AusCERT

AusCERT Certificate Services Manager

Initiating Domain Control Validation (DCV)

AusCERT
The University of Queensland
Brisbane QLD 4072
Australia

Domain Control Validation in AusCERT Certificate Services Manager

The purpose of this document is to explain the new domain control validation (DCV) processes that will be implemented in AusCERT Certificate Services 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.

AusCERT has simplified the DCV process for our customers by seamlessly integrating DCV fulfillment wizards into the CSM 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 auscert@auscert.org.au.

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 AusCERT 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 AusCERT CSM for 1 year (meaning subsequent certificates can be issued to the same domain without requiring another round of DCV).
- You can complete DCV using any one of three supported methods - Email, CNAME or HTTP. You 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 Organisation or a Department, AusCERT CSM 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 play when an existing domain is next up for renewal.

What implementation choices are available?

There are three supported methods of DCV: Email, HTTP and CNAME. All three methods are automated and will take just a few minutes to complete.

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. AusCERT'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.edu, webmaster@domain.edu, hostmaster@domain.edu, administrator@domain.edu and postmaster@domain.edu.

How to initiate Email DCV

HTTP

AusCERT CSM generates a specific text (.txt) file which must be placed on the root directory of the domain undergoing DCV. AusCERT'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 DCV

CNAME

AusCERT CSM will generate two specific hashes which must be entered as a CNAME DNS record. AusCERT'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:

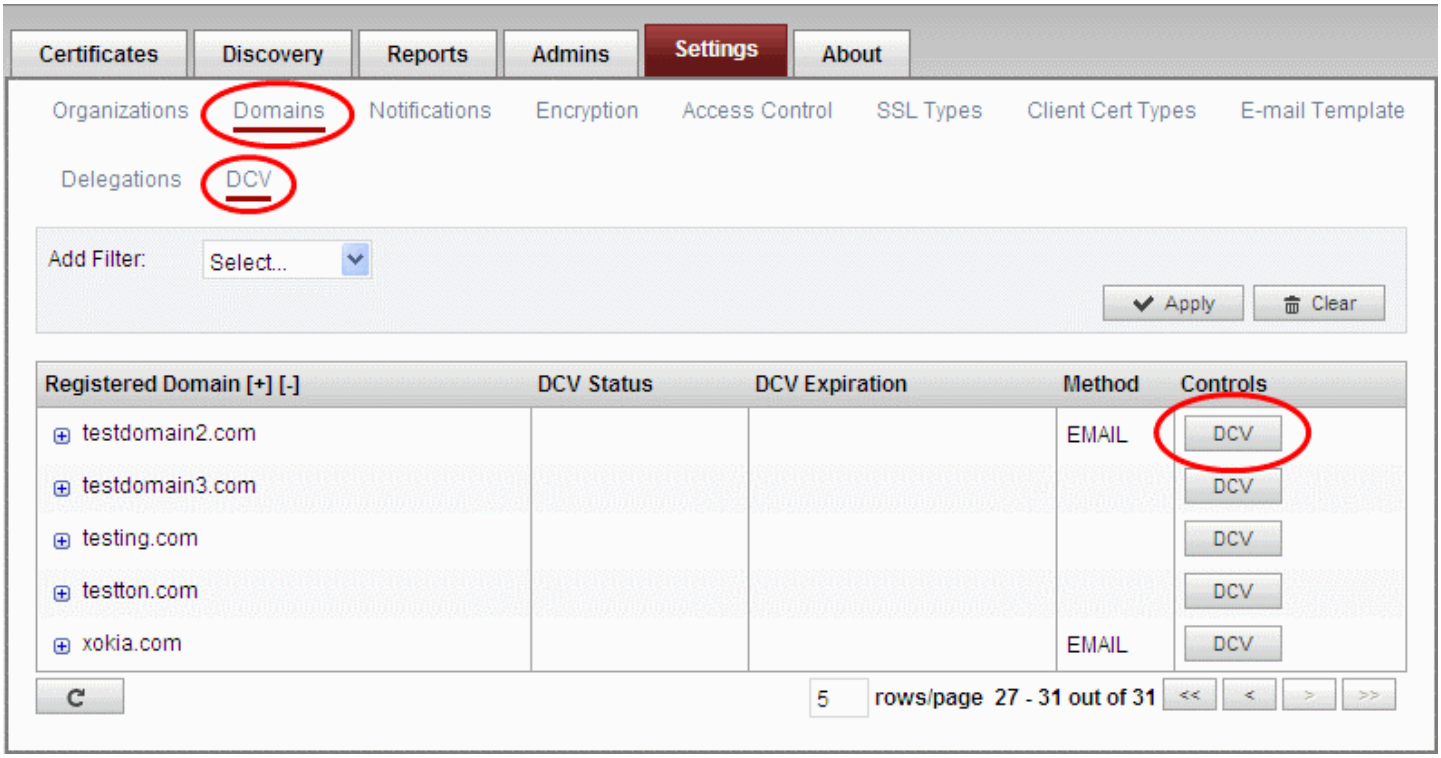
<MD5 hash>.yourdomain.com CNAME <SHA-1 hash>.comodoca.com

