Domain Control Validation in Comodo Certificate Manager

The purpose of this document is to explain the new domain control validation (DCV) processes for the Comodo Certificate Manager.

DCV is an industry wide directive that requires all Certificate Authorities (CAs) to verify domain control prior to the issuance of a certificate to a domain. This affects all new certificate applications and certificate renewals. DCV requirements apply to all SSL web-server certificate types ordered via any channel. This includes our retail customers, resellers, affiliates and enterprise customers.

Comodo has simplified the DCV process for our customers by seamlessly integrating DCV fulfillment wizards into the CCM interface. We are always looking for feedback from our customers so, if you have any questions not answered by this document, then please contact us at **CSMSupport@comodo.com**.

- **What is DCV?**
- **What implementation choices are available?**
- **How to initiate DCV in CCM?**

What is DCV?

- Before any SSL certificate can be issued, the registrable domain name (e.g. domain.com, domain.edu, domain.net, etc.) must pass DCV. This confirms to Comodo that the applicant has control of the domain for which the certificate application is being made. Once passed, DCV will remain valid for domain names within CCM for 1 year (meaning subsequent certificates can be issued to the same domain without requiring another round of DCV).

- Customers can initiate DCV on an individual basis or, if all domains share a common 'WhoIs' email record, may initiate DCV on multiple domains at once.

- Customers can complete DCV using any one of three supported methods - Email, CNAME or HTTP/HTTPS. Customers can use any combination of the three methods across their domains as per business preference.

- 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 Multi-Domain Certificates and Unified Communications Certificates, all listed domains must pass DCV.

- Your existing domains will continue to work. DCV only comes into effect when an existing domain is next up for renewal. However, we recommend that you complete DCV for all of your domains as quickly as possible.

What implementation choices are available?

There are three supported methods of DCV - Email, HTTP/HTTPS and CNAME.

Email

When using the email challenge-response system, the applicant must be able to receive an email sent to an address at the domain for which the application is being made.

The email will contain a unique validation code that the applicant has to paste into a confirmation web-page before the application can proceed. Comodo's automated system will retrieve addresses registered to the domain from the Whois database and present them to the application for selection. The system also presents a selection of 'typical' addresses, such as admin@domain.com, webmaster@domain.com,

hostmaster@domain.com, administrator@domain.com and postmaster@domain.com.

The Email method can be used for both validating a single domain and multiple domains at a time.

How to initiate Email DCV

HTTP / HTTPS

CCM generates a specific text (.txt) file which must be placed on the root directory of the domain undergoing DCV. Comodo's automated system will check for the presence and content of this file to complete the validation process. Administrators need to upload it only to the location mentioned in the wizard before clicking the 'Test' button.

How to initiate HTTP / HTTPS DCV

CNAME

CCM will generate two specific hashes which must be entered as a CNAME DNS record. Comodo's automated system will check for the presence of the two hashes in your DNS records. DCV will be achieved after a successful CNAME check. Please use this format:
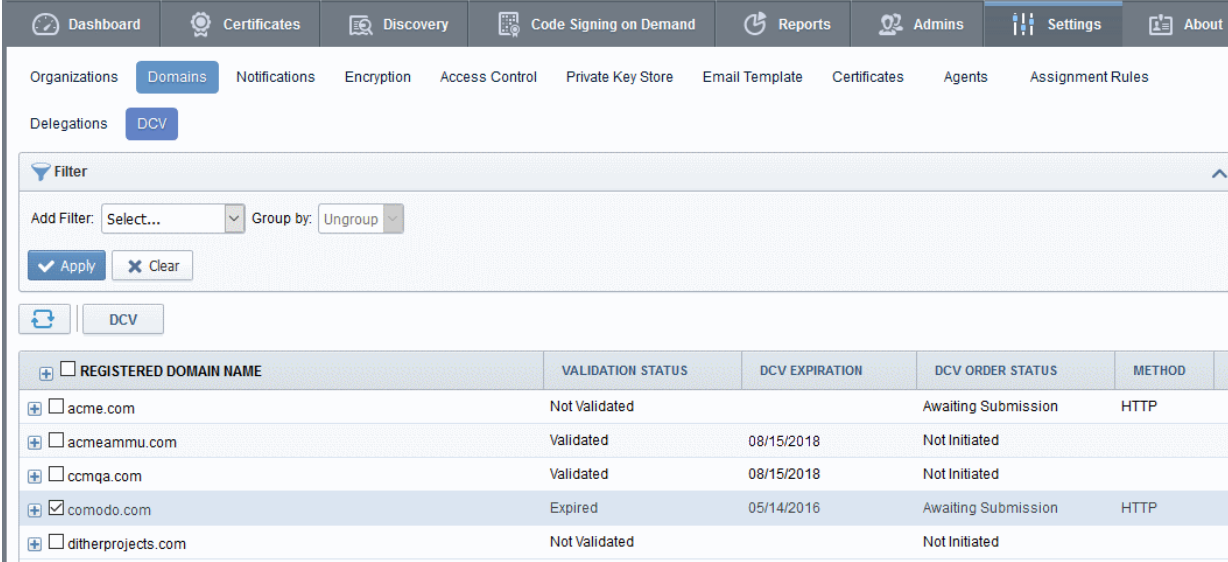
<MD5 hash>.yourdomain.com CNAME <SHA-1 hash>.comodoca.com

