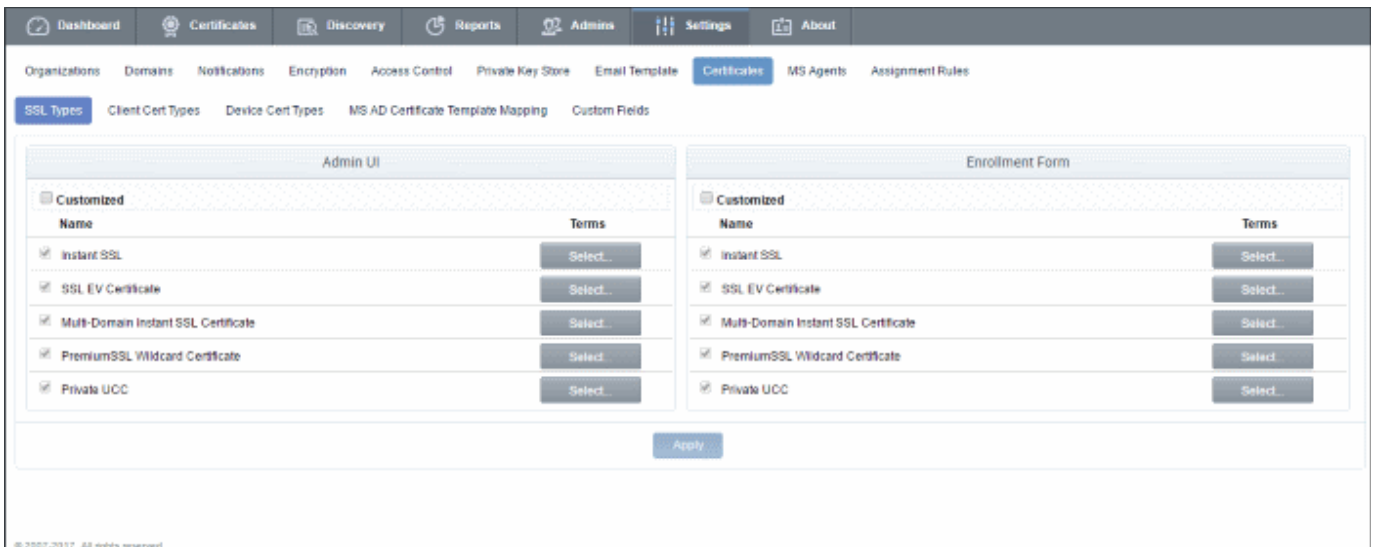


6.9 Certificates

6.9.1 Section Overview

The 'Certificates' tab allows MRAO administrators to customize the type and term length of certificates available to CCM organizations. The certificates configured here will be made available in the **Built-In Application Form** and **Self Enrollment Form**. The Custom Field tab in this area allows MRAOs to add fields to those forms. This section also allows administrators to map Microsoft AD Templates to CCM certificate types in order to issue Device and Private UCC SSL certificates. Refer to the section **Mapping MS AD Certificate Templates to CCM Certificate Types** for more details on how to configure MS Active Directory certificate templates to CCM certificate types.

Note: The Custom Field tab will be available only if this feature is enabled for your account. If this is not available and want to add this option, please contact your Comodo account manager.

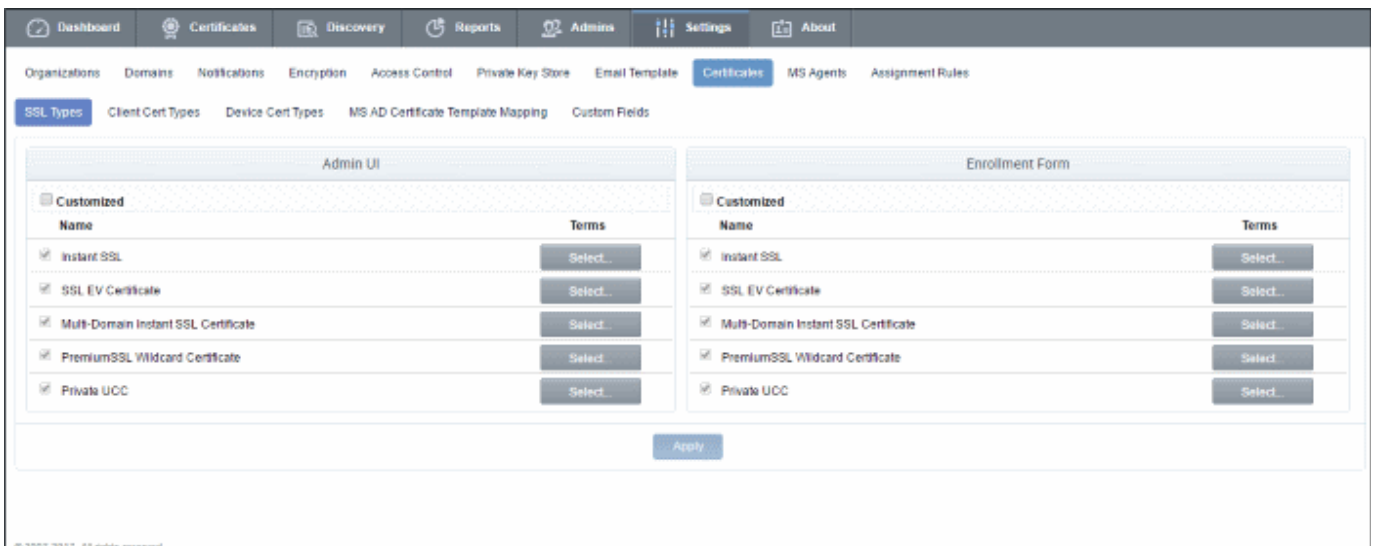


Note: The Certificates area is visible to and accessible only by MRAO Administrators.

6.9.2 SSL Types

The 'SSL Types' tab allows administrators to customize the types and terms of SSL certificates available to CCM organizations in the built-in and self enrollment application forms. It can be useful to limit the types of certificates available to simplify the certificate selection procedure for end-users on the forms.

Note: The SSL Types area is visible to and accessible only by MRAO Administrators.



- **Admin UI** - Determines the SSL certificate types that will be available to applicants using the **Built-In Application form**
- **Enrollment Form** - Determines the SSL certificate types that will be available to applicants using the **Self Enrollment Form**.
- It is possible to make different certificates available on the Built-in form than are available on the Self-Enrollment form.

| SSL Types - Table of Parameters | | |
|---------------------------------|---|--|
| Field Name | Type | Description |
| Customized | Checkbox | Checking this box enables customization of the SSL types. Leaving this unchecked means all the certificate types are available through both the Built-in Application form and the Self Enrollment form. |
| Name | List of Certificate types with checkboxes | Lists the SSL types that are assigned to your account by your account Manager. For more details on certificates types, refer to Comodo SSL Certificates . Note: If a certificate or certificate term is not present here, administrators should contact their account manager to have it added. |
| Terms | Drop-down options | Clicking the 'Select' button opens a drop-down box displaying the term lengths available for the certificate type. |

By default, the 'Customized' option is left unchecked so that all the certificate types are available through both types of application form.

6.9.2.1 Customize SSL Certificate Types

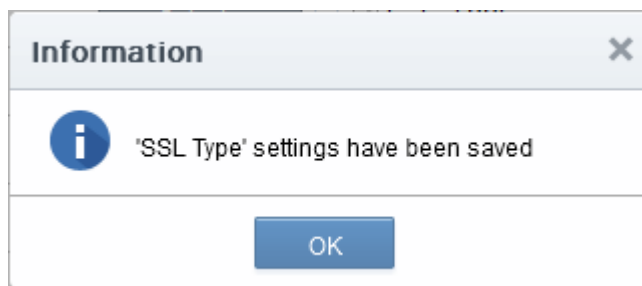
Note. 'Admin UI' = The 'Built in' application form in the CCM interface. 'Enrollment Form' = The 'Self-enrollment' application form which external applicants can use to apply for certificates.

To restrict the SSL types and their durations

1. Select the 'Customized' option below 'Admin UI' and/or 'Enrollment Form'.
2. Select the names of the certificates you wish to be available and leave the others unchecked.
3. Click the 'Select' button next to the certificate name to choose which terms will be available.

The screenshot shows the 'SSL Types' configuration page in the Comodo Certificate Manager. The page is divided into two columns: 'Admin UI' and 'Enrollment Form'. Each column has a 'Customized' checkbox and a table of certificate types with 'Terms' dropdown menus. The 'Admin UI' table shows 'EliteSSL Certificate', 'PlatinumSSL Wildcard Certificate', 'Comodo Unified Communication Certificate', 'Comodo EV SSL Certificate', and 'Comodo EV Multi Domain SSL'. The 'Enrollment Form' table shows 'EliteSSL Certificate', 'PlatinumSSL Wildcard Certificate', 'Comodo EV SSL Certificate', 'Comodo EV Multi Domain SSL', and 'Comodo Unified Communication Certificate'. An 'Apply' button is at the bottom.

4. Click 'Apply'. The confirmation dialog on saving your settings appears.



Only the types and terms of SSL certificates that are selected in the 'SSL Types' interface will now be available in the 'Type' and 'Term' drop-down fields of the 'built-in' application form and the 'self-enrollment' form.

Built-in Enrollment Form

Request New SSL Certificate

*-required fields

Organization* Okakayanibud

Department* ANY

[Click here to edit address details](#)

Certificate Type* Instant SSL

Certificate Term* Instant SSL

Server Software* Multi-Domain Instant SSL Certificate
PremiumSSL Wildcard Certificate
Comodo EV SSL Certificate
Comodo EV Multi Domain SSL
SSL EV Certificate

Provide CSR Autogenerate CSR and Manage Private Key

CSR*

Max CSR size is 32K

Certificate Parameters

Common Name*

Requester John Smith

External Requester

Comments

Telephone

Subscriber Agreement

1 Comodo ePKI Certificate Manager Agreement – EV Enabled THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS. IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON 'I ACCEPT' BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND

I agree.* Scroll to bottom of the agreement to activate check box.

Self Enrollment Form

COMODO
Certificate Manager

SSL Enrollment

Access Code: *

Email: * admin@coradithers.com

[Click here to edit address details](#)

Certificate Type: * Instant SSL

Certificate Term: * Instant SSL

Server Software: * Multi-Domain Instant SSL Certificate
SSL EV Certificate

CSR: *

Max CSR size is 32K

Common Name: *

Please provide a Self Enrollment Passphrase. A passphrase is necessary for certificate revocation and renewal.

Self Enrollment Passphrase:

Re-type Self Enrollment Passphrase:

Comments:

Fax: *

Telephone:

Subscriber Agreement

1 Comodo ePKI Certificate Manager Agreement – EV Enabled THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS. IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON 'I ACCEPT' BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

I Agree.*
Scroll to bottom of the agreement to activate check box.

Notes:

- The 'SSL Types' tab can be accessed only by MRAO administrators and is not visible to RAO and DRAO admins.
- The selection of SSL Types and their term lengths applies to all Organizations. For restricting SSL types available for a specific Organization, refer to **Customize an Organization's SSL Certificate Types**.

- The certificate types or terms that are disabled through the SSL Types tab will not be available even in the **'Bind SSL Types' interface**. To add a specific certificate type/term for a particular Organization, RAO SSL Administrators should seek the advice of an MRAO Administrator.

6.9.3 Client Cert Types

Comodo offers different client certificate types for different purposes. The capabilities of a client certificate depend on the Key Usage Templates (KUTs) bound to it. For example, KUT's can be applied to client certificates for the purposes of 'Signing Only', 'Encryption Only', 'Dual Use' (Signing + Encryption) or 'Smart Card Logon and Authentication'

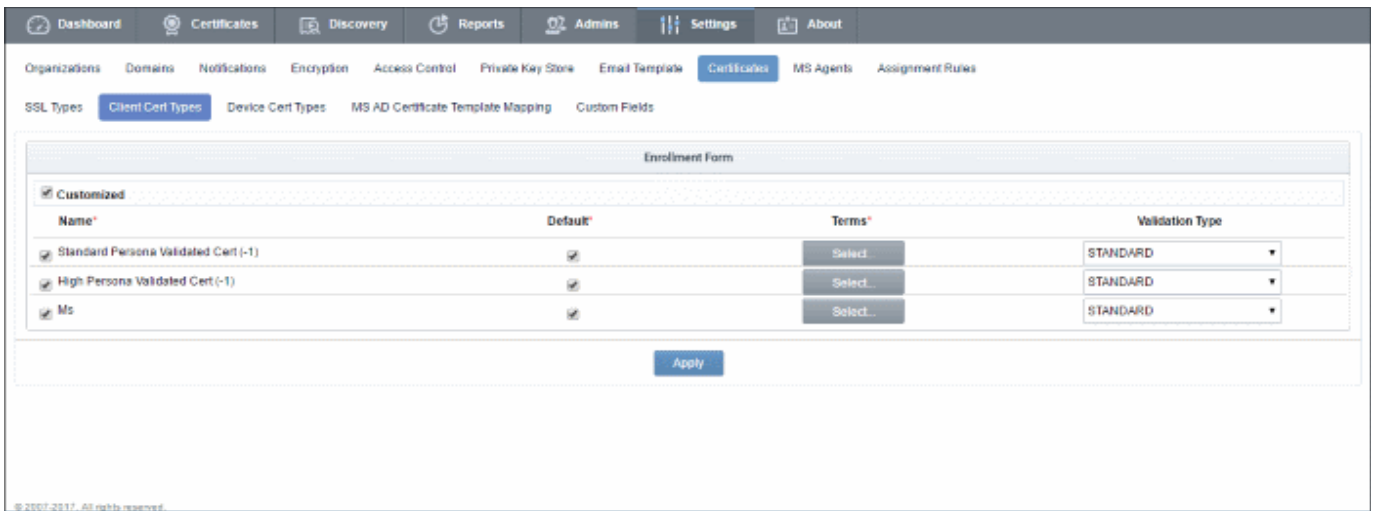
The following table shows a sample of available KUTs/Client Certificate types:

| Name | Description of Purpose |
|-------------------------------------|--|
| Signing Only | Digital Signing |
| Dual Use | Digital Signing and Encryption |
| Encryption Only | Encryption and Decryption only |
| Authentication Only | Authentication only |
| Comodo Dual Use | Dual use certificates (Digital Signing and Encryption) as defined by Comodo Certification Practice Statement (CPS) |
| SOAP Signing & Encryption | Digital Signing and Encryption of Simple Object Access Protocol (SOAP) messages |
| Data Encipherment | Data Encipherment |
| AD User | Authentication to AD server |
| Smart Card Logon and Authentication | For use with Smart Card Logon and Authentication |
| EFS | Encryption of files |

MRAO administrators can request the Comodo Account Manager to create and enable client certificates of multiple types for their account. It is also possible to create custom client certificate types by applying a single KUT or selected combinations of them.

The 'Client Cert Types' tab displays the list of client certificate types enabled for the account and allows the MRAO Administrator to customize the types of client certificates and their term lengths that are available for the end-users for all Organizations/Departments through self enrollment form (both Access Code based and Secret ID based). It can be useful to create such a targeted 'certificate roster' as it simplifies the certificate selection procedure at the application forms and helps avoid applications for certificates which are inappropriate.

Note: The 'Client Cert Types' area is visible to and accessible only by MRAO Administrators.



Client Cert Types - Table of Parameters

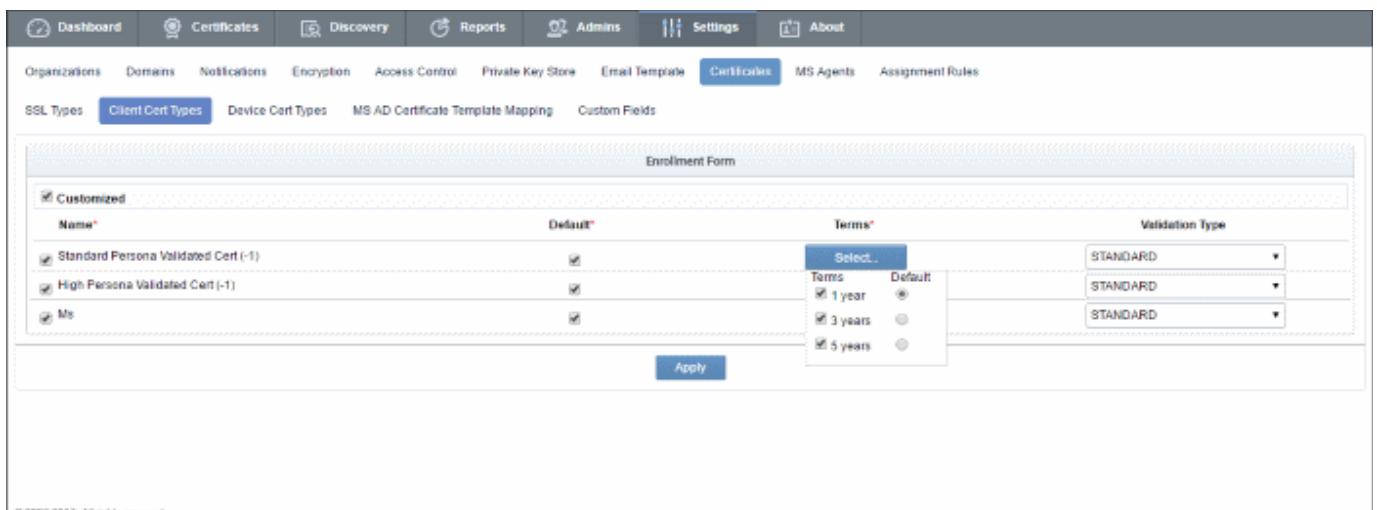
| Field Name | Type | Description |
|-----------------|---|---|
| Customized | Checkbox | Checking this box enables customization of the Client Cert types. Leaving this unchecked means all the certificate types are available to the end-users. |
| Name | List of Certificate types with checkboxes | Lists the Client Certificate types that are assigned available for your account by your account Manager. Note: If a certificate or certificate term is not present here, administrators should contact their account manager to have it added. |
| Default | Checkbox | Allows the Administrator to set the certificate type as Default type for the Organizations. The client certificate type(s) for which the default checkbox is selected, will stand as default option(s) in the Self Enrollment forms for applying for Client Cert by end-users. Note: At least one certificate type has to be selected as default type. |
| Terms | Drop-down options | Clicking the 'Select' button opens a drop-down box displaying the Term lengths available for the Certificate type. |
| Validation Type | Drop-down options | Allows the administrator to specify the type of validation to be applied to the end-user. The two options available are 'Standard' and 'High' validation types. The difference between the two lies in the degree of user authentication is carried out prior to issuance. 'Standard' validation type can be completed quickly and takes advantage of the user authentication mechanisms that are built into CCM. Under 'Standard Personal Validation' type, the user is authenticated using the following criteria: <ul style="list-style-type: none"> • User must apply for a certificate from an email address @ a domain that has been delegated to the issuing Organization • The Organization has been independently validated by an web-trust accredited Certificate Authority as the owner of that domain • User must know either a unique Access Code or Secret ID that should be entered at the certificate enrollment form. These will have been communicated by the administrator to the user via out-of-band |

| | | |
|--|--|--|
| | | <p>communication.</p> <ul style="list-style-type: none"> User must be able to receive an automated confirmation email sent to the email address of the certificate that they are applying for. The email will contain a validation code that the user will need to enter at the certificate collection web page. <p>'High Personal Validation' type requires that the user undergo the validation steps listed above AND</p> <ul style="list-style-type: none"> Face-to-Face meeting with the issuing Organization <p>Note: The additional validation steps must be completed PRIOR to the administrator selecting 'High Personal Validation' type.</p> |
|--|--|--|

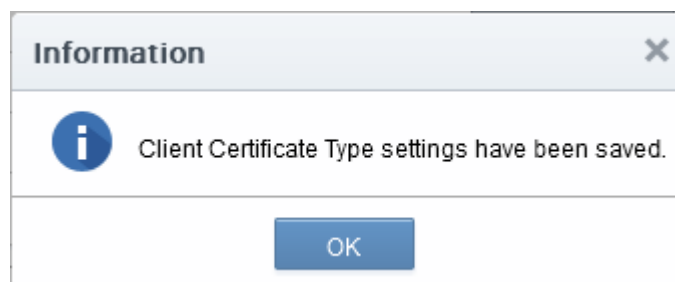
6.9.3.1 Customize Client Certificate Types

To specify which Client Cert types are available:

1. Select the 'Customized' checkbox.
2. Check the names of the certificates you wish to be available and leave the others unchecked.
3. Select the 'Default' checkbox if you wish this certificate type to be shown as the default option in both access code based and secret ID based self-enrollment forms.
4. Click the 'Select' button next to the certificate name to choose which terms will be available. If you want to set the selected term as default term for the selected certificate type, select the 'Default' radio button.



5. Select the Validation type from the drop-down. For more information on validation types, refer to the [table](#) in the [Overview](#).
6. Click 'Apply'. A confirmation dialog will appear:



Only the types and terms of client certificates that are selected in the 'Client Cert Types' interface will now be available in the 'Type' drop-down field of the Self Enrollment form.

Notes:

- The 'Client Cert Types' tab can only be accessed by MRAO administrators and is not visible to RAO and DRAO admins.
- The types of client certificates you make available here will apply all organizations. To restrict client certificate types for a specific Organization, refer to **Customize an Organization's SSL Certificate Types**.
- The certificate types or terms that are disabled here will not be available even in the **'Bind Client Cert Types'** interface. To add a specific certificate type/term for a particular Organization, RAO SSL administrators should seek the advice of an MRAO Administrator.

6.9.4 Device Cert Types

In addition to issuing Comodo device certificates via AD and API, CCM allows administrators to add device certificates from private certificate authorities. These certificates can be requested by applicants through the self-enrollment forms and/or enrolled for, through Simple Certificate Enrollment Protocol (SCEP). Certificates from Private CAs can be deployed via API method too.

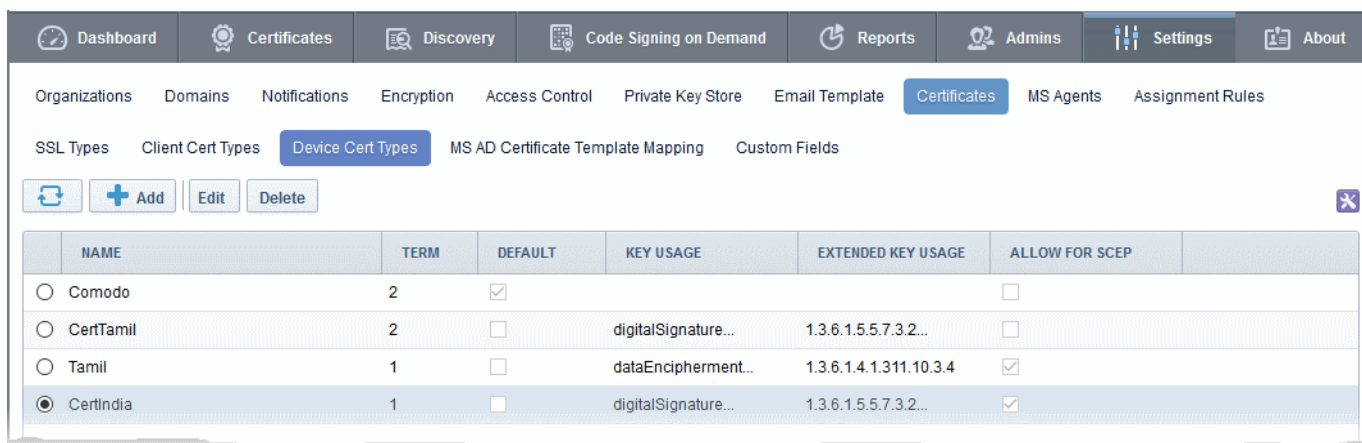
Note - Private CAs must be enabled for your account. Please contact your Comodo account manager for more details.

The capabilities of a device certificate are determined by the Key Usage Templates (KUTs) bound to it. For example, device certificate types can be created for 'Signing Only', 'Encryption Only', 'Non repudiation' etc.

The following table shows a sample of available KUTs/Device Certificate types:

| Name | Description of Purpose |
|---------------------------|--|
| Key Usage | |
| Data Encipherment | Data encryption |
| Digital Signature | Digital Signing |
| Key Agreement | Key Agreement |
| Key Encipherment | Key encryption |
| Non Repudiation | Non Repudiation |
| Extended Key Usage | |
| Client Authentication | User authentication |
| Email Protection | Digital signature, key agreement, non-repudiation, and/or key encipherment |
| MS Smart Card Logon | Smart Card authentication |
| MS Encrypted File System | Encryption of files |

Note: The 'Device Cert Types' area is only available to MRAO Administrators.



| Device Cert Types tab - Table of Parameters | | |
|---|------|--|
| Column | | Description |
| Name | | The name of the device certificate |
| Term | | The validity period of the device certificate |
| Default | | A default device certificate has to be added in order for the 'Device Cert' feature be active. This is usually done by Comodo at the time of activation. This default certificate will not be available for self-enrollment. |
| Key Usage | | Indicates the purpose(s) of the certificate. For example, authentication, encryption and more. |
| Extended Key Usage | | Displays the extended key usage capabilities |
| Allow for SCEP | | Indicates whether the device certificate type can be obtained through SCEP enrollment. For more details on SCEP enrollment, refer to the section Issuance of Device Certificates through SCEP . |
| Control Buttons | Add | Allows administrators to add a new device cert type. Refer to the section ' Adding Device Cert Types ' for more details. |
| | Edit | Allows administrators to update the device certificates |

Note: The type of control buttons that are displayed above the column header depends on the state of the selected certificate.

- Clicking the 'Name', 'Term', 'Default' and 'Allow for SCEP' column headers sorts the items in alphabetical/ascending/descending order.

6.9.4.1 Adding Device Cert Types

MRAO administrators can add new device certificate types for **self-enrollment** as follows:

To add a new device cert type

- Click 'Settings' > 'Certificates' > 'Device Cert Types'.
- Click the 'Add' button at the top

The 'Add New Device Cert Type' form will be displayed.

The screenshot shows the Comodo Certificate Manager interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Code Signing on Demand, and Reports. Below these are sub-sections: Organizations, Domains, Notifications, Encryption, Access Control, Private Key Store, and Email Template. Further down, there are more sub-sections: SSL Types, Client Cert Types, Device Cert Types (highlighted), MS AD Certificate Template Mapping, and Custom Fields. A toolbar contains buttons for Refresh, Add (circled in red), Edit, and Delete. Below the toolbar is a table with columns: NAME, TERM, DEFAULT, KEY USAGE, and EXTENDED KEY USAGE. The first row shows 'Comodo' with a term of '2' and a checked 'DEFAULT' box. A red arrow points from the 'Add' button to a modal window titled 'Add New Device Cert Type'. This modal window contains a form with the following fields and options:

- Name***: Text input field.
- Term***: Text input field.
- CA name***: Dropdown menu with 'CertIndia' selected.
- Allow for SCEP**:
- Show on Selfenrollment**:
- Key Usage**:
 - Digital Signature
 - Non repudiation
 - Key Encipherment
 - Data Encipherment
 - Key Agreement
- Extended Key Usage**:
 - Client Authentication
 - Email Protection
 - MS Smartcard Login
 - MS Encrypted File System
 - OID-1

At the bottom of the modal window are 'OK' and 'Cancel' buttons.

| Form Element | Type | Description |
|----------------------------------|-------------|---|
| Name (required) | Text Field | Enter an appropriate name for the device certificate |
| Term (required) | Text Field | The validity period of the device certificate |
| CA Name (required) | Drop-down | The drop-down will display the Private CAs that are added for your account. Contact your Comodo account manager to add more Private CAs. |
| Allow for SCEP | Check Box | Select this option to allow enrollment via SCEP for this device cert type. |
| Show on Self Enrollment | Check Box | Select this option if you want device certs of this type to be available for selection in the Self Enrollment Form for device certificates. For more details on self enrollment, refer to the section Issuance of Device Certificate through Self Enrollment |
| Key Usage and Extended Key Usage | Check Boxes | Determines the device certificate capabilities. Refer to the table in the previous section for details. |

- Click 'OK' after entering the details in the form.

The new device cert type will be added as configured and will be available for enrollment via the self-enrollment forms, API integration and SCEP.

6.9.4.2 Editing and Deleting a Device Cert Type

MRAO administrators can edit or delete a device cert type in the list. Please note you cannot edit or delete the default device cert type.

To update the details of a device cert type, select it and click the 'Edit' button at the top.

The screenshot shows the 'Edit Device Cert Type' dialog box with the following fields and options:

- Name***: CertIndia
- Type ID***: 54
- Term***: 1
- CA name***: CertIndia
- Allow for SCEP**:
- Show on Selfenrollment**:
- Key Usage**:
 - Digital Signature
 - Non repudiation
 - Key Encipherment
 - Data Encipherment
 - Key Agreement
- Extended Key Usage**:
 - Client Authentication
 - Email Protection
 - MS Smartcard Login
 - MS Encrypted File System
 - OID-1

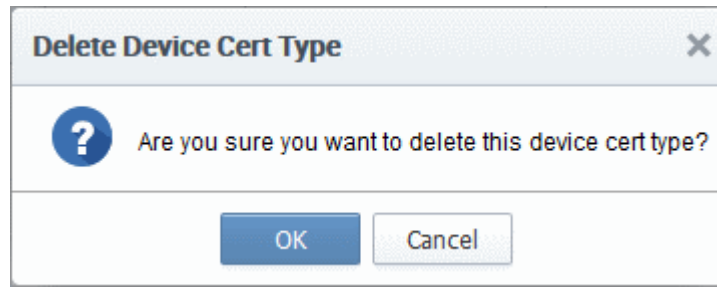
Buttons: OK, Cancel

The 'Edit Device Cert Type' dialog will be displayed. This is similar to the add device cert type form except a new 'Type ID' row which displays the auto-generated number for that cert type. This cannot be edited. Other fields can be edited and is similar to the [add new device cert type](#) form explained in the previous section.

- Click 'OK' after updating the details.

Certificates already issued and installed for this updated device cert type will not be affected. It will run its previously defined term.

To delete a device cert type, select it and click the 'Delete' button at the top. A confirmation dialog will be displayed.



- Click 'OK' to confirm

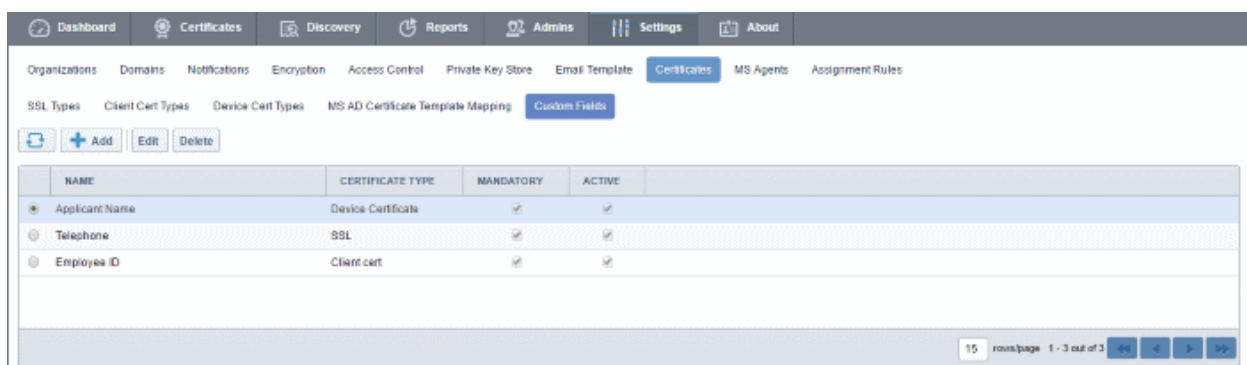
Certificates already issued and installed for this deleted device cert type will not be affected. It will run its previously defined term.

6.9.5 Custom Fields

An SSL, Client or a Device certificate has standard fields that contain information about the Owner, Domain, Organization, Department, Address and so on. Some businesses may wish to also track additional information such as 'Employee Code' or 'Telephone Number'. Comodo Certificate Manager allows customers to include such additional information by adding custom fields to enrollment forms.

MRAO administrators can add additional fields to the enrollment forms of both SSL and Client certificates. They can also specify whether the new fields should be mandatory or optional.

- Custom fields must be enabled for your account and can only be managed by MRAO administrators. Please contact your account manager if you would like to enable this feature.
- Once enabled, custom fields can be configured by clicking 'Settings' > 'Certificates' > 'Custom Fields'.
- MRAO administrators can configure the name of the field, the certificate type to which it should apply (SSL, client or device certificates), whether or not the field should be mandatory and whether or not the custom field should be active.
- Custom fields can be edited at any time. Deactivating a custom field will remove it from the enrollment forms but all associated data will be retained. However, deleting a field will delete all data associated with the field.
- Once added, the custom fields will appear on the enrollment and renewal forms for your certificates.



'Custom Fields' - Descriptions of Columns

| Column Name | Description |
|------------------|---|
| Name | Name of the custom field. |
| Certificate Type | The type of the certificate to which the custom field is applicable. Can be either 'SSL', 'Client Cert' or 'Device Cert'. |

| 'Custom Fields' - Descriptions of Columns | | |
|---|---------|--|
| Column Name | | Description |
| Mandatory | | Allows administrators to toggle between mandatory and optional states. If a field is made mandatory then the form cannot be submitted without completing the field. Mandatory fields will be marked with an asterisk* on the form. |
| Active | | Toggle the custom field between active and inactive states. If a field is made inactive, it will be hidden in the future application forms. However, existing data for this field will be retained in the database. |
| Control Buttons | Add | Allows the administrator to add a new custom field. |
| | Refresh | Updates the currently displayed list of custom fields. |
| Custom Field Control Buttons | Edit | Allows the administrator to edit the parameters of a particular custom field. |
| | Delete | Deletes the custom field. Unlike deactivation, deleting a field will also delete all data associated with this field. |

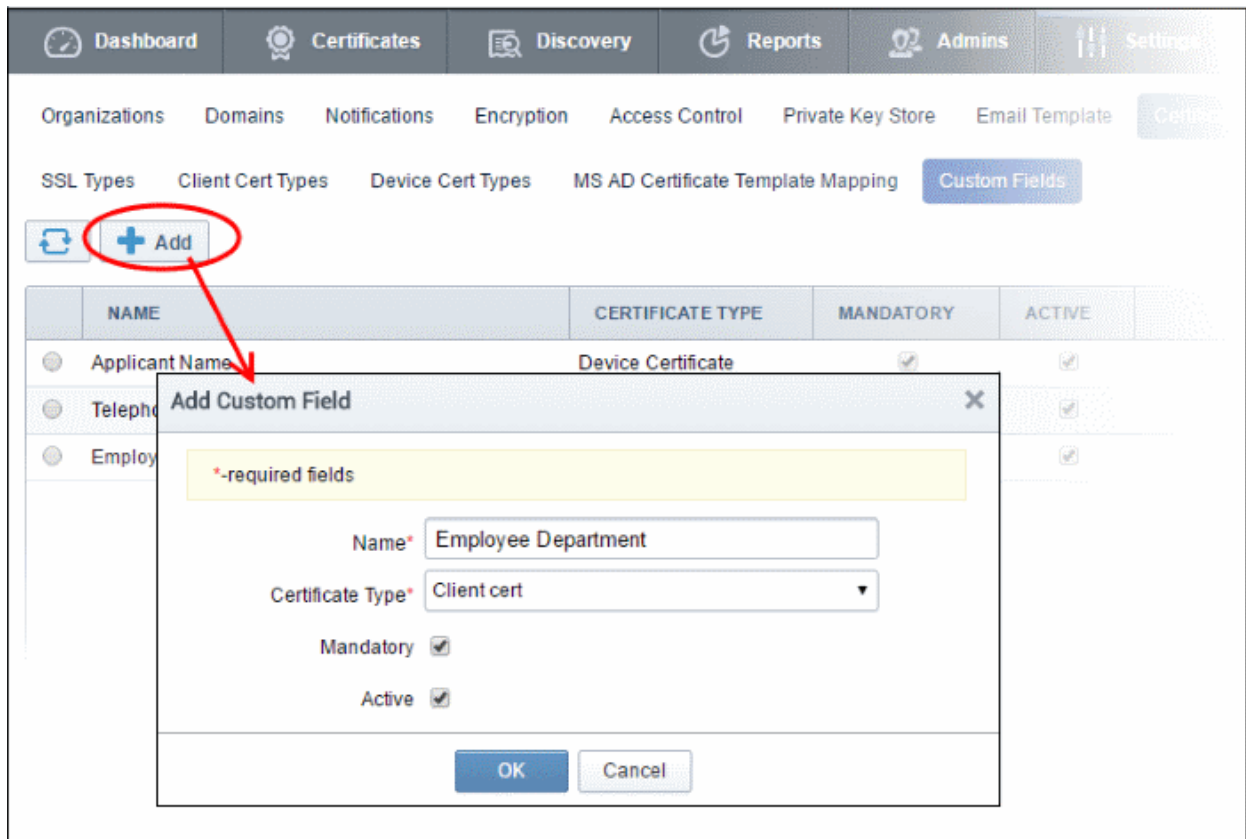
Note: Control buttons will appear only after selecting a particular custom field

6.9.5.1 Adding a new Custom Field

An MRAO administrator can add custom fields for SSL, Client and Device certificate types. The new fields will be displayed in the self-enrollment and built-in application forms of the chosen certificate type.

To add a new custom field

- Click 'Settings' > 'Certificates' > 'Custom Fields'
- Click the 'Add' button at the top of the interface. The 'Add Custom' Field dialog will appear.



Add Custom Field - Table of Parameters

| Field Name | Values | Description |
|------------------|----------------------|--|
| Name | String (required) | The name of the field to be added. (Max 256 characters). This will be the label of the field on the enrollment form. |
| Certificate Type | Drop-down (required) | Select the certificate type to which the new field should apply. |
| Mandatory | Check-box | Specify whether the field is mandatory or optional. |
| Active | Check-box | Activate or deactivate the field. Deactivating a custom field will remove it from the enrollment forms but all associated data will be retained. |

- After completing the 'Add Custom Field' dialog, click 'OK'. If you selected 'Active', the new field will be added to the application forms for the certificate type selected.

The total number of custom fields that you can add is specified by your Comodo account manager. If you reach the maximum permitted, the 'Add' button will not be displayed in the interface. Please contact your Comodo Account Manager, if you wish to have more fields added to your account.

Once a custom field is added, the field appears in both the self-enrollment form and the built-in application form for the selected certificate type.

As an example, the 'Built-in' and 'Self-enrollment' application forms for an SSL certificate are shown below. Both examples show two custom fields - 'Fax Number' and 'Telephone'.

Built-in Enrollment Form

Request New SSL Certificate

*required fields

Organization* Okakayanibud

Department* ANY

[Click here to edit address details](#)

Certificate Type* Instant SSL

Certificate Term* 1 year

Server Software* AOL

CSR

Provide CSR Autogenerate CSR and Manage Private Key

CSR*

Max CSR size is 32K

Certificate Parameters

Common Name*

Requester John Smith

External Requester

Comments

Telephone

Fax*

Subscriber Agreement

1 Comodo ePKI Certificate Manager Agreement – EV Enabled THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS. IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON 'I ACCEPT' BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND

I agree.* Scroll to bottom of the agreement to activate check box.

Self-Enrollment Form

COMODO
Certificate Manager

SSL Enrollment

Access Code* ●●●●●●

Email* admin@coradithers.com

[Click here to edit address details](#)

Certificate Type* Instant SSL

Certificate Term* 1 year

Server Software* AOL

CSR*

Max CSR size is 32K

Common Name*

Please provide a Self Enrollment Passphrase. A passphrase is necessary for certificate revocation and renewal.