How to initiate CNAME DCV

How to Initiate DCV in CSM

Note - Prior to initiating DCV, administrators (RAO or DRAO) should add domains to AusCERT CSM, delegate the domain to either an organisation or a department and await approval by AusCERT. Once the domain shows as "Approved" in the CSM:

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



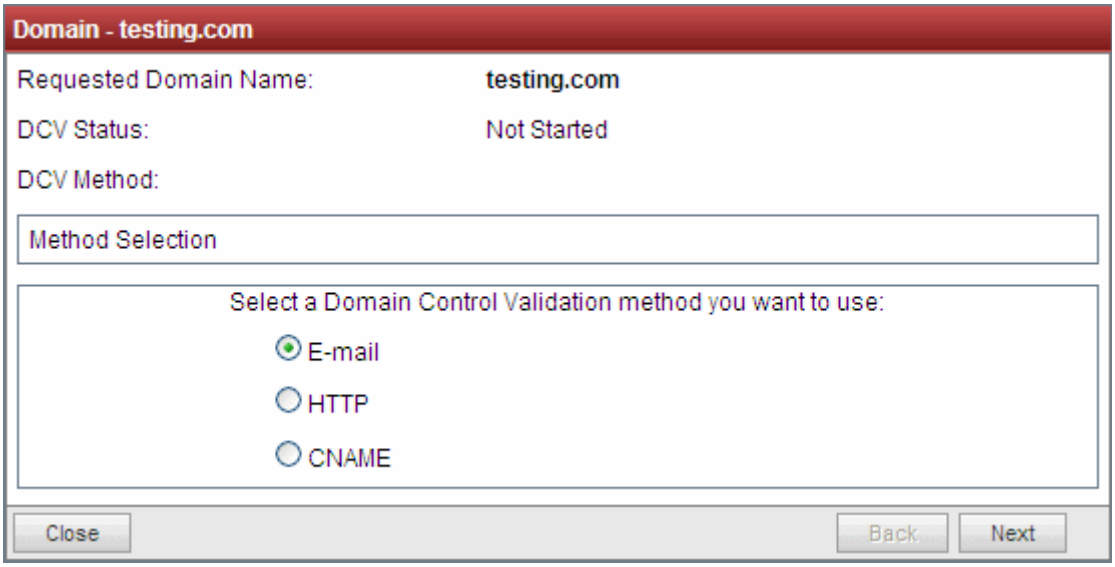
Column Display	Description
Registered Domain	A list of all available Domains created for this account. Clicking the '+' beside a domain name displays the sub-domains of the registered domain.

DCV Status	Indicates the validation status of the domain. The status can be one of the following:
	• Not Started - 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:
	  ◦ HTTP
	  ◦ CNAME
	• Submitted - The DCV request has been submitted to the domain administrator.
	• Validated - The registered high level domain (HLD) has been successfully validated
	• Expired - The DCV request has expired for the HLD.

DCV Expiration	Indicates the expiry date of the DCV request.
Method	Indicates the DCV method chosen by the administrator for validating the domain.