How to initiate CNAME DCV

How to initiate DCV in CCM

Note - Prior to initiating DCV, administrators should add domains to CCM, delegate the domain to either an Organization or a Department and await approval by Comodo. Once the domain shows as "Approved" in the CCM:

- First open the DCV configuration screen by selecting 'Settings' > 'Domains' > 'DCV'

	Dashboard	Certificates	Discovery	Code Signing on Demand	Reports	Admins	Settings	About

Organizations | Domains | Notifications | Encryption | Access Control | Private Key Store | Email Template | Certificates | Agents | Assignment Rules

Delegations | DCV

🔻 Filter ⌃

Add Filter: Select... ⌄   Group by: Ungroup ⌄
✔ Apply   ✖ Clear

🔁   DCV

REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV EXPIRATION	DCV ORDER STATUS	METHOD
⊞ ☐ acme.com	Not Validated		Awaiting Submission	HTTP
⊞ ☐ acmeammu.com	Validated	08/15/2018	Not Initiated	
⊞ ☐ ccmqa.com	Validated	08/15/2018	Not Initiated	
⊞ ☑ comodo.com	Expired	05/14/2016	Awaiting Submission	HTTP
⊞ ☐ ditherprojects.com	Not Validated		Not Initiated	

Column Header	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.
Validation Status	Whether the domain has passed DCV or not. Status can be one of the following: • Not Validated - DCV has not been initiated or is in-progress for the registered high level domain (HLD). • Validated - The registered high level domain has passed DCV • Expired - DCV on the domain has expired and has to be renewed. The DCV process has to be restarted for the domain
DCV Expiration	Indicates the date when Domain Control Validation for the domain expires. The DCV has to be done again after the expiry period.

DCV Order Status	Progress of validation on the domain. Status can be one of the following:
	• Not Initiated - DCV has not been started for the registered high level domain (HLD).
	• Awaiting Submittal - DCV has been initiated but the request has not yet been sent to the domain administrator (the admin who has control of the web server on which the domain is hosted). The 'Awaiting...' status is only available for the following DCV methods:
	  • HTTP / HTTPS
	  • CNAME
	• Submitted - The DCV request has been sent to the domain administrator for implementation.
	• Validated - The registered high level domain (HLD) has passed DCV.
	• Expired - DCV has expired on the domain. The DCV process has to be restarted for the domain .

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.

The following sections explain on:

- Validating a single domain
- Validating multiple domains at a time

Validating a Single Domain

- Initiate DCV by selecting the domain and clicking the 'DCV' button that appears at the top. This will open the DCV wizard:

Select one of these DCV methods:

- **Email**
- **HTTP / HTTPS**
- **CNAME**

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.