Self Enrollment Passphrase:

Re-type Self Enrollment Passphrase:

Comments:

Fax*

Telephone:

Subscriber Agreement

1 Comodo ePKI Certificate Manager Agreement – EV Enabled THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS. IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE MANAGER ACCOUNT OR THE CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR, ACCESSING, OR PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR ACCESSING CERTIFICATE MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON 'I ACCEPT' BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

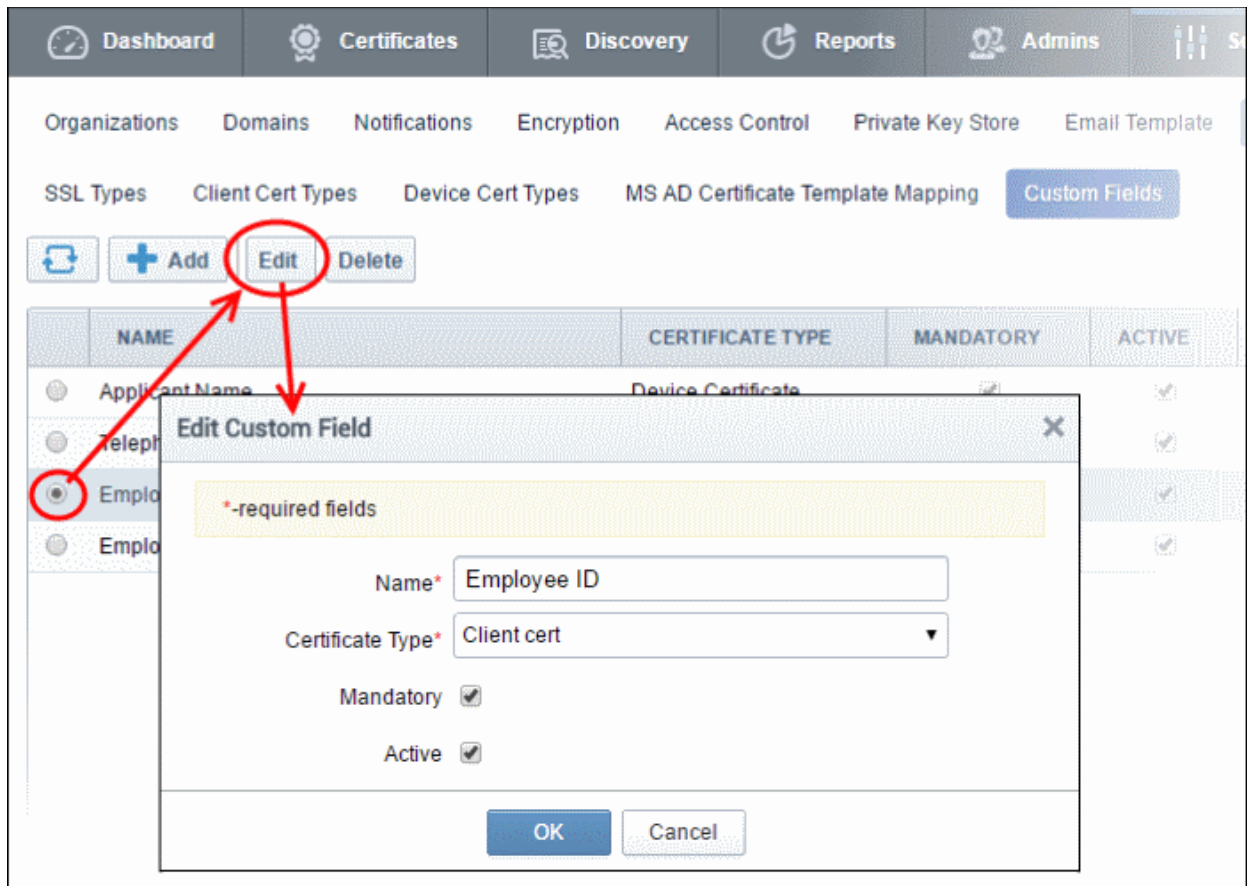
I Agree.* Scroll to bottom of the agreement to activate check box.

Note: The added custom fields will be available in the Built-in and Self Enrollment forms for both SSL and Client certificate types and will not be available for enrollment of certificates through Web API.

6.9.5.2 Editing an Existing Custom Field

- Select the field and click the 'Edit' button located at the top of the interface

The 'Edit Custom' Field dialog will appear.



The dialog fields are explained in [Add Custom Field](#)

6.9.5.3 Removing an Existing Custom Field

If a custom field turns out to be unnecessary, administrators can remove the field in two ways:

- [Disabling the field](#)
- [Deleting the field](#)

In general, Comodo recommends disabling rather than deleting a custom field. That way, all associated data will be retained and you can always re-insert the field at a later date if required. If you find that you can no longer add new custom fields, it is because you have reached the maximum number of fields permitted for your account. However, this is easily overcome by contacting your Comodo account manager and requesting more fields are added to your account.

Disabling the field

- Open the [Edit Custom Field](#) dialog
- Deselect the 'Active' check box and click OK.

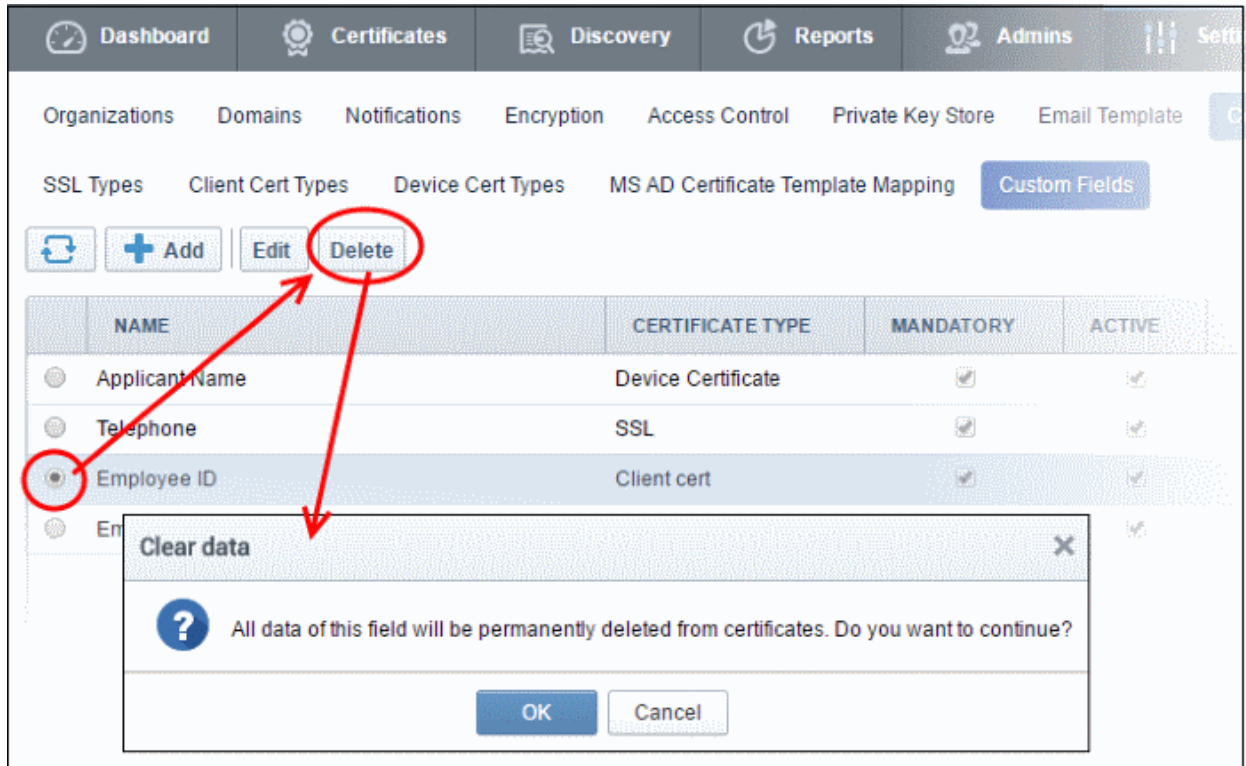
MRAO Administrators can deselect the 'Active' box to disable a field. If a field is made inactive, it will not be displayed in future application forms but the existing data relevant to the field will be retained in the database. The administrator cannot add a new custom field to replace the inactive field if the maximum number of fields has been reached. Disabling a field allows administrators to re-insert the field at a later date.

Deleting the field

MRAO Administrators can delete a field if it is not going to be used in future. All previously stored data associated with the deleted field will be removed from the database. If a field is deleted, administrators can replace it with a new custom field.

To delete a field

- Click 'Settings' > 'Certificates' > 'Custom Fields' to open the Custom Fields interface.
- Select the field and click the 'Delete' button located at the top of the interface



- Click 'OK' to confirm.

The field will be removed.

6.10 Mapping MS AD Certificate Templates to CCM Certificate Types

The 'MS AD Certificate Template Mapping' interface allows admins to map templates to private CA certificate types.

CCM can issue private certificates with custom parameters by mapping CCM certificate types to custom Active Directory certificate templates. Custom parameters include key usage, extended key usages, key sizes, validity period and so on.

- Open the mapping interface by clicking 'Settings' > 'Certificates' > "MS AD Certificate Template Mapping"

| MS AD CERTIFICATE TEMPLATE | MS TEMPLATE KEY USAGE | MS TEMPLATE EXTENDED KEY USAGE | CERTIFICATE TYPE |
|--|----------------------------------|--|--------------------|
| <input type="radio"/> Computer | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.2;1.3.6.1.5.5.7.3.1 | Device Certificate |
| <input type="radio"/> Workstation Authentication | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.2 | Device Certificate |
| <input type="radio"/> CCM web server | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.1 | SSL |
| <input type="radio"/> CCM Administrator | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.2;1.3.6.1.5.5.7.3.4;1.3.6.1.4.1.311.10 | Client cert |
| <input type="radio"/> CCM User | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.2;1.3.6.1.5.5.7.3.4;1.3.6.1.4.1.311.10 | Client cert |

- Domain administrators can create certificate templates with custom parameters and values on their AD server
- CCM Administrators can map these templates to a certificate type through the CCM interface.
- Domain administrators can then apply for a custom certificate from their AD server by selecting the certificate template mapped to a CCM certificate type.
- CCM will issue a certificate with parameters as configured in the mapped templates

Notes:

- The MS Agent should have been installed on the AD server of the Organization/Department from which the templates are to be mapped. The agent should have been configured to act as CA Proxy. Refer to the section **MS Agents for AD server Integration** for more details on installation and configuration of MS Agent.
- Private certificates should be enabled for your account in order to map them to MS AD templates. Please contact your account manager to enable private certificates for your account.
- Certificate types with mapped templates can only be enrolled for through an AD server using the certificate enrollment service or a group enrollment policy.
- For SSL Certificates - CCM currently only supports MS AD template mapping for the 'Private UCC SSL' certificate type. Other private CA certificate types will be enabled for template mapping in future versions.
- For Device Certificates - Administrators can request their account manager to add private CA's to their account and create device certificate types as required from 'Settings' > 'Certificates' > 'Device Certificate Types'. Refer to section **Adding Device Cert Types** for more details. These device certificate types can be mapped to MS AD certificate templates.

The following sections explain more about:

- **Configuring Custom MS AD Certificate Template on AD Server**
- **The 'MS AD Certificate Mapping' Area**

- [Adding MS AD Certificate Template to CCM](#)
- [Editing MS AD Certificate Template](#)
- [Deleting MS AD Certificate Template](#)

6.10.1 Configuring Custom MS AD Certificate Templates on AD server

Active Directory (AD) domain administrators can create custom certificate templates on their AD server for mapping to private certificate types in CCM. Templates can be created for SSL, Client and Device certificate types.

This section explains how AD Domain administrators can create certificate templates.

Prerequisite: The MS Agent should have been installed on the AD server of the Organization/Department from which the templates are to be mapped. The agent should have been configured to act as CA Proxy. Refer to the section [MS Agents for AD server Integration](#) for more details on installation and configuration of MS Agent.

To create a certificate template

- Open the Microsoft Management Console (MMC) on the server by entering 'mmc' in the 'Run' dialog
- Click 'File' and choose 'Add/Remove Snap-in'

The 'Add or Remove Snap-ins' dialog will appear.

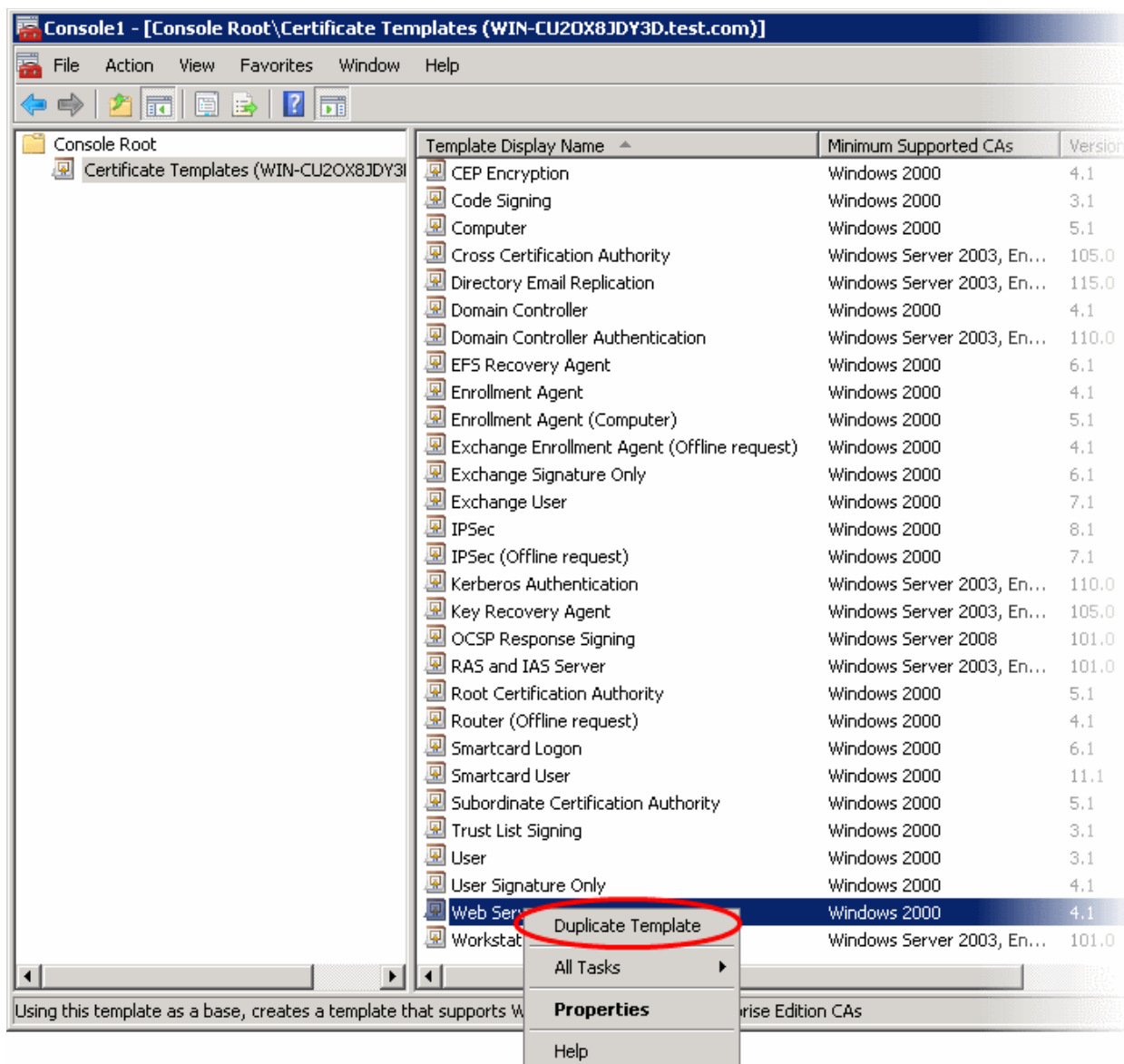
- Choose 'Certificate Templates' from the list of 'Available snap-ins' on the left then click the 'Add' button
- Click 'OK'

The Certificate Template snap-in will be added to the console.

- Expand the Certificate Templates to view existing templates

You can create a new template by cloning an existing template and editing its parameters.

- Right-click on the template you wish to clone and choose 'Duplicate Template'



- Enter a name for the new template in the properties dialog:

Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Cryptography | Subject Name

Template display name:
CCM Web Server

Minimum Supported CAs: Windows Server 2008

After you apply changes to this tab, you can no longer change the template name.

Template name:
CCMWebServer

Validity period: 2 years | Renewal period: 6 weeks

Publish certificate in Active Directory
 Do not automatically reenroll if a duplicate certificate exists in Active Directory

For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

OK | Cancel | Apply | Help

- Configure the validity and renewal periods for the new template based on the certificate type. You can also configure other parameters by clicking the different tabs. Guidance on configuring the parameters is available in the Microsoft Technet Library page [https://technet.microsoft.com/en-us/library/cc725621\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc725621(v=ws.10).aspx).
- Click 'Apply' to save your changes
- Click 'OK' to save the new template

The new template will be available for selection for mapping to a required certificate type in the CCM interface. Refer to the section **Adding MS AD Certificate Template Mapping** for more details.

Once mapped, domain administrators can enroll for certificates from CCM by selecting the respective certificate template from AD Certificate Enrollment Service or by creating a group enrollment policy. CCM will issue the certificate(s) in accordance with the parameter set forth in the mapped template. All certificates issued can be managed from the CCM interface.

6.10.2 The 'MS AD Certificate Mapping' Area

The 'MS AD Certificate Template Mapping' area allows admins to add certificate templates on an AD server to CCM and map appropriate certificate types to them. Templates can also be updated or deleted later on if not required.

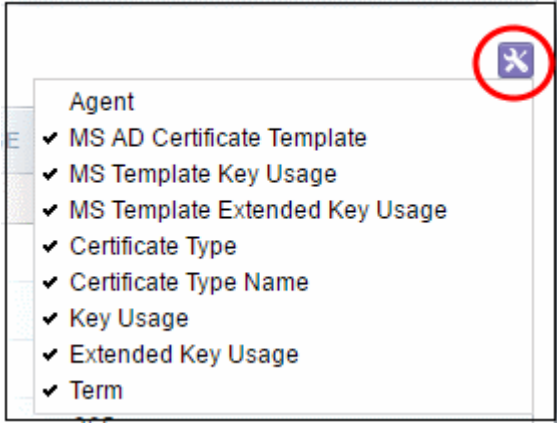
To open the interface, click 'Settings' > 'Certificates' > 'MS AD Certificate Template Mapping':

The screenshot shows the 'MS AD Certificate Template Mapping' section in the Comodo Certificate Manager. It features a filter section with 'Add Filter' and 'Group by: Agent' options. Below the filter is a table with columns: MS AD CERTIFICATE TEMPLATE, MS TEMPLATE KEY USAGE, MS TEMPLATE EXTENDED KEY USAGE, CERTIFICATE TYPE, CERTIFICATE TYPE NAME, KEY USAGE, EXTENDED KEY USAGE, and TERM. The table lists several entries under 'Agent 51', including 'CCM web server', 'CCM Administrator', 'CCM User', 'Prep Copy Web Server', 'Demo Web Server', and 'Workstation Authentication'.

MS AD Certificate Template Mapping Area - Table of Parameters

| Fields | Values | Description |
|--------------------------------|----------------|--|
| MS AD Certificate Template | String | Name of the certificate template in the AD server |
| MS Template Key Usage | String | Key usage defined in the certificate template |
| MS Template Extended Key Usage | Numeric | Extended key usage defined in the certificate template |
| Certificate Type | String | Certificate type configured for the certificate template |
| Certificate Type Name | String | Name of the certificate type configured for the certificate template |
| Key Usage | String | Key usage defined for the certificate |
| Extended Key Usage | String/Numeric | Extended key usage defined for the certificate |
| Term | Numeric | The validity period of the certificate |

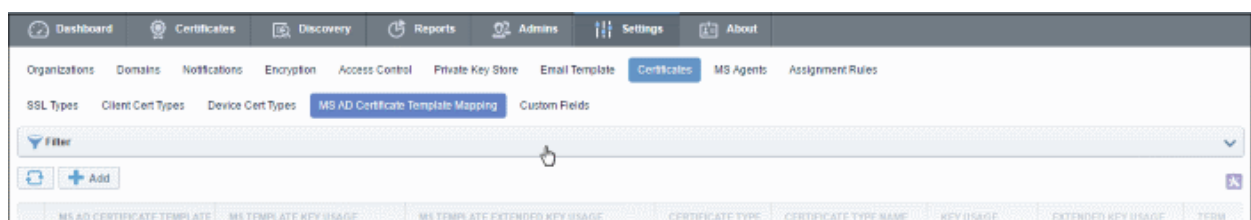
Note: An administrator can select the columns to be displayed in the table from the drop-down at the right end of the table header:

| MS AD Certificate Template Mapping Area - Table of Parameters | | |
|---|--|---|
| Fields | Values | Description |
| |  | |
| Control Buttons Note: The 'Edit' and 'Delete' control buttons appear only on selecting a certificate template | Add | Allows MRAO admins to add a mapped certificate template on an AD server to CCM. |
| | Refresh | Refreshes the list |
| | Edit | Allows administrators to modify the certificate type for the certificate template |
| | Delete | Deletes the mapped certificate template from the list |

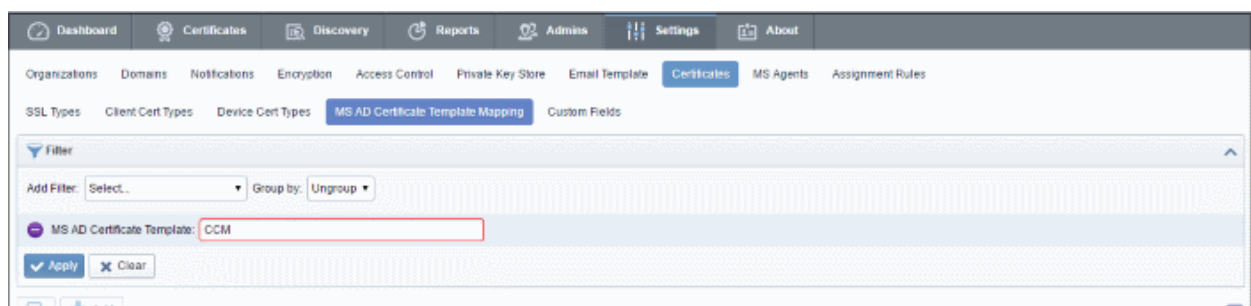
Sorting and Filtering options

- Click the "MS AD Certificate Template" and "Term" column headers to sort items in alphabetical, ascending or descending order.

Administrators can search for a particular certificate template by using the filters.



To apply filters, click anywhere on the 'Filters' stripe. You can add filters by selecting from the 'Add Filter' drop-down. You can also search for filters by template name.



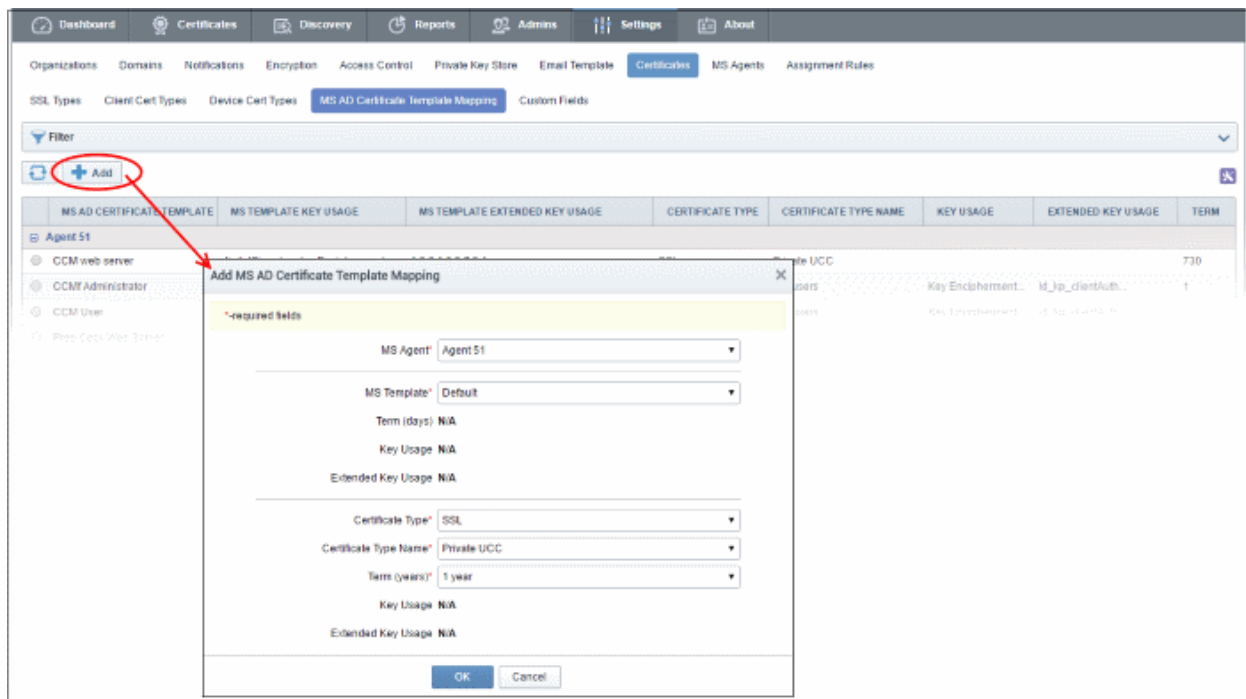
To remove the filters, click the 'Clear' button.

Note: Search filters will be automatically saved. When you reopen the 'Organizations' interface in future, the configured filters will be in effect and filtered results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

6.10.3 Adding MS AD Certificate Template Mapping

MRAO administrators can add certificate templates from AD servers to CCM in order to define a certificate type for that template.

To add a certificate template to CCM, click 'Settings' > 'Certificates' > 'MS AD Certificate Template Mapping' and click the 'Add' button.



| Form Element | Type | Description |
|-------------------------------|----------------|---|
| MS Agent <i>(required)</i> | Drop-down list | The drop-down lists MS agents found on AD servers. Select the agent that you want to map with CCM for the template. |
| MS Template <i>(required)</i> | Drop-down list | The drop-down lists certificate templates found on the AD server. Select the template that you have configured and mapped as explained in ' Configuring MS AD Certificate Template to CCM Certificate Types '. |
| Term | Text Field | The validity period of the certificate as defined in the selected template. |
| Key Usage | Text Field | Details of key usage defined in the selected template |
| Extended Key Usage | Text Field | Details of extended key usage defined in the selected template |
| Certificate Type | Drop-down list | Available certificate categories are SSL, Client and Device. The certificate types are as configured on CCM . <ul style="list-style-type: none"> SSL - Currently only Private UCC is available. Other private CA certificate types will be enabled for template mapping in future versions. Client Cert - All client cert types available for your account. See |

| Form Element | Type | Description |
|-----------------------|----------------|--|
| | | <p>'Client Cert Type' for more details.</p> <ul style="list-style-type: none"> Device Cert - All private device cert types added to your account. See 'Device Cert Types' for more details. |
| Certificate Type Name | Drop-down list | Certificate sub-type. The certificates available in this drop-down are determined by the 'Certificate Type' chosen in the field above. |
| Term | Drop-down list | The terms configured for the selected sub-type in CCM. |
| Key Usage | Text Field | The key usage of the certificate sub-type as defined in CCM |
| Extended Key Usage | Text Field | The extended key usage of the certificate as defined in CCM |

- Click 'OK' after configuring the certificate type for the selected template.

6.10.4 Editing MS AD Certificate Template

An existing AD certificate template can be updated at any time per your requirements.

To update a certificate template:

- Go to 'Settings' > 'Certificates' > 'MS AD Certificate Template Mapping'
- Select a template from the list
- Click the 'Edit' button

The screenshot shows the 'Edit MS AD Certificate Template Mapping' dialog box. The left-hand menu has a list of 'MS AD CERTIFICATE TEMPLATE' items: CCM web server, CCM Administrator, CCM User, Prep Copy Web Server (selected), Demo Web Server, Workstation Authentication, and Computer. The 'Edit' button in this menu is circled in red, with a red arrow pointing to the 'Edit' button in the dialog box. The dialog box contains the following fields:

- MS Agent* Agent 51
- MS Template* Prep Copy Web Server
- Term (days) 730
- Key Usage digitalSignature, keyEncipherment
- Extended Key Usage 1.3.6.1.5.5.7.3.1
- Certificate Type* SSL
- Certificate Type Name* Private UCC
- Term (years)* 1 year
- Key Usage N/A
- Extended Key Usage N/A

Buttons for 'OK' and 'Cancel' are at the bottom of the dialog box.

- The 'Edit' form is similar to the 'Add MS AD Certificate Template Mapping' form except the MS Agent is non-editable. See the previous section, 'Adding MS AD Certificate Templates', for details about the

- parameters.
- Click 'OK' to save your changes.

6.10.5 Deleting MS AD Certificate Template

A certificate template can be deleted from the list when it is no longer required.

To delete a certificate template:

- Go to 'Settings' > 'Certificates' > 'MS AD Certificate Template Mapping'
- Select a template from the list.
- Click the 'Delete' button

The screenshot shows the 'MS AD Certificate Template Mapping' page in the Comodo Certificate Manager. The 'Delete' button is circled in red, and a red arrow points to it. A modal dialog box titled 'Certificate Manager' is open, asking 'Are you sure?' with 'OK' and 'Cancel' buttons. The 'Computer' template is selected in the table below.

| MS AD CERTIFICATE TEMPLATE | MS TEMPLATE KEY USAGE | MS TEMPLATE EXTENSION |
|--|----------------------------------|-------------------------|
| <input type="radio"/> CCM web server | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.1 |
| <input type="radio"/> CCM Administrator | | 1.3.6.1.5.5.7.3.2;1.3.6 |
| <input type="radio"/> CCM User | | 1.3.6.1.5.5.7.3.2;1.3.6 |
| <input type="radio"/> Prep Copy Web Server | | 1.3.6.1.5.5.7.3.1 |
| <input type="radio"/> Demo Web Server | | 1.3.6.1.5.5.7.3.1 |
| <input type="radio"/> Workstation Authentication | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.2 |
| <input checked="" type="radio"/> Computer | digitalSignature;keyEncipherment | 1.3.6.1.5.5.7.3.2;1.3.6 |

- Click 'OK' to confirm removal.

6.11 Email Templates

CCM can send automatic email notifications to certificate applicants, administrators and end-users upon events like certificate updates, approvals, collection and revocation etc. Notifications are set by administrators in the **Notifications** area. The 'Email Templates' area allows MRAO administrators to customize the content of the email templates.

Security Roles:

- MRAO - Can view and edit email notification templates for any certificate type for any Organization or Department.
- RAO Administrators - Cannot view the Email Templates area. They can, instead, edit email templates for their Organization by clicking the 'Edit' button in the Organizations area ('Settings' > 'Organizations' > 'Edit')
- DRAO Administrators - Cannot view the Email Templates area. They can, instead, edit email templates for their Department by clicking the 'Edit' button in the Departments area ('Settings' > 'Organizations' > 'Edit')

| NAME |
|---|
| <input type="radio"/> Email Invitation |
| <input type="radio"/> Email Validation |
| <input type="radio"/> Client Certificate Revoked (by admin) |
| <input type="radio"/> Client Certificate Revoked (by user) |
| <input type="radio"/> Client Certificate Expiration |
| <input type="radio"/> SSL Enrolled |
| <input type="radio"/> SSL Awaiting Approval |
| <input type="radio"/> SSL Approved |
| <input type="radio"/> SSL Declined |
| <input type="radio"/> SSL Issuance Failed |
| <input type="radio"/> SSL Revoked (by admin) |
| <input type="radio"/> SSL Revoked (by user) |
| <input type="radio"/> SSL Expiration |
| <input type="radio"/> SSL Certificated Installed Remotely |
| <input type="radio"/> Discovery Scan Summary |

The name column lists the types of automated email notifications sent on different stages.

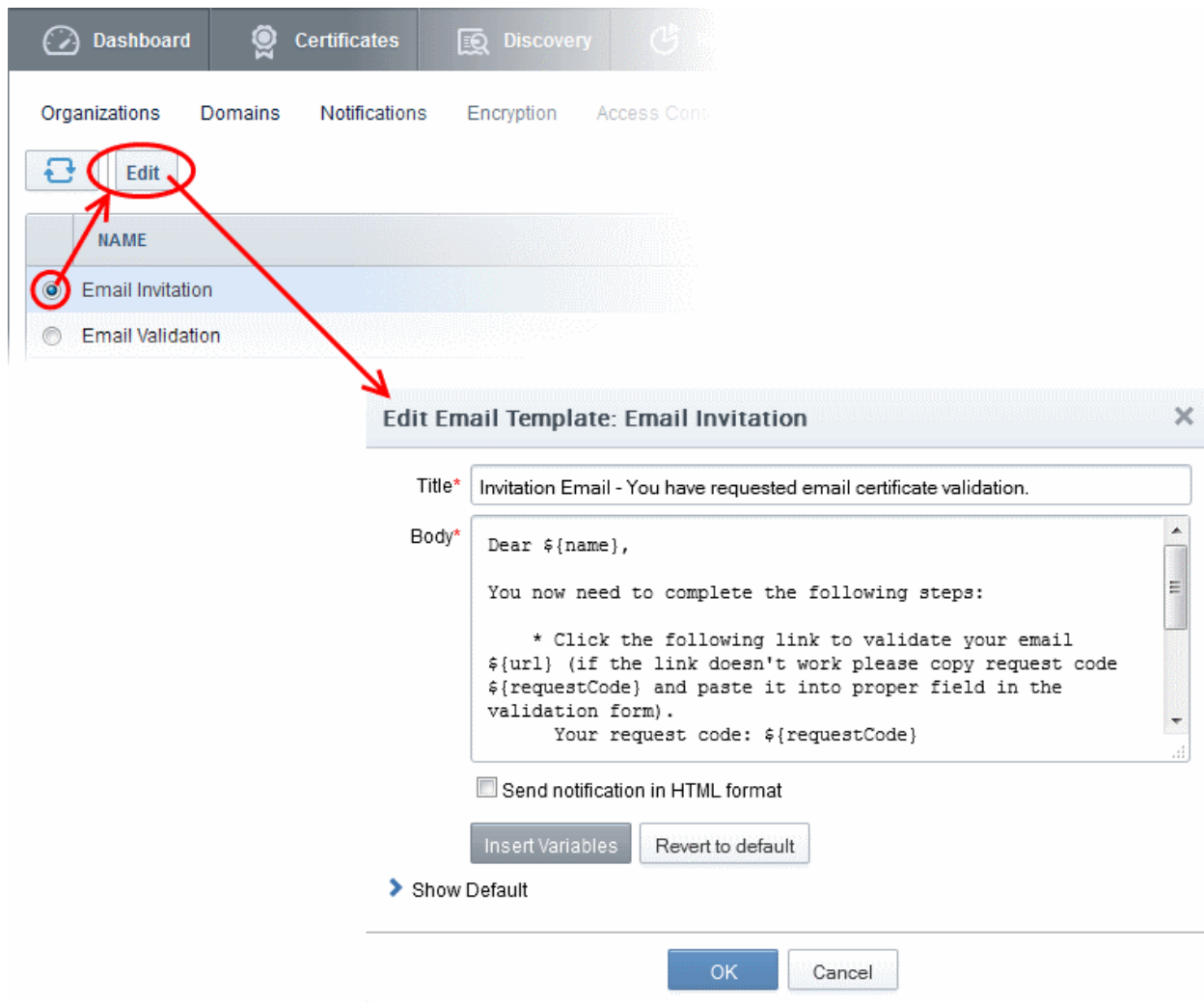
6.11.1 Viewing and Editing the Email Templates

Administrators can view and edit the email template messages from the 'Edit Email Template' dialog.

To view and edit email template message

- Select the email template
- Click the 'Edit' button from the top

The 'Edit Email Template' dialog will open. An example is shown below.

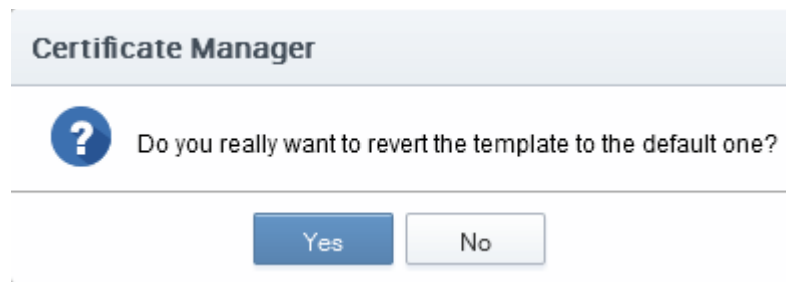


The 'Title' field displays the subject line of the email to be sent. The 'Body' field contains the body content of the email message. The body content contains the text portions and the variables which will be replaced with the exact values from the details of the corresponding certificate/domain while sending the email automatically. The dialog allows the administrator to directly customize the content and add or remove the variables according to the need.

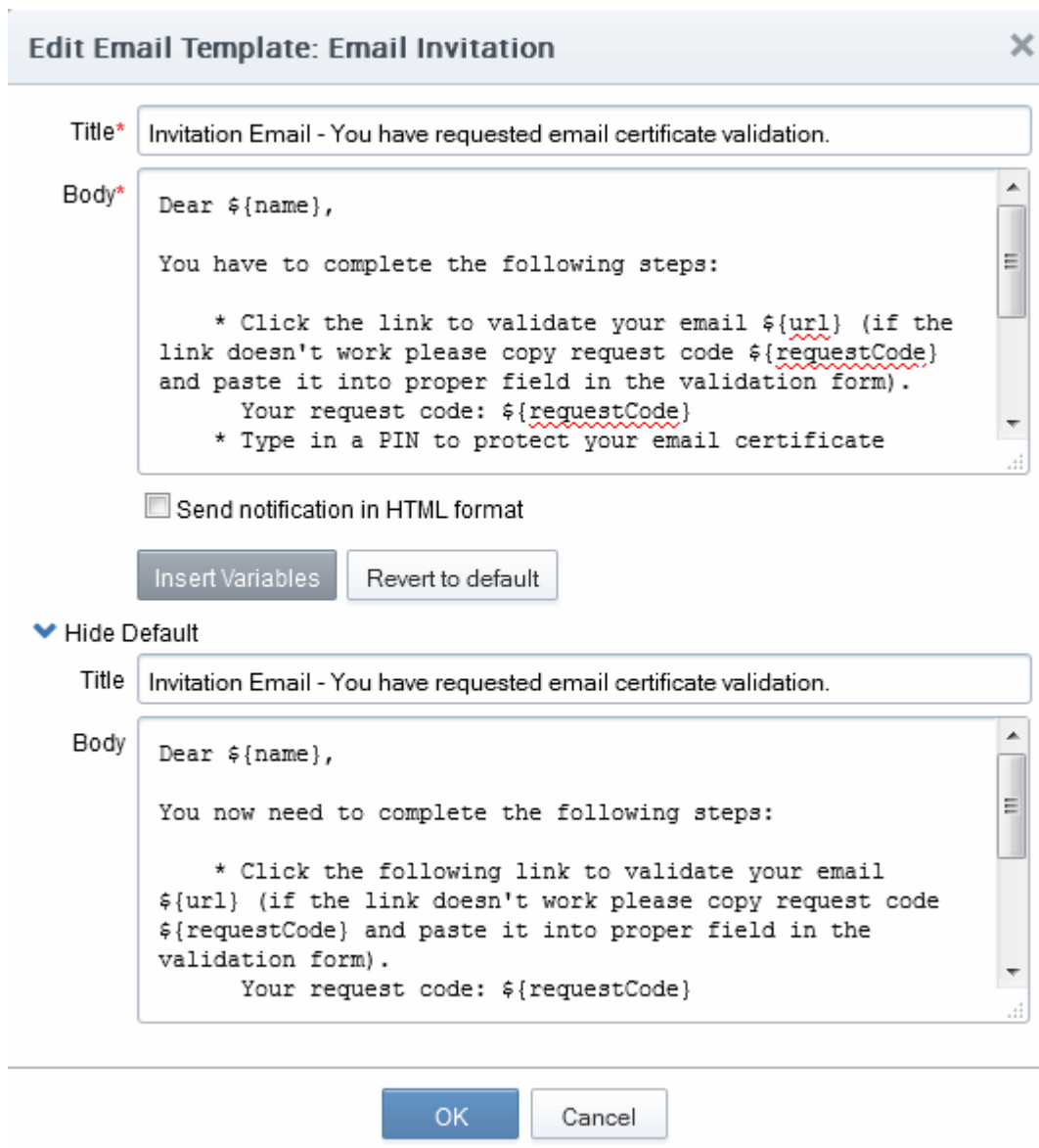
- Selecting the checkbox 'Send notification in HTML format' will send automated email notifications to administrators, applicants and end-users in HTML format.
- Clicking 'Insert Variables' will display a list of the variables used in the specific template. The administrator can select the variable to be inserted into the content from the list. This is useful if the administrator has accidentally deleted variable(s) which are essentially required in the template.



- Clicking 'Revert to default' enables the administrator to reset to the default content as shipped with CCM.



- Clicking 'Show Default' will display the default content for administrator to refer.



6.12 MS Agents for AD server Integration

Administrators can add Active Directory servers to CCM in order to fetch certificates installed on servers, devices and endpoints, and for provisioning Device Authentication Certificates.