Column Display	Description
Controls	Contains a control enabling the MRAO and RAO/DRAO SSL Administrators to initiate or restart the DCV process for a Domain.

- Next, initiate DCV by clicking the 'DCV' button next to one of your domains. This will open the DCV wizard:

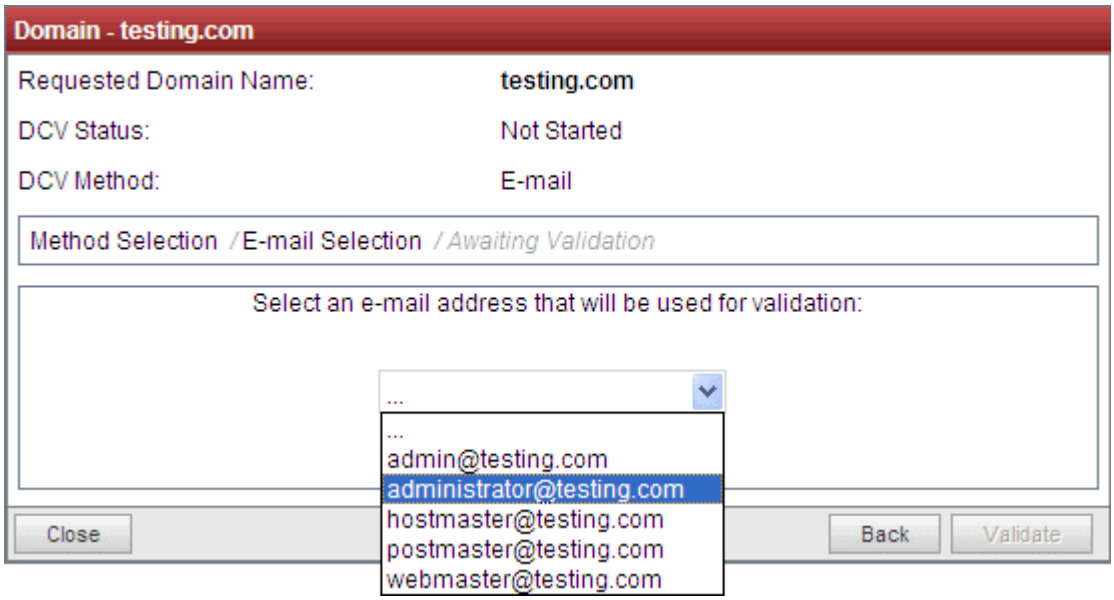


Select a DCV method from:

- **Email**
- **HTTP**
- **CNAME**

Email

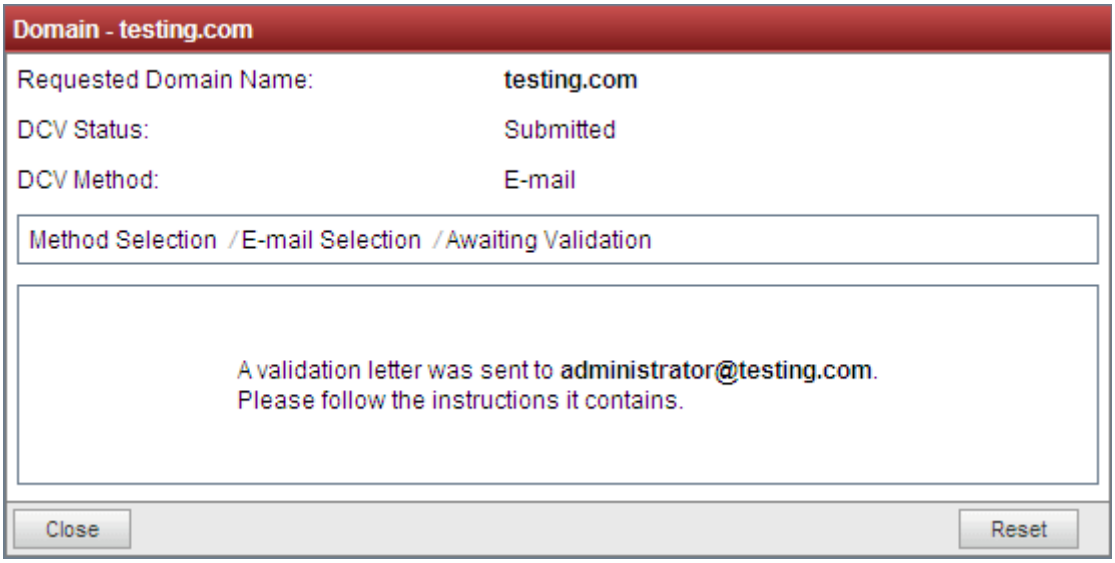
After choosing 'Email', the next step is to choose the address to which the DCV challenge-response email will be sent. The applicant must, of course, be able to receive emails at this address. DCV will be completed when the applicant verifies domain control by clicking a link in the email.



