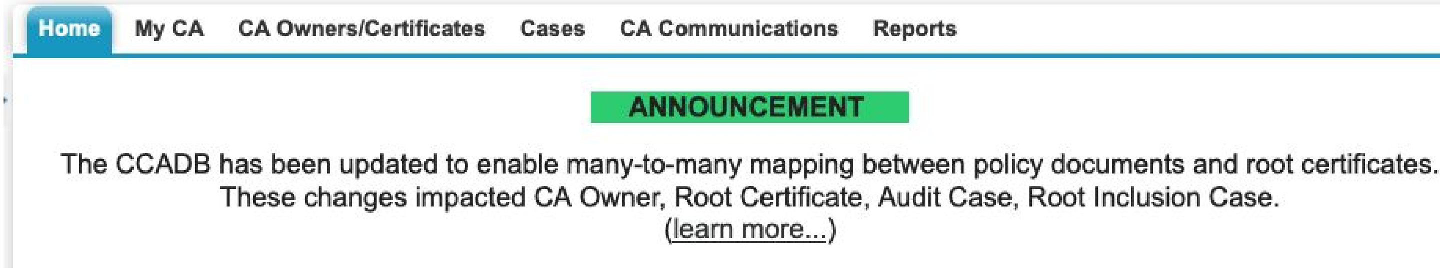
CCADB News - CABF F2F October 2020

Multiple CP/CPS Documents

The ability to associate multiple policy documents with multiple root certificates went live in August. (Screen Shots)

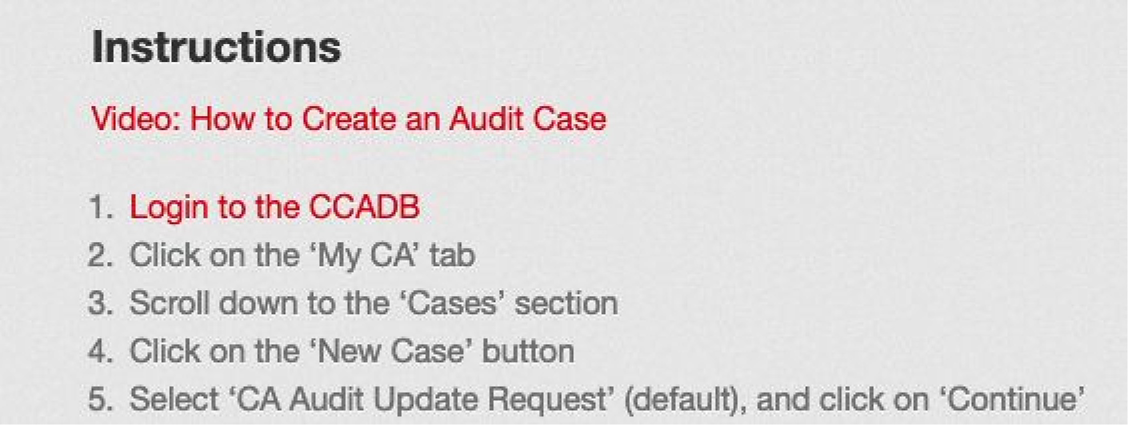


ANNOUNCEMENT

The CCADB has been updated to enable many-to-many mapping between policy documents and root certificates.
These changes impacted CA Owner, Root Certificate, Audit Case, Root Inclusion Case.
(learn more...)

The instructions on the CCADB.org website have been updated, and a video added that shows how to create an Audit Case in the CCADB.

www.ccadb.org -> For CAS -> Submitting Annual Updates
https://www.ccadb.org/cas/updates



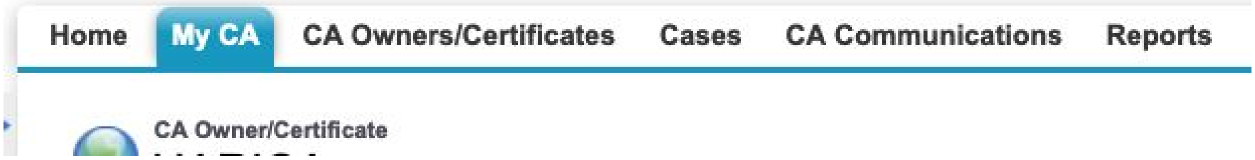
Instructions

Video: How to Create an Audit Case

1. Login to the CCADB
2. Click on the ‘My CA’ tab
3. Scroll down to the ‘Cases’ section
4. Click on the ‘New Case’ button
5. Select ‘CA Audit Update Request’ (default), and click on ‘Continue’