Comodo Certificate Manager uses MS Agents for certificate discovery and provisioning device certificates:

Certificate Discovery

Administrators should download the MS agent from 'Settings' > 'MS Agents' and install it on each AD server they wish to manage. Once installed, the agent periodically scans the server, fetches the network/object structure, detects all certificates on the domain, then forwards these details to the CCM server. The results can be viewed from the Discovery > Network Assets interface. Refer to the section **Active Directory** for more details.

Provisioning of Device Authentication Certificates

MS agents installed on AD servers also act as a CA proxy. To provision device authentication certificates, the AD server must have a Network Device Enrollment Service (NDES) server integrated and a Group Policy which will enroll Device certificates for devices added to AD. Once done, the MS agent will receive certificate requests and forward them to CCM. The agent will track all orders and, after the Device Certificate has been issued by CCM, will fetch the certificates and forward it to the NDES server. The NDES server, in turn, will forward the certificates to the devices. Refer to **The Device Certificates Area** for more details.

Note: In order for the MS agent to act as CA proxy, the CA Proxy role must be enabled during its installation.

Mapping MS AD Certificate Templates to CCM Certificate Types

MS agents installed on AD servers allow templates on the server to be mapped with CCM certificate types, enabling CCM to act as a Private CA for an Organization/Department. Domain admins can create custom certificate templates on their server as required and request CCM admins to map these templates to private certificate types. Domain administrators can enroll for certificates from the AD server by selecting the respective template.

Note:

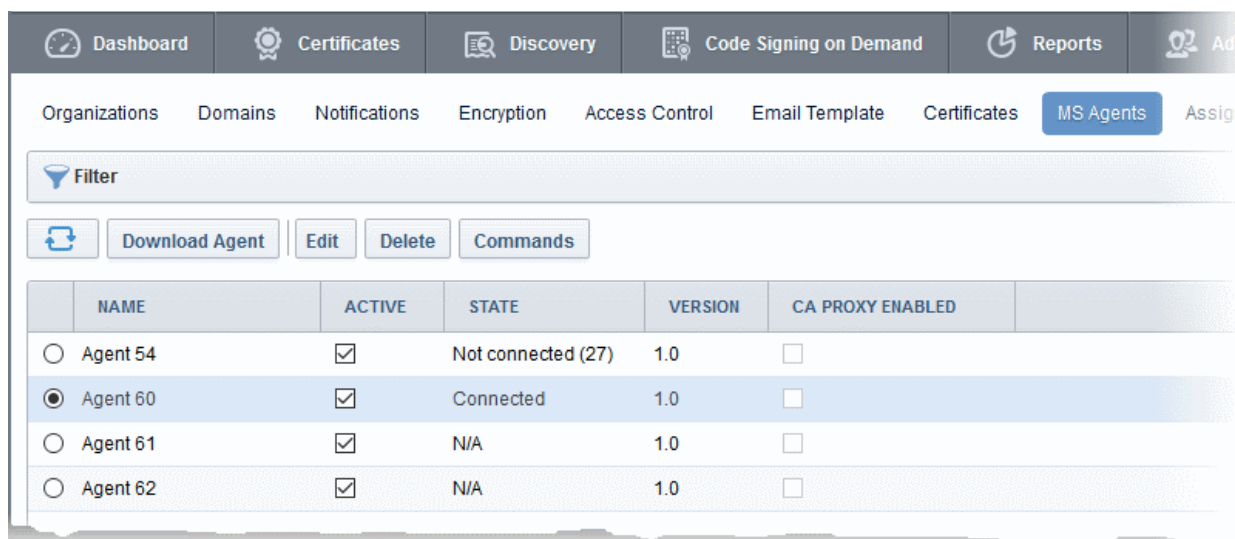
- The MS Agent should have been installed on the AD server of the Organization/Department from which the templates are to be mapped. The agent should have been configured to act as CA Proxy. Refer to the section **MS Agents for AD server Integration** for more details on installation and configuration of MS Agent.
- Private certificates should be enabled for your account in order to map them to MS AD templates. Please contact your account manager to enable private certificates for your account.
- For SSL Certificates - CCM currently only supports MS AD template mapping for the 'Private UCC SSL' certificate type. Other private CA certificate types will be enabled for template mapping in future versions.
- For Device Certificates - Administrators can request their account manager to add private CA's to their account and create device certificate types as required from 'Settings' > 'Certificates' > 'Device Certificate Types'. Refer to section **Adding Device Cert Types** for more details. These device certificate types can be mapped to MS AD certificate templates.

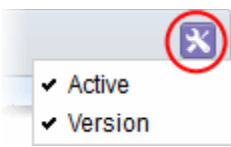
Security Roles:

- MRAO - Can add AD servers of any Organization/Department.

The MS Agent Interface

- To open the MS Agent interface, click the 'Settings' tab and choose the 'MS Agents' sub-tab



| Column Header | Description | |
|--|--|---|
| Name | Name of the MS Agent. | |
| Active | Indicates whether or not the agent is active. Administrators can change the state if required. | |
| State | Displays whether or not the agent is connected to CCM. | |
| Version | Displays the version number of the MS Agent. | |
| CA Proxy Enabled | Indicates whether the MS agent is enabled as a CA proxy to receive device certificate requests from the NDES server. | |
| <p>Note: Administrators can enable or disable the columns as desired, from the drop-down button at the right end.</p>  | | |
| Controls | Download Agent | Allows admins download and create a new MS Agent for installation on to an AD server that you wish to integrate. |
| | Refresh | Updates the list of agents. |
| Agent Controls | Edit | Enables administrators to modify the agent configuration settings. |
| | Delete | Removes the agent. |
| | Commands | Enables administrators to view commands executed by the agent. Commands include configuration updates and scanning the AD server. |

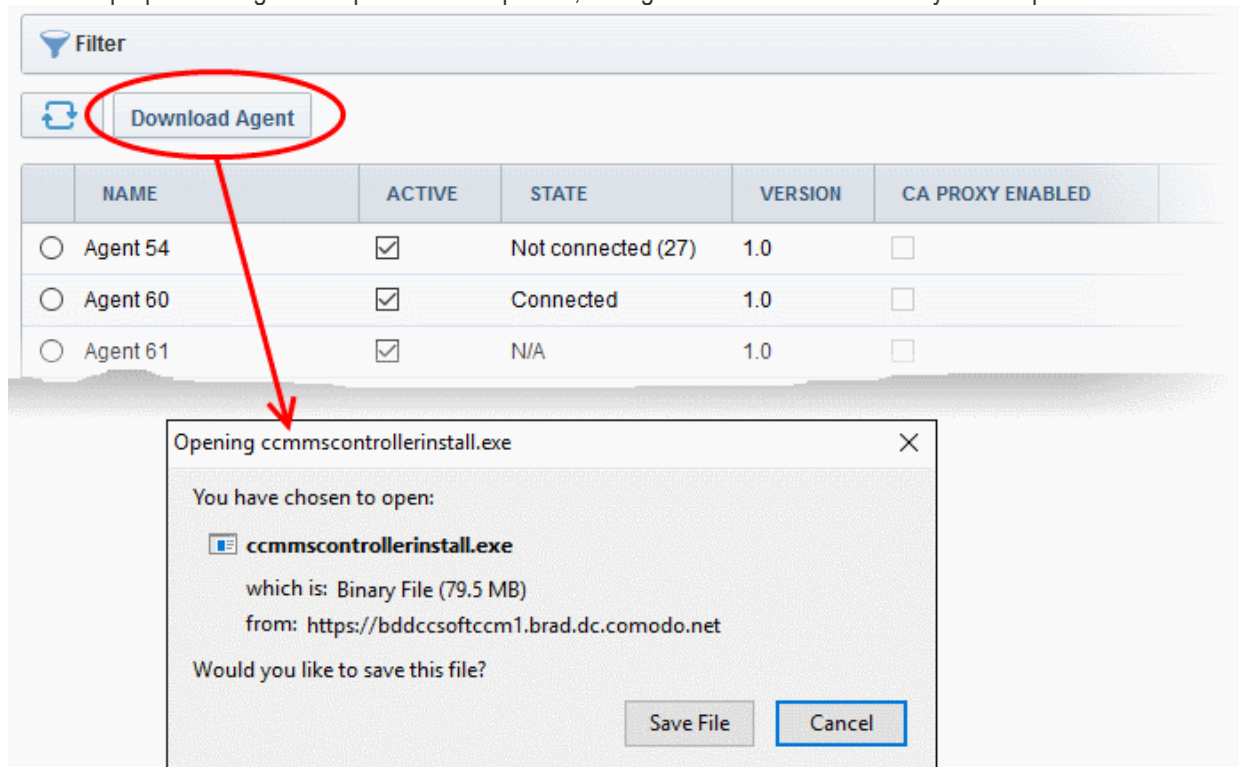
Configuring the MS Agent for Certificate Discovery through AD server

You can integrate an AD server to CCM by installing the MS agent on the server.

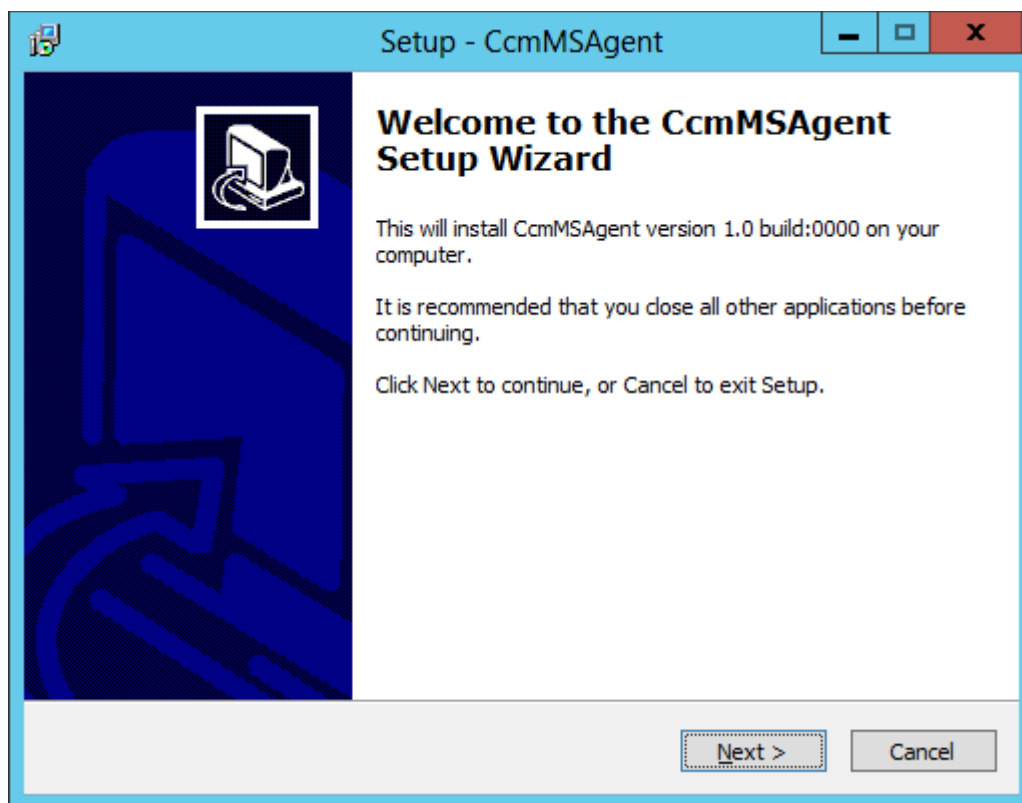
To download and install the MS Agent

- Click the 'Settings' tab and choose the 'MS Agent' sub-tab
- Click the 'Download Agent' button

CCM will prepare the agent setup file. On completion, the agent will be downloaded to your computer.

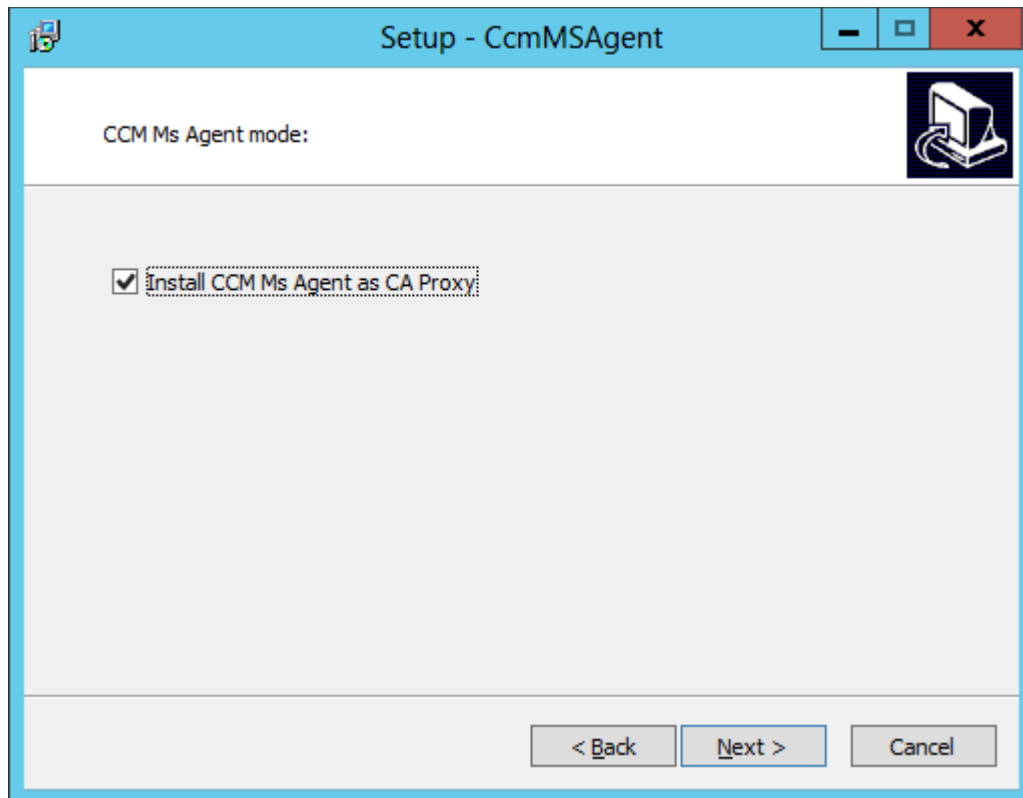


- Download the agent, transfer it to the AD server.
- Double click on the setup file to start the installation wizard and follow the wizard.

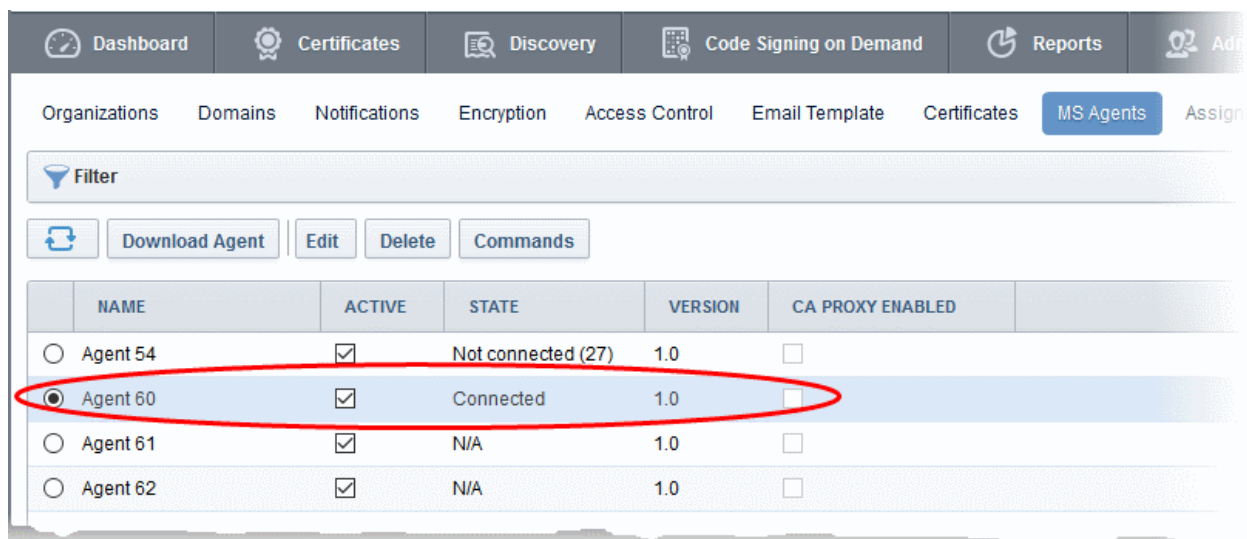


- Click 'Next' and follow the wizard

- If you want to enable the agent as a CA Proxy, for Device Certificates enrollment through NDES, in addition to discovery of certificates, then select 'Install CCM MS Agent as CA Proxy' in Step 2 of the wizard and continue the installation.



- On completion of installation, the Agent will be added to the CCM interface.



The next step is to configure the Agent to scan the server and forward the details to CCM.

- To Edit the Agent Properties, click the 'Edit' button at the top after selecting the Agent

The screenshot shows the 'Edit Agent' dialog box with the 'Common' tab selected. A yellow highlight is under the '*-required fields' label. The form contains the following fields and values:

- Name*: Agent 60
- Domains to Scan: Enter domains to scan
- Max Depth of the Scan: 0
- Version: 1.0
- IP address: 10.108.51.242
- Active:
- Auto update: Disabled
- CA proxy: Enabled
- Secret Key (min 10 symbols)*: JPOqeS8CcsZGrkKyUd5h
- Organization*: Dithers Organization
- Department: None
- Term: 1 year
- Comments: (empty text area)

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

The 'Edit Agent' dialog has two tabs:

- **Common** - Allows you to configure General Properties
- **Schedule** - Allows you to schedule the agent to scan the server and forward the details

General Properties:

| Edit Agent > Common Tab - Table of Parameters | | |
|---|-----------------------|---|
| Field Name | Type | Description |
| Name | <i>String</i> | Displays the name of the agent. The administrator can to edit the name of the Agent. |
| Domains to Scan | <i>String</i> | Allows the administrator to enter the Active Directory domains to be scanned. |
| Max Depth of the Scan | <i>String</i> | Select the number of network hierarchy levels to be scanned. The depth of the scan should cover all required endpoints/users and other AD objects in the network. |
| Version | | Displays the version number of the MS Agent. |
| IP Address | <i>Text box</i> | Displays the IPv6 Loopback address, IPv4 loopback address, IPV6 IP Address, IPv4 IP Address or the physical address of the server on which the agent is installed |
| Active | <i>Checkbox</i> | Enables the Administrator to set the Agent in active state or inactive state. |
| Auto update | <i>String</i> | Indicates whether the agent is enabled for auto update |
| CA proxy | String | Indicates whether the agent is enabled as a CA Proxy to forward device certificate requests from the NDES server to CCM. |
| Secret Key | <i>String</i> | Displays the secret key generated by the Agent to authenticate itself to Remote Comodo CM server. The administrator can copy and save the secret key in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server, to authenticate itself to the CCM server for scanning the same internal network. |
| Organization | <i>Drop-down list</i> | Enables administrators to change the Organization associated the Agent. |
| Department | <i>Drop-down list</i> | Enables administrators to change the Department associated with the Agent. |
| Term | <i>Drop-down list</i> | Allows administrators to choose the validity period for the agent. |
| Comments | <i>String</i> | Enables the Administrator to type a descriptive comment on the purpose of the Agent |

- Edit the values if required. To set a scan schedule for the agent, click the 'Schedule' tab.

Schedule

The screenshot shows the 'Edit Agent' dialog box with the 'Schedule' tab selected. The 'Scan Frequency' section contains three fields: 'Frequency' (Manual), 'Time zone' (UTC+05:30 - IST, SLT), and 'Time' (16 : 03). The 'OK' button is highlighted in blue.

Edit Agent > Schedule Tab - Table of Parameters

| Field Name | Type | Description |
|------------|-----------|---|
| Frequency | Drop-down | Allows the administrator to choose the frequency at which the scans are to be run. The available options are: <ul style="list-style-type: none"> Manual Daily Weekly Monthly Semi-annually Annually |
| Time Zone | Drop-down | Allows the administrator to set the time zone to be followed by the agent. |
| Time | Textbox | Allows the administrator to specify the time at which the scans are to be done on selected days, as per the set time zone. |

- Click 'OK' in the 'Edit Agent' dialog for your configuration to take effect.

Once integrated, the agent will scan the network through the AD server for installed certificates as per the schedule and forward details to CCM. Network objects enrolled to the AD server and all types of certificates installed on them can be viewed by expanding the 'Active Directory' category in 'Discovery' > 'Network Assets'. Refer to the section [Active Directory](#) for more details.

6.13 Auto-Assignment Rules for Unmanaged Certificates

Administrators can create rules to automatically assign 'Unmanaged' certificates found after a discovery scan to a specific Organization or Department.

Assignment Rules will assign certificates to a particular entity based on one or more conditions set by the administrator.

The rules can be applied while configuring Discovery Tasks, so that each Unmanaged certificate found by a Discovery Scan and satisfying conditions in any of the rules applied to the scan, will be automatically assigned to the respective Organization(s)/Department(s). For more details on configuring Discovery Scans, refer to the section **Discovery Tasks**.

The 'Assignment Rules' interface allows the Administrators to create rules for use in Discovery Scans.

To open the 'Assignment Rules' interface:

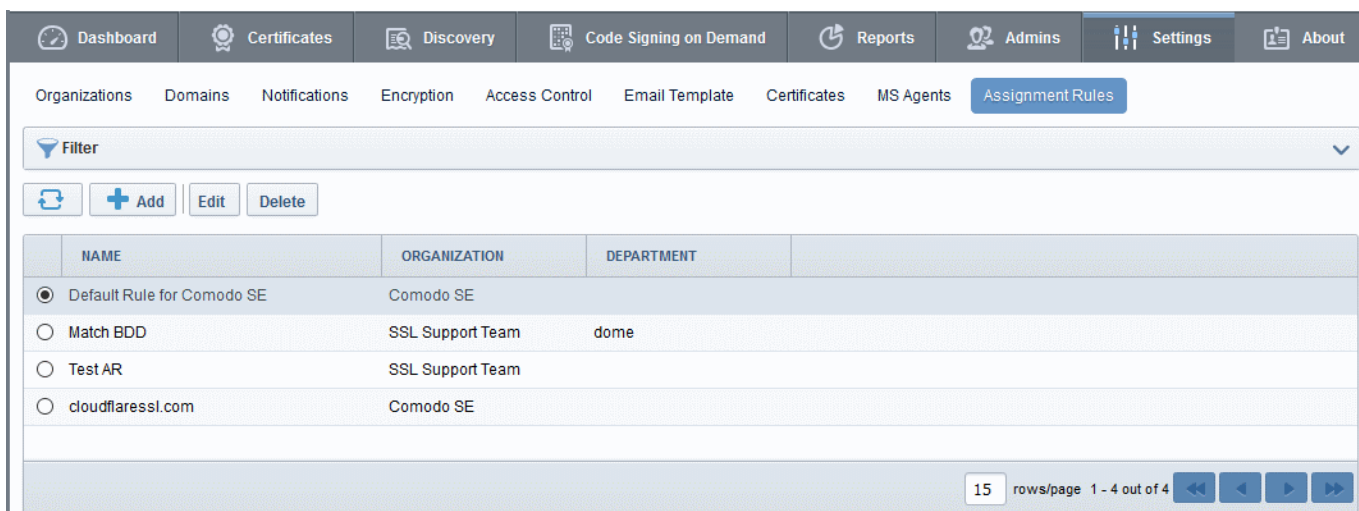
- Click 'Settings' > 'Assignment Rules'

Security Roles:

- MRAO - can create and manage rules to assign discovered certificates on any network to any Organization/Department.
- RAO - can create and manage rules to assign certificates discovered on their networks to Organizations and sub-Departments Departments which have been delegated to them.
- DRAO - can create and manage rules to assign certificates discovered on their networks to Departments which have been delegated to them.

The 'Assignment Rules' interface displays a list of the available rules, allows administrators to create new rules and manage existing rules.

- To open the Assignment Rules interface, click the 'Settings' tab and choose the 'Assignment Rules' sub-tab

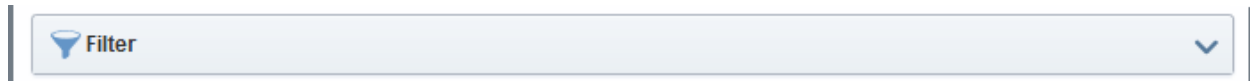


| Assignment Rules - Table of Column Descriptions | |
|---|---|
| Column Header | Description |
| Name | Name of the unmanaged certificate assignment rule |
| Organization | Name of the Organization to which the certificates matching the criteria specified in the rule will be auto-assigned. |
| Department | Name of the Department to which the certificates matching the criteria specified in the rule will be auto-assigned. |

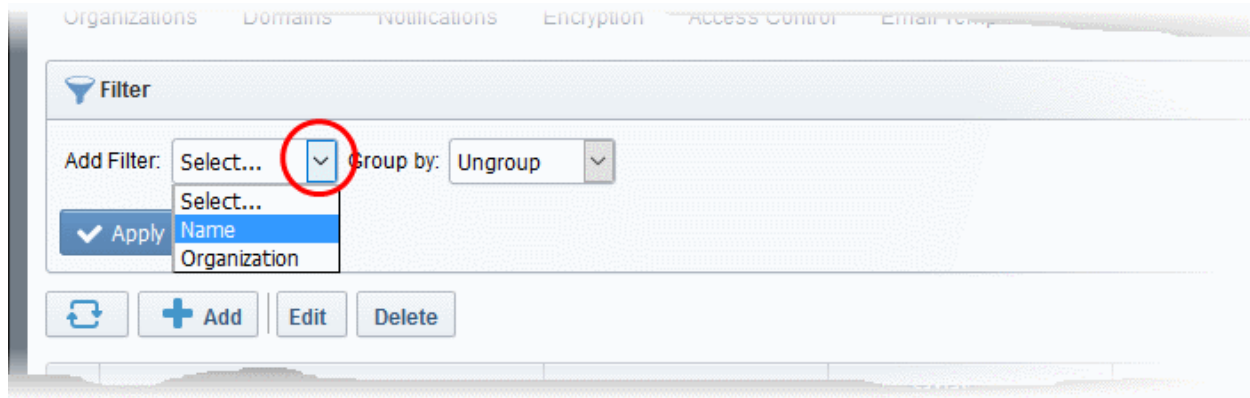
Sorting and Filtering Options

- Clicking on a column headers 'Name', 'Organization' and 'Department' sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for a particular discovery task by using filter.



You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



| Filter Criteria | Filter Parameter |
|-----------------|---|
| Name | Enter the name of the rule in full or part |
| Organization | Select the Organization and/or the Department to which the certificate will be assigned as per the rule, from the 'Organization' and 'Department' drop-downs. |

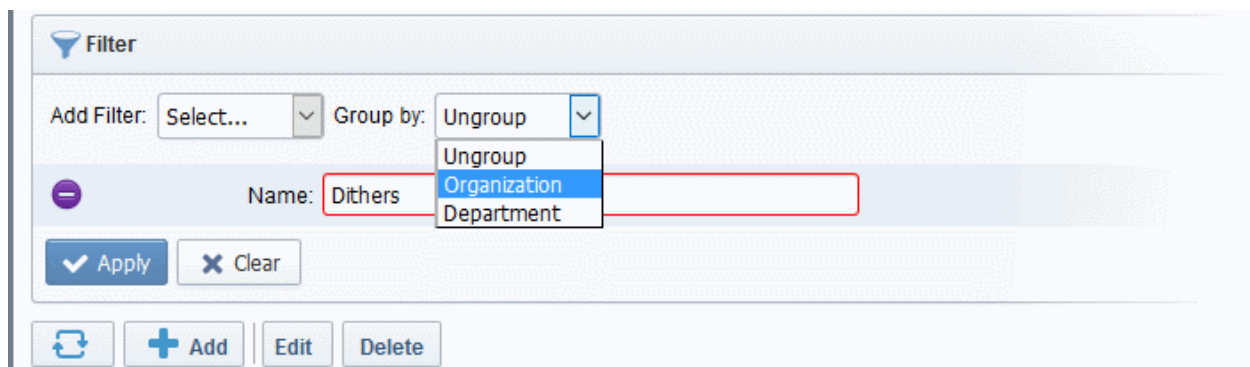
To add a filter

- Select a filter criteria from the 'Add Filter' drop-down
- Enter or select the filter parameter as per the selected criteria.

Tip: You can use more than one filter at a time. To remove a filter criteria, click the '-' button to the left of it

- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter

For example, if you want to filter the rules with a specific Common Name starting with 'Dithers' and group the results by 'Organizations/Departments', then select 'Name' from the 'Add Filter' drop-down, enter 'Dithers' and select 'Organization/Department' from the 'Group by' drop-down. The tasks, having 'test' in their name will be displayed as a list.



The filtered items based on the entered parameters will be displayed:

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Assignment Rules' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

Following sections explain in details about:

- **Creating a new certificate assignment rule**
- **Editing an assignment rule**

To create a new rule

- Click 'Add' from the 'Assignments Rules' interface

The screenshot shows the 'Assignments Rules' interface with a table of existing rules. The 'Add' button is highlighted with a red circle, and a red arrow points to the 'Create New Assignment Rule' dialog box. The dialog box has the following fields:

- Assignment Rule Name***: A text input field.
- When a certificate is discovered that meets bellow condition(s)**: A section with three dropdown menus: 'Common Name', 'Matches', and 'Condition Value', followed by '+' and '-' buttons.
- Assign to ...**: A dropdown menu with 'Comodo SE' and 'None' as options.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom.

- Enter a name shortly describing the rule in the Assignment Rule Name text box.
- Set the condition for identifying the certificate to be auto-assigned as per the rule.
 - Select the field of the certificate to be searched from the first drop-down
 - Select the relationship between the field value and the condition value from the second drop-down
 - Enter the condition value in the text field.

For example, if you want to auto-assign certificates with common name dithers.com, then choose 'Common Name' from the first drop-down, select 'Matches' from the second drop-down and enter dithers.com in the text field.

- Choose the Organization and/or Department to which the certificates meeting the conditions to be auto-

assigned, from the respective 'Assign to' drop-downs.

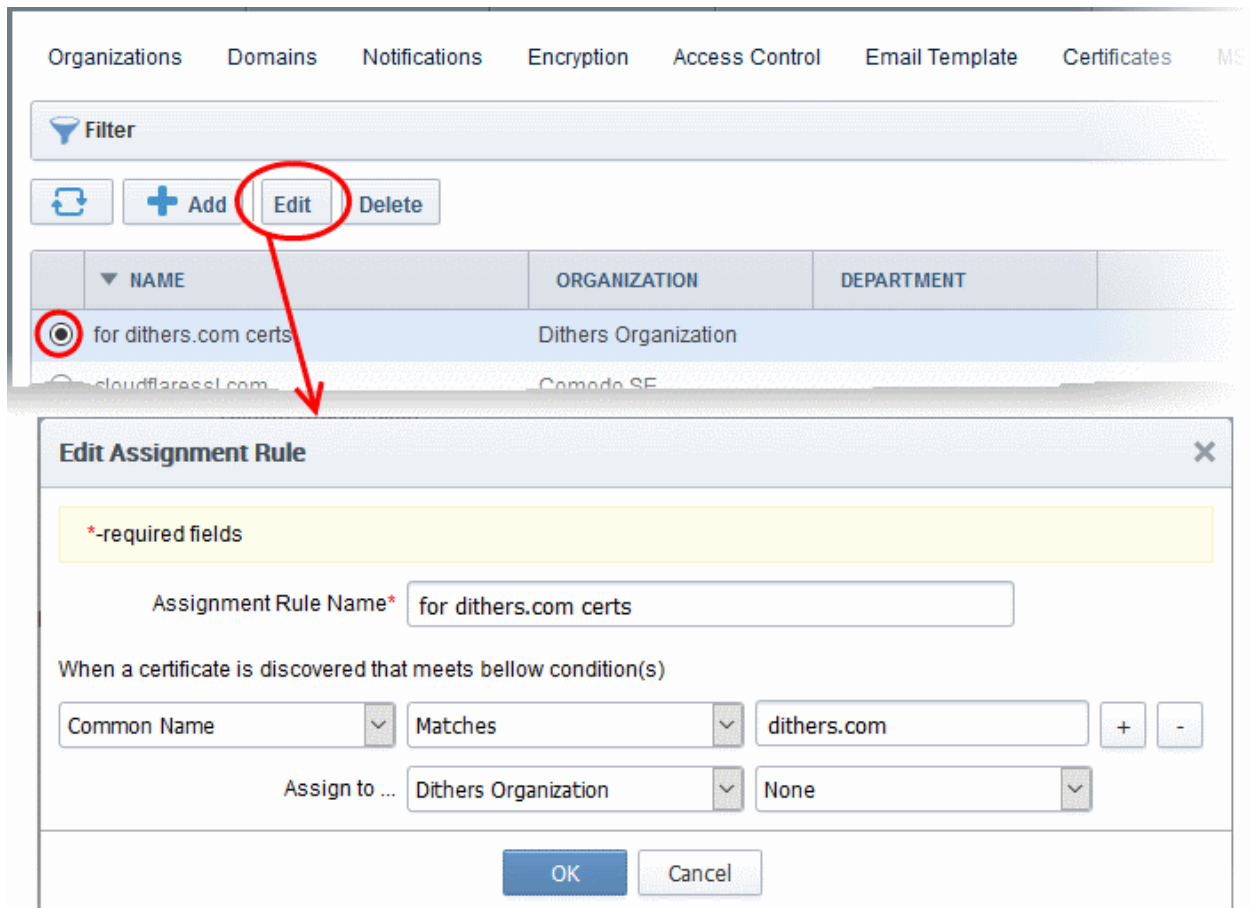
- Click OK.

The Rule will be added to the list. The rule will be available for selection while configuring a Discovery Task. For more details on configuring Discovery Scans, refer to the section [Discovery Tasks](#).

- Repeat the process to add more rules.

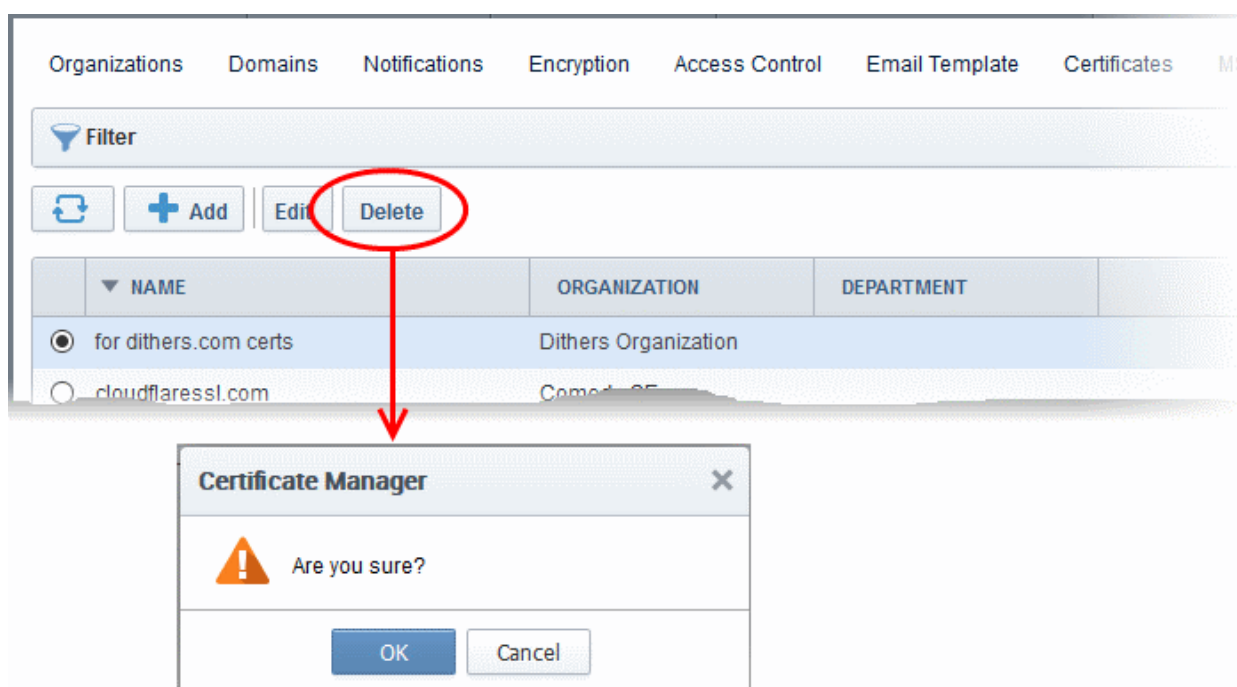
To edit a rule

- Select the rule and click the 'Edit' button



The 'Edit Assignment Rule' dialog will open. The dialog is similar to 'Add Assignment Rule' dialog. For description of the parameters, refer to the explanation of adding a new rule

- Edit the parameters and click 'OK'
- To remove a rule, select the rule and click 'Delete'



A confirmation dialog will appear.

- Click 'OK' in the confirmation dialog.

7 Certificate Discovery and Agents

CCM allows administrators to scan networks for SSL certificates installed on them, including certificates issued to network devices, certificates issued by third party vendors and self-signed certificates. CCM also identifies the web servers on the network and the domains hosted by them, with their SSL security status. Agents installed on the network facilitate this discovery process. In addition, the agents are also used for automatic installation of SSL certificates on Apache httpd, Apache Tomcat and IIS 7, 7.5, and 8. Refer to the following sections for more detailed explanation on each area.

- **Network Assets** - Contains explanations on viewing the results from scans. The results include SSL certificates installed on the network, web-servers identified from the network with their details and devices added to CCM by Active Directory Integration.
- **Certificate Discovery** - Contains explanations on adding, scheduling and running discovery tasks on networks.
- **Agents** - Contains explanations on downloading CCM extra agent and deployment on to networks for certificate discovery and auto-installation of SSL certificates.

7.1 Network Assets

The 'Network Assets' area displays the SSL, client, code signing and device authentication certificates installed on servers and other devices connected to the network, as discovered from the scans. It also displays the list of web-servers identified from the network with the details on domains hosted from them. If integrated with the AD server, the devices enrolled to AD are listed as a tree structure. Selecting a node/device in the trees structure displays the details of certificates installed on it.

| | IP ADDRESS | COMMON NAME | VALID TO | VALID FROM | KEY ALGORITHM | KEY SIZE | SIGNATURE ALGORITHM | INVENTORY |
|-------------------------------------|-------------------|----------------------------|------------|------------|---------------|----------|---------------------|-----------|
| <input checked="" type="checkbox"/> | 10.104.70.11:443 | 10.104.70.11 | 01/03/2025 | 01/06/2015 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.12:443 | 10.104.70.12 | 01/03/2025 | 01/06/2015 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.133:443 | 10.104.70.133 | 05/13/2026 | 05/15/2016 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.230:443 | IPMI | 04/12/2014 | 04/12/2012 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.234:443 | IPMI | 03/14/2017 | 03/14/2014 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.2:443 | KM272C9E | 12/01/2037 | 03/26/2016 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.7:443 | NPI038E8D.comodo | 08/01/2022 | 08/01/2012 | RSA | 1024 | MD5withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.5:443 | NPI03EE9B | 08/01/2022 | 08/01/2012 | RSA | 1024 | MD5withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.73:443 | SAGESERVER.como | 12/08/2015 | 06/08/2015 | RSA | 2048 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.233:443 | doris | 06/10/2009 | 06/10/2008 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.236:443 | iDRAC6 default certificate | 09/16/2019 | 09/18/2009 | RSA | 1024 | SHA1withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.202:443 | mail.jc.office.comodo | 05/19/2018 | 05/18/2016 | RSA | 2048 | SHA256withRSA | Managed |
| <input type="checkbox"/> | 10.104.70.221:443 | win2k12.comododev | 06/25/2017 | 06/24/2016 | RSA | 2048 | SHA256withRSA | Managed |

Different categories of the identified Network Assets are displayed as tree structure in the left pane and the details/certificates identified from the selected node in the tree structure is displayed in the right pane.

Refer to the following sections for more detailed explanation on each category of Network Assets.

- [Network Discovery](#)
- [Web Servers](#)
- [Active Directory](#)

7.1.1 Network Discovery

The 'Network Discovery' category view allows administrators to view a summary of all certificates installed on every network scanned and a history of previous scans. Administrators can also generate reports on discovered certificates and assign unmanaged certificates identified by discovery scans to respective organizations.