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

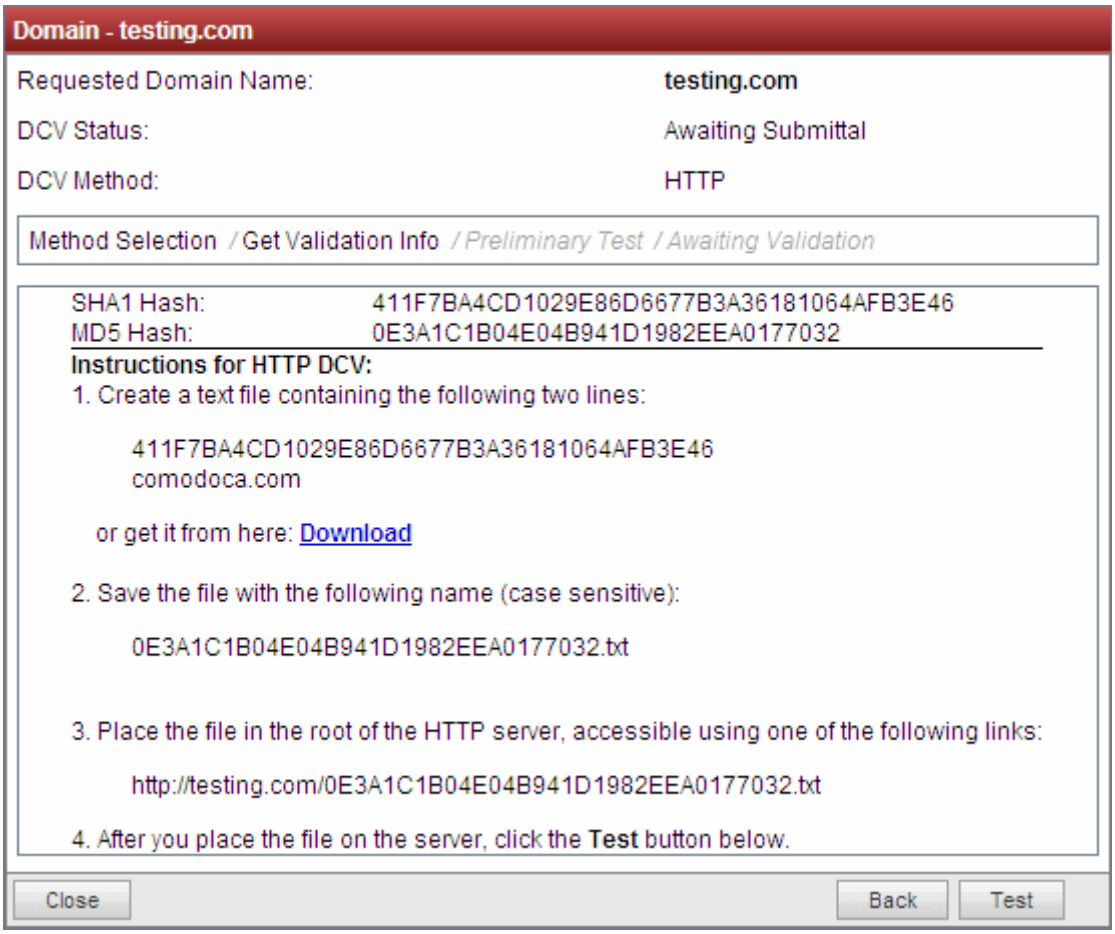
Click the 'Validate' button after making your selection. A challenge-response email will be sent to the selected email address. The DCV status of the domain will change to 'Submitted'.