Validate domain – ditherprojects.com ✕

1 Email Selection ———— **2** Order Submission

Registered Domain Name	**ditherprojects.com**
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	Email

Email Address

Select an email address:* admin@ditherprojects.com ▼

...
admin@ditherprojects.com
administrator@ditherprojects.com
hostmaster@ditherprojects.com
postmaster@ditherprojects.com
webmaster@ditherprojects.com

[Save & Close] [Back] [Submit]

The drop-down menu contains a list of registered email addresses for this domain that have been dynamically drawn from Whois. It also contains 'typical' email addresses such as:

- admin@domain.com
- administrator@domain.com
- hostmaster@domain.com
- postmaster@domain.com
- webmaster@domain.com

Click the 'Validate' button after making your selection. A challenge-response email will be sent to the selected email address. The DCV status of the domain will change to 'Submitted'.

Upon receiving the email, the applicant should click the link in the email and enter the unique code into a validation web-form. If DCV is successful, the status of the domain will change to 'Validated'.

HTTP/HTTPS

CCM generates a specific text (.txt) file which must be placed on the root directory of the domain undergoing DCV. Comodo systems will check for the presence and content of this file and if verified as correct, the domain will pass DCV.

- Click the 'here' link in item 1 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.

- Click 'Save & Close'. CCM will save the hash value generated for future comparison.

- 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.

- Once the Domain Administrator has placed the .txt file on the HTTP HTTPS server, open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV' tab

- Resume the DCV process by selecting the domain and clicking the 'DCV' button

- Click 'Submit'. The DCV Order status of the domain will change to 'Submitted'.

- • CCM will check whether the file has been placed in the web server root and validate the domain. On successful validation, the DCV Order status of the domain will change to 'Validated'.

DNS CNAME

The CNAME method allows you to complete DCV by creating a CNAME DNS record which includes two unique hash values (MD5 & SHA1) generated for you by CCM. The CNAME record should be passed to your domain administrator for implementation, if necessary. The format we look for:

<MD5 hash>.yourdomain.com CNAME <SHA-1 hash>.comodoca.com

- 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.

- Click 'Save & Close'. CCM will save the hash value generated for future comparison.

- After the Domain Administrator has created the record, open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV' tab

- Resume the DCV process by selecting the domain and clicking the 'DCV' button.

- Click 'Submit'.The DCV Order status of the domain will change to 'Submitted'.

Validate domain - ditherprojects.com ✕

1 Get Validation Info ———— **2** Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	CNAME_CSR_Hash

SHA256 Hash	5452a0a15d3a9b3d51765a1f68b6d440c80f517eed1eac31bd9cbcd8cd86900b
MD5 Hash	546f0fd9977f2339752e6ac5d6fd09f2

A request for CNAME validation of **ditherprojects.com** has been successfully submitted.

Awaiting the validation result...

Reset   OK

- CCM will check whether the record has been created. If it is found created, the DCV Order status of the domain will change to 'Validated'.