Note: An 'Unmanaged' certificate is one that was not obtained via Comodo Certificate Manager. This includes, for example, certificates from other CA's, self-signed certificates, and certificates issued by Comodo CA but not obtained via CCM. CCM identifies all certificates installed on a scanned network including 'Unmanaged' certificates and allows the administrator to assign them to respective Organization/Department for which the certificates were enrolled.

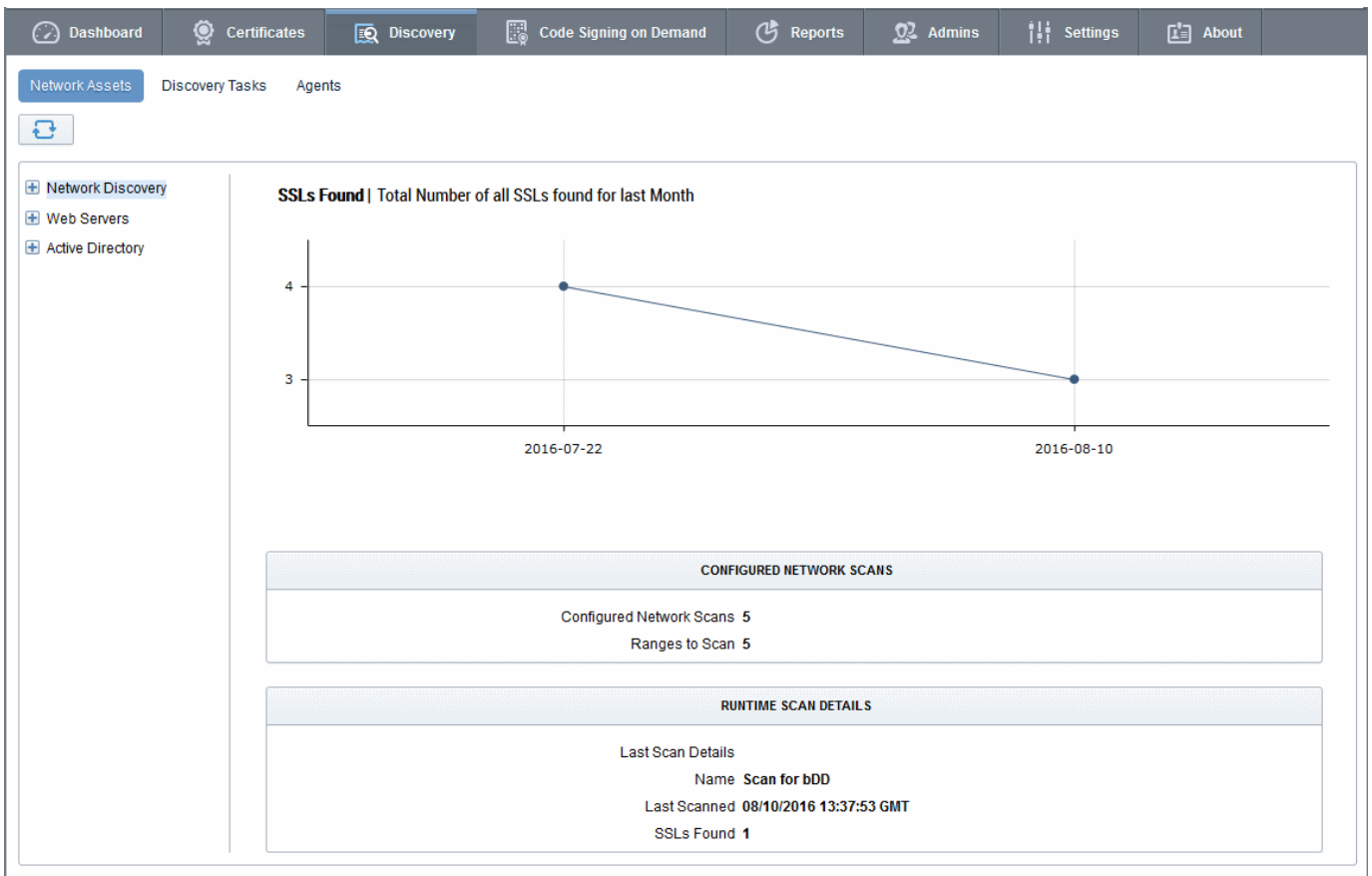
For more details on configuring discovery scans refer to the section [Discovery Tasks](#).

Security Roles:

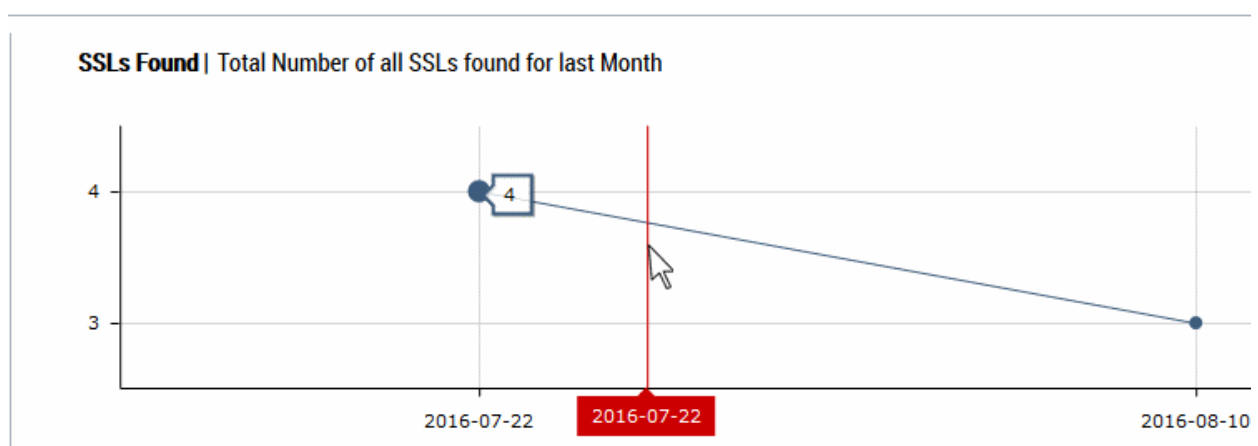
- MRAO - can view the certificates installed on all networks on which the scans were run.
- RAO SSL Admins - can view the certificates installed on networks of Organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO SSL Admins - can view the certificates installed on networks of Department(s) that have been delegated to them.

To view an over all statistical summary of SSL certificates installed on all scanned networks

- Click 'Discovery' tab and choose 'Network Assets' from the left.
- Choose 'Network Discovery' category from the left



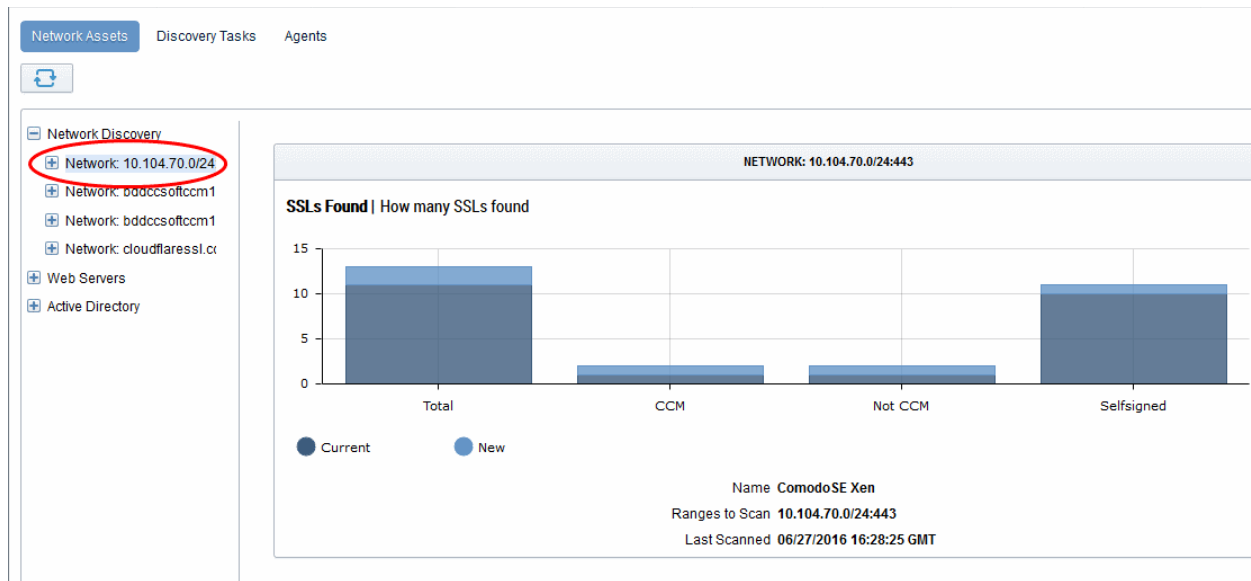
The right pane shows a time graph of number of SSL certificates and details of discovery scans run on the networks. Hovering the mouse over a date/month displays the number of SSL certificates identified on that date/month.



For more details on configuring discovery scans refer to the section [Discovery Tasks](#).

To view the statistical summary of SSL certificates installed on a selected network

- Click 'Discovery' tab and choose 'Network Assets' from the left.
- Expand the 'Network Discovery' category and choose the network



The right pane displays a comparison graph of total number of SSL certificates with numbers of certificates that are managed by CCM, unmanaged certificates and self-signed certificates installed on the network. The details of the discovery scan task name, network and IP ranges scanned and date/time of last run scan are displayed below the graph.

To view the list of SSL certificates installed on a selected network

- Click 'Discovery' tab and choose 'Network Assets' sub-tab.
- Expand the 'Network Discovery' category to view the networks on which discovery scans were run.
- Expand the selected network and choose 'SSL certificates'.

| IP ADDRESS | COMMON NAME | VALID TO | VALID FROM | KEY ALGORITHM | KEY SIZE | SIGNATURE ALGORITHM | INVENTORY |
|---|----------------------|------------|------------|---------------|----------|---------------------|-----------|
| <input checked="" type="checkbox"/> 17.149.160.16:443 | extensions.apple.com | 08/16/2015 | 07/24/2013 | RSA | 2048 | SHA1withRSA | |
| <input type="checkbox"/> 17.149.160.22:443 | helpqt.apple.com | 12/23/2014 | 10/23/2012 | RSA | 2048 | SHA1withRSA | |
| <input type="checkbox"/> 17.149.160.23:443 | helposx.apple.com | 12/23/2014 | 10/23/2012 | RSA | 2048 | SHA1withRSA | |
| <input type="checkbox"/> 17.149.160.240:443 | www.apple.com | 05/30/2014 | 07/11/2012 | RSA | 2048 | SHA1withRSA | |

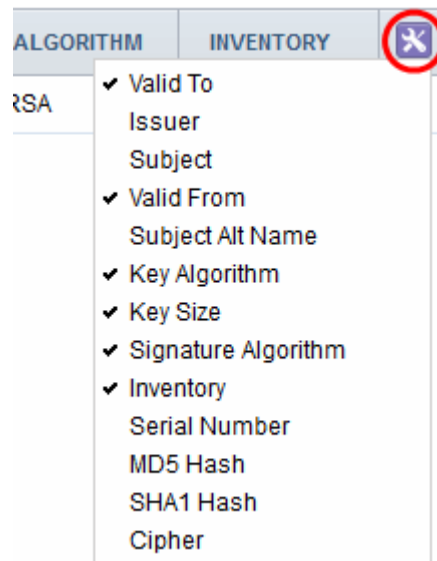
The list of certificates detected from the network during the last scan is displayed with their details as a table. Selecting a certificate allows displays options for viewing its details and to manually assign Unmanaged certificates to required Organization/Department.

The interface also allows you to create a report on the discovered certificates.

| List of Discovered Certificates - Column Descriptions | |
|---|---|
| Column Header | Description |
| IP Address | The IP address of the server on which the certificate was discovered. |
| Common Name | The domain name for which the certificate was issued. |

| | |
|---------------------|--|
| Valid to | Displays the expiry date of the certificate. |
| Valid From | The issuance date of the certificate. |
| Key Algorithm | Displays the type of algorithm used for the encryption. |
| Key Size | Displays the key size used by certificate for the encryption. |
| Signature Algorithm | Displays the type of algorithm used for the signing the certificate. |
| Inventory | <p>Indicates whether the certificate is 'Managed' or 'Unmanaged'.</p> <ul style="list-style-type: none"> Clicking the 'Managed' link opens the 'Certificate Details' screen of the certificate. Refer to the explanation under 'Viewing Details of a Certificate' for more details. You can open the certificate details dialog by selecting the certificate and clicking the 'Details' button at the top. Selecting an 'Unmanaged' certificate displays the option for assigning it to required Organization/Department. Refer to the explanation under Manually Assigning a Certificate to an Organization/Department for more details. <p>Tip - CCM also allows you to can configure for automatic assignment of Unmanaged certificates identified by a discovery scan to respective Organizations and Departments. Refer to the section Overview of Process under Discovery Tasks for more details.</p> |

Note: The administrator can add more columns from the drop-down button beside the last item in the column:

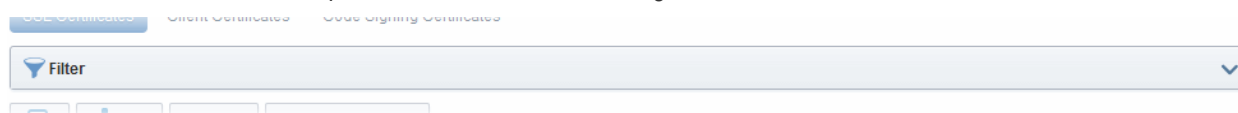


| | |
|------------------|--|
| Issuer | Displays the details of the Certificate Authority that issued the certificate and the name of the certificate. |
| Subject | Displays the details of the common name, organizational unit , organization and more, contained in the 'Subject' field of the certificate. |
| Subject Alt Name | Displays the names of domain(s) for which the certificate is used for. |
| Serial Number | Displays the serial number of the certificate that is unique and can be used to identify the certificate. |
| MD5 Hash | Displays the MD5 hash (thumbprint/fingerprint) for the certificate. |
| SHA1 Hash | Displays the SHA1 hash (thumbprint/fingerprint) for the certificate. |
| Cipher | The cipher suite used for encryption. |

Sorting and Filtering Options

- Clicking on a column header sorts the items in the alphabetical order of the entries in that column.

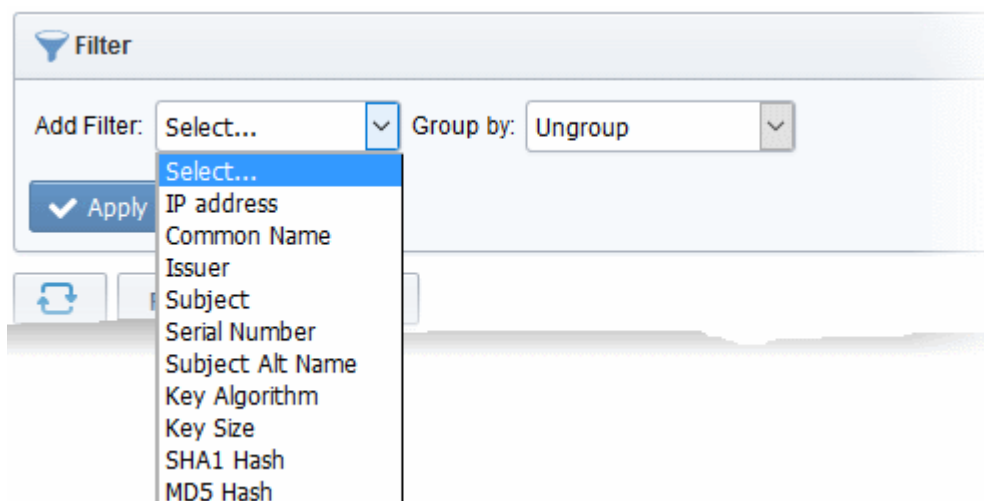
Administrators can search for particular SSL certificates using filters.



- To apply filters, click on the 'Filters' stripe. The filter options will be displayed. You can add filters by selecting from the options in the 'Add Filter' drop-down and group the results with other options that appears depending on the selection from the 'Add Filter' drop-down.

To add a filter

- Select a filter criteria from the 'Add Filter' drop-down



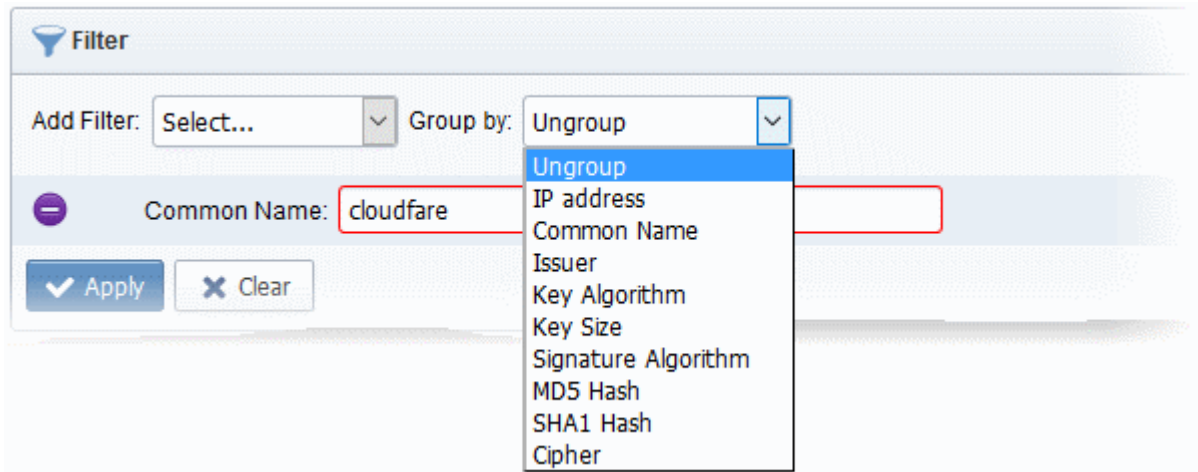
- Enter or select the filter parameter as per the selected criteria.

The available filter criteria and their filter parameters are given in the following table:

| Filter Criteria | Filter Parameter |
|------------------|--|
| IP Address | Enter the IP address from which the certificate was discovered |
| Common Name | Enter the common name or domain name for the certificate fully or in part |
| Issuer | Enter the name of the issuer of the certificate |
| Subject | Enter the details in the Subject field of the certificate in full or part. |
| Serial Number | Enter the serial number of the certificate in full or part. |
| Subject Alt Name | Enter the subject alternative name for the certificate fully or in part |
| Key Algorithm | Enter the key algorithm of the certificate |
| Key Size | Enter the key size in bits |
| SHA1 Hash | Enter the SHA1 Hash (thumbprint/fingerprint) of the certificate |
| MD5 Hash | Enter the MD5 Hash (thumbprint/fingerprint) of the certificate |

Tip: You can add more than one filter at a time to narrow down the filtering. To remove a filter criteria, click the '-' button to the left of it.

- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter



For example, if you want to filter the certificates with a specific Common Name starting with 'cloudfare.com' and group the results by their 'Issuer', then select 'Common Name' from the 'Add Filter' drop-down, enter 'cloudfare.com' and select 'Issuer' from the 'Group by' drop-down. The certificates, having 'cloudfare.com' in their common name will be displayed as a list, grouped based on their issuers.

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'SSL certificates' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

Viewing Details of a Certificate

The 'Certificate Details' dialog displays the complete details of the selected SSL certificate with its certificate chain details.

- To view the SSL certificate details dialog, select the certificate from the list and click the 'Details' button at the top.
- Alternatively, click the 'Managed' link in the Inventory column

The screenshot displays two panels for an SSL certificate. The left panel, titled 'CERTIFICATE DETAILS', shows the following information:

- Common Name: ssl358305.cloudflaressl.com
- State: Unmanaged
- Vendor: Comodo CA Limited
- IP Address(es): 104.16.20.233:443
- Alternative Names: *.helahalsingland.se, helahalsingland.se
- Term: (blank)
- Valid From: 01/04/2016
- Valid To: 01/01/2017
- Serial Number: A0:BA:8C:F5:FB:07:E1:23:85:79:7F:FC:3E:2E:50:87
- Signature Algorithm: SHA256withECDSA
- Public Key Algorithm: EC
- Public Key Size: 256
- MD5 Hash: c32d46634b636a003ce9c8d4fa5fbea3

The right panel, titled 'CERTIFICATE CHAIN DETAILS', shows the following information:

- Root, Intermediate, End Entity (all with green checkmarks)
- Common Name: COMODO ECC Certification Authority
- Vendor: AddTrust AB
- Term: 20 years
- Requested: (blank)
- Expires: 05/30/2020
- Serial Number: 43:52:02:3F:FA:A8:90:1F:13:9F:E3:F4:E5:C1:44:4E
- Signature Algorithm: SHA384WITHRSA
- Public Key Algorithm: EC
- Public Key Size: 378
- MD5 Hash: c790a56c69cbaf0bf3f30a40d0a2aecc
- SHA1 Hash: ae223cbf20191b40d7ffb4ea5701b65fdc68a1ca
- Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
- Subject: CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB

A 'Close' button is located at the bottom center of the dialog.

For more details on the information displayed in the Certificate Details dialog, refer to the section [Certificate 'Details' Dialog](#).

Manually Assigning a Certificate to an Organization/Department

The certificates that are issued through CCM, otherwise called 'Managed' certificates are pre-assigned to their respective Organizations or Departments, specified during their enrollment process. But the certificates that are not obtained via CCM and found installed on the network by discovery scans are classified as 'Unmanaged' certificates. These certificates are not pre-assigned to any Organization or Department by default.

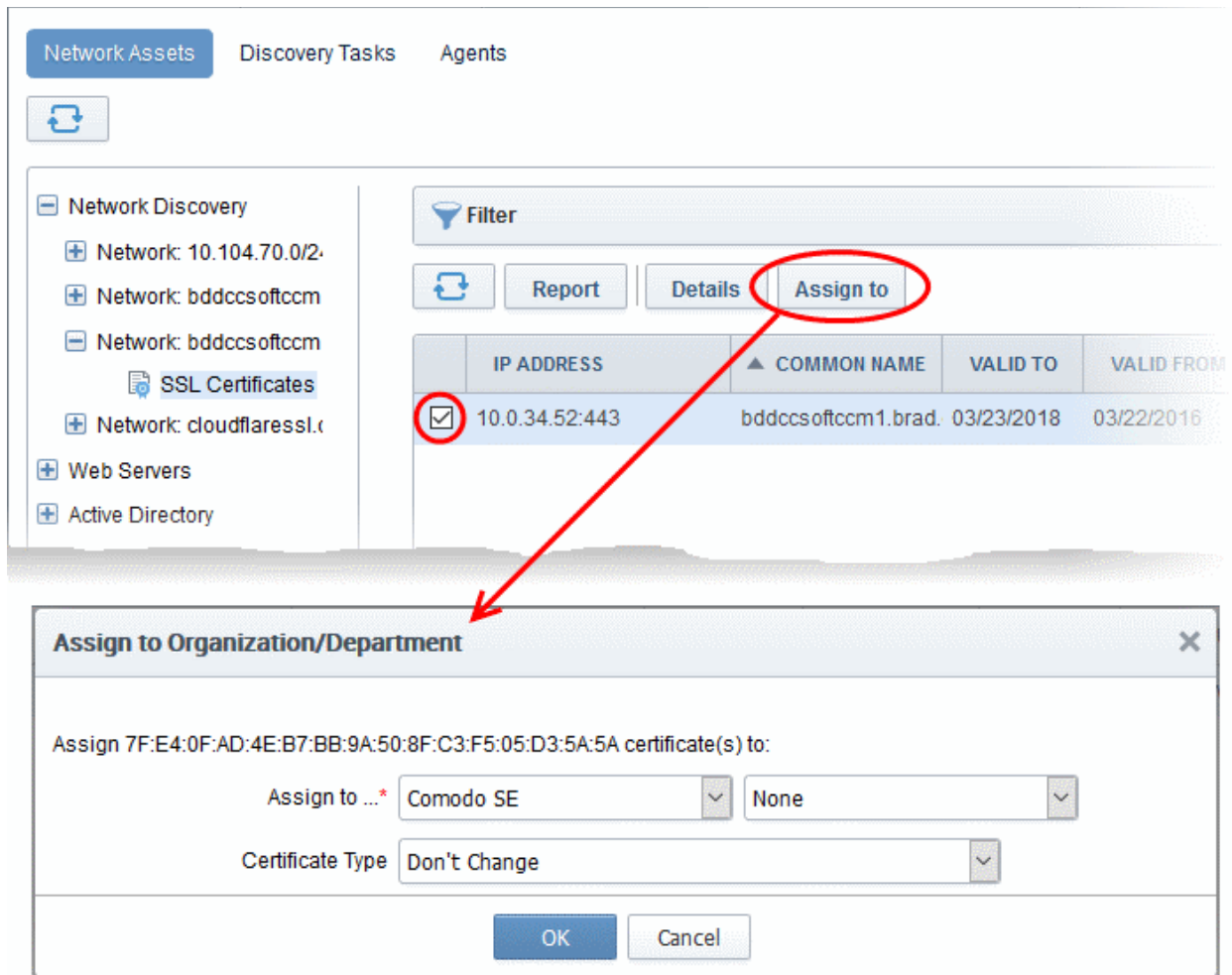
You can assign certificates to required Organizations/Departments from the list of certificates displayed under 'Network Assets'.

Tip: You can configure a discovery scan to automatically assign the unmanaged certificates identified by it to respective Organizations and Department by specifying Auto-Assignment Rules.

- For more details on configuring a discovery scan, refer to the section [Adding IP Range and Start Scanning](#) under [Discovery Tasks](#).
- For more details on configuring Auto Assignment Rules, refer to the section [Auto-Assignment Rules for Unmanaged Certificates](#)

To manually assign certificates

- Click 'Discovery' tab and choose 'Network Assets' sub-tab.
- Expand the 'Network Discovery' category to view the list of scanned networks
- Expand the selected network and choose 'SSL certificates'. The list of SSL certificates found installed on the network will be displayed.
- Select the unmanaged certificate from the list and click 'Assign To'



The 'Assign to Organization/Department' dialog will appear.

| Assign to Organization/Department dialog - Table of parameters | |
|--|--|
| Form Element | Description |
| Assign to | Select the Organization and Department (optional) from the respective drop-downs to which the certificate has to be assigned. |
| Certificate Type | If you want to manually define the type of certificate, depending on whether it is a SSL, Client, Code signing or a device authentication certificate, choose the certificate type from the drop-down. |

- Click OK.

The certificate will be assigned to the chosen Organization or Department.

Generating Report on Discovered Certificates

You can generate a report on the list of certificates discovered on selected network from the Network Assets interface.

To generate a report

- Click 'Discovery' tab and choose 'Network Assets' sub-tab.
- Expand the 'Network Discovery' category to view the list of scanned networks
- Expand the selected network and choose 'SSL certificates'. The list of SSL certificates found installed on the network will be displayed.

- Click the Report button at the top of the list.

The report will be generated as a spreadsheet file containing the list of certificate with their details. You can download the report in .xls format, which can be opened in spreadsheet software like Microsoft Excel or OpenOffice Calc.

7.1.2 Web Servers

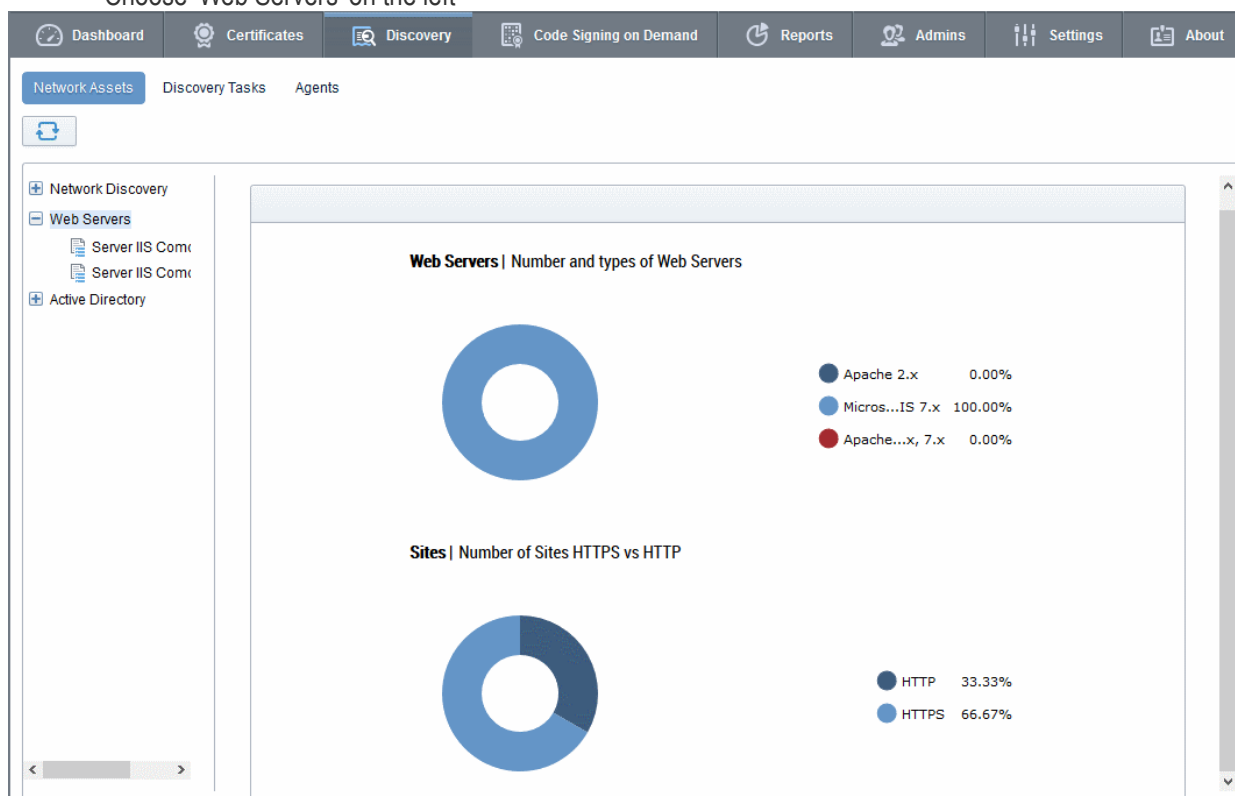
The 'Web Servers' category view allows administrators to view a summary of all web-servers identified from every network scanned and a list of websites/domains hosted on each identified server.

Security Roles:

- MRAO - can view details of all web servers from all networks on which the scans were run.
- RAO SSL Admins - can view details of web servers pertaining to Organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO SSL Admins - can view details of web servers pertaining to Department(s) that have been delegated to them.

To view a dashboard summary of web servers identified on all scanned networks

- Click the 'Discovery' tab and choose the 'Network Assets' sub-tab.
- Choose 'Web Servers' on the left



The pie-charts on the right show the percentage of scanned web-servers using different operating systems and the percentage of those servers using HTTPS versus HTTP.

- Placing your mouse over a chart segment or legend item displays additional details such as the exact number of servers/number of sites in that category.

Sites | Number of Sites HTTPS vs HTTP



To view details of websites/domains hosted on each server in scanned networks

- Click the 'Discovery' tab and choose the 'Network Assets' sub-tab.
- Expand the 'Web Servers' category to view the list of identified web servers
- Choose the server whose details you want to view

The screenshot shows the 'Discovery' tab with 'Network Assets' selected. The left sidebar shows 'Web Servers' expanded, with 'Server IIS Comodo SE 59' circled in red. The main pane displays details for 'SERVER IIS COMODO SE 59', including Name, Vendor (Microsoft IIS 7.x), and State (ACTIVE). Below this is a table of discovered websites.

| NAME | COMMON NAME | PROTOCOL | IP ADDRESS | PORT | STATUS | SSL |
|-------------------|-------------------|----------|------------|------|--------|--------------------------|
| ccm2.t1.ccmqa.com | ccm2.t1.ccmqa.com | HTTP | * | 80 | No SSL | |
| ccm2.t1.ccmqa.com | ccm2.t1.ccmqa.com | HTTPS | * | 443 | Failed | External |
| ccm2.t2.ccmqa.com | ccm2.t2.ccmqa.com | HTTPS | * | 8443 | No SSL | |

The right hand pane displays general server details and a list of websites/domains hosted on the server:

| List of Discovered Websites - Column Descriptions | |
|---|--|
| Column Header | Description |
| Name | The name of the website/domain. |
| Common Name | The registered domain name for website/domain. |
| Protocol | Displays the data transfer protocol used by the website. |
| IP Address | The address where the site is hosted. |
| Port | The server port number through which the site is served |

| | |
|--------|--|
| Status | Indicates whether the site is secured with SSL/TLS. |
| SSL | For HTTPS sites, indicates whether the certificate used by the site is managed by CCM or not. Clicking the entry opens the 'Certificate Details' screen. For more details on the information shown in this screen, refer to Certificate 'Details' Dialog |

7.1.3 Active Directory

The 'Active Directory' category allows administrators to view all types of certificates, including device authentication certificates, installed on each endpoint in a network.

Prerequisite - Active Directory (AD) servers can be added to CCM by installing the MS agent on them. The agent periodically scans the server, fetches network structure and users, then forwards these details to CCM server. For more details on downloading and installing the MS agent for AD integration, refer to [MS Agents for AD server Integration](#).

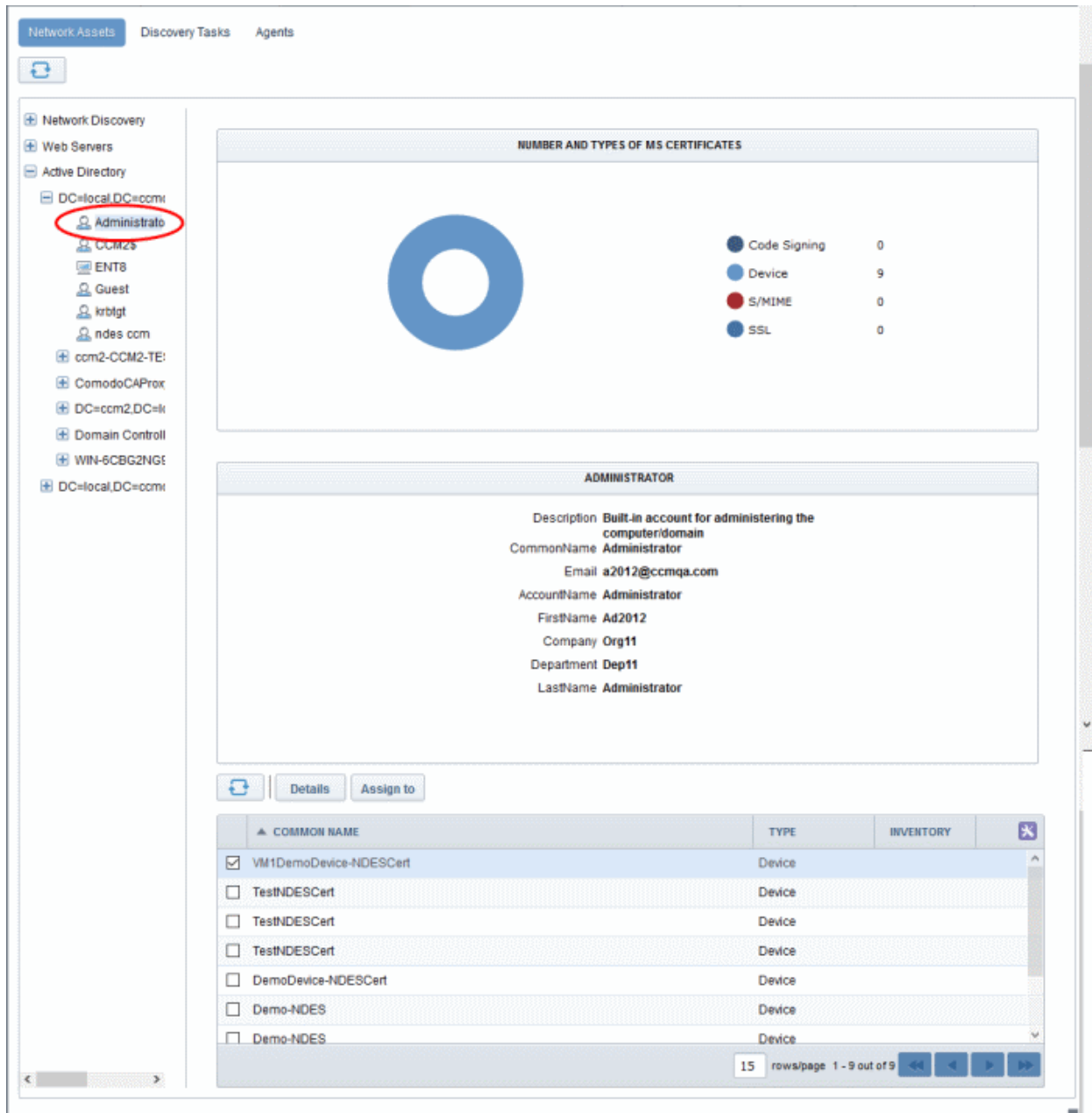
Security Roles:

- MRAO - can view details from all AD servers and networks for all Organizations.

To view network structure and details of certificates installed on endpoints

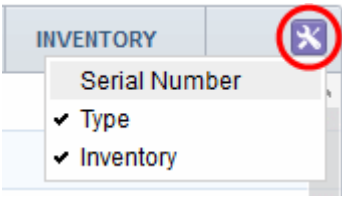
- Click the 'Discovery' tab and choose the 'Network Assets' sub-tab.
- To view details of certificates installed on all networks, choose the 'Active Directory' category on the left.
- To view details of certificates installed on a selected network, expand the 'Active Directory' category and choose a network.
- To view details of certificates installed for/on a specific network object, like a user account or an endpoint, expand the network and choose an object

The following example shows the details on certificates for a user object.



The pie chart on the right shows the different types of certificates found on the endpoints enrolled to the AD server. The middle pane displays the details about the selected AD object. The lower pane lists all certificates found on the network servers and endpoints installed for the object.

| List of Discovered Certificates - Column Descriptions | |
|---|---|
| Column Header | Description |
| Common Name | The domain name/username/device name for which the certificate was issued. |
| Type | Indicates whether the certificate is SSL, S/MIME, code signing or a device authentication certificate. |
| Inventory | Indicates whether the certificate is 'Managed' or 'Unmanaged'. <ul style="list-style-type: none"> Clicking the 'Managed' link opens the 'Certificate Details' screen of the certificate. Refer to the explanation under Viewing Details of a Certificate for more details. You can open the certificate details dialog by selecting the certificate and clicking the 'Details' button at the top. |

| | |
|---|--|
| | <ul style="list-style-type: none"> • Selecting an 'Unmanaged' certificate displays the option for assigning it to required Organization/Department. Refer to the explanation under Manually Assigning a Certificate to an Organization/Department for more details. <p>Tip - CCM also allows you to can configure for automatic assignment of Unmanaged certificates identified by a discovery scan to respective Organizations and Departments. Refer to the section Overview of Process under Discovery Tasks for more details.</p> |
| <p>Note: Administrators can add more columns using the drop-down button at the right of the column headers:</p>  | |
| Serial Number | Displays the unique serial number of the certificate which can be used to identify the certificate. |

- Placing your mouse over a chart segment or legend item displays additional details such as the exact number of servers/sites in that category.
- Selecting a certificate and clicking the 'Details' button at the top opens the Certificate Details screen. For more details on the information displayed in the Certificate Details screen, refer to the section **Certificate 'Details' Dialog**.

7.2 Discovery Tasks

The Certificate Discovery option is a very convenient tool for scanning and monitoring a network for all installed SSL certificates (including Comodo Certificates that may or may not have been issued using Comodo Certificate Manager, any 3rd party vendor certificates and any self-signed certificates.)

Administrators can configure Discovery Tasks for different networks to be scanned and can optionally set a schedule for them for periodical scanning. Each discovery task can also be added with auto-assignment rules so that unmanaged certificates identified from that discovery scan will be assigned to the respective Organizations/Departments and added to the 'Certificates' > 'SSL Certificates' interface.

Security Roles:

- MRAO - can scan for certificates installed on any network pertaining to Organization or Department.
- RAO - can scan for certificates installed on networks pertaining to Organizations (and any sub-ordinate Departments) that have been delegated to them.
- DRAO - can scan for certificates installed on networks pertaining to the Department that have been delegated to them.