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

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



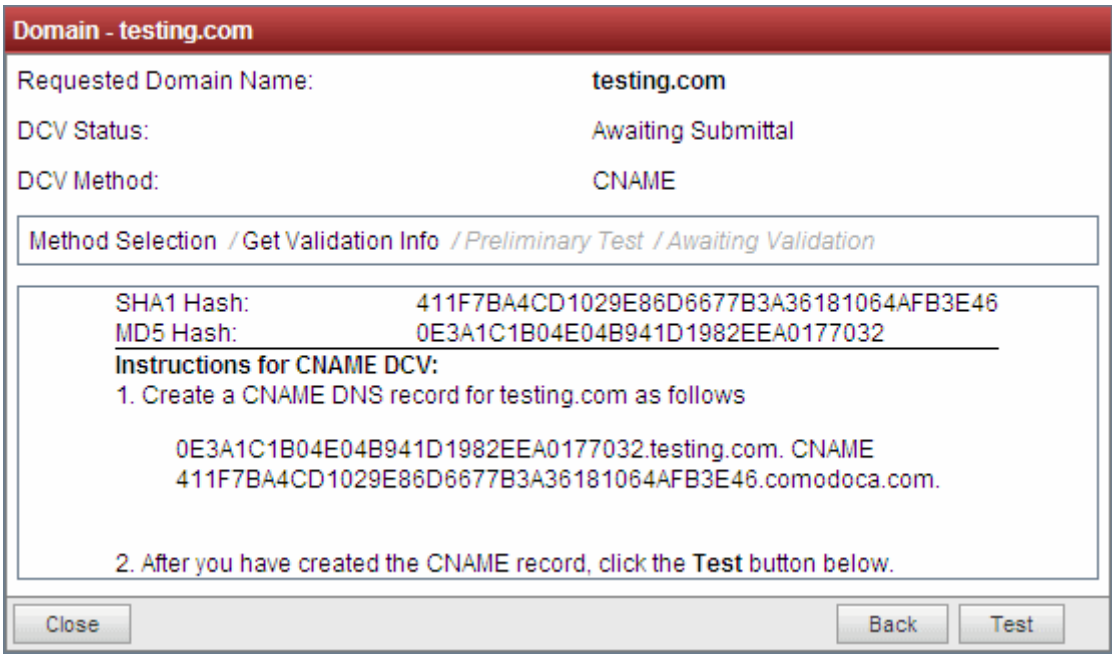
Place the file in the root directory of the domain in question so that it is publicly accessible at one of the paths specified in step number three (see image above). Click 'Test' to check that the file has been uploaded correctly. If correct, the 'Submit' dialog will appear and the DCV status of the domain will change to 'Submitted'. AusCERT systems will now attempt to perform DCV by checking for this file. If successful, the DCV status of the domain will change to 'Validated'.

If you need time to get the file uploaded to your server, you can close this wizard and submit later. This can be done by returning to the main DCV interface (Settings > Domains > DCV) then clicking the DCV button alongside the appropriate domain. Again, you need to click 'Test' then 'Submit'.

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 AusCERT CSM. 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 provided and pass it to your domain administrator. Click 'Test' to check the record is correct. If correct, the 'Submit' dialog will appear. The DCV status of the domain will change to 'Submitted'. AusCERT systems will now attempt to perform DCV by checking for this record. If successful, the DCV status of the domain will change to 'Validated'.

If you need time to get the record created, you can close this wizard and submit later. This can be done by returning to the main DCV interface (Settings > Domains > DCV) then clicking the DCV button alongside the appropriate domain. Again, you need to click 'Test' then 'Submit'.

Additional Resources

- AusCERT RAO Admin Guide - Section 4.4.2.1.2 DCV
- AusCERT's partner Comodo's Support Knowledge Base: https://support.comodo.com/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=1367