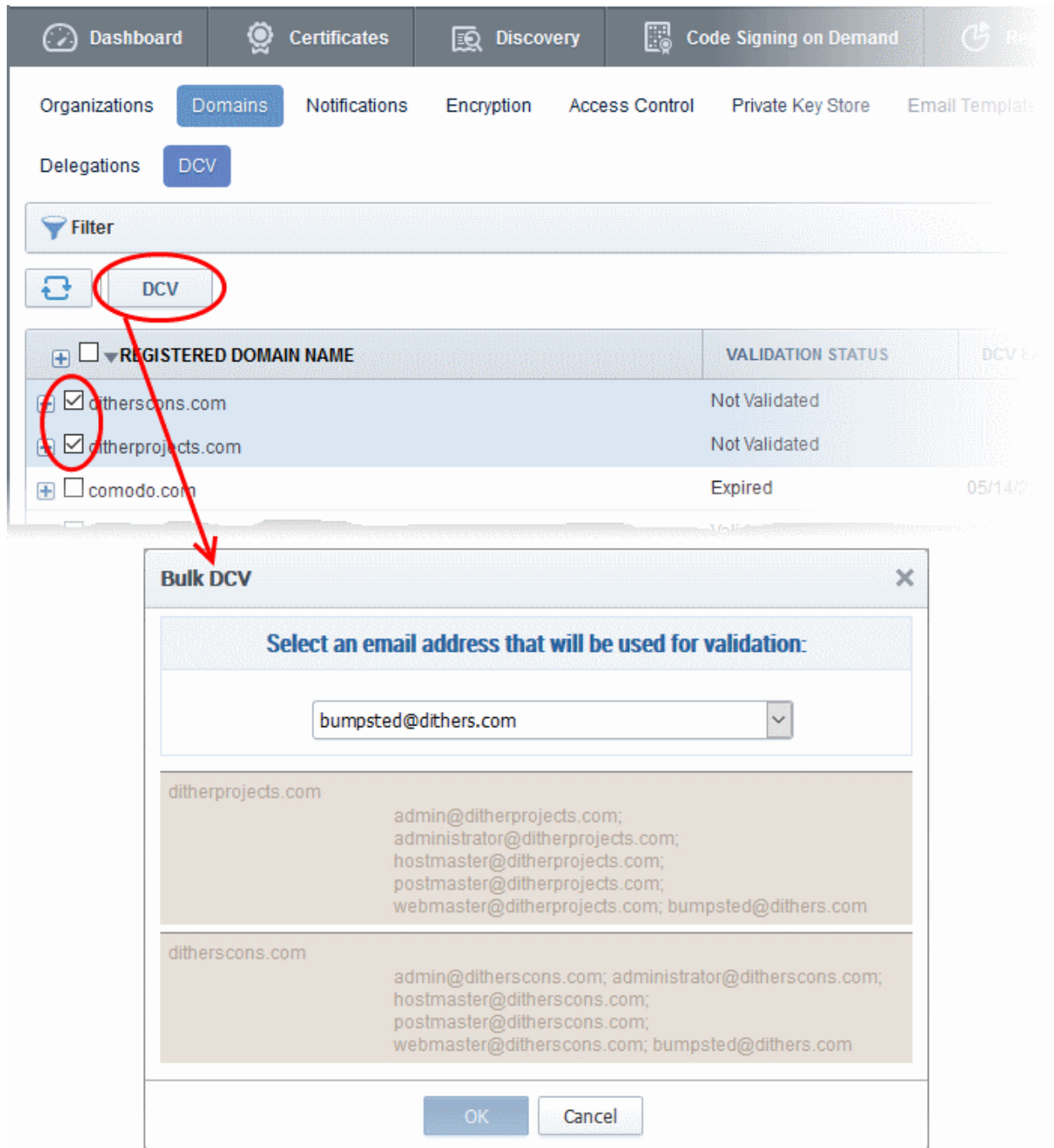### Validating Multiple Domains at a time

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. Select the domains that share common domain administrator email address
2. Click the 'DCV' button

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.
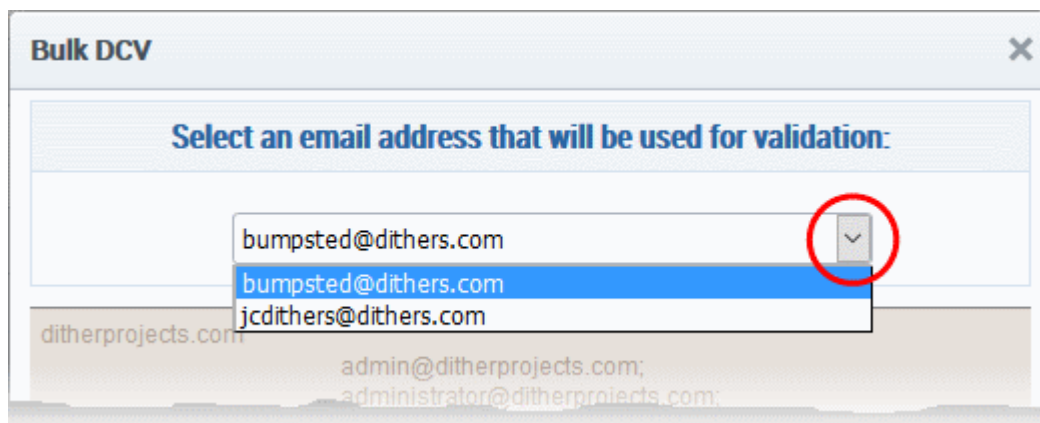
3. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'OK'.

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'.

Additional Resources

*   Certificate Manager MRAO Admin Guide - Section 6.4.2.1.2 DCV
*   Certificate Manager RAO Admin Guide - Section 6.4.2.1.2 DCV
*   Comodo Support Knowledge Base: https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1367

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

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

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

For additional information on Comodo, visit http://www.comodo.com