The 'Discovery Tasks' interface displays the list of tasks added to CCM and allows Administrators to create new Discovery Tasks and edit existing tasks.

| NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|--------------|-------------------------|----------------------|----------|---------------------|
| global1 | cloudfliaressl.com | Successful | Manual | 08/10/2016 17:09:06 |
| ComodoSE Xen | 10.104.70.0/24 | Canceled | Manual | 06/27/2016 21:58:25 |
| bdd | bddccsoftccm1.brad.dc.c | Successful | Manual | 07/22/2016 19:16:31 |
| Scan for bDD | bddccsoftccm1.brad.dc.c | Partially Successful | Manual | 08/10/2016 19:07:53 |
| test | 10.104.70.0/24 | Scan in Progress 0% | Manual | |

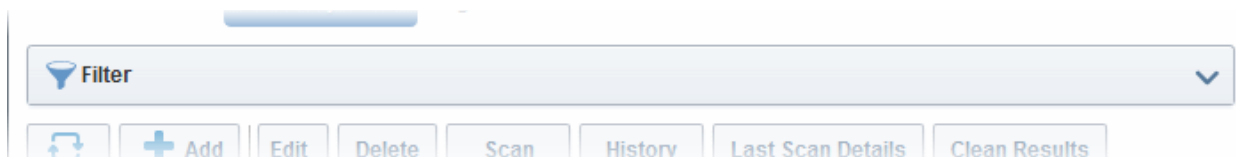
| Discovery Tasks area - Table of Parameters | | |
|--|---------|--|
| Field Element | Values | Description |
| Name | String | Name of the certificate discovery task |
| Ranges to Scan | String | Displays the IP ranges that will be scanned during this task |
| State | String | Displays the status of the scan, that is, whether it is successful, failed, in progress or canceled. Clicking on the state displays respective result. For example, clicking on 'Successful' will display the number of certificates discovered. |
| Schedule | String | Displays whether the scan is to be run manually or scheduled |
| Last Scanned | String | Displays the date and time of the last scan performed |
| <p>Note: The administrator can enable or disable desired columns from the drop-down at the right end of the table header:</p> | | |
| Control Buttons | Add | Enables administrator to add a new certificate discovery task |
| | Refresh | Updates the list of displayed discovery tasks |
| Discovery Task control Buttons | Edit | Enables administrator to edit the selected discovery task such as change the IP range and more |

| | | |
|---|-------------------|---|
| <p>Note: The Discovery Task control buttons are visible only on selecting a domain</p> | Delete | Enables administrator to delete a discovery task from the list |
| | Scan | Enables administrator to start a new scan for the selected discovery task |
| | Cancel | Enables administrator to cancel a discovery scan. This button will appear after starting a new scan |
| | History | Displays the details of past scans performed for the selected discovery task and allows administrators to download scan reports |
| | Last Scan Details | Displays the results of the last scan for the selected discovery task |
| | Clean Results | Removes all the discovered certificates from the SSL certificates tab |

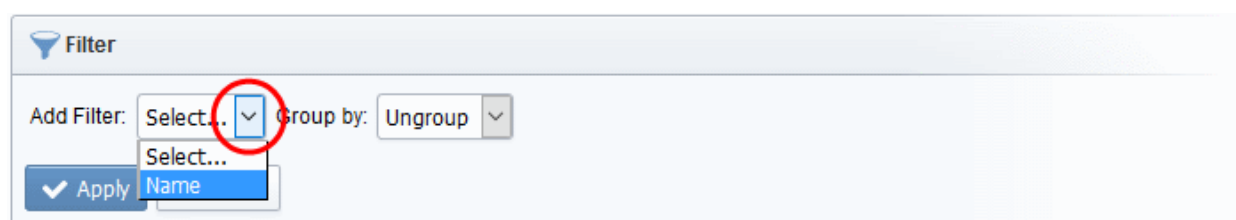
7.2.1 Sorting and Filtering Options

- Clicking on a column headers 'Name', 'Organization', 'Department', 'Schedule' or 'Last Scanned' sorts the items in the alphabetical order of the entries in the respective column.

Administrators can search for a particular discovery task by using filter.



You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.



| Filter Criteria | Filter Parameter |
|-----------------|---|
| Name | Enter the name of the discovery task fully or in part |

To add a filter

- Select a filter criteria from the 'Add Filter' drop-down
- Enter or select the filter parameter as per the selected criteria.
- Select the criteria by which the results are to be grouped from the 'Group by' drop-down and enter or select the grouping parameter

For example, if you want to filter the discovery tasks with a specific Common Name starting with 'Dithers' and group the results by 'Scheduled', then select 'Name' from the 'Add Filter' drop-down, enter 'Dithers' and select 'Schedule' from the 'Group by' drop-down. The tasks, having 'test' in their name will be displayed as a list.

The filtered items based on the entered parameters will be displayed:

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Discovery Tasks' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

7.2.2 Prerequisites

The administrator has installed the certificate controller agent and has configured it.

7.2.3 Overview of Process

- Run a scan of networks in order to find all deployed SSL certificates.
- CCM will automatically integrate all newly discovered certificates and add:
 - Certificates with Managed status and certificates with 'Unmanaged' status but auto-assigned to respective Organizations/Departments based on Assignment Rules applied to the discovery task, to '**SSL Certificates**' area ('Certificates' > 'SSL' Certificates)
 - All certificates to the lists of certificates, including 'Unmanaged' certificates that are not assigned to any Organization/Department, under respective networks in the '**Network Assets**' area. Administrators can assign manually assign 'Unmanaged' certificates to Organizations/Departments to which they pertain, to bring them under management through the SSL Certificates area. See **Network Discovery** for more details.

Note: An 'Unmanaged' certificate is one that was not obtained via Comodo Certificate Manager. This includes, for example, certificates from other CA's, self-signed certificates, and certificates issued by Comodo CA but not obtained via CCM. CCM identifies all certificates installed on a scanned network including 'Unmanaged' certificates and allows the administrator to assign them to respective Organization/Department for which the certificates were enrolled.

- CCM will update the status of existing certificates that were issued using CCM (if necessary)
- 'Unmanaged' certificates can become 'Managed' by renewing the particular certificate
- The compiled results of the scan can be viewed in the '**Discovery Scan Log**'

7.2.4 Adding IP Range and Start Scanning

- To add a discovery scan task, click 'Discovery' > 'Discovery Tasks' > 'Add' to open the scan configuration form

The form has three tabs. The first to configure scan settings, the second to apply auto-assignment rules

and the third to schedule the scan.

2. First, complete the 'Common' tab:

| Form Element | Description |
|----------------|---|
| Name | Enter a name to describe the discovery task |
| Agent | Select the CCM controller agent to be used for scanning. CCM uses agents installed on internal servers to scan for certificates. For more details, refer to the section Agents. |
| Ranges to Scan | IP address ranges of servers to be scanned. |
| Add | Add IP ranges for scanning. |
| Edit | Edit the selected scan range |
| Remove | Delete the selected scan range |
| OK | Add the discovery task to the list |
| Cancel | Cancel the task. |

3. Click the 'Add' button to add a CIDR, IP address or host name:

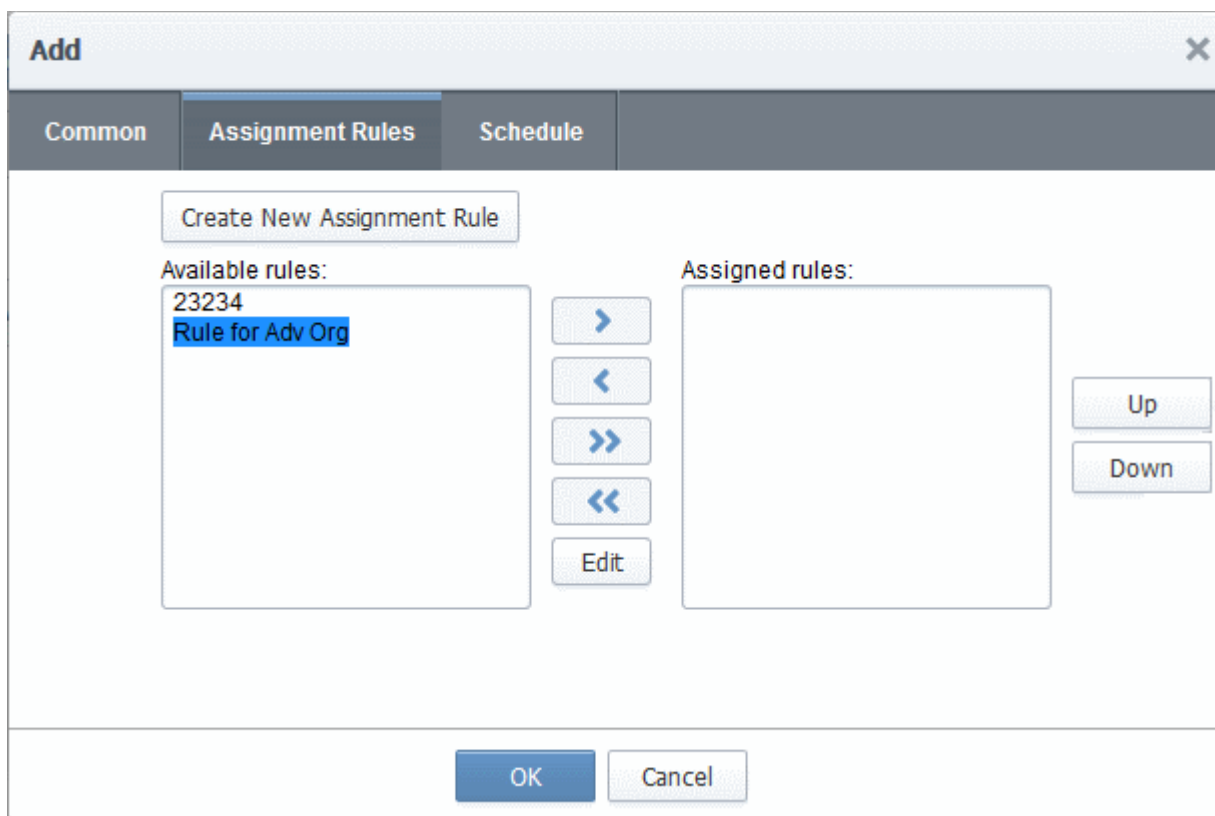
| Form Element | Element Type | Description |
|---------------------------------|--------------|---|
| CIDR | Text Field | Short for 'Classless Internet DOMAIN Routing'. Type the IP address you wish to scan followed by network prefix, e.g. 123.456.78.91/16 should be specified here. |
| IP | Text Field | Type the IP address you wish to scan |
| Host name | Text Field | Enter the host name you wish to scan |
| Ports to Scan <i>(required)</i> | Text Field | The port number(s) for IP range. |
| OK | Control | Enables the administrator to add specified data into the scan list. |
| Cancel | Control | Enables the administrator to add cancel the process |

4. Click 'OK' after selecting and entering the appropriate details.

Administrators can add more scan ranges for the same discovery task. Repeat the process as explained above.

The entered scan ranges will be displayed. Administrators can edit or remove the scan range after selecting it and clicking 'Edit' or 'Remove'.

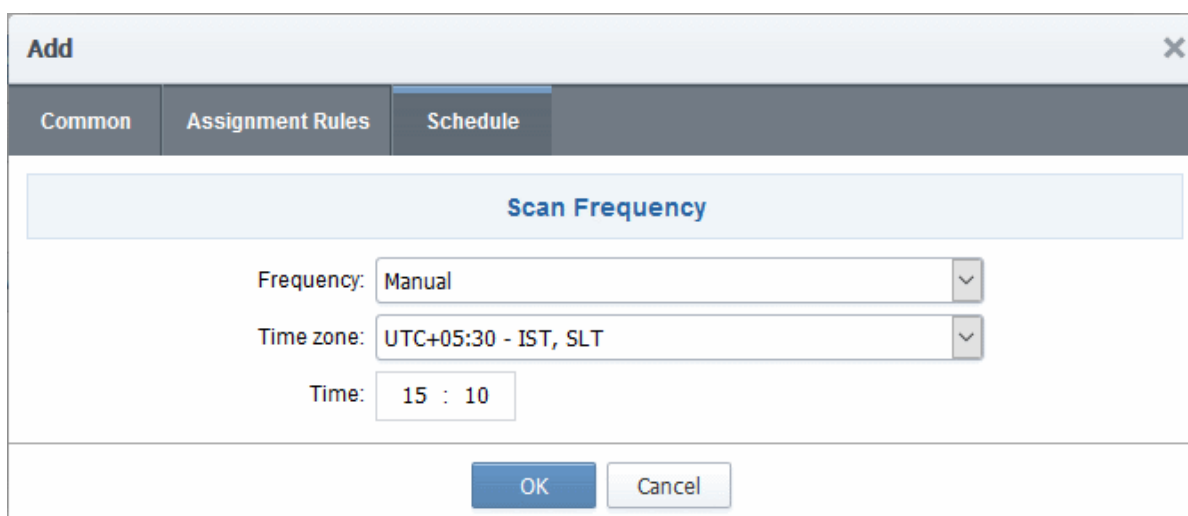
5. Click the 'Assignment Rules' tab to add rules which will assign unmanaged certificates identified by the scan to an organization or department.



All available rules are shown on the left. Use the arrow buttons to add rules to the discovery task. Rules can be configured in the 'Settings' > 'Assignment Rules' interface. For more details on managing auto-assignment rules, refer to [Auto-Assignment Rules for Unmanaged Certificates](#).

- To create a new rule, click the 'Create New Assignment Rule' button. For more guidance refer to the explanation under [Creating a new certificate assignment rule](#) in the section [Auto-Assignment Rules for Unmanaged Certificates](#). The rule will be added to the list of Available Rules. Select it and move to the 'Assigned rules' list
- To edit a rule, select it and click the Edit button. For more guidance refer to the explanation of [Editing an assignment rule](#) in the section [Auto-Assignment Rules for Unmanaged Certificates](#).

6. Click the 'Schedule' tab to set the scan day, date and start time, and the frequency of the task:



Available scan frequencies are: Manual (on demand), Daily, Weekly, Monthly, Quarterly, Semi-Annually and

Annually.

7. Click 'OK'.

The newly created discovery task will be displayed in the list.

Network Assets **Discovery Tasks** Agents

Filter

Refresh Add Edit Delete Scan History Last Scan Details Clean Results

| | NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|----------------------------------|---------------|-------------------------|--------------------------------------|----------|---------------------|
| <input type="radio"/> | global1 | cloudflaressl.com | Successful | Manual | 08/10/2016 17:09:06 |
| <input type="radio"/> | ComodoSE Xen | 10.104.70.0/24 | Canceled | Manual | 06/27/2016 21:58:25 |
| <input type="radio"/> | bdd | bddccsoftccm1.brad.dc.c | Successful | Manual | 07/22/2016 19:16:31 |
| <input type="radio"/> | Scan for bDD | bddccsoftccm1.brad.dc.c | Partially Successful | Manual | 08/10/2016 19:07:53 |
| <input type="radio"/> | test | 10.104.70.0/24 | Scan in Progress 0% | Manual | |
| <input checked="" type="radio"/> | certs for adv | bddccsoftccm1.brad.dc.c | | Manual | |

Repeat the process to add more Discovery Tasks.

8. To run a scan, select it select the respective 'Discovery Task' from the list

The control buttons for managing the task will be displayed at the top.

9. Click the 'Scan' button to commence the discovery scan for the selected task.

Filter

Refresh Add Edit Delete **Scan** History Last Scan Details Clean Results

| | NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|----------------------------------|---------------|-------------------------|--------------------------------------|----------|---------------------|
| <input type="radio"/> | global1 | cloudflaressl.com | Successful | Manual | 08/10/2016 17:09:06 |
| <input type="radio"/> | ComodoSE Xen | 10.104.70.0/24 | Canceled | Manual | 06/27/2016 21:58:25 |
| <input type="radio"/> | bdd | bddccsoftccm1.brad.dc.c | Successful | Manual | 07/22/2016 19:16:31 |
| <input type="radio"/> | Scan for bDD | bddccsoftccm1.brad.dc.c | Partially Successful | Manual | 08/10/2016 19:07:53 |
| <input type="radio"/> | test | 10.104.70.0/24 | Scan in Progress 0% | Manual | |
| <input checked="" type="radio"/> | certs for adv | bddccsoftccm1.brad.dc.c | | Manual | |

Information ✕

i Scan has started.

CCM allows administrators to run multiple discovery tasks at a time. After a scan has started, select another task and click the scan button at the top.

Discovery scanning uses a 2 second timeout for each IP/Port combination with 10 threads running at once. This information can be used to approximate how long a scan will take.

$((\# \text{ IP Addresses}) * (\# \text{ ports per address})) / 300 = \text{Number of minutes for scan.}$

Note: The timeout interval and number of threads per minute may be subject to minor fluctuation. Admins are advised to treat these figures as a approximate calculation of scanning times.

2.Example:

Scanning a single range xxx.xxx.0.0/16 for a single port (443) equals 65,536 IP addresses.

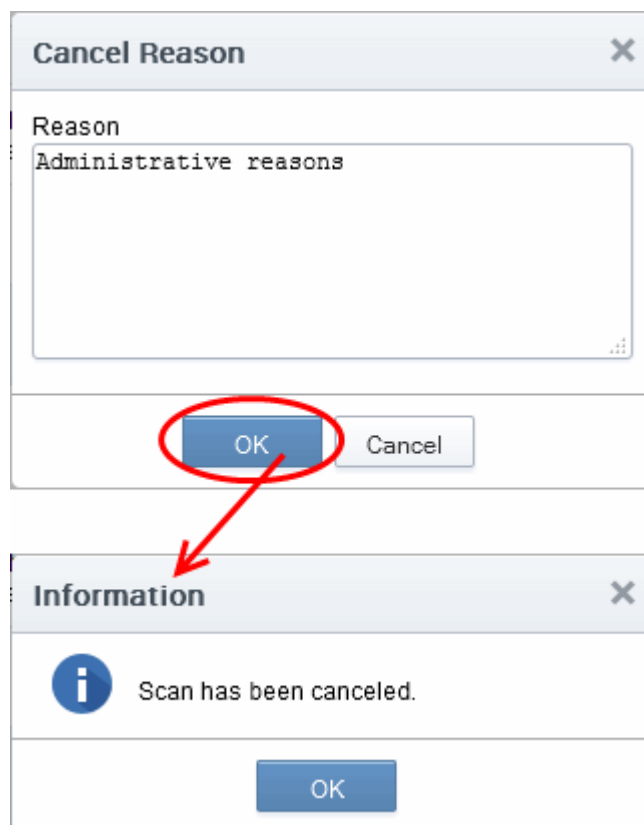
$((65536)(1))/300 = \text{approx 218 minutes.}$

The progress of the scan can be viewed in the row of the selected discovery task under the 'State' column.

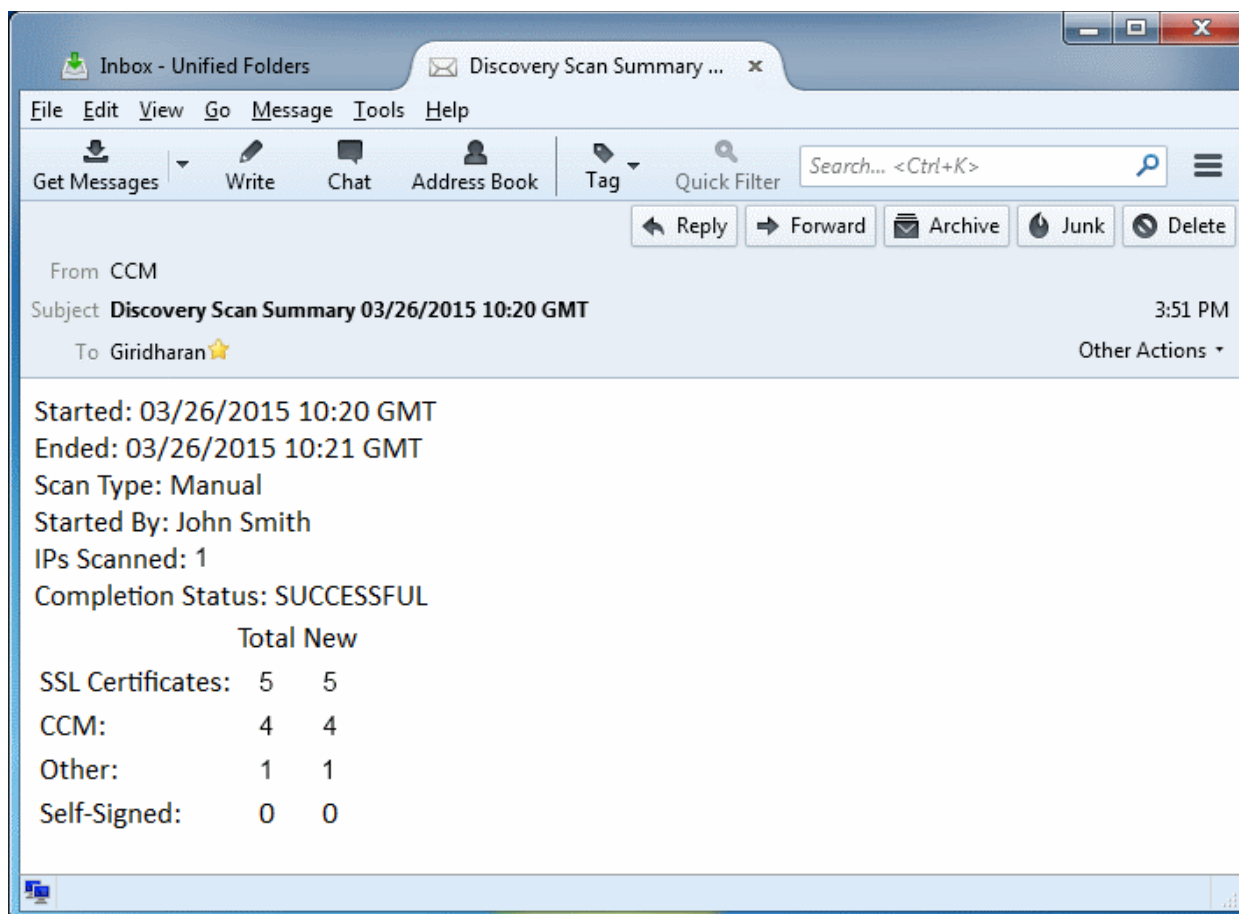
10. Click the 'Cancel' button if you want to cancel the scanning process.

If you cancel the scanning process, the entire system will revert to the state that existed before the scan was started (i.e., any data collected during scanning will not be applied until the scanning process is completed).

If you cancel the scanning, you should specify the reason for in the 'Cancel Reason' dialog and click OK.



After the scan is complete, administrators will be notified of the result via email. Please note the email notification should have been configured in the **Discovery Scan Summary** notifications area.



The results of the scan can be viewed at '[SSL certificates](#)' sub-tab of the '[Certificate Management](#)' section and the '[Reports](#)' section.

7.2.5 Editing a Discovery Task

Administrators can edit an existing discovery task by selecting it in the list and clicking the 'Edit' button at the top.

The screenshot shows the 'Discovery Tasks' interface. At the top, there are navigation tabs: Dashboard, Certificates, Discovery, Reports, and Admins. Below these are sub-tabs: Network Assets, Discovery Tasks (selected), and Agents. A filter bar is present, followed by action buttons: Refresh, Add, Edit (circled in red), Delete, Cancel, and History. A table lists discovery tasks with columns: NAME, RANGES TO SCAN, STATE, SCHEDULE, and LAST SCANNED. Two tasks are listed: 'Certs for Dither Purchase Dept' and 'certs for adv'. The 'Edit' button for the second task is circled in red, with a red arrow pointing to the 'Edit' dialog box below. The dialog box has tabs for 'Common', 'Assignment Rules', and 'Schedule'. The 'Common' tab is active, showing a form with the following fields: Name* (certs for adv), Agent (Agent org1 52), and Ranges to Scan* (10.100.51.18 : 443). There are 'Add', 'Edit', and 'Remove' buttons for the ranges, and 'OK' and 'Cancel' buttons at the bottom.

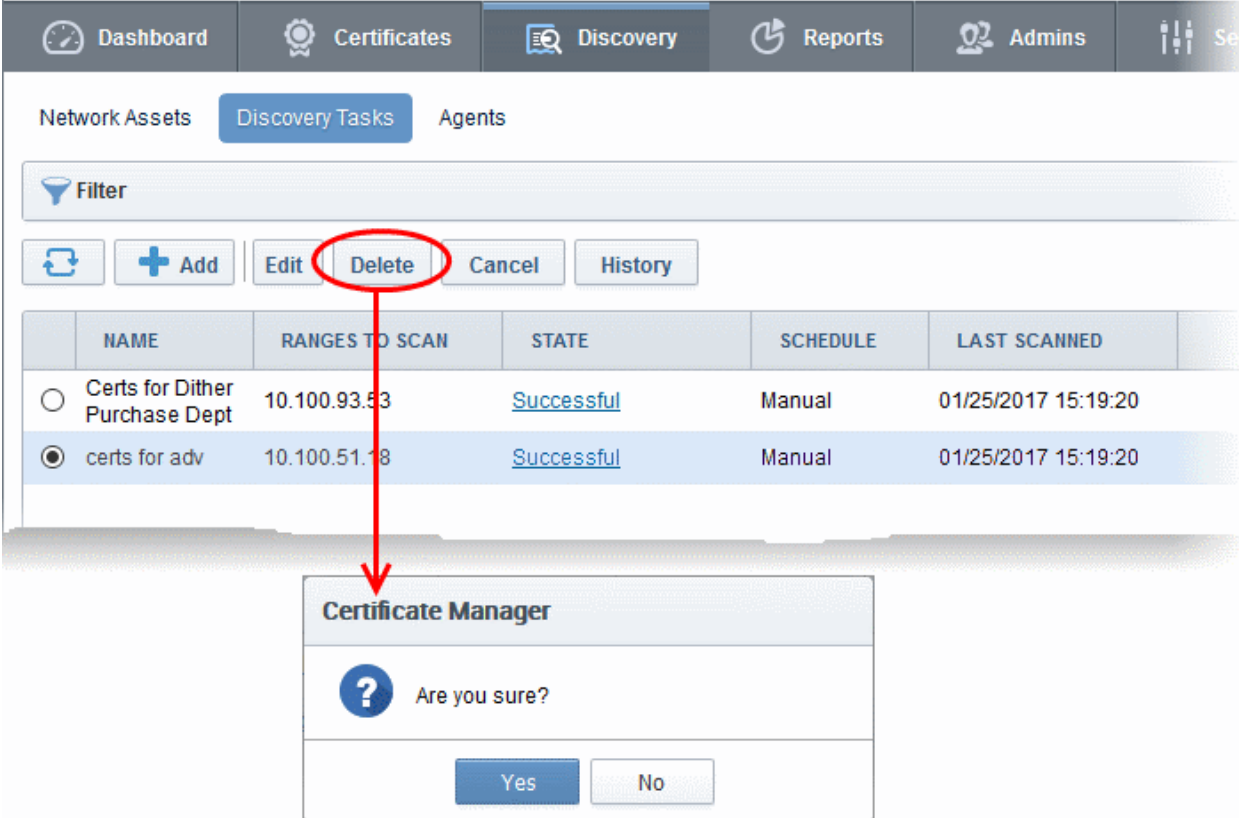
| | NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|----------------------------------|--------------------------------|----------------|----------------------------|----------|---------------------|
| <input type="radio"/> | Certs for Dither Purchase Dept | 10.100.93.53 | Successful | Manual | 01/25/2017 15:19:20 |
| <input checked="" type="radio"/> | certs for adv | 10.100.51.18 | Successful | Manual | 01/25/2017 15:19:20 |

The 'Edit' interface will open.

The interface allows administrators to change the task name, select another agent, add a new scan range, edit existing scan ranges or remove it. In the schedule tab, the scan frequency can be edited. For more details refer to section [Adding IP Range and Start Scanning](#).

7.2.6 Deleting a Discovery Task

To delete a discovery task from the list, select it and click the 'Delete' button at the top.



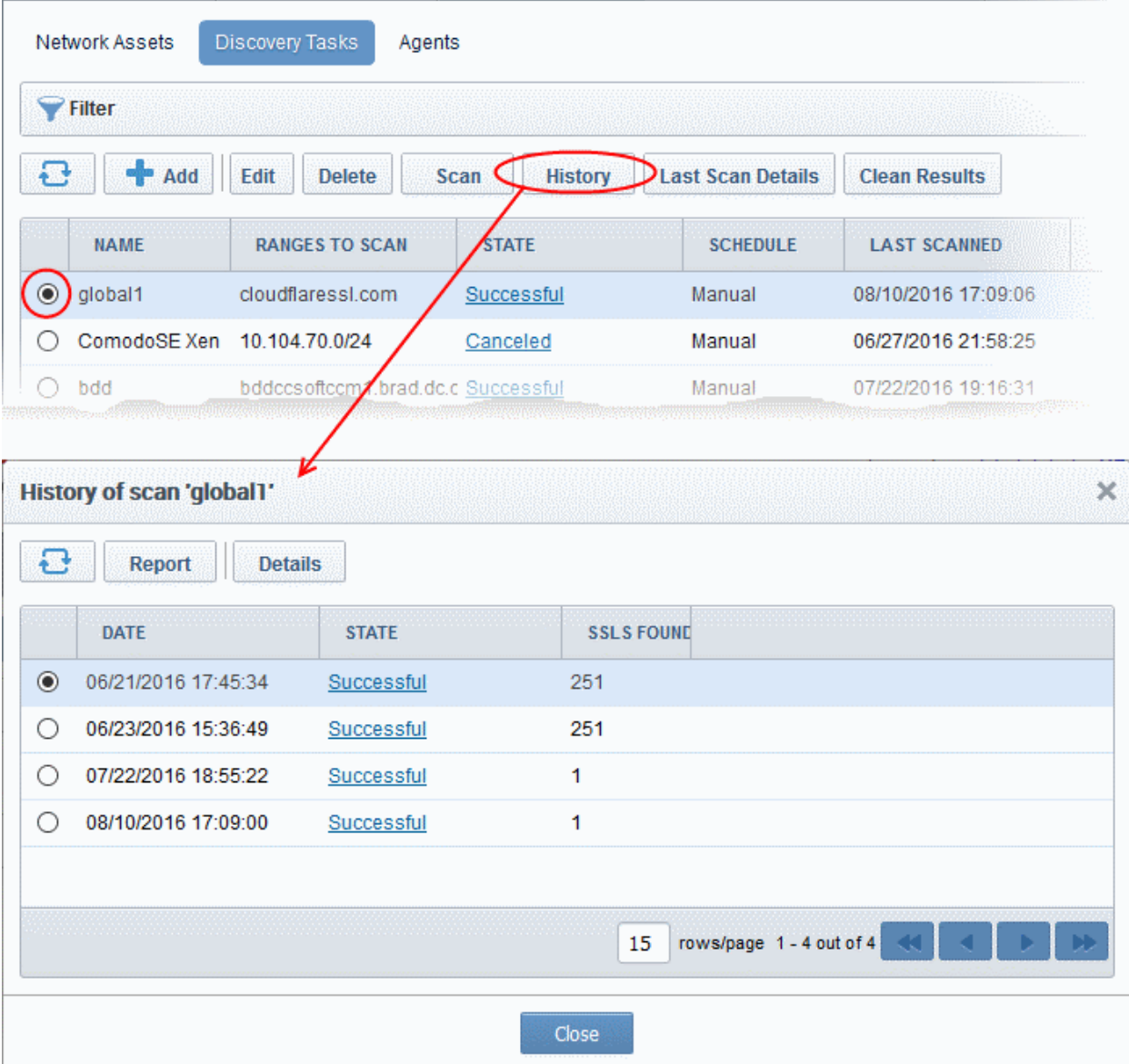
The screenshot shows the 'Discovery Tasks' section of the Comodo Certificate Manager interface. The 'Delete' button is circled in red, and a red arrow points from it to a 'Certificate Manager' dialog box. The dialog box contains a question mark icon and the text 'Are you sure?' with 'Yes' and 'No' buttons.

| | NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|----------------------------------|--------------------------------|----------------|----------------------------|----------|---------------------|
| <input type="radio"/> | Certs for Dither Purchase Dept | 10.100.93.53 | Successful | Manual | 01/25/2017 15:19:20 |
| <input checked="" type="radio"/> | certs for adv | 10.100.51.18 | Successful | Manual | 01/25/2017 15:19:20 |

7.2.7 Viewing History of Discovery Tasks

CCM allows administrators to view the previous five scan results of each discovery task. You can also download a report on each task and can assign unmanaged, discovered certificates to an organization or department.

- To view the history of a discovery task, select it and click the 'History' button at the top.



The screenshot displays the 'Discovery Tasks' section of the Comodo Certificate Manager. At the top, there are tabs for 'Network Assets', 'Discovery Tasks', and 'Agents'. Below these is a 'Filter' section and a row of action buttons: 'Add', 'Edit', 'Delete', 'Scan', 'History', 'Last Scan Details', and 'Clean Results'. The 'History' button is circled in red. Below the buttons is a table with columns: NAME, RANGES TO SCAN, STATE, SCHEDULE, and LAST SCANNED. The first row, 'global1', is selected and its 'STATE' is 'Successful'. A red arrow points from the 'History' button to a dialog box titled 'History of scan 'global1''. This dialog box contains a 'Report' button and a 'Details' button. Below these is a table with columns: DATE, STATE, and SSLS FOUND. The first row is selected and shows a date of 06/21/2016 17:45:34 with a state of 'Successful' and 251 SSLs found. At the bottom of the dialog box, there is a 'Close' button.

| NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|--------------|-------------------------|------------|----------|---------------------|
| global1 | cloudflaressl.com | Successful | Manual | 08/10/2016 17:09:06 |
| ComodoSE Xen | 10.104.70.0/24 | Canceled | Manual | 06/27/2016 21:58:25 |
| bdd | bddccsoftccm1.brad.dc.c | Successful | Manual | 07/22/2016 19:16:31 |

| DATE | STATE | SSLs FOUND |
|---------------------|------------|------------|
| 06/21/2016 17:45:34 | Successful | 251 |
| 06/23/2016 15:36:49 | Successful | 251 |
| 07/22/2016 18:55:22 | Successful | 1 |
| 08/10/2016 17:09:00 | Successful | 1 |

The 'History of scan...' dialog will be displayed.

- Click the 'Report' button to download all discovery scan reports as a .csv file.
- To view the list of certificates discovered during a scan, choose the scan and click the 'Details' button that appears at the top.

History of scan 'global1'

Report Details

| | DATE | STATE | SSLS FOUND |
|----------------------------------|---------------------|----------------------------|------------|
| <input checked="" type="radio"/> | 06/21/2016 17:45:34 | Successful | 251 |
| <input type="radio"/> | 06/23/2016 15:36:49 | Successful | 251 |
| <input type="radio"/> | 07/22/2016 18:55:22 | Successful | 251 |

Details of scan 'global1' run at 06/21/2016

Filter

Report Details Assign to

| | IP ADDRESS | COMMON NAME | VALID TO | VALID FROM | KEY ALGORITHM | KEY SIZE | SIGNATURE ALG |
|-------------------------------------|-------------------|----------------------|------------|------------|---------------|----------|-----------------|
| <input checked="" type="checkbox"/> | 104.16.20.23:443 | rbs.create.edu.sg | 04/07/2016 | 02/23/2015 | RSA | 2048 | SHA256withRSA |
| <input type="checkbox"/> | 104.16.20.251:443 | 2014-04-09.tinyspec | 04/09/2016 | 04/09/2014 | RSA | 2048 | SHA1withRSA |
| <input type="checkbox"/> | 104.16.20.254:443 | holylandmoments.or | 05/07/2016 | 01/28/2015 | RSA | 4096 | SHA256withRSA |
| <input type="checkbox"/> | 104.16.20.8:443 | novartis.com | 07/19/2016 | 07/15/2015 | RSA | 2048 | SHA256withRSA |
| <input type="checkbox"/> | 104.16.20.118:443 | ssl384981.cloudflare | 07/24/2016 | 01/15/2016 | EC | 255 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.112:443 | ssl384966.cloudflare | 07/24/2016 | 01/15/2016 | EC | 254 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.189:443 | ssl384990.cloudflare | 07/24/2016 | 01/15/2016 | EC | 256 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.220:443 | ssl382925.cloudflare | 07/24/2016 | 01/15/2016 | EC | 256 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.116:443 | ssl385035.cloudflare | 07/24/2016 | 01/15/2016 | EC | 256 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.54:443 | ssl384289.cloudflare | 07/25/2016 | 01/20/2016 | EC | 256 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.98:443 | ssl384295.cloudflare | 07/25/2016 | 01/20/2016 | EC | 256 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.47:443 | ssl385311.cloudflare | 08/01/2016 | 01/26/2016 | EC | 253 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.232:443 | ssl362514.cloudflare | 08/01/2016 | 01/27/2016 | EC | 253 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.114:443 | ssl383912.cloudflare | 08/01/2016 | 01/29/2016 | EC | 255 | SHA256withECDSA |
| <input type="checkbox"/> | 104.16.20.197:443 | ssl385353.cloudflare | 08/01/2016 | 01/27/2016 | EC | 256 | SHA256withECDSA |

15 rows/page 1 - 15 out of 251

- Click the 'Details' button to view full certificate information. Refer to [SSL Certificate 'Details' Dialog](#) for more on the certificates details panel.
- To manually assign unmanaged certificate(s) to an Organization or Department, select the certificate(s) and click the 'Assign to' button. For more on this, refer to [Manually Assigning a Certificate to an Organization/Department](#) in the section [Network Discovery](#).
- Click the 'Last Scan Details' button to view the latest certificates discovered by a discovery task

The screenshot shows the 'Discovery Tasks' section of the Comodo Certificate Manager. A table lists various scan tasks. The 'Last Scan Details' button is circled in red. An arrow points from this button to a detailed view window for the scan 'Certs for Dithers org'.

| NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|-----------------------|-------------------------|----------------------|----------|---------------------|
| global1 | cloudflaressl.com | Successful | Manual | 08/10/2016 17:09:06 |
| ComodoSE Xen | 10.104.70.0/24 | Canceled | Manual | 06/27/2016 21:58:25 |
| bdd | bddccsoftccm1.brad.dc.c | Successful | Manual | 07/22/2016 19:16:31 |
| Scan for bDD | bddccsoftccm1.brad.dc.c | Partially Successful | Manual | 08/10/2016 19:07:53 |
| test | 10.104.70.0/24 | Scan in Progress 0% | Manual | |
| Certs for Dithers org | bddccsoftccm1.brad.dc.c | Successful | Manual | 08/18/2016 16:06:47 |

| IP ADDRESS | COMMON NAME | VALID TO | VALID FROM | KEY ALGORITHM | KEY SIZE | SIGNATURE ALG |
|--|---------------------|------------|------------|---------------|----------|---------------|
| <input checked="" type="checkbox"/> 10.0.34.52.443 | bddccsoftccm1.brad. | 03/23/2018 | 03/22/2016 | RSA | 2048 | SHA256withRSA |

The details of certificates discovered during the the last scan ran for the selected task will be displayed.

7.2.8 View Scan Results

After each discovery scan, Comodo Certificate Manager updates the lists of certificates in the **Network Assets** area and the **'SSL Certificates'** area ('Certificates' > 'SSL' Certificates).

Certificates are assigned to these two areas as follows:

SSL Certificates interface

- Managed Certs
- Unmanaged certs which are assigned to an Org/Dep.

Network Assets interface

- Managed certs

- Unmanaged certs which are assigned to an Org/Dep.
- Unmanaged certs which are **not** assigned to an Org/Dep.

Network Assets Area:

The Network Assets area displays certificates discovered from all nodes of every scanned network, including web servers, domains and certificates discovered from AD servers integrated to CCM.

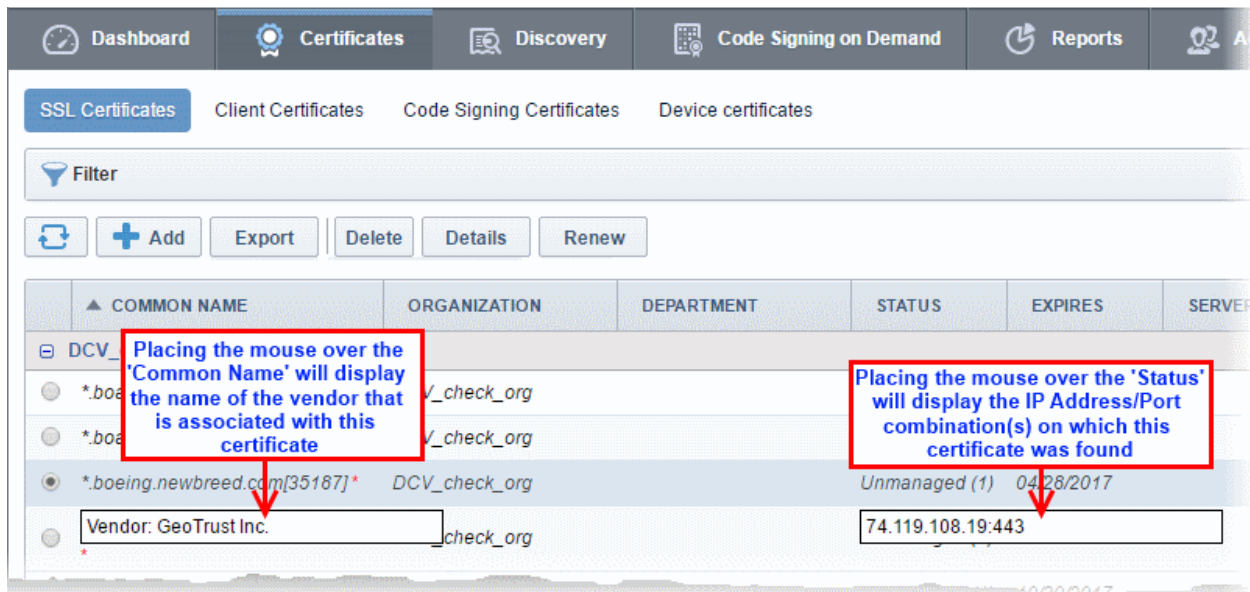
- **Network Discovery** - Displays a tree structure of scanned networks. Selecting a node displays all certificates identified on it, including managed certificates, unmanaged certificates that have been assigned to an Organization/Department by a rule, and unmanaged certificates that have not been assigned to a Organization/Department. You can view details of each certificate and manually assign unmanaged certificates to an Organization or Department. Doing so will grant them 'Managed' status and thus make them visible in the 'SSL Certificates' interface. Refer to the section **Network Discovery** for more details.
- **Web Servers** - Displays a summary of all web-servers identified from every network scanned and a list of websites/domains hosted on each identified server. Refer to the section **Web Servers** for more details.
- **Active Directory** - Displays a tree structure of Active Directory domains that have been integrated to CCM by installing the MS agent. Expanding a tree and selecting an object (like a user account, device or computer) will open a list of all certificates associated with that object. You can view details of each certificate and manually assign unmanaged certificates to Organizations or Departments. Doing so will make them available in the SSL Certificates interface. Refer to the section **Active Directory** for more details.

SSL Certificates Area:

After a discovery scan, CCM will add newly discovered 'unmanaged' certificates which have been assigned to an Org/Dep to the SSL certificates area. It will also update the status of any existing certificates. There are, therefore, two types of SSL certificates that could be discovered:

- **Certificates issued by Comodo Certificate Manager (also known as 'Managed' certificates).** Comodo Certificate Manager will simply update the certificate's existing entry with any status changes that may have occurred. These certificates will stay assigned to the Organizations that they are currently assigned to.
- **Certificates that were *not issued* by Comodo Certificate Manager (also known as 'Unmanaged certificates)** If the certificate was NOT issued by CCM, they will be assigned 'Unmanaged' status. The 'Unmanaged' category covers:
 - Self-signed certificates
 - Certificates issued by Comodo CA but not via Comodo Certificate Manager
 - Certificates issued by 3rd party vendors / other certificate authorities

Note: Only those 'Unmanaged' certificates that are assigned to an Org/Dep (either manually or by an assignment rule) will be added to the 'SSL Certificates' area at the end of a Discovery Scan. Discovered certificates which are not assigned to any Organization or Department will not be added to the SSL Certificates area. They can be viewed in the Network Assets interface.



To bring an 'Unmanaged' certificate under the control of Comodo Certificate Manager you have to 'Renew' that certificate (to be more precise you will be effectively 'replacing' that certificate with an equivalent Comodo certificate). Clicking the 'Renew' button will begin the ordering process for a new Comodo SSL certificate with the same parameters.

| Certificate Type | | View in the SSL Certificates Sub-Tab | | | |
|---------------------------------|-------------------------------------|---|--|--|--|
| | | State | View | | |
| Certificates, not issued by CCM | Certificates, issued by CCM | One of the SSL certificates state listed here . | <input type="checkbox"/> testdomain.com Test Organization Test Department 1 Applied <input type="checkbox"/> example.com Demo Organization Demo Department Declined <input type="checkbox"/> www.senthil Test Organization Expired 08/18/2012 | | |
| | Self-signed certificates | Unmanaged | ✖ landfill.addons.allizom.org Demo Organization Unmanaged (1) 02/13/2021 Self-signed certificates are marked with red cross alongside their common name. (Background - 'Self Signed' means that the certificate was not signed (issued) by a Trusted Certificate Authority. As such, these certificates will not be recognized by popular Internet browsers such as IE, Firefox, Opera, Safari and Chrome.) From the 'SSL Certificates' interface, you can: <ul style="list-style-type: none"> • View details of these certificates • 'Renew' these certificates by replacing them Comodo equivalents | | |
| | Issued by Comodo CA but not via CCM | Unmanaged | test2.ccmqa.com Demo Organization Unmanaged 01/03/2014 From the 'SSL Certificates' interface, you can: <ul style="list-style-type: none"> • View details of these certificates • Revoke these certificates • 'Renew' these certificates | | |
| | Issued by 3rd party vendor | Unmanaged | example.com Test Organization Unmanaged (1) 08/08/2015 From the 'SSL Certificates' interface, you can: | | |

| Certificate Type | View in the SSL Certificates Sub-Tab | |
|------------------|--------------------------------------|---|
| | State | View |
| | | <ul style="list-style-type: none"> View details of these certificates 'Renew' these certificates by replacing them Comodo equivalents |

You can download the results of a discovery scan in .csv format in a **Discovery Scan Log** report from the **Reports** interface.

The **Discovery Scan Log** report contains information concerning overall scan options and discovered SSL certificates information.

Comodo advises administrator to:

- i. Schedule regular discovery scans as a matter of course;
 - ii. Run a manual scan after every change to SSL certificate configuration. Otherwise, it is possible that the 'SSL Certificates' area will show inaccurate information. (e.g. you may have uploaded a certificate to your website but in CCM the certificate will have a state of 'Issued' and a discovery status of '**Not deployed**' if you haven't re-run the scan).
 - iii. Run a manual scan after any change to the network in general.
- To remove the certificates discovered from a particular discovery scan, navigate to 'Discovery' > 'Discovery Tasks', select the discovery task and click the 'Clean Results' button.

The screenshot shows the 'Discovery Tasks' section of the Comodo Certificate Manager. A table lists the following tasks:

| NAME | RANGES TO SCAN | STATE | SCHEDULE | LAST SCANNED |
|--------------|-------------------------|------------|----------|---------------------|
| global1 | cloudflaressl.com | Successful | Manual | 08/10/2016 17:09:06 |
| ComodoSE Xen | 10.104.70.0/24 | Canceled | Manual | 06/27/2016 21:58:25 |
| bdd | bddccsoftccm1.brad.dc.c | Successful | Manual | 07/22/2016 19:16:31 |

A dialog box titled 'Certificate Manager' is open, showing a warning icon and the message: 'The certificates found during this scan will be deleted from the SSL Certificates Tab.' with 'OK' and 'Cancel' buttons.

- Click 'OK' to confirm removal of the certificates in the SSL Certificates interface.

7.3 Agents

Comodo Certificate Manager uses agents for:

- **Automatic installation of certificates (on Apache Httpd, Apache Tomcat and IIS 7. 7.5 and 8 only)** - The controller/agent installed on the web server, will periodically poll CCM for requests for certificates that have been enabled for auto-installation. If a request exists, it will automatically generate a CSR on the web server and present the application for administrator approval via the CCM interface. On approval, the agent submits the CSR to Comodo CA and tracks the order number. Once the certificate is issued by the CA, the agent downloads the certificate and allows the administrator to install the certificate from the CCM interface. A controller installed on a single server can be configured to communicate with, and install certificates on, other remote servers in the network.
- **Discovery of SSL certificates installed on internal servers** - An agent installed on a web server or any local machine in the network will scan and monitor internal servers for all installed SSL certificates. It is possible for administrators to configure Comodo CM to scan externally facing IP addresses directly from the 'Discovery Tasks' area (as explained in [Discovery Tasks](#)). However, Comodo CM can only scan internal hosts IF an agent which is configured to communicate with the Comodo CM servers is installed on the local network. After scanning the local network, the agent will send a report back to the Comodo CM console.

Note: The 'auto-installer' feature must be enabled for your account in order for it to execute certificate installation tasks. If this feature is not enabled then the agent will only be capable of certificate discovery. Please contact your account manager if you require auto-installation to be enabled.

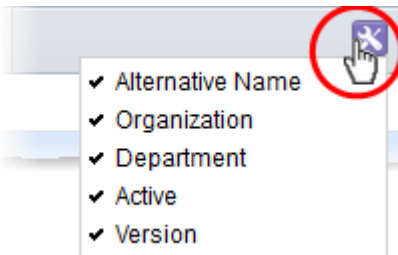
Security Roles:

- **MRAO** - Can set up Certificate Controller Agent for installing certificates and scanning internal servers of any Organization or Department, for certificates requested, issued, expired, revoked and replaced.
- **RAO SSL** - Can set up Certificate Controller agent for installing certificates and scanning internal servers of Organizations (and any sub-ordinate Departments) that have been delegated to them, for certificates requested, issued, expired, revoked and replaced.
- **DRAO SSL** - Can set up Certificate Controller agent for installing certificates and scanning internal servers of Department that have been delegated to them for certificates requested, issued, expired, revoked and replaced.

The Agents Interface:

| NAME | ALTERNATIVE NAME | ORGANIZATION | DEPARTMENT | ACTIVE | STATE | VERSION |
|--|------------------|--------------|------------|-------------------------------------|---------------|---------|
| <input type="radio"/> Agent Comodo SE 76 | | Comodo SE | | <input checked="" type="checkbox"/> | N/A | 1.9 |
| <input type="radio"/> Agent Comodo SE 91 | | Comodo SE | | <input checked="" type="checkbox"/> | Connected | 2.0 |
| <input type="radio"/> Agent Comodo SE 92 | | Comodo SE | | <input checked="" type="checkbox"/> | Not connected | 2.0 |

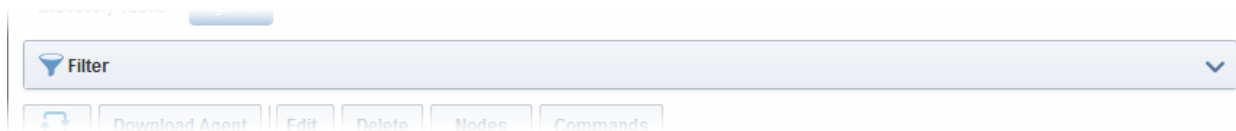
| Column Header | Description |
|------------------|--|
| Name | Displays the name specified for the Certificate Controller Agent. |
| Alternative Name | Displays the alternative name specified for the Certificate Controller Agent. |
| Organization | Displays the Organization to which the Certificate Controller Agent is associated. |
| Department | Displays the Department to which the Certificate Controller Agent is associated. |

| | | |
|--|---|--|
| Active | The checkbox displays whether the agent is active or inactive and allows the administrator to change the state if required. | |
| State | Displays whether or not the agent is connected to CCM. | |
| Version | Displays the version number of the Certificate Controller Agent. | |
| <p>Note: The administrator can enable or disable the columns as desired, from the drop-down button at the right end of the table header.</p>  | | |
| Controls | Download Agent | Enables the administrator to create a new Certificate Controller Agent and download the setup file. |
| | Refresh | Updates the list of displayed Agents. |
| Agent Controls | Edit | Enables administrators to modify the Agent configuration settings. |
| | Delete | Removes the Agent. |
| | Nodes | Enables administrators to view and edit the server nodes for which the Agent is configured. |
| | Commands | Enables administrators to view the details of the commands like generation of CSR, scanning internal servers, executed by the Agent. |

7.3.1 Sorting and Filtering Options

- Clicking on the column headers 'Name', 'Alternative Name', 'Organization', or 'Department' sorts the items in the alphabetical order of the entries in the respective column.

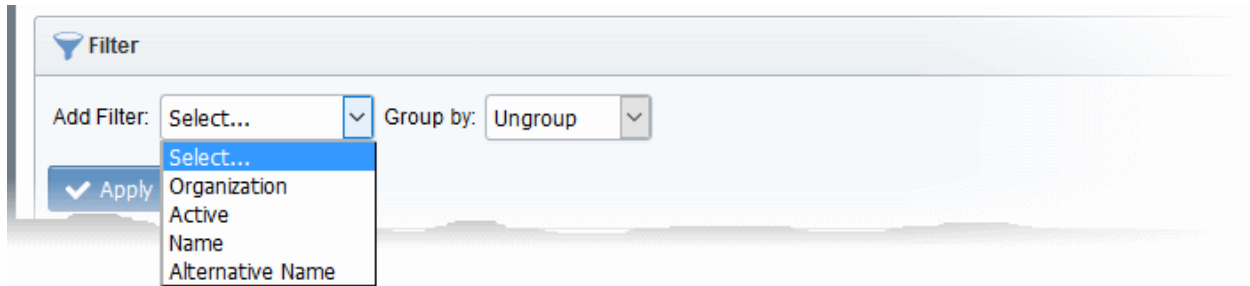
Administrators can search for a particular agent by using the filter.



You can add filters by selecting from the options in the 'Add Filter' drop-down and group the selection with other options that appears depending on the selection from the 'Add Filter' drop-down.

| Filter Options | Description |
|------------------|--|
| Organization | Enables Administrators to filter the list of Agents by Organization. |
| Active | Enables Administrators to view only the active agents. |
| Name | Enables to filter the agents by entering the name fully and partially. |
| Alternative Name | Enables to filter the agents by entering the alternative name fully and partiall |

For example if you want to search for an agent by the name filter and belonging to a particular Organization and Department:



- Choose 'Name' from the 'Add Filter' drop-down and enter the name of the agent in full or part.
- Select 'Organization' or 'Department' in the 'Group by:' drop-down.
- Click the 'Apply' button.

The filtered items based on the entered and selected parameters will be displayed:

Filter is applied

Add Filter: Group by:

| | NAME | ALTERNATIVE NAME | ORGANIZATION | DEPARTMENT | ACTIVE | STATUS |
|----------------------------------|--------------------|------------------|--------------|------------|-------------------------------------|--------|
| <input type="radio"/> | Agent Comodo SE 76 | | Comodo SE | | <input checked="" type="checkbox"/> | N/A |
| <input type="radio"/> | Agent Comodo SE 91 | | Comodo SE | | <input checked="" type="checkbox"/> | Conne |
| <input checked="" type="radio"/> | Agent Comodo SE 92 | | Comodo SE | | <input checked="" type="checkbox"/> | Not co |

- To remove the filter options, click the 'Clear' button.

Note: The search filters once configured for the interface will be automatically saved. When you are re-opening the 'Agents' interface in future, the configured filters will be in action and only the search results will be displayed. If you do not want the filters to be saved, click the 'Clear' button.

7.3.2 Configuring the Agent for Auto-Installation and Internal Scanning - Overview of the Process

This section is a brief summary of the steps needed to set up a certificate controller/agent for automatic installation and renewal of SSL certificates and run an internal scan. Click any of the bullet points below to go to a more

detailed explanation of that stage:

1. **Add a new IP range for Internal Scanning by creating a new CIDR in the Discovery Tasks tab.**
2. **Download and Install the agent on a server**
3. **Configure the Agent for adding CIDR ranges for certificate discovery and specifying local and remote servers on to which the certificates are to be auto-installed.**
4. **Return to the 'Discovery Tasks' tab and click 'Scan'.**
5. **The results can be viewed by selecting the 'Discovery Scan Log' under the 'Reports' tab. Newly discovered certificates will be added to the 'SSL Certificates' area of 'Certificates Management' and assigned to the Organization that has been set for that agent.**

7.3.3 Prerequisites

The administrator has defined at least one Organization. The Organization will be designated as the owner of certificates discovered by the agent during the agent configuration and installation process.

7.3.4 Configuring the Agent for Auto-Installation and Internal Scanning - Detailed Explanation of the Process

1. Add a new IP range for Internal Scanning by creating a new CIDR in the 'Discovery Tasks' tab and specify the ports to be scanned. The IPs you enter here should, naturally, be internal addresses. Once added, you will be able to initiate internal scans from this interface by clicking the 'Scan Now' button. See **Adding IP range and Start Scanning** for further reading.

Add Scan Range (CIDR > Scan) [X]

CIDR
e.g. 10.10.10.10/32

IP*
10.108.17.117

Host name
e.g. host1.domain.com

Port*
443

OK Cancel

Note: CCM is capable of scanning for installed certificates in external servers via Internet. If there is no agent installed in the server to be scanned, CCM will request the user to install the agent.

2. Download and Install the agent on a server in the network.

Note: The Agent is also responsible for automatic application and installation of SSL certificates. The Agent installed on one of the servers can be configured to communicate with the other web servers in the network without the need of any additional software, hence is capable of installing certificates on to the remote servers automatically. The important aspect is that the all the servers should be able to connect to CCM.

- To download the Certificate Controller Agent setup file, click 'Download Agent' from the Agents interface.

The screenshot shows the 'Agents' interface in Comodo Certificate Manager. The 'Download Agent' button is highlighted with a red circle. A red arrow points from this button to a 'Download' dialog box. The dialog box contains the following text and controls:

After the download has been completed, please install the Agent.
In the event that you already have an Agent configured, you can edit existing data.

Organization* Dithers Organization

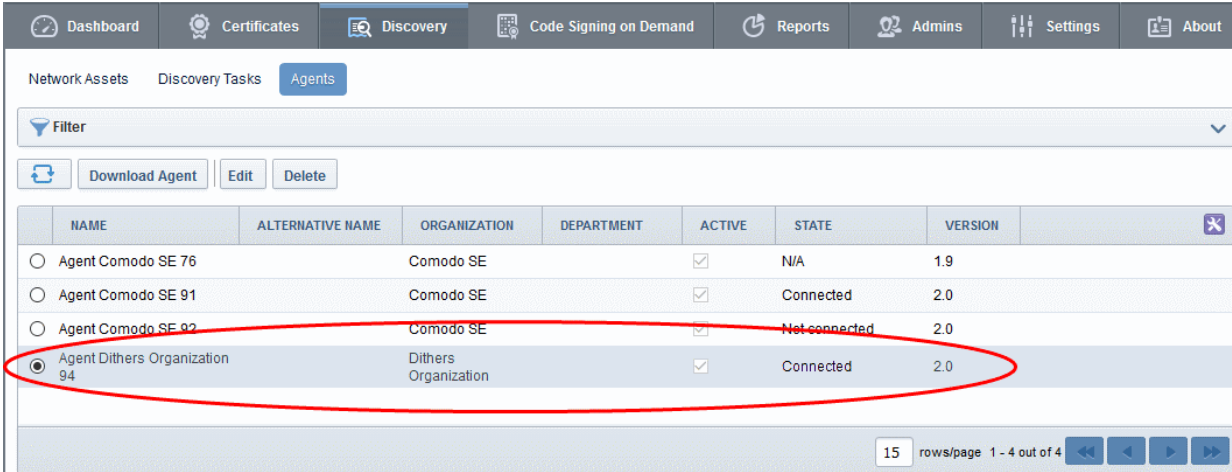
Department* ANY

Please select your Operating System

Windows Linux x86 Linux x64

Download Cancel

- Select the Organization/Department(s) for which you want to use the Certificate Controller Agent for auto-installation and discovery of certificates and choose Windows version or Linux version of the Agent setup file depending on the Operating system of the server.
- Click 'Download' and browse to the location where you want to save the setup file.
- The certificate controller / agent needs administrative privileges for installation. To install the Agent, right click on the setup file and select 'Run as Administrator' and follow the setup instructions in the wizard. If you are installing the Linux version of the Agent, run the installation from the command line.
- On completion of installation, the Agent will be added to the CCM interface.



| NAME | ALTERNATIVE NAME | ORGANIZATION | DEPARTMENT | ACTIVE | STATE | VERSION |
|--|------------------|----------------------|------------|-------------------------------------|---------------|---------|
| <input type="radio"/> Agent Comodo SE 76 | | Comodo SE | | <input checked="" type="checkbox"/> | N/A | 1.9 |
| <input type="radio"/> Agent Comodo SE 91 | | Comodo SE | | <input checked="" type="checkbox"/> | Connected | 2.0 |
| <input type="radio"/> Agent Comodo SE 92 | | Comodo SE | | <input checked="" type="checkbox"/> | Not connected | 2.0 |
| <input checked="" type="radio"/> Agent Dithers Organization 94 | | Dithers Organization | | <input checked="" type="checkbox"/> | Connected | 2.0 |

- The next step is to configure the Agent to:
 - apply for and install SSL certificates on the local server
 - apply for and install SSL certificates on the remote servers in the network
 - scan the internal network by linking it to the CIDR created under the 'Discovery' tab for internal scanning, by specifying the IP Range of the internal network
- To Edit the Agent Properties, click the 'Edit' button at the top after selecting the Agent

Edit Agent (Last activity: a moment ago)
✕

*-required fields

Name*

Version 2.0

IP address

Local configuration URI <https://192.168.155.150:9090> ⓘ

Alternative Name

Active

Auto update Enabled

Organization*

Department*

Secret Key (min 10 symbols)*

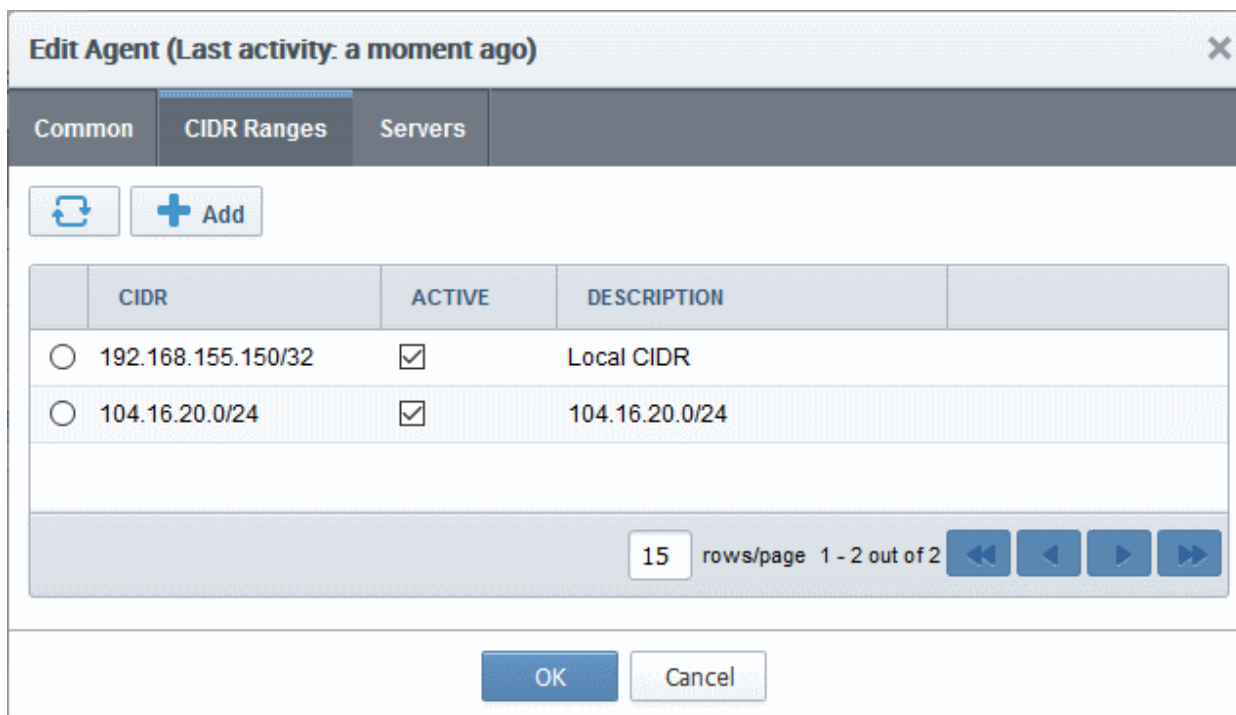
Keystore password DxU1Mztjgx

Comments

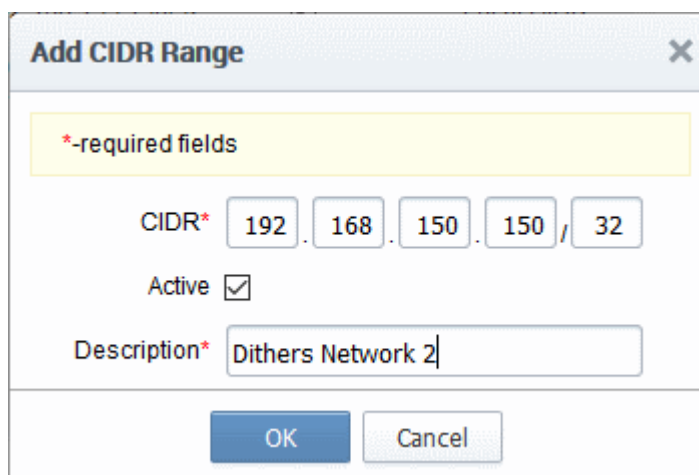
| Edit Agent > Common Tab - Table of Parameters | | |
|---|---------------|---|
| Field Name | Type | Description |
| Name | <i>String</i> | Enables the Administrator to edit the name of the Certificate Controller Agent. |
| Version | | Displays the version number of the Agent. |
| IP Address | | Displays the IPv6 Loopback address, IPv4 loopback address, IPV6 IP Address, IPv4 IP Address or the physical address of the server on which the agent is installed |
| Local Configuration | | Displays the IP of the server in which the agent is installed. This URL is used to access the agent via a web browser for managing. Refer to the |

| Edit Agent > Common Tab - Table of Parameters | | |
|---|-----------------------|---|
| URI | | section Configuring the Certificate Controller Agent through Web Interface for more details. |
| Alternative Name | <i>String</i> | Enables the Administrator to specify an alternative name for the Agent |
| Active | <i>Checkbox</i> | Enables the Administrator to set the Agent in active state or inactive state. |
| Auto update | <i>String</i> | Indicates whether the agent is enabled for auto update |
| Organization | <i>Drop-down list</i> | Enables the Administrator to change the Organization associated the Agent. |
| Department | <i>Drop-down list</i> | Enables the Administrator to change the Department associated with the Agent. |
| Secret Key | <i>String</i> | Displays the secret key generated by the Agent to authenticate itself to Remote Comodo CM server. The secret key must have 10 characters. The administrator can copy and save the secret key in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server, to authenticate itself to the CCM server for scanning the same internal network. |
| Keystore password | <i>String</i> | Displays the key store password generated by the Agent. The administrator can copy and save the secret key store password in a safe location for use in a new agent, in case the agent has to be reinstalled in the same server. |
| Comments | <i>String</i> | Enables the Administrator to type a descriptive comment on the purpose of the Agent |

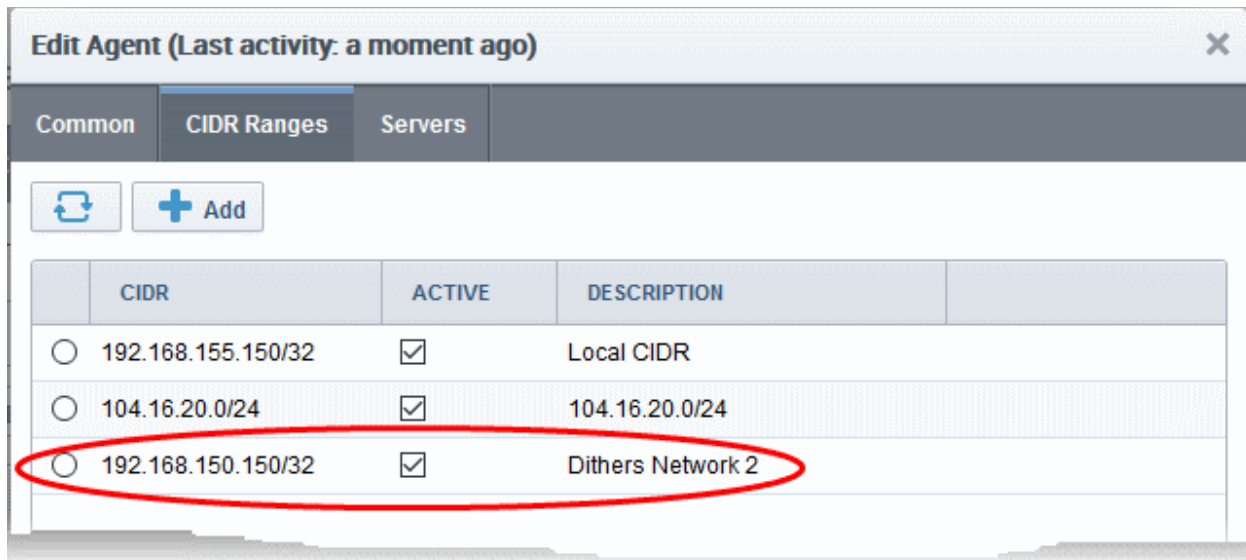
- Edit the values if required. To edit the CIDR ranges, click the 'CIDR Ranges' tab. The CIDR Ranges tab will open.



- To add a new CIDR range, click 'Add'. The 'Add CIDR Range' dialog will open.

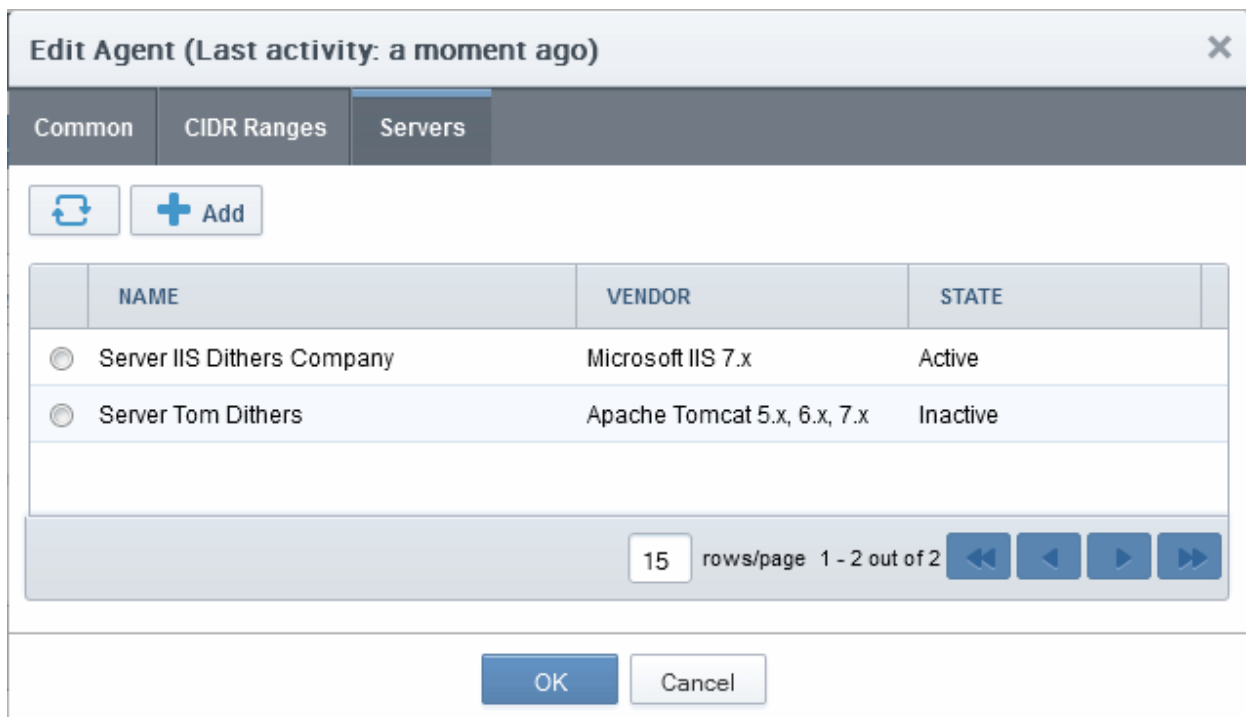


- Enter the internal IP address range to be scanned, set whether the Agent is to be Active and type a description for the range in the dialog and click 'OK'. The CIDR Range will be added in the 'CIDR Ranges' tab.



You can add as many ranges as you want by repeating the same procedure.

- To edit an existing CIDR range, select it and click 'Edit' from the top. The Edit CIDR Range dialog will open.
- To delete an existing CIDR range, select it and click 'Delete' and click 'OK' in the confirmation dialog
- To configure servers for auto-installation of certificates and scanning by the agent, click the 'Servers' tab.



The Servers tab displays the list of Servers for which the agent is configured for auto-installation of certificates. On installation, the agent discovers the server upon which it is installed and adds it to the list automatically, enabling auto-installation of certificates on it.

You can edit the properties of the server by selecting it and clicking the Edit button from the top.

Edit Web Server - Table of Parameters

| Field Name | Type | Description |
|---------------------------|-----------------------|---|
| Name | <i>String</i> | Enables the Administrator to edit the name of the Server. |
| Vendor | <i>Drop-down list</i> | Enables the Administrator to select the vendor of the server. |
| Path to web server | <i>String</i> | Enables the Administrator to specify the network path for Apache. This is required only if Apache server is not accessible from the CCM console. |
| State | | Indicates whether or not the server is connected to CCM. |
| Remote | <i>Checkbox</i> | Enables the Administrator to specify whether the server is local or remote. For the server in which the agent is installed, the checkbox should remain un-selected. |

Configuring the Certificate Controller for Automatic Certificate Installation on Remote Servers

You can add other remote servers in the network to enable the agent to communicate with them. The agent polls CCM periodically for certificate requests for the added remote servers. If a request exists, it will automatically generate a CSR on the web server and present the application for administrator approval via the CCM interface. On approval, the agent will submit the CSR to Comodo CA and track the order number. Once the certificate is issued by the CA, the agent will download the certificate and allow the administrator to install the certificate from the CCM interface.

To add a remote server to the agent

- Select the agent and click the 'Edit' but at the top and move to the 'Servers' tab by clicking 'Next' two times in the 'Edit Agents' dialog
- Click 'Add' under the 'Servers' tab in the 'Edit Agent' dialog

Add Web Server
✕

*-required fields

Name*

Vendor*

State Init

Path to web server ⓘ

Remote

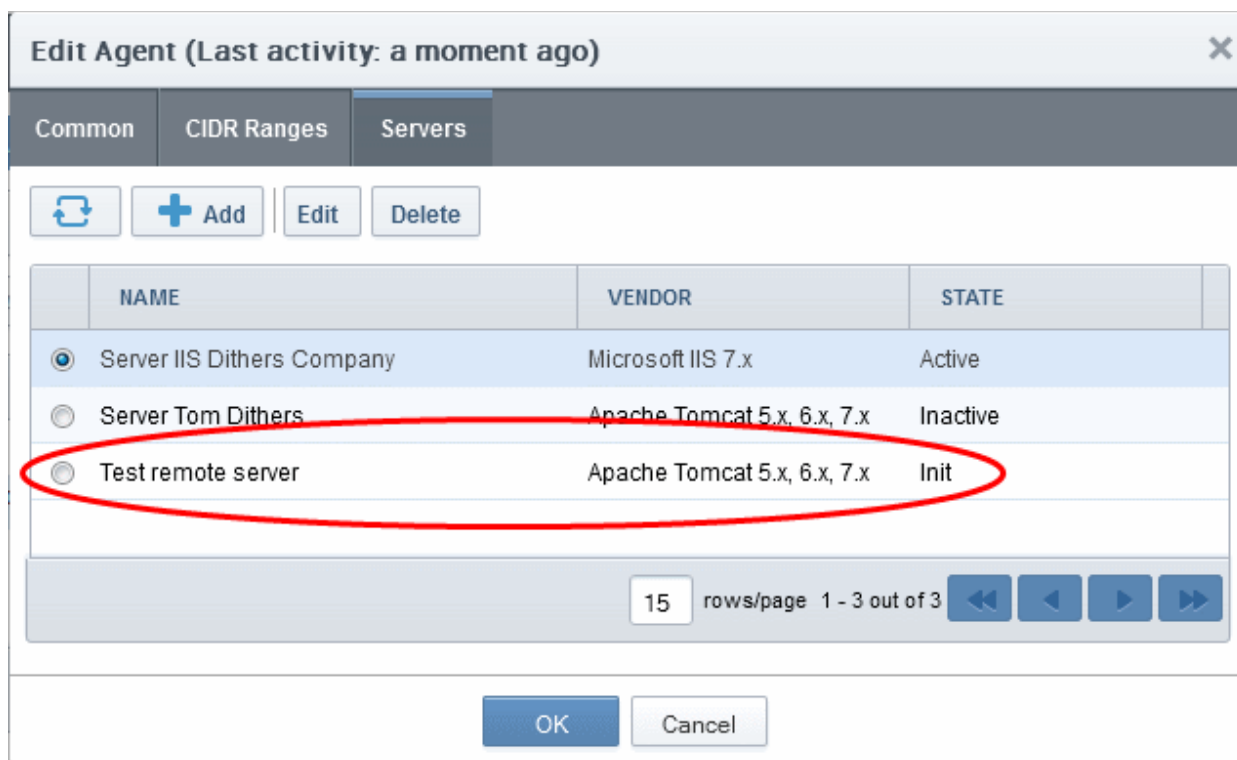
IP address / Port* . . . :

Username

Password

| Add Web Servers - Table of Parameters | | |
|---------------------------------------|------------------|--|
| Field Name | Type | Description |
| Name | <i>String</i> | Enter the name of the server. |
| Vendor | <i>drop-down</i> | Choose the vendor of the server. |
| State | <i>String</i> | Indicates whether or not the server is initialized. |
| Path to Web Server | <i>String</i> | Enables the Administrator to specify the network path for remote Apache 2.x and Tomcat servers. This is required only if Apache server is not accessible from the CCM console. |
| Remote | <i>Checkbox</i> | Enables the Administrator to specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected. |
| IP Address / Port | <i>String</i> | Specify the IP address and connection port of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected. |
| User Name | <i>String</i> | Specify the username of the administrator for logging-into the server. Note: This field will be enabled only if 'Remote' is selected. |
| Password | <i>String</i> | Specify the log-in password for the administrator account for logging-into the server Note: This field will be enabled only if 'Remote' is selected. |

- Enter the parameters and click OK.



The remote server will be added with the state 'Initialized'.

- Click 'OK' in the 'Edit Agents' dialog to save your changes.

The agent will discover the newly added server and connect to it within a few minutes and the state will be changed to 'Connected'.

The Agent, is now configured to auto-install the certificates in the remote server and to scan the internal network. The Agent authenticates itself to remote Comodo CM server via combination of the secret key and awaits further instructions. The Agent polls CCM every 1 minute to find out whether there are any instructions such as an instruction to 'Scan Now'. When the 'Scan Now' button is clicked, CCM will tell the agent which CIDRs to scan. The agent performs this scan and sends the results back.

The Agent properties can be configured through the Agent's web interface accessible by typing `http://<IP Address/host name of the server on which the agent is installed>:9090` in the browser address bar. The administrator can change the connection settings, polling interval, certificate management settings and server settings from the web interface. Refer to the section [Configuring the Certificate Controller Agent through Web Interface](#) for more details.

3. Go back to 'Certificates Discovery' tab and click 'Scan Now'. You can also schedule the scans to run periodically to discover the SSL certificates installed in the internal servers. See [Adding IP range and Start Scanning](#) for more details.
4. Certificate discovery results can be viewed by selecting the 'Discovery Scan Log' under the 'Reports' tab. Newly discovered certificates will be added to the 'SSL Certificates' area of 'Certificates Management'. All certificates will be assigned to the Organization that was specified for the agent in [Step 2](#).
 - See the section, [View Scan Results](#), for a more detailed account of scan reports and managing newly discovered certificates. Administrators that have not already done so may also want to familiarize themselves with the information in section [The SSL Certificates Area](#).

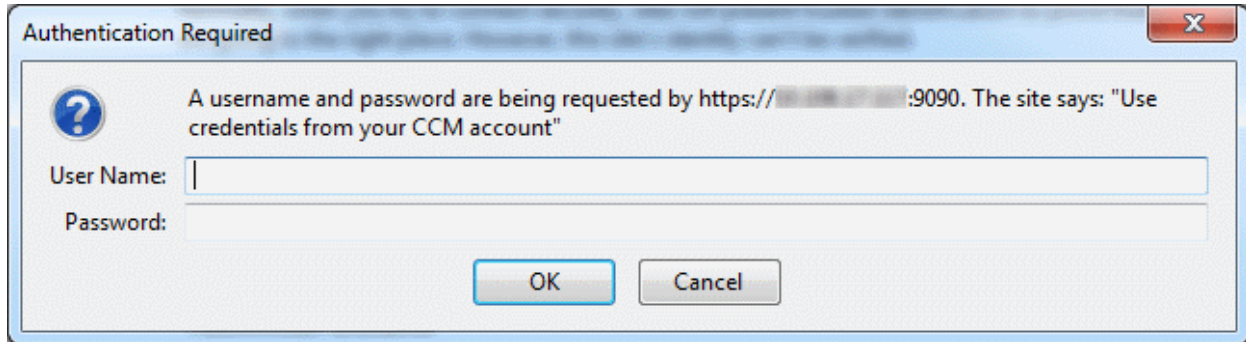
7.3.5 Configuring the Certificate Controller Agent through Web Interface

The Certificate Controller Agent can be configured by logging-in to its web-interface.

To access the Agent configuration web interface

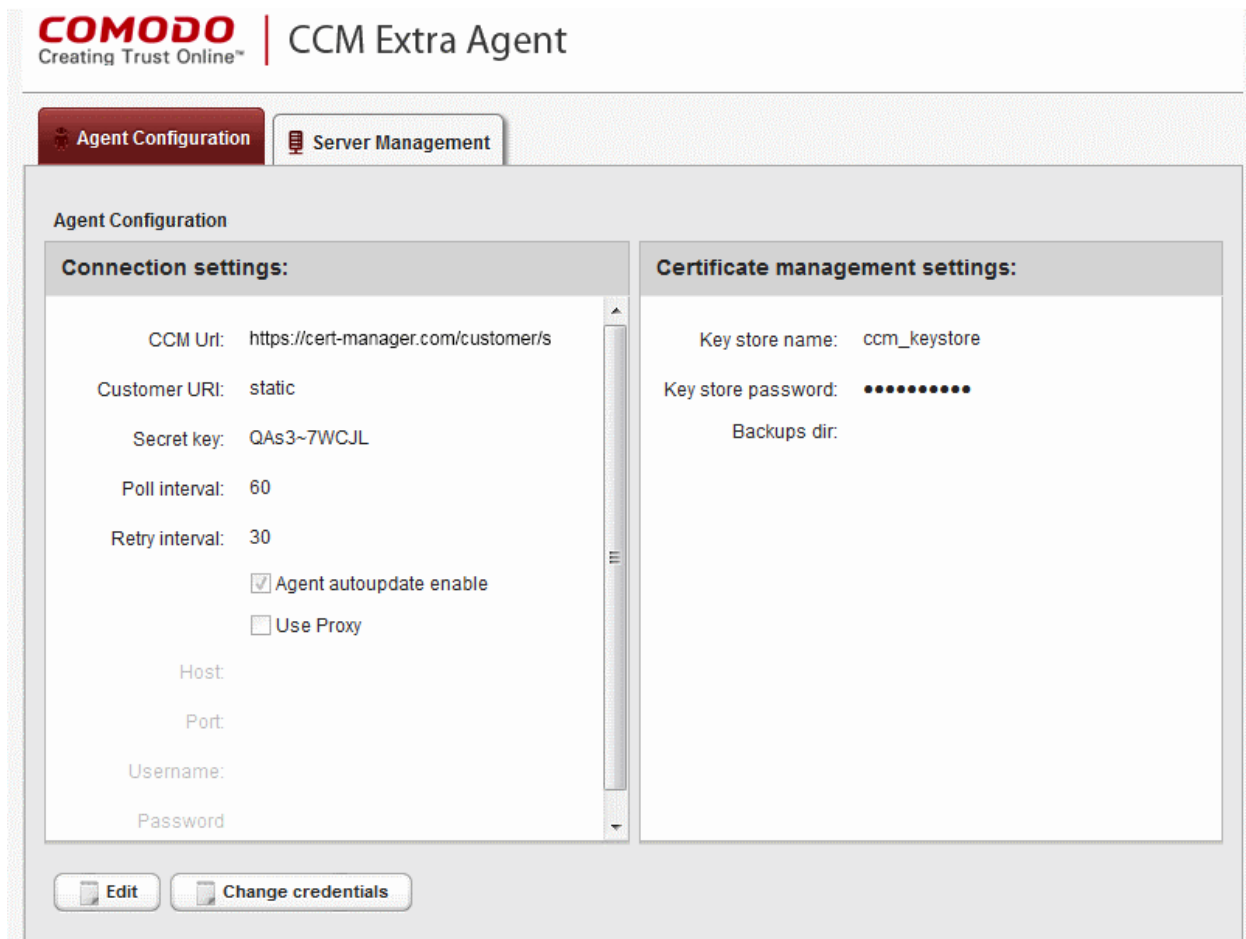
- Type `http://<IP Address/host name of the server on which the agent is installed>:9090` in the address of your browser.

The login dialog will appear:



- Enter your CCM username and password.

The Agent configuration interface will open.

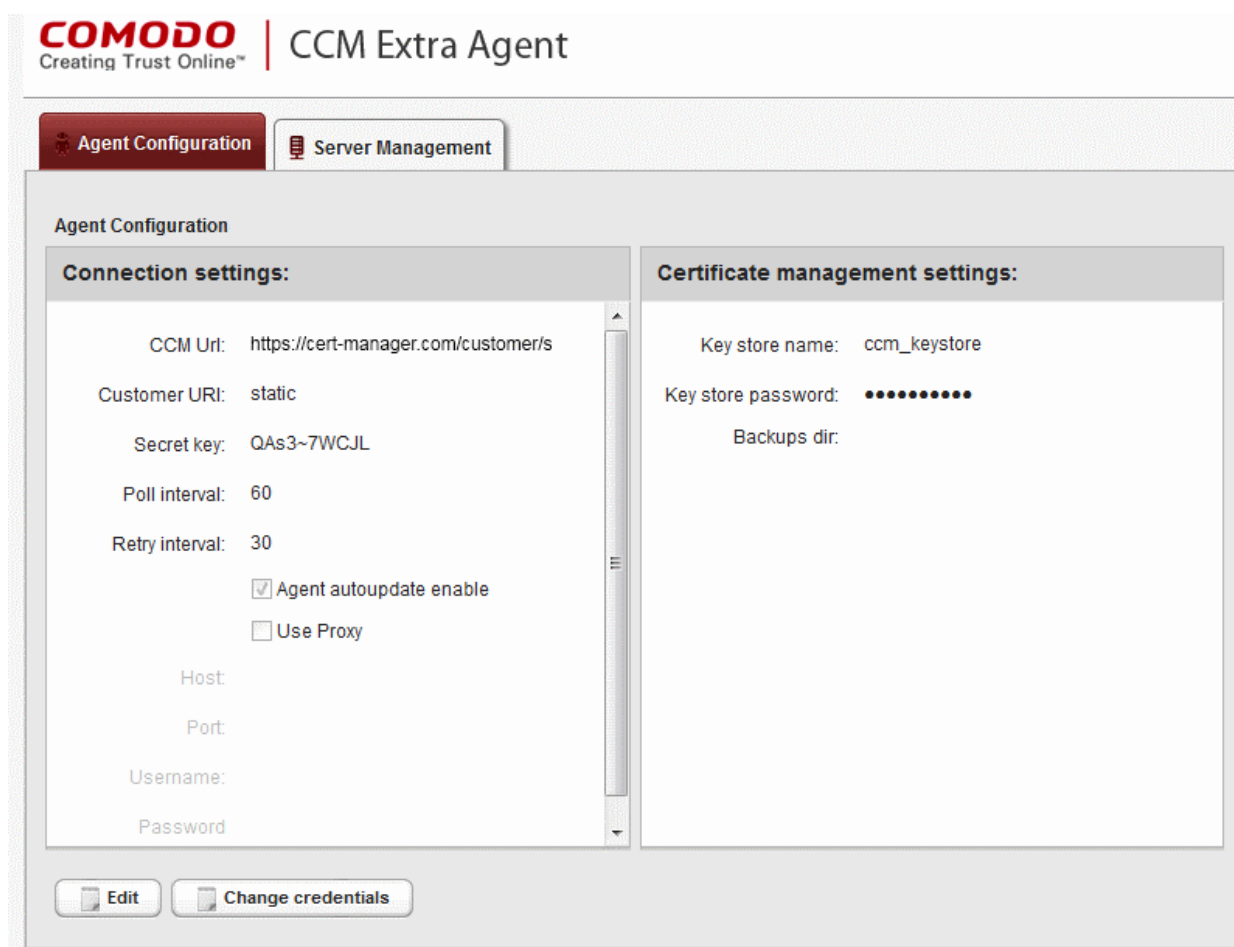


It has two tabs:

- **Agent Configuration**
- **Server Management**

7.3.5.1 Agent Configuration

The Agent Configuration tab displays the connection management settings and certificate management settings of the agent and enables the administrator to edit them, if required.

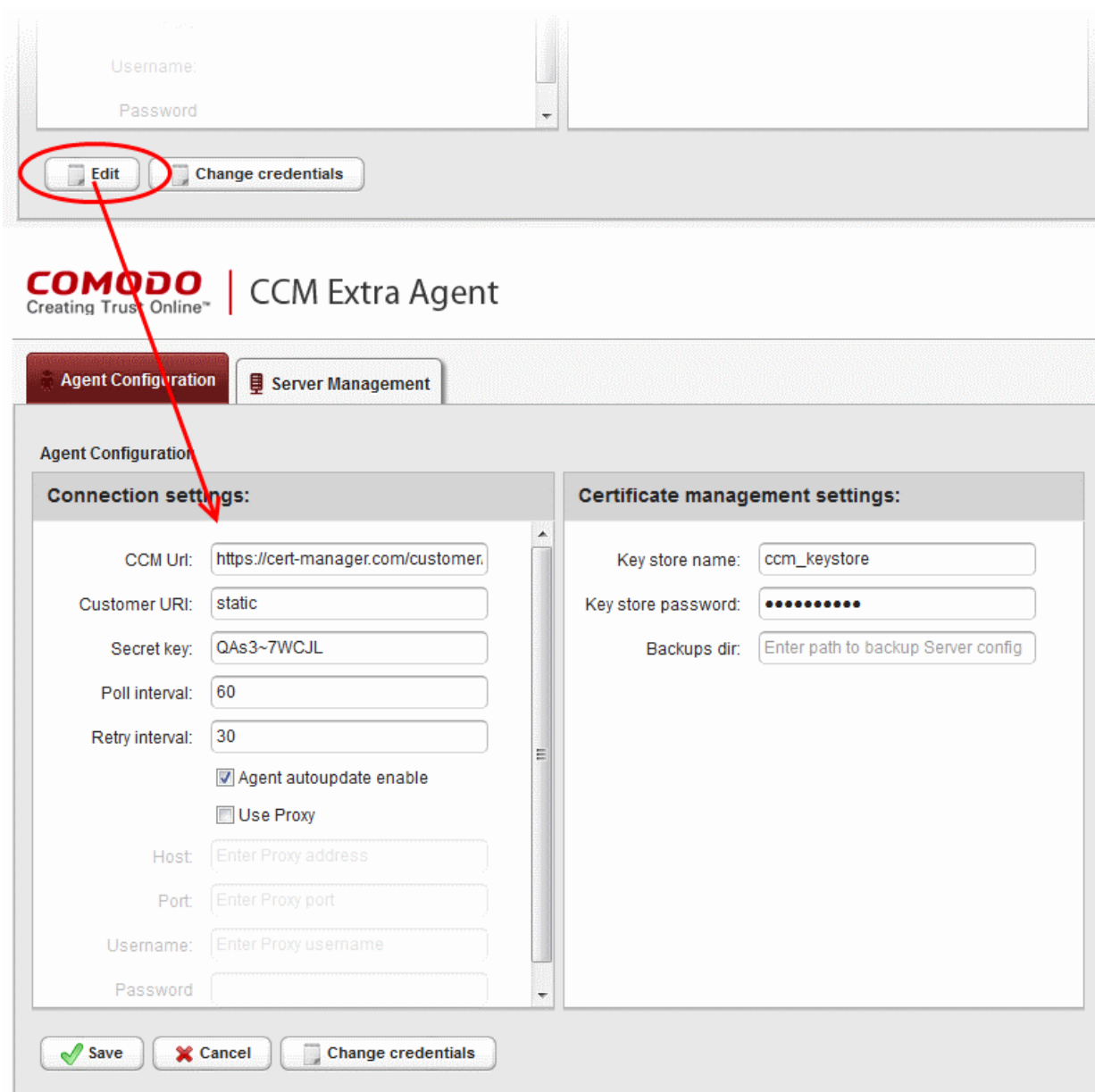


Agent Configuration - Table of Parameters

| Field | Type | Description |
|--------------------------------|-------------------|---|
| Connection Settings | | |
| CCM url | <i>Text field</i> | Displays the URL of CCM server |
| Customer URI | <i>Text field</i> | Displays the uniform resource identifier (URI) of the customer |
| Secret key | <i>Text field</i> | Displays the secret key unique to the agent, which it uses to identify it to CCM. This value should not be altered |
| Poll Interval | <i>Text field</i> | Displays the time interval at which the agent polls the CCM for new certificate requests (in seconds) and enables the administrator to edit it in edit mode. |
| Retry interval | <i>Text field</i> | Displays the time interval set for retrying polling on CCM server if polling fails (in seconds) and enables the administrator to edit it in edit mode. |
| Agent autoupdate enable | <i>Checkbox</i> | Indicates whether the agent is enabled for auto-update. The checkbox enables the administrator to switch the auto-update on/off in edit mode. |
| Use Proxy | <i>Checkbox</i> | Indicates whether the agent is configured to use a proxy server. The checkbox and the text fields below it enable the Administrator to instruct the agent to use proxy server and to specify the proxy server details, if |

| | | |
|--|-------------------|---|
| | | required. |
| Host | <i>Text field</i> | Displays the IP/Host name of the proxy server and enables the Administrator to specify it in edit mode |
| Port | <i>Text field</i> | Displays the port of the proxy server for the agent to connect and enables the Administrator to specify it in edit mode |
| Username | <i>Text field</i> | Displays the username of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode |
| Password | <i>Text field</i> | Displays the password of the administrator account to login to the proxy server and enables the Administrator to specify it in edit mode |
| Certificate Management Settings | | |
| Key store name | <i>Text field</i> | The name of the CCM keystore file, pertaining to the agent. By default, it will be 'ccm_keystore'. The Administrator can edit it in the edit mode |
| Keystore password | <i>Text field</i> | The password to access the CCM keystore file. The Administrator can edit it in the edit mode |
| Backup dir | <i>Text field</i> | Displays the folder path for backup of keystore file. The Administrator can edit it in the edit mode. |

- To edit the agent configuration settings, click the 'Edit' button at the bottom left. The Agent Configuration page will open in edit mode.



- Edit the required fields and click 'Save' for your changes to take effect.

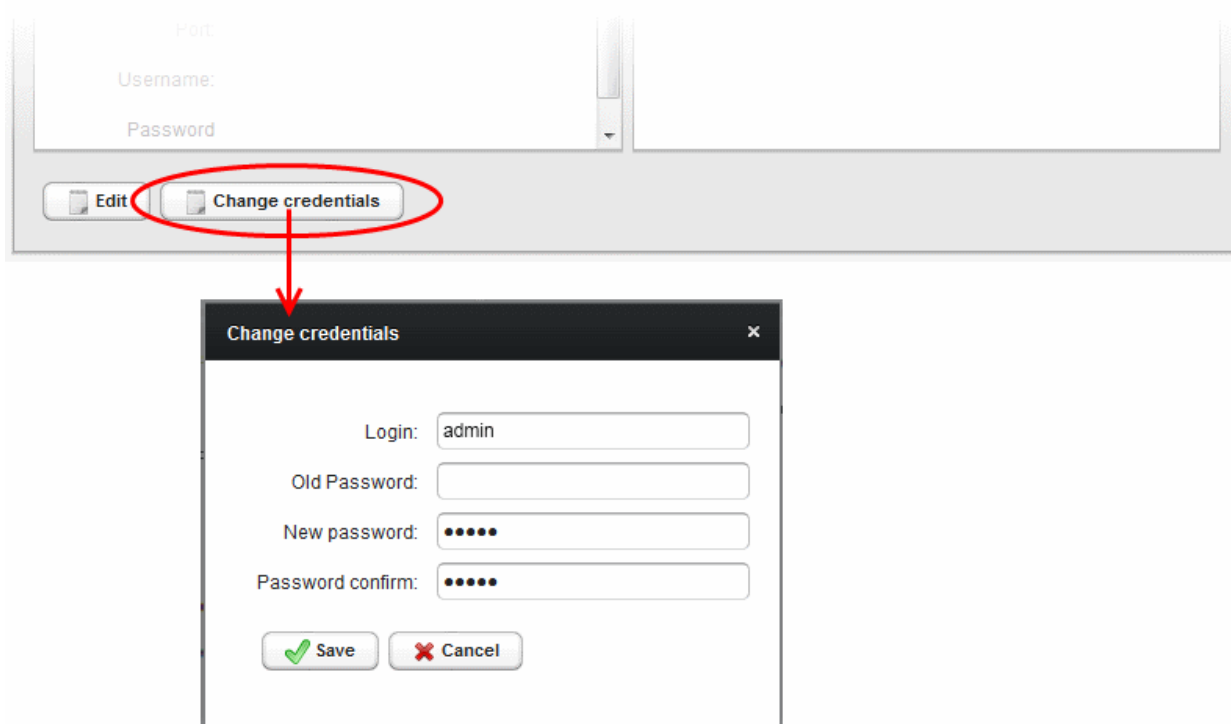
Changing Login Credentials for the Agents Configuration Console

By default, the administrator can use the username and password of their CCM account to login to the agent configuration. If needed, the administrator can change their username and password for the agent configuration console at any time.

To change the username and password

- Click 'Change credentials' from the agent configuration interface.

The 'Change Credentials' dialog will appear.

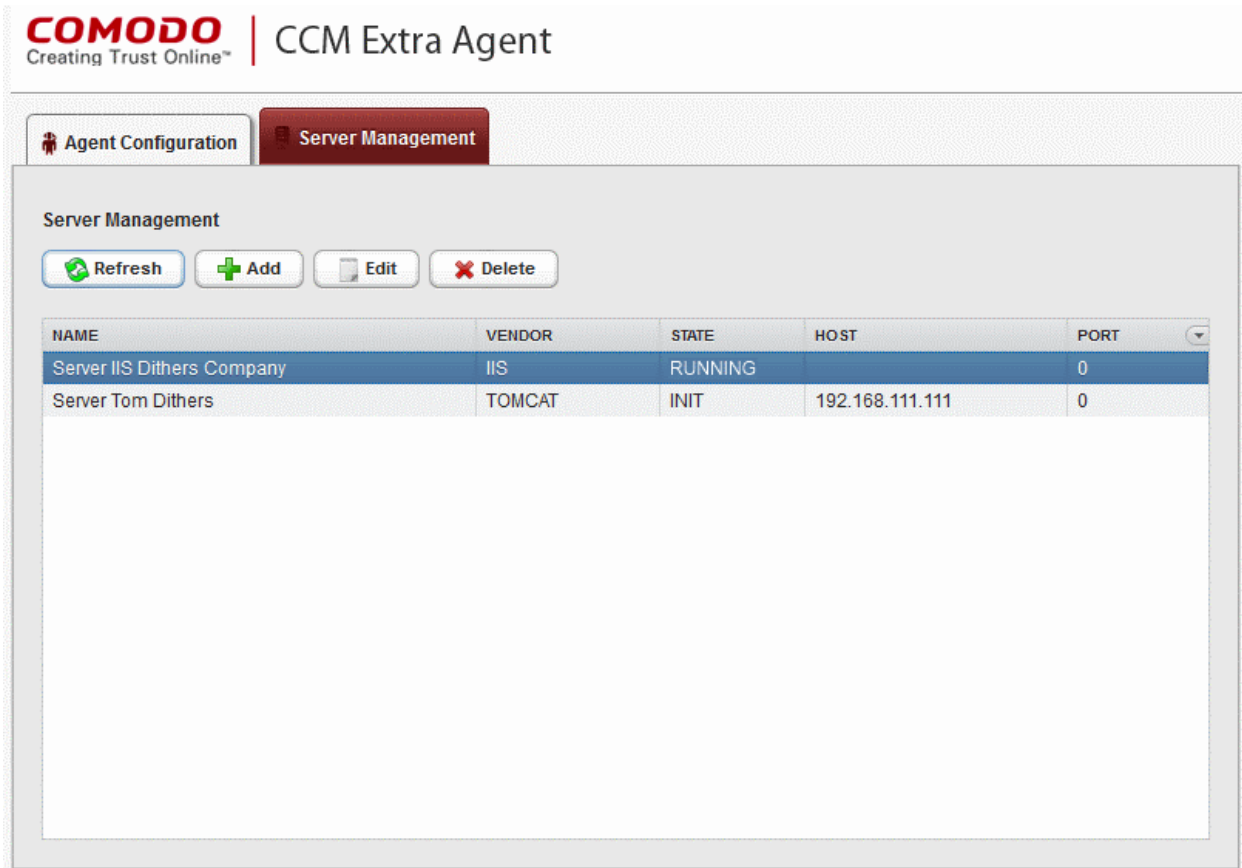


- To change your username, directly edit the Login field
- Enter your existing password in the 'Old Password' field
- Enter your new password in the New password field and reenter it for confirmation in the Password Confirmation field
- Click 'Save'

From the next login to the agent configuration console, you need to use the new username and password.

7.3.5.2 Server Management

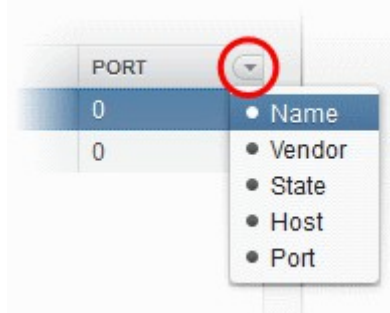
The 'Server Management' tab enables the administrator to view, add and edit the servers for which the agent is configured.



The 'Server Management' tab displays the list of servers added to the agent with the vendor and activation status details. The administrator can add new servers and edit the details like the login username and password for the existing servers through this interface.

| Column Display | Description |
|----------------|--|
| Name | Displays the name of the server. |
| Vendor | Displays the vendor of the server. |
| State | Indicates whether or not the server is initialized. |
| Host | Displays the IP address or the host name of the server for remote connection |
| Port | Displays the connection port of the server for remote connection. |

Note: The administrator can enable or disable desired columns from the drop-down at the right end of the table header:



| | | |
|----------|-----|--|
| Controls | | |
| | Add | Enables the Administrator to add a new server to the agent |

| | | |
|--|---------|---|
| | Refresh | Updates the list of displayed servers. |
| Server Controls Note: The Server control buttons will appear only on selecting a server. | Edit | Enables administrators to modify the Server configuration settings. |
| | Delete | Removes the Server. |

To add a server

- Click 'Add' from the top left. The 'Add new server' dialog will appear.

The screenshot shows the 'Server Management' interface. At the top, there are tabs for 'Agent Configuration' and 'Server Management'. Below the tabs, there are buttons for 'Refresh', 'Add', 'Edit', and 'Delete'. The 'Add' button is circled in red. Below the buttons is a table with columns: NAME, VENDOR, STATE, HOST, and PORT. The table contains two rows: 'Server IIS Dithers Company' (IIS, RUNNING, 0) and 'Server Tom Dithers' (TOMCAT, INIT, 192.168.111.111, 0). Below the table is a dialog box titled 'Add new server'. The dialog box contains the following fields: 'Server name: *' (text input), 'Server vendor: *' (dropdown menu set to TOMCAT), 'Path: *optional* Enter path to tomcat' (text input), a 'Remote' checkbox, 'Host: Enter remote host ip' (text input), 'Port: 0' (text input), 'User name: Enter remote username' (text input), and 'Password:' (text input). At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

Add new server - Table of Parameters

| Field Name | Type | Description |
|-------------|--------|-------------------------------|
| Server name | String | Enter the name of the server. |

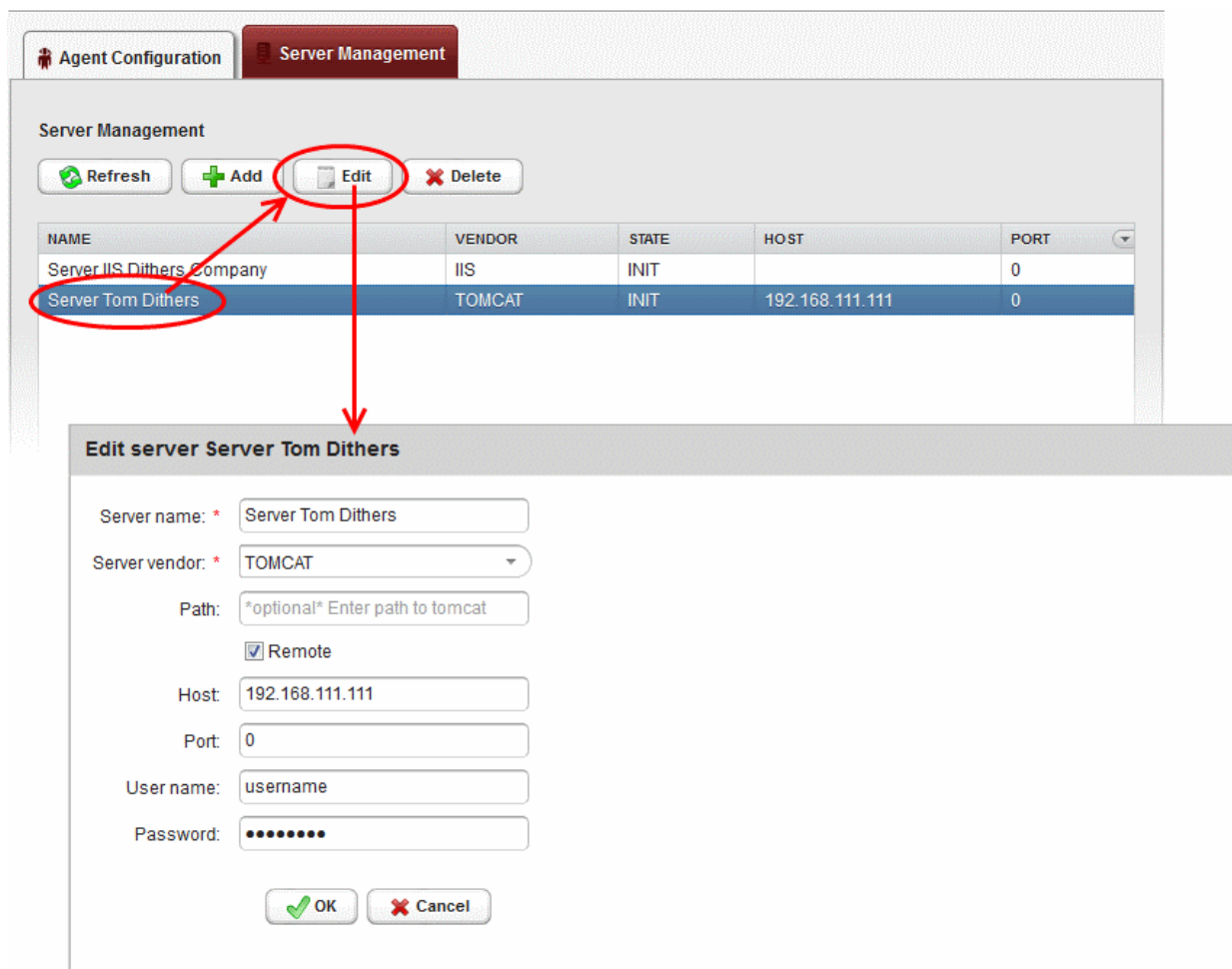
| Add new server - Table of Parameters | | |
|--------------------------------------|------------------|--|
| Server vendor | <i>drop-down</i> | Choose the vendor of the server from the drop-down. |
| Path | <i>String</i> | Specify the network path for the Tomcat server. This is required only if the Tomcat server is not accessible from the CCM console. Note: This field will appear only if Tomcat server is selected in the Server vendor drop-down. |
| Remote | <i>Checkbox</i> | Specify whether the server is Remote or Local. While adding remote servers for agent-less automatic certificate installation, this checkbox should be selected and the login credentials for an administrative account on the server are to be provided. |
| Host | <i>String</i> | Specify the IP address or host name of the server for remote connection. Note: This field will be enabled only if 'Remote' is selected. |
| Port | <i>String</i> | Specify the connection port of the server for remote connection. Note: This field will be enabled only for remote 'Tomcat' server. |
| User Name | <i>String</i> | Enter the username of the administrator for logging-into the server. Note: This field will be enabled only if 'Remote' is selected. |
| Password | <i>String</i> | Enter the log-in password for the administrator account for logging-into the server. Note: This field will be enabled only if 'Remote' is selected. |

- Enter the parameters and click 'OK'.

The new server will be added and enabled for automatic installation of SSL certificates and to run scans for certificate discovery.

To edit a server

- Select the server and click the 'Edit' button that appears on top.



The 'Edit server' dialog will open. The interface is similar to **Add new server** interface.

- Edit the required fields and click 'OK' for your changes to take effect.

8 Reports

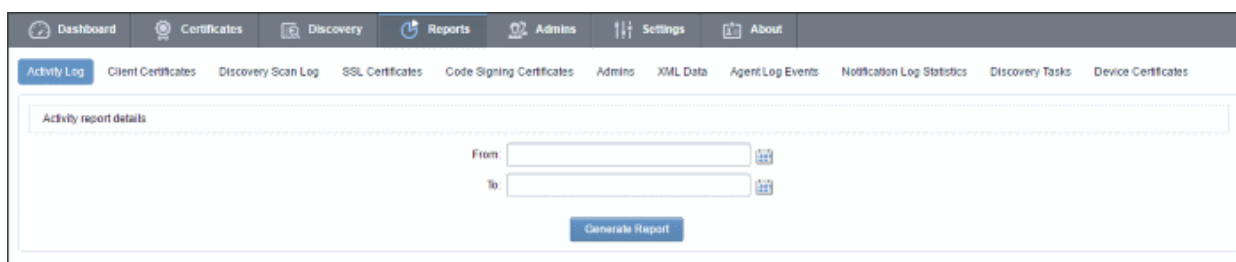
8.1 Overview

The 'Reports' interface lets administrators generate and view reports related to usage, provisioning and monitoring of SSL, Client and Code Signing Certificates. The following reports are available:

- The **Activity Log report** allows MRAO administrators to view a history of all events concerning all types of certificates: Client, SSL and Code Signing.
- The **Client Certificates report** allows administrators to view a history of all events related to client certificates.
- The **Discovery Scan Log** report allows administrators to view information about scan options and discovered SSL certificates
- The **SSL Certificates** report allows administrators to view a history of all events related to SSL certificates.
- The **Code Signing Certificate** report allows administrators to view history of all events related to code signing certificates.
- The **Code Signing Request** report allows administrators to view Code Signing on Demand (CSoD)

requests and related activities.

- The **Admins report** allows MRAO administrators to view a list of all administrators and their privilege levels.
- The **XML Data report** allows MRAO administrators to download a report in XML format which contains complete details about Organizations, Departments, administrators and certificates
- The **DCV Report** allows MRAO administrators and RAO/DRAO SSL administrators to download a report showing details of registered domains and their Domain Control Validation (DCV) status.
- The **Agent Log Events** report allows MRAO administrators to view the discovery scan and certificate installation activities of CCM Controller agents.
- The **Notification Log Statistics Report** allows MRAO administrators to download reports showing details about notifications emails
- The **Private Key Controller Activity** report allows MRAO administrators to view actions executed by the Private Key Controller installed on the local network. This includes data about CSR generation and private key storage for certificates issued using the auto-CSR generation and Private Key management features.
- The **Discovery Tasks** report allows MRAO administrators and RAO/DRAO SSL administrators to view details about configured Discovery Tasks
- The **Device Certificates Reports** allows administrators to view a history of all events related to Device certificates.
- Administrators will find the reports especially useful when troubleshooting any issues related to the provisioning, installation and management of certificates.



The reports interface contains fourteen tabs (depending on the features enabled). The following table contains more detailed descriptions of the reports listed above:

| Report Type | Description |
|---------------------|--|
| Activity log | Enables the MRAO to generate and view reports providing a highly detailed log of ALL actions recorded by Comodo Certificate Manager for the selected period of time. (for example - Admin Login times, Modifications to users, certificate requests, changes in certificate statuses etc) |
| Client Certificates | <p>Enables administrators to generate and view reports regarding Client Certificate Activity. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely:</p> <ul style="list-style-type: none"> • Any (<i>all certificates of any status</i>) • Enrolled - Downloaded • Enrolled - Pending Download • Revoked • Expired • Not Enrolled <p>The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.</p> |

| Report Type | Description |
|---------------------------|--|
| Discovery Scan Log | <p>Enables administrators to generate and view log reports from the scanning processes. Reports are delivered in .csv format.</p> <p>The reports can be further sorted by Organization/Department.</p> |
| SSL Certificates | <p>Enables administrators to generate and view reports regarding SSL Certificate Activity. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely:</p> <ul style="list-style-type: none"> • Any (<i>all certificates of any status</i>) • Requested • Issued • Revoked • Expired <p>The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.</p> |
| Code Signing Certificates | <p>Enables administrators to generate and view reports regarding Code Signing Certificate Activity. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely:</p> <ul style="list-style-type: none"> • Any (<i>all certificates of any status</i>) • Enrolled - Downloaded • Enrolled - Pending Download • Revoked • Expired <p>The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.</p> |
| Code Signing Requests | <p>Enables MRAO, RAO/DRAO Code Signing Administrators to view reports containing the details of Code Signing on Demand (CSoD) requests and their activities. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely:</p> <ul style="list-style-type: none"> • Any (<i>all requests of any status</i>) • Created • In Progress • Declined • Signed • Expired • Failed <p>The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.</p> |
| Admin | <p>Enables the MRAO to generate and view reports providing the details of the enrolled Administrators of all privilege levels.</p> |
| XML Data | <p>Enables the MRAO to generate a report containing complete details of all the Organizations, Departments, their administrators and the all the certificates in XML format.</p> |

| Report Type | Description |
|-------------------------------------|---|
| DCV Report | <p>Enables the MRAO and RAO/DRAO SSL administrators to generate and view a report on registered domains with their Domain Control Validation (DCV) status. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely:</p> <ul style="list-style-type: none"> • Any (<i>all certificates of any status</i>) • Not Started • Awaiting Submittal • Submitted • Validated • Validated Renewing • Expired <p>The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.</p> <p>Note: DCV Report will be available only if DCV feature has been enabled for your account.</p> |
| Agent Log Events | Enables the MRAO Administrator to generate reports on certificate discovery and remote installation activity logs of certificate controller agents. |
| Notification Log Statistics Report | Enables the MRAO to generate reports containing complete details of all notification emails sent to other administrators. Reports are delivered in .csv format. |
| Private Key Controller Activity Log | Enables MRAO Administrators to generate the report containing actions executed by the Private Key Controller like generation of CSR and storage of private key for certificates applied using the auto-CSR generation and Private Key management feature, storage of Private Keys manually uploaded by the administrators and so on. Reports are delivered in .csv format. |
| Discovery Tasks | Enables the MRAO Administrators and RAO/DRAO SSL Administrators to generate reports on configured Discovery tasks. Reports are delivered in .csv format. |
| Device Certificates | <p>Enables administrators to generate and view reports regarding Device Certificates. Reports are delivered in .csv format and can be filtered to show only certificates with a specific current status, namely:</p> <ul style="list-style-type: none"> • Any (<i>all certificates of any status</i>) • Requested • Enrolled - Pending Download • Issued • Revoked • Expired <p>The reports can be further sorted by Organization/Department, (status specific) Date and by Time Interval.</p> |

8.2 Reports - Security Roles Access Table

The following table provides a summary of the ability of the administrators to generate different types of reports.

| Report Type/Organization | MRAO Administrator | RAO Administrator | | | | DRAO Administrator | | | |
|-------------------------------------|--|--|--------|--------------|-------------|--|--------|--------------|-------------|
| | | SSL | S/MIME | Code Signing | Device Cert | SSL | S/MIME | Code Signing | Device Cert |
| Report Type | | | | | | | | | |
| Activity Log | ✓ | ✗ | | | | ✗ | | | |
| Client Certificates | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Discovery Scan Log | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| SSL Certificates | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Code Signing Certificates | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Code Signing requests | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| Admins | ✓ | ✗ | | | | ✗ | | | |
| XML Data | ✓ | ✗ | | | | ✗ | | | |
| DCV Report | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Agent Log Events | ✓ | ✗ | | | | ✗ | | | |
| Private Key Controller Activity Log | ✓ | ✗ | | | | ✗ | | | |
| Notification Log Statistics Report | ✓ | ✗ | | | | ✗ | | | |
| Discovery Tasks | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Device Certificates | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Organizations/ Departments | MRAO | RAO SSL, RAO S/MIME, RAO Code Signing, RAO Device Cert | | | | RAO SSL, RAO S/MIME, RAO Code Signing, RAO Device Cert | | | |
| | All Organizations are available for selection. | Only the Organizations (and any subordinate Departments) that have been delegated to them are available for selection. | | | | Only the Departments that have been delegated to them are available for selection. | | | |

8.3 Activity Log Report

The 'Activity Log' tab enables the MRAO to generate and view reports that reflect ALL the activities (for example - Admin Login times, Modifications to users, certificate requests, changes in certificate statuses etc) recorded by the CCM for a selected period of time.

Once the 'Activity Log' type of reports is selected the following form appears:

8.3.1 Report Type: Activity Log - Table of Parameters

| Form Element | Control | Description |
|-----------------|---|--|
| Date Range | Calendar Buttons to select the date range | Enables administrator to generate a report in .csv format for Activity Log for a specified period of time. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for <i>all</i> the log entries, regardless of the entry date. |
| Generate Report | Control | Starts the report generation. |

8.4 Client Certificates Reports

The 'Client Certificates' tab enables the MRAO and RAO/DRAO S/MIME administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of client certificates. The administrator is able to filter the reports by certificate status. The certificate statuses can be Any, Enrolled - Downloaded, Enrolled - Pending Download, Revoked, Expired, and Not Enrolled. Reports can also be filtered by Organization, status specific dates and time interval.

Once the 'Client Certificates' type of reports is selected the following form appears:

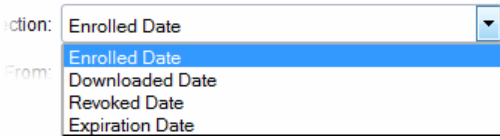
The screenshot shows the 'Client Certificates' report generation interface. It features a navigation bar with 'Reports' selected. Below the navigation bar, there are several tabs: 'Activity Log', 'Client Certificates', 'Discovery Scan Log', 'SSL Certificates', 'Code Signing Certificates', 'Code Signing Requests', 'Admins', 'XML Data', and 'DCV'. The main content area is titled 'Cert report details' and contains the following controls:

- Current Status:** A dropdown menu set to 'Any'.
- Date Selection:** A dropdown menu set to 'Enrolled Date'.
- From:** A date input field with a calendar icon.
- To:** A date input field with a calendar icon.
- Refresh:** A button with a circular arrow icon.
- Organization/Department:** A list of organizations with checkboxes:
 - Comodo SE
 - Device Org
 - Dithers Organization
 - SSL Support Team
 - test to delete[deleted]

At the bottom of the form, there are two links: 'Expand All' and 'Select All', and a 'Generate Report' button.

8.4.1 Report Type: Client Certificates - Table of Parameters

| Form Element | Control | Description |
|----------------|--|--|
| Current Status | <p>Drop-down list</p> <p>Status: Any</p> <p>Enrolled - Downloaded</p> <p>Enrolled - Pending Download</p> <p>Revoked</p> <p>Expired</p> <p>Not Enrolled</p> | <p>Enables administrator to generate a report in .csv format for Client Certificates with a specific current status:</p> <p>Any - Generates a report for ALL client certificates regardless of their current status.</p> <p>Enrolled - Downloaded - Generates a report of only those client certificates that have been successfully enrolled for by the end-user and subsequently downloaded.</p> <p>Enrolled - Pending Download - Generates a report of only those client certificates that have been successfully enrolled for by the end-user but have not yet been downloaded.</p> <p>Revoked - Generates a report for client certificates that have been revoked.</p> <p>Expired - Generates a report only for client certificates that have expired and are due for renewal.</p> <p>Not Enrolled - Generates a report containing only those end-users that belong to an Organization and are listed in the 'Client Certificates' tab as a client certificate user but haven't enrolled for their client</p> |

| Form Element | Control | Description |
|-------------------------|---|--|
| | | certificate. |
| Date Selection | Drop-down list  | <p>Enables administrator to set a specific date for collecting a report. It can be date of certificate enrollment, date of certificate download, date of certificate revocation or expiration. The choices displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down.</p> <p>Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated.</p> <p>If no dates are specified, the report will be generated for all the scans, regardless of the dates.</p> |
| Organization/Department | Checkboxes | <p>Enables the administrator to generate reports for specific Organizations/Departments.</p> <p>If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column.</p> <p>Clicking on Expand All expands the tree structure to display all the Departments under each Organization.</p> <p>Clicking Select All will generate a report for ALL Organizations that were assigned to that administrator.</p> <p>If NO Organization/Department is selected, the report will be generated for <i>all</i> the Organizations/Departments, delegated to the specific administrator.</p> |
| Refresh | Control | Enables the administrator to update the information in the form. |
| Generate Report | Control | Starts the report generation. |

8.5 Discovery Scan Log Reports

The 'Discovery Scan Log' tab enables the MRAO and RAO/DRAO SSL administrators to generate and view log reports from the scanning processes.

The administrator is able to select any one of the following two types of the Discovery Scan Log Reports:

- **Summary**
- **Detail**

8.5.1 Discovery Scan Log Report: Summary type

The Summary type discovery scan log report is generated for a specified time period. The .csv format report generated will have the following information corresponding to each scan run in the specified period:

- Certificate ID;
- Start Date;
- End Date;
- IP Ranges Scanned;
- IP addresses Scanned;
- SSL certificates Found;
- New SSL certificates Found;
- Comodo certificates Found;
- New Comodo SSL certificates Found;
- Other SSL certificates Found;
- New Other SSL certificates Found;
- Self-signed certificates Found;
- New Self-signed certificates Found;
- Scan Type (manual or scheduled);
- Completion Status: (Scan Completed | Scan Failed (if the scan is failed - the fail reason) | Scan Canceled by User);
- Reason for failure (in case of failed scan);
- The person who requested the scan (for manual scans);
- The person who canceled the scan (for manual and scheduled scans);
- Reason for canceling the scan (in case of canceled scan);
- Settings (CIDR range, port settings etc).

On selecting the Summary type, the following form appears.

The screenshot displays the Comodo Certificate Manager interface. The top navigation bar includes: Dashboard, Certificates, Discovery, Code Signing on Demand, Reports, Admins, and Settings. Below this, a secondary navigation bar shows: Activity Log, Client Certificates, Discovery Scan Log (highlighted), SSL Certificates, Code Signing Certificates, Code Signing Requests, Admins, and XML Data. The main content area is titled "Discovery report details" and contains the following form fields:

- Type: Summary Detail
- From:
- To:
- Organization:
- Department:

A "Generate Report" button is located at the bottom right of the form area.

8.5.1.1 Report Type: Discovery Scan Log :Summary - Table of Parameters

| Form Element | Control | Description |
|-----------------|------------------|---|
| Type | Radio buttons | Enables administrators to choose between a detailed report or a summary report. Both types are generated in .csv format. |
| Scan Date | Calendar buttons | Enables the administrator to generate a report in .csv format for Discovery Scan Log for a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the scans, regardless of the dates. |
| Organization | Drop-down | Enables the administrator to specify an Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Organizations that have been delegated to the specific administrator. This option is not visible to DRAO administrator. |
| Department | Drop-down | Enables the administrator to specify a Department belonging to the selected Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Departments belonging to the selected Organization. For DRAO admins, selecting 'Any' will generate a report for all the Departments that are delegated to him/her. |
| Generate Report | Control | Starts the report generation |

8.5.2 Discovery Scan Log Report: Detail type

The Detail type discovery scan log report is generated for a specific manual or scheduled scan and will contain in-depth details of the certificates found during the selected scan. The report generated in .csv format will contain the following information:

- Organization;
- Department;
- IP Address:Port;
- Common Name;
- Valid From;
- Valid to;
- Issuer;
- Subject
- Serial Number
- Subject Alt Name;
- City

- State
- Country;
- Key Algorithm;
- Key size;
- MD5 Hash;
- SH1 Hash;
- Date and Time found;
- Cipher.

On selecting the Detail type, a list of previously run manual/scheduled scans (up to last 10 scans with the most recent on top) are displayed. The administrator can select a scan by clicking on it to generate a detailed discovery scan log report.

8.5.2.1 Report Type: Discovery Scan Log :Detail - Table of Parameters

| Form Element | Control | Description |
|--------------|---------------|---|
| Type | Radio buttons | Enables administrators to choose between a detailed report or a summary report. Both types are generated in .csv format. |
| Organization | Drop-down | Enables the administrator to specify an Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Organizations that have been delegated to the specific administrator. This option is not visible to DRAO administrator. |
| Department | Drop-down | Enables the administrator to specify a Department belonging to the selected Organization for which the discovery scan log has to be generated. Selecting 'Any' will generate a report for the Departments belonging to the selected Organization. For DRAO admins, selecting 'Any' will generate a report for all the Departments that are delegated to him/her. |

| List of most recent scans | | <p>Enables the administrator to select a scan for which the detailed discovery scan report has to be generated. After selecting an entry from the list, click the 'Generate Report' button to generate the detailed report (.csv format).</p> <table border="1"> <thead> <tr> <th>DATE</th> <th>STATUS</th> <th>SSLs FOUND</th> <th>REQUESTER</th> </tr> </thead> <tbody> <tr> <td>08/18/2016 16:06:07</td> <td>Successful</td> <td>1</td> <td>Administrator MRAO</td> </tr> <tr> <td>08/18/2016 15:38:47</td> <td>Successful</td> <td>1</td> <td>Administrator MRAO</td> </tr> <tr> <td>08/10/2016 19:07:28</td> <td>Partially</td> <td>1</td> <td>Administrator MRAO</td> </tr> <tr> <td>08/10/2016 17:09:00</td> <td>Successful</td> <td>1</td> <td>Administrator MRAO</td> </tr> <tr> <td>07/22/2016 19:16:00</td> <td>Successful</td> <td>1</td> <td>Administrator MRAO</td> </tr> <tr> <td>07/22/2016 19:14:51</td> <td>Successful</td> <td>1</td> <td>Administrator MRAO</td> </tr> <tr> <td>07/22/2016 18:55:22</td> <td>Successful</td> <td>1</td> <td>Administrator MRAO</td> </tr> </tbody> </table> | DATE | STATUS | SSLs FOUND | REQUESTER | 08/18/2016 16:06:07 | Successful | 1 | Administrator MRAO | 08/18/2016 15:38:47 | Successful | 1 | Administrator MRAO | 08/10/2016 19:07:28 | Partially | 1 | Administrator MRAO | 08/10/2016 17:09:00 | Successful | 1 | Administrator MRAO | 07/22/2016 19:16:00 | Successful | 1 | Administrator MRAO | 07/22/2016 19:14:51 | Successful | 1 | Administrator MRAO | 07/22/2016 18:55:22 | Successful | 1 | Administrator MRAO |
|---------------------------|------------|---|--------------------|--------|------------|-----------|---------------------|------------|---|--------------------|---------------------|------------|---|--------------------|---------------------|-----------|---|--------------------|---------------------|------------|---|--------------------|---------------------|------------|---|--------------------|---------------------|------------|---|--------------------|---------------------|------------|---|--------------------|
| DATE | STATUS | SSLs FOUND | REQUESTER | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 08/18/2016 16:06:07 | Successful | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 08/18/2016 15:38:47 | Successful | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 08/10/2016 19:07:28 | Partially | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 08/10/2016 17:09:00 | Successful | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 07/22/2016 19:16:00 | Successful | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 07/22/2016 19:14:51 | Successful | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 07/22/2016 18:55:22 | Successful | 1 | Administrator MRAO | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Generate Report | Control | Starts the report generation. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

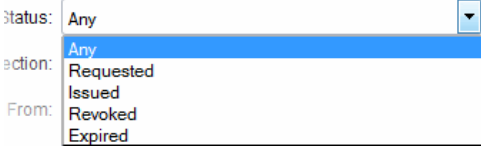
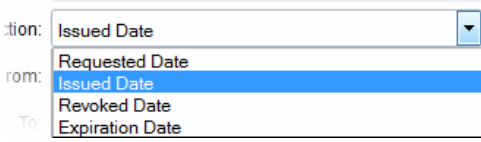
8.6 SSL Certificates Reports

The 'SSL Certificates' tab enables the MRAO and RAO/DRAO SSL administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of SSL certificates. The administrator is able to generate the following types of reports: Requested, Issued, Revoked and Expired SSL certificates. Additionally, there is an ability to filter the certificates by date of request, issuance, revocation or expiration. Once the 'SSL Certificates' type of reports is selected the following form appears:

The screenshot shows the 'Reports' section of the Comodo Certificate Manager interface. The 'SSL Certificates' tab is selected. The form includes the following elements:

- Navigation:** Discovery, Code Signing on Demand, Reports (selected), Admins, Settings, About.
- Sub-navigation:** Scan Log, SSL Certificates (selected), Code Signing Certificates, Code Signing Requests, Admins, XML Data, DCV Report, Agent Log Events.
- Filters:**
 - Current Status: Any (dropdown)
 - Date Selection: Issued Date (dropdown)
 - From: [Date Picker]
 - To: [Date Picker]
 - Refresh button
- Organization/Department Selection:**
 - Comodo SE
 - Device Org
 - Dithers Organization
 - SSL Support Team
- Actions:** Expand All, Select All
- Generate Report:** A large blue button at the bottom.

8.6.1 Report Type: SSL Certificates - Table of Parameters

| Form Element | Control | Description |
|-------------------------|--|--|
| Current Status | Drop-down list  | <p>Enables the administrator to generate a report in .csv format for SSL certificate with a specific current status:</p> <p>Any - Generates a report for ALL SSL certificate types regardless of their current status.</p> <p>Requested - Generates a report only for SSL certificates that have been requested.</p> <p>Issued - Generates a report of those SSL certificates that have been issued successfully.</p> <p>Revoked - Generates a report only for SSL certificates that have been revoked.</p> <p>Expired - Generates a report only for SSL certificate types that have expired and are due for renewal.</p> |
| Date Selection | Drop-down list  | <p>Enables the administrator to set a specific date parameter for the report. The parameters are Issued Date, Requested Date, Revoked Date and Expiration Date. The choices displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down.</p> <p>Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated.</p> <p>If no dates are specified, the report will be generated for all the scans, regardless of the dates.</p> |
| Organization/Department | Checkboxes | <p>Enables the administrator to specify reports containing SSL certificates belonging to particular Organizations/Departments.</p> <p>If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column.</p> <p>Clicking on Expand All expands the tree structure to display all the Departments under each Organization.</p> <p>Clicking on Select All will generate a report for ALL Organizations that were assigned to that administrator.</p> <p>If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the</p> |

| | | |
|-----------------|---------|--|
| | | specific administrator. |
| Refresh | Control | Enables administrator to update the information in the form. |
| Generate Report | Control | Starts the report generation. |

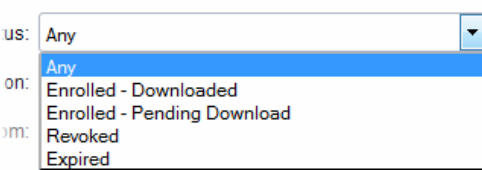
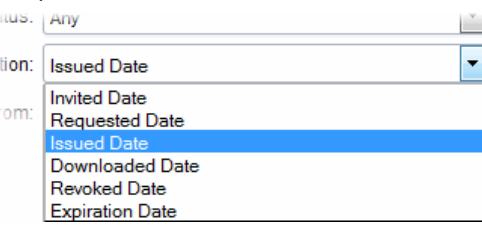
8.7 Code Signing Certificates Report

The 'Code Signing Certificates' tab enables the MRAO and RAO/DRAO Code Signing administrators to generate and view reports that reflect an activity and other statistics related to usage, provisioning and monitoring of Code Signing certificates. The administrator is able to filter the reports by certificate status. The certificate statuses can be Any, Enrolled - Downloaded, Enrolled - Pending Download, Revoked and Expired. Reports can also be filtered by Organization, status specific dates and time interval. Once the 'Code Signing Certificates' type of reports is selected the following form appears:

The screenshot shows the 'Code Signing Certificates' report form. At the top, there is a navigation bar with tabs: 'SSL Certificates', 'Code Signing Certificates' (selected), 'Code Signing Requests', 'Admins', 'XML Data', 'DCV Report', and 'Agent Log E'. Below the navigation bar, the form includes the following elements:

- Current Status:** A dropdown menu set to 'Any'.
- Date Selection:** A dropdown menu set to 'Issued Date'.
- From:** A date input field with a calendar icon.
- To:** A date input field with a calendar icon.
- Refresh:** A button with a circular arrow icon.
- Organization/Department:** A list of checkboxes with expandable plus signs:
 - Comodo SE
 - Device Org
 - Dithers Organization
 - SSL Support Team
 - test to delete[deleted]
- Expand All Select All:** Two links below the organization list.
- Generate Report:** A large blue button at the bottom of the form.

8.7.1 Report Type: Code Signing Certificates - Table of Parameters

| Form Element | Control | Description |
|--------------------------|---|---|
| Current Status | Drop-down list  | <p>Enables administrator to generate a report in .csv format for Code Signing Certificates with a specific current status:</p> <p>Any - Generates a report for ALL Code Signing Certificates regardless of their current status. Does not display any SSL certificates.</p> <p>Enrolled - Downloaded - Generates a report of those Code Signing Certificates that have been successfully enrolled for by the end-user and subsequently downloaded.</p> <p>Enrolled - Pending Download - Generates a report of those Code Signing Certificates that have been successfully enrolled for by the end-user but have not yet been downloaded.</p> <p>Revoked - Generates a report for Code Signing Certificates that have been revoked.</p> <p>Expired - Generates a report only for Code Signing Certificates that have expired and are due for renewal.</p> |
| Date Selection | Drop-down list  | <p>Enables administrator to set a specific date for collecting a report. It can be date of sending invitation by the administrator, certificate enrollment, date of certificate request, date of certificate issuance, download, date of certificate revocation or expiration. The choices displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down.</p> <p>Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated.</p> <p>If no dates are specified, the report will be generated for all the scans, regardless of the dates.</p> |
| Organization/ Department | Checkboxes | <p>Enables the administrator to generate reports for specific Organizations/Departments.</p> <p>If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column.</p> <p>Clicking on Expand All expands the tree structure to display all the Departments under each Organization.</p> <p>Clicking Select All will generate a report for ALL Organizations that were assigned to that</p> |

| Form Element | Control | Description |
|-----------------|---------|---|
| | | administrator. If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator. |
| Refresh | Control | Enables the administrator to update the information in the form. |
| Generate Report | Control | Starts the report generation. |

8.8 Code Signing Requests Report

The 'Code Signing Requests' tab enables the MRAO and RAO/DRAO Code Signing administrators to generate and view reports that reflect an activity and other statistics related to requests made for Code Signing on Demand (CSoD) by developers. The administrator is able to filter the reports by the request status. The statuses can be Any, Created, In progress, Declined, Signed, Expired and Failed. Reports can also be filtered by Organization, status specific dates and time interval.

Note: The Code Signing Requests reports tab will be available only if CSoD feature is enabled for your account.

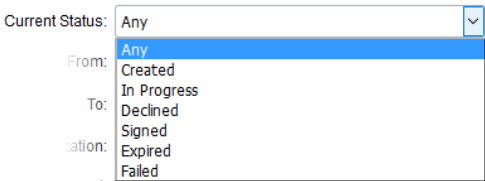
Once the 'Code Signing Requests' type of reports is selected the following form appears:

The screenshot shows the 'Code Signing Requests' report form. At the top, there is a navigation bar with tabs for 'Code Signing on Demand', 'Reports', 'Admins', 'Settings', and 'About'. Below this, there is a sub-navigation bar with tabs for 'SSL Certificates', 'Code Signing Certificates', 'Code Signing Requests' (which is selected), 'Admins', 'XML Data', 'DCV Report', and 'Age'. The main form area contains the following fields:

- Current Status:** A dropdown menu with 'Any' selected.
- From:** A date input field with a calendar icon.
- To:** A date input field with a calendar icon.
- Organization:** A dropdown menu with 'ANY' selected.
- Department:** A dropdown menu with 'ANY' selected.

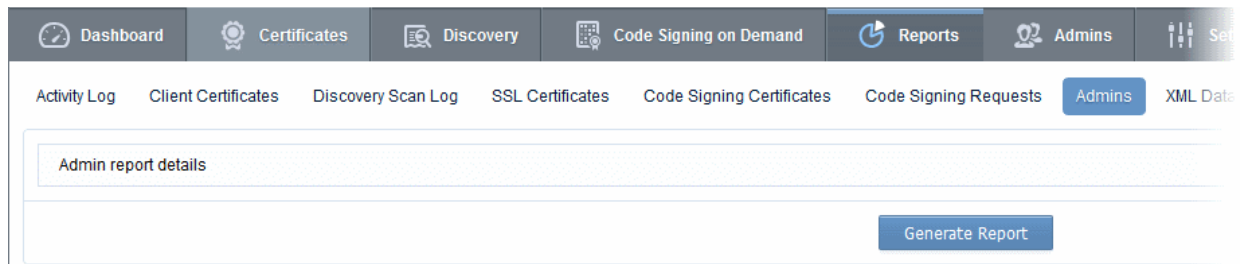
At the bottom of the form, there is a blue button labeled 'Generate Report'.

8.8.1 Report Type: Code Signing Requests - Table of Parameters

| Form Element | Control | Description |
|--------------------------|---|--|
| Current Status | Drop-down list  | Enables administrator to generate a report in .csv format for Code Signing Certificates with a specific current status: Any - Generates a report for ALL Code Signing Certificates regardless of their current status. Does not display any SSL certificates. Created - Generates a report of those Code Signing Requests that are with 'Created' status. In progress - Generates a report of those Code Signing Requests that are in progress status. Declined - Generates a report of those Code Signing Requests that were declined by MRAO or RAO/DRAO Code Signing admins status. Signed - Generates a report of those Code Signing Requests that were declined by MRAO or RAO/DRAO Code Signing admins status. Expired - Generates a report of those Code Signing Requests that were expired. Failed - Generates a report of those Code Signing Requests that were failed. |
| Date Selection | Drop-down list | Enables administrator to set a period for report generation. Clicking on the calendar buttons beside From: and To: text boxes enables the administrator to select a date range for which the report has to be generated. |
| Organization/ Department | Drop-downs | Enables the administrator to generate reports for specific Organizations/Departments. If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator. |
| Generate Report | Control | Starts the report generation. |

8.9 Admins Report

The 'Admins' tab enables the MRAO to generate and view reports providing details on all the enrolled administrators, their roles and the Organizations/Departments delegated to them. Once the 'Admins' type of reports is selected the following dialog appears:

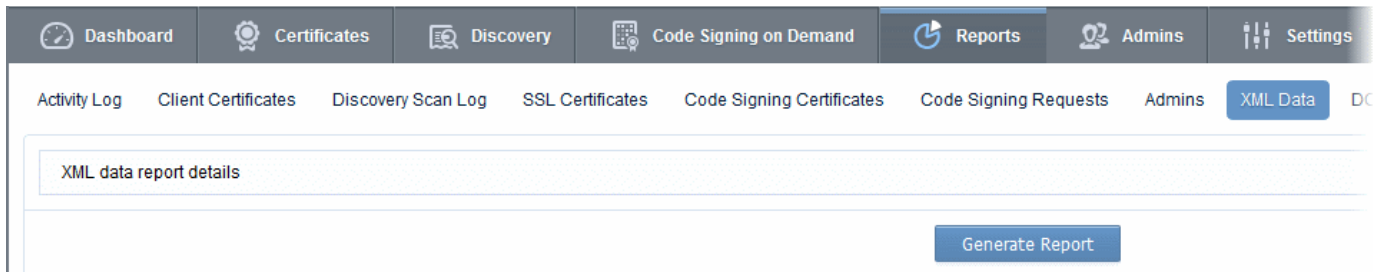


- Clicking on 'Generate Report' starts generating the report in .csv format.

The report provides the details of the Name, Login, Email and Role of each of the administrators and the Organizations.

8.10 XML Data Report

The 'XML Data' tab enables the MRAO to generate and view reports containing complete details of the Organizations, Departments, their administrators and the all the certificates in XML format. Once the 'XML Data' type of reports is selected the following dialog appears:



- Clicking on 'Generate Report' starts generating the report in .xml format.

The XML file enables the administrator to maintain a local database of all the details such as Departments, Administrators delegated, Certificates issued, Certificate settings etc. for each Organization. The XML file can also be imported into a database for collecting any data for any Organization at any time by raising queries.

8.11 DCV Report

The 'DCV Report' tab enables the MRAO and RAO/DRAO SSL administrators to generate and view reports that contain a list of all domains with their validation status and expiration of the DCV process. The administrator is able to filter the reports based on the DCV status. The DCV status can be Any, Awaiting Submittal, Submitted, Validated, Validated Renewing and Expired. Reports can also be filtered by Organization/Department, specific dates and time interval. Once the 'DCV Report' type of reports is selected the following form appears:

Note: DCV Report will be available only if DCV feature has been enabled for your account.

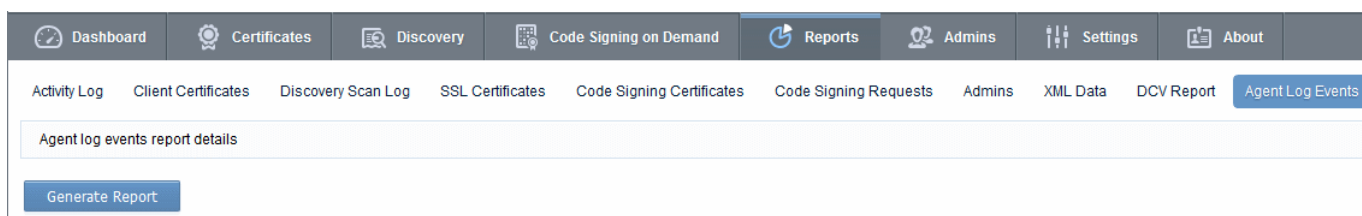
8.11.1 Report Type: DCV Report - Table of Parameters

| Form Element | Control | Description |
|----------------|------------------------|--|
| Current Status | Drop-down list | <p>Enables the administrator to generate a report of domains with a specific current DCV status</p> <p>Any - Generates a report for Domains regardless of their current status.</p> <p>Not Started - Generates a report on domains that have been added to CCM but have not yet started the DCV process.</p> <p>Awaiting Submittal - Generates a report only for Domains that are being waiting for submission of DCV request to the Domain administrator.</p> <p>Submitted - Generates a report only for Domains for which DCV request has been submitted.</p> <p>Validated - Generates a report on domains that have been successfully validated.</p> <p>Validated Renewing - Generates a report only for Domains that require renewal of Validation.</p> <p>Expired - Generates a report only for Domains for which the DCV request has expired.</p> |

| Form Element | Control | Description |
|-------------------------|------------|---|
| Expiration Date | | <p>Enables the administrator to set an expiration date range for DCV request to generate a report on Domains whose DCV request is expiring within the date range.</p> <p>Clicking on the calendar buttons beside From: and To: text boxes enables the administrator to select a date range for which the report has to be generated.</p> <p>If no dates are specified, the report will be generated for all Domain Control Validated domains, regardless of the dates.</p> |
| Organization/Department | Checkboxes | <p>Enables the administrator to select Organizations/Departments to generate report on Domains of specific Organizations/Departments.</p> <p>If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations / Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column.</p> <p>Clicking on Expand All expands the tree structure to display all the Departments under each Organization.</p> <p>Clicking on Select All will generate a report for ALL Organizations that were assigned to that administrator.</p> <p>If NO Organization/Department is selected, the report will be generated for all the Organizations/Departments, delegated to the specific administrator.</p> |
| Refresh | Control | Enables administrator to update the information in the form. |
| Generate Report | Control | Starts the report generation. |

8.12 Agent Log Events Report

The 'Agent Log Events' tab enables the MRAO to generate and view reports containing complete details of the scanning and certificate installation activities of the Certificate controller agents. Once the 'Agent Log Events' type of reports is selected the following dialog appears:



- Clicking on 'Generate Report' starts generating the report in .xml format.

8.13 Notification Log Statistics Report

The 'Notification Log Statistics Report' tab enables the MRAO administrator to generate and view log reports on the notification emails sent to other RAO and DRAO administrators for various events, as configured in the [Settings > Notifications](#) area.

The administrator is able to select any one of the following three types of the Notification Log Statistics Reports:

- **E-Mail**
- **Notification Type**
- **Full Log**

8.13.1 Notification Log Statistics - Email

The Email log report can be generated for a specified time period. The .csv format report generated will show the number of notification emails sent to each RAO and DRAO administrator during the specified period.

On selecting the Email type, the following form appears.

8.13.1.1 Report Type: Notification Log Statistics :Emails - Table of Parameters

| Form Element | Control | Description |
|-----------------|------------------|--|
| Type | Radio buttons | Enables administrators to choose between email report, notification type report or a full log report. |
| Date Range | Calendar buttons | Enables the administrator to generate a report in .csv format for the notification emails sent within a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the notification emails, regardless of the dates. |
| Generate Report | Control | Starts the report generation |

8.13.2 Notification Log Statistics - Notification Type

The Notification type log report can be generated for a specified time period. The .csv format report generated will show the number of notification emails sent for each notification type as configured in **Settings > Notifications** area to all the RAO and DRAO administrators during the specified period.

On selecting 'Notification Type', the following form appears.

8.13.2.1 Report Type: Notification Log Statistics :Notification Type - Table of Parameters

| Form Element | Control | Description |
|-----------------|------------------|--|
| Type | Radio buttons | Enables administrators to choose between email report, notification type report or a full log report. |
| Date Range | Calendar buttons | Enables the administrator to generate a report in .csv format for the number of emails sent for different notification types within a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the notifications, regardless of the dates. |
| Generate Report | Control | Starts the report generation |

8.13.3 Notification Log Statistics - Full Log

The full log report for notification emails can be generated for a specified time period. The report generated will show the list of emails sent for various notification types to different RAO and DRAO administrators, for each notification type as configured in **Settings > Notifications** area during the specified period. The report generated in .csv format will contain the following information:

- Notification Type
- Email address of the administrator to which the notification email was sent
- Subject line of the notification email
- Date and time at which the email as sent

On selecting the 'Full Log' type, the following form appears.

8.13.3.1 Report Type: Notification Log Statistics :Full Log - Table of Parameters

| Form Element | Control | Description |
|-----------------|------------------|---|
| Type | Radio buttons | Enables administrators to choose between email report, notification type report or a full log report. |
| Date Range | Calendar buttons | Enables the administrator to generate a report in .csv format for the full log of notification emails within a specified time period. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the notifications, regardless of the dates. |
| Generate Report | Control | Starts the report generation |

8.14 Private Key Controller Activity Log

The 'Private Key Controller Activity Log' tab enables MRAO administrators to generate and view reports that reflect all activity by the Private Key Controller. The activities of the controller include CSR generation, storage of private keys from the Auto-CSR feature and a record of keys manually uploaded/downloaded by administrators. Reports can be generated for events for a selected period of time and can be downloaded in .csv format.

Once the 'Private Key Controller Activity Log' type of reports is selected the following form appears:

8.14.1 Report Type: Private Key Controller Activity Log - Table of Parameters

| Form Element | Control | Description |
|-----------------|---|--|
| Date Range | Calendar Buttons to select the date range | Enables administrator to generate a report in .csv format for Private Key Controller Activity Log for a specified period of time. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. If no dates are specified, the report will be generated for all the log entries, regardless of the entry date. |
| Generate Report | Control | Starts the report generation. |

8.15 Discovery Tasks Report

The 'Discovery Tasks' tab allows MRAO Administrators and RAO/DRAO Administrators to generate and view reports on Discovery Tasks, configured for their Organization(s) and Department(s). Once the 'Discovery Tasks' type of reports is selected, the following form appears:

- Click 'Generate Report' to download the report in .csv format.

8.16 Device Certificate Reports

The 'Device Certificates' tab enables the MRAO and RAO/DRAO Device Cert administrators to generate and view reports that reflect the activity and other statistics related to request and issuance of device certificates. The administrator is able to filter the reports by certificate status. The certificate statuses can be Any, Requested, Enrolled - Pending Download, Issued, Revoked and Expired. Reports can also be filtered by Organization, status

specific dates and time interval.

Once the 'Device Certificates' type of reports is selected the following form appears:

8.16.1 Report Type: Device Certificates - Table of Parameters

| Form Element | Control | Description |
|----------------|---|---|
| Current Status | Drop-down list Current Status: <input type="text" value="Any"/> <ul style="list-style-type: none"> Any Requested Enrolled - Pending Download Issued Revoked Expired | Enables administrator to generate a report in .csv format for Client Certificates with a specific current status: Any - Generates a report for ALL device certificates regardless of their current status. Requested - Generates a report of only those device certificates that have been applied via self-enrollment and awaiting administrator approval. Enrolled - Pending Download - Generates a report of only those device certificates that have been approved by the administrator but have not yet been downloaded. Revoked - Generates a report for device certificates that have been revoked. Expired - Generates a report only for device certificates that have expired and are due for renewal. |
| Date Selection | Drop-down list Date Selection: <input type="text" value="Requested Date"/> <ul style="list-style-type: none"> Requested Date Expiration Date From: <input type="text" value="01/20/2017"/> <input type="text" value=""/> To: <input type="text" value="01/20/2017"/> <input type="text" value=""/> Refresh | Enables administrator to set a specific date for collecting a report. It can be date of certificate requisition, date of revocation or date of certificate expiration. The choices displayed on this drop-down menu is dependent on the status chosen in the 'Current Status' drop down. Clicking on the calendar buttons beside from: and To: text boxes enables the administrator to select a date range for which the report has to be generated. |

| Form Element | Control | Description |
|-----------------------------|------------|--|
| | | If no dates are specified, the report will be generated for all types, regardless of the dates. |
| Organization/ Department | Checkboxes | <p>Enables the administrator to generate reports for specific Organizations/Departments.</p> <p>If multiple Organizations/Departments are selected then the administrator will receive a single report that covers those selected Organizations/Departments. Each Organization will be displayed on a separate row in the 'Organizations' column and each Department will be displayed in a separate row in the 'Departments' column.</p> <p>Clicking on Expand All expands the tree structure to display all the Departments under each Organization.</p> <p>Clicking Select All will generate a report for ALL Organizations that were assigned to that administrator.</p> <p>If NO Organization/Department is selected, the report will be generated for <i>all</i> the Organizations/Departments, delegated to the specific administrator.</p> |
| Refresh | Control | Enables the administrator to update the information in the form. |
| Generate Report | Control | Starts the report generation. |

9 Version and Feature Information

The 'About' tab allows administrators to view CCM version information and to view which CCM features have been enabled.

- MRAO admins - Can see a list of all features.
- RAO admins - Can see features of the certificate types over which they have admin rights (RAO SSL, RAO Code Signing etc)
- DRAO admins - Can see features of the certificate types over which they have admin rights (DRAO SSL, DRAO Code Signing etc)

| STATE | | CLIENT CERTS | |
|--------------------------------------|----------|---|----------|
| Version | 5.8 | Allow Client Certs | Enabled |
| Extra Agent Version | 2.2 | Web API | Enabled |
| Private Key Agent Version | 1.1 | Allow principal name in certificates | Enabled |
| Code Signing on Demand Agent Version | 2.3 | Allow customization of principal name SAN field | Enabled |
| Active Directory Agent Version | 2.0 | Web Enrollment Type | |
| Balance (tokens) | 0 | Invitation | Enabled |
| | | AccessCode | Enabled |
| | | Secret ID | Disabled |
| | | Auto Revoke | Enabled |
| | | Allow Empty PIN | Disabled |
| | | Allow send notification upon upload from csv | Disabled |
| DOMAIN | | | |
| Domain Dual Approval by MRAO | Disabled | | |
| SSL CERTS | | | |
| Allow SSL | Enabled | | |
| Web API | Enabled | | |
| DCV Validation | Enabled | | |
| CODE SIGNING CERTS | | | |
| Allow Code Signing Certificates | Enabled | | |
| MaxTerm | 1 | | |

© 2007-2017. All rights reserved.

If any of the features are to be enabled or disabled, the MRAO Administrator can contact Comodo and request for them.

10 My Profile

The 'My Profile' area contains a details summary for the Administrator that is currently logged into the CCM. Administrators can view their login name, their full name, the email address that is associated with their account and their administrative role. The administrator can also view and edit the address details, and preferences.

To access this interface, click the username text link beside the 'Logged as' label at the top right side of the interface.

ger

Logged as Administrator MRAO

My Profile

Login admin

Name Administrator MRAO

Email admin@dithers.com

Role MRAO Admin

Title Mr.

Telephone Number +111234567890

Street Mount Road

Locality Riverdale

State/Province Alabama

Postal Code 123456

Country United States

Relationship System Administrator

Current locale en

Time format mm/dd/yyyy

Password Change

Grid settings Reset to default

Save Cancel

This area also allows the Administrator to edit the following details:

Address Details:

- Title
- Telephone Number
- Street
- Locality
- State/ Province
- Postal Code
- Country
- Relationship

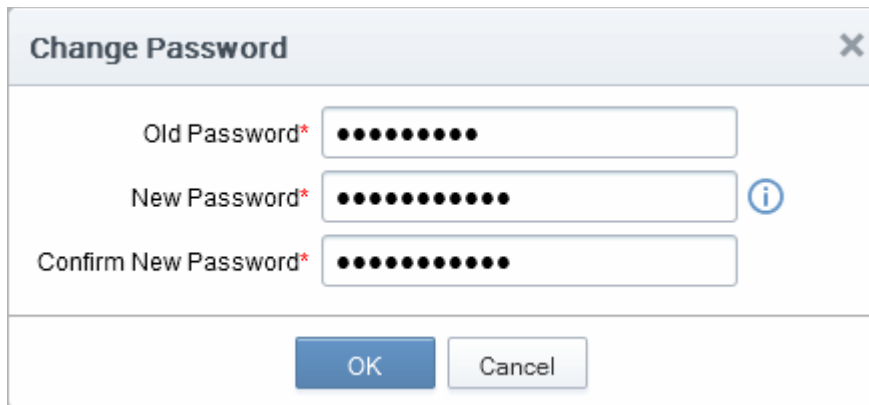
Preferences:

- Interface Language - CCM interface is available in multiple languages. The 'Current locale' drop-down menu enables the administrators to change the interface language according to their preferences. The settings will take effect only on clicking the 'Save' button.
- Grid Settings - Click Reset to default to adjust the column widths and sorting preferences customized in various interfaces of CCM to default values.
- Time Format - Choices available are 'mm/dd/yyyy' or 'dd/mm/yyyy'.

Note: This only affects the way dates are represented in the CCM interface (for example, the 'Expires' column of the 'SSL Certificates sub-tab' in 'Certificates Management'. It does not affect the way that dates are displayed in

the certificates themselves (this is not modifiable and is set in the format 'MM/dd/yy'). The settings will take effect only on clicking the 'Save' button.

- Password - To change the administrators password, click the 'Change' button next to 'Password' label.

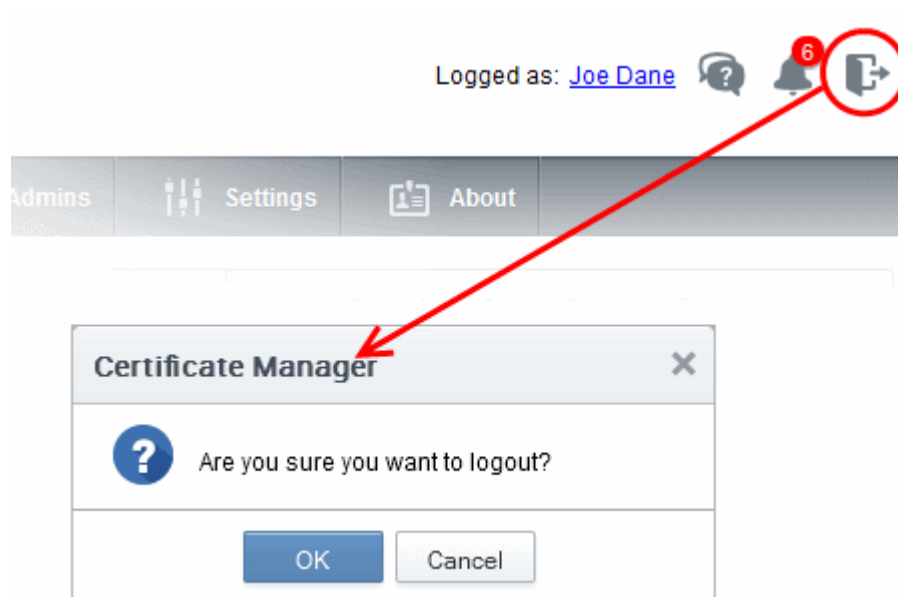


The image shows a 'Change Password' dialog box with three input fields: 'Old Password*', 'New Password*', and 'Confirm New Password*'. Each field contains a series of black dots representing masked text. To the right of the 'New Password*' field is a blue circular information icon. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Hover the mouse cursor on the 'info' button to view the password policy and change the password accordingly.

11 Logging Out of Comodo Certificate Manager

Administrator can log out from the interface by clicking on the 'Logout' button located at the top right side of the interface.



Appendix 1 - Your responsibilities when ordering SSL Certificates

In order to make the certificate issuance process as fast and seamless as possible for immediate certificate issuance, the Certificate Manager Account holder has a number of responsibilities. It is your responsibility to ensure the following:

You have the right to use the domain name contained in the SSL application. You must only approve applications for domain names you own.

The named individual in the Corporate Secure Email Certificate is a bonafide employee or representative of your company.

Making an illegitimate certificate application could affect the contract you signed with Comodo and your Certificate Manager Account and could be a breach of the Certificate Manager Subscriber Agreement.

Appendix 2 - Private Certificates for Internal Hosts

Many companies use publicly trusted SSL certificates from a certificate authority (CA) to secure internal hosts, reserved IP addresses and intranets. However, after November 1st 2015 CA's are no longer able to issue publicly trusted certificates that contain internal names. By November 1st 2016, all such certificates must be revoked. Companies that rely on these publicly trusted certificates for internal services risk service disruption, error messages, user confusion and loss of security.

Private SSL certificates offer continuity by allowing businesses to continue using internal certificates with non-registered names. Under our Private CA system, Comodo will help you create your own private root certificate which is capable of signing end-entity certificate for all your internal servers and users. Once enabled, Private Certificates can be ordered by choosing 'Private UCC' when requesting a new certificate:

The screenshot shows the 'Request New SSL Certificate' dialog box in the Comodo Certificate Manager interface. The dialog is titled 'Request New SSL Certificate' and has a close button (X) in the top right corner. It contains several fields and buttons:

- Organization***: A dropdown menu with 'Org1' selected.
- Department***: A dropdown menu with 'ANY' selected.
- Refresh**: A button with a circular arrow icon.
- Click here to edit address details**: A blue link.
- Certificate Type***: A dropdown menu with 'Private UCC' selected.
- Certificate Term***: A dropdown menu with '1 year' selected.
- Server Software***: A dropdown menu with 'AOL' selected.
- CSR***: A large text area for the Certificate Signing Request, currently empty.
- Max CSR size is 32K**: A label above two buttons: 'Get CN from CSR' and 'Upload CSR'.
- Common Name***: A text input field containing 'test.loc'.
- Subject Alternative Names**: A text input field containing 'test.domain.local'. Below the field is the text '(optional, comma separated)'. There is a small 'X' icon in the top right corner of the field.
- Requester**: A text input field containing 'mrao'.
- External Requester**: A text input field, currently empty.
- Comments**: A large text area for additional information, currently empty.
- OK** and **Cancel**: Buttons at the bottom of the dialog.

Private certificates use the same key sizes, signing algorithms, validity periods and CA protections as public certificates. After issuance, they can be managed, tracked and installed via CCM just like any other certificate type.

Features in brief:

- Create a private root for your company which is used to sign all internal server certificates
- Avoid the complexity, expense and risk involved with setting up an internal CA
- CCM discovers all internal certificates on company networks and allows you to seamlessly replace them
- Comodo expertly supports your deployment and makes sure your certificates are always in compliance with future regulations

If you would like to know more about the Private CA service, please speak to your Comodo account manager or contact us directly on 1-888-256-2608 / enterprisesolutions@comodo.com.

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford
Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: EnterpriseSolutions@Comodo.com

For additional information on Comodo - visit <http://www.comodo.com>.