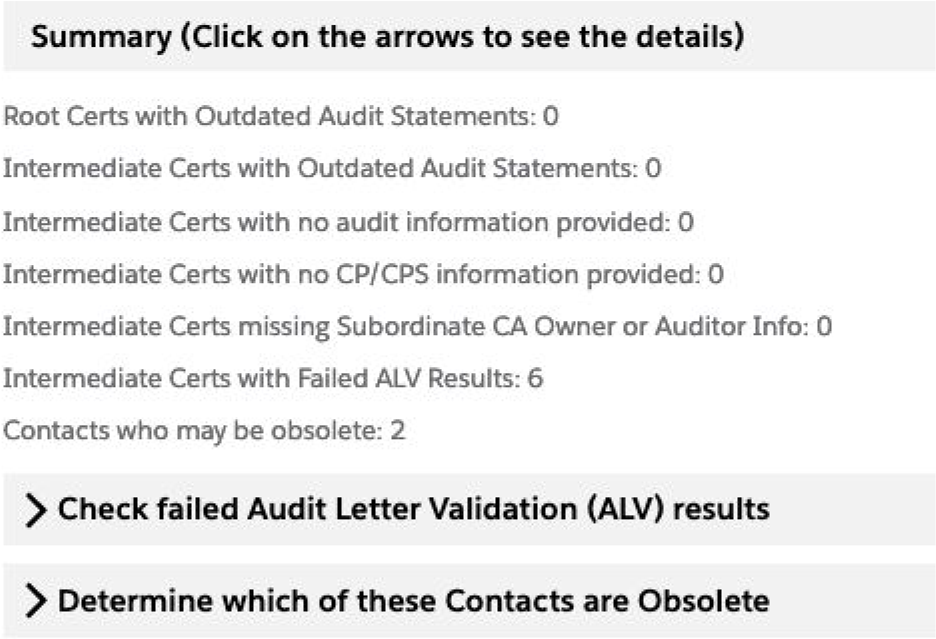
Added ‘My CA’ Tab

Added a tab called ‘My CA’, which will take you directly to your CA Owner Page.



CCADB Home Page Task List

Check the task list on your CCADB Home Page for items that need to be addressed.



Summary (Click on the arrows to see the details)

Root Certs with Outdated Audit Statements: 0

Intermediate Certs with Outdated Audit Statements: 0

Intermediate Certs with no audit information provided: 0

Intermediate Certs with no CP/CPS information provided: 0

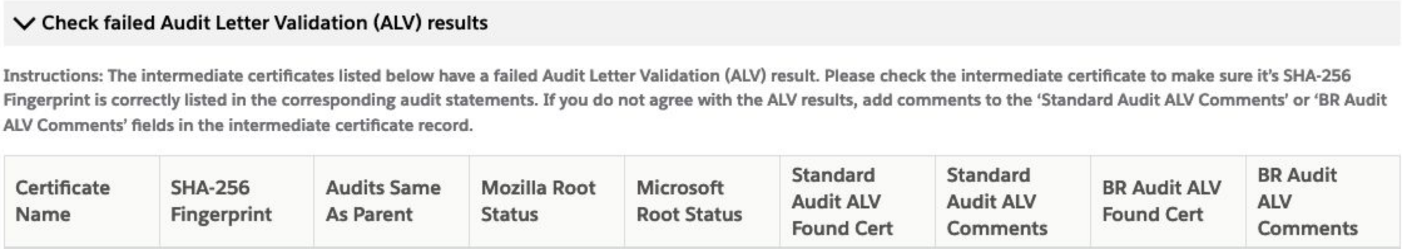
Intermediate Certs missing Subordinate CA Owner or Auditor Info: 0

Intermediate Certs with Failed ALV Results: 6

Contacts who may be obsolete: 2

> Check failed Audit Letter Validation (ALV) results
> Determine which of these Contacts are Obsolete

For non-zero items, there will also be a corresponding report. Click on the “>” next to the report name to expand the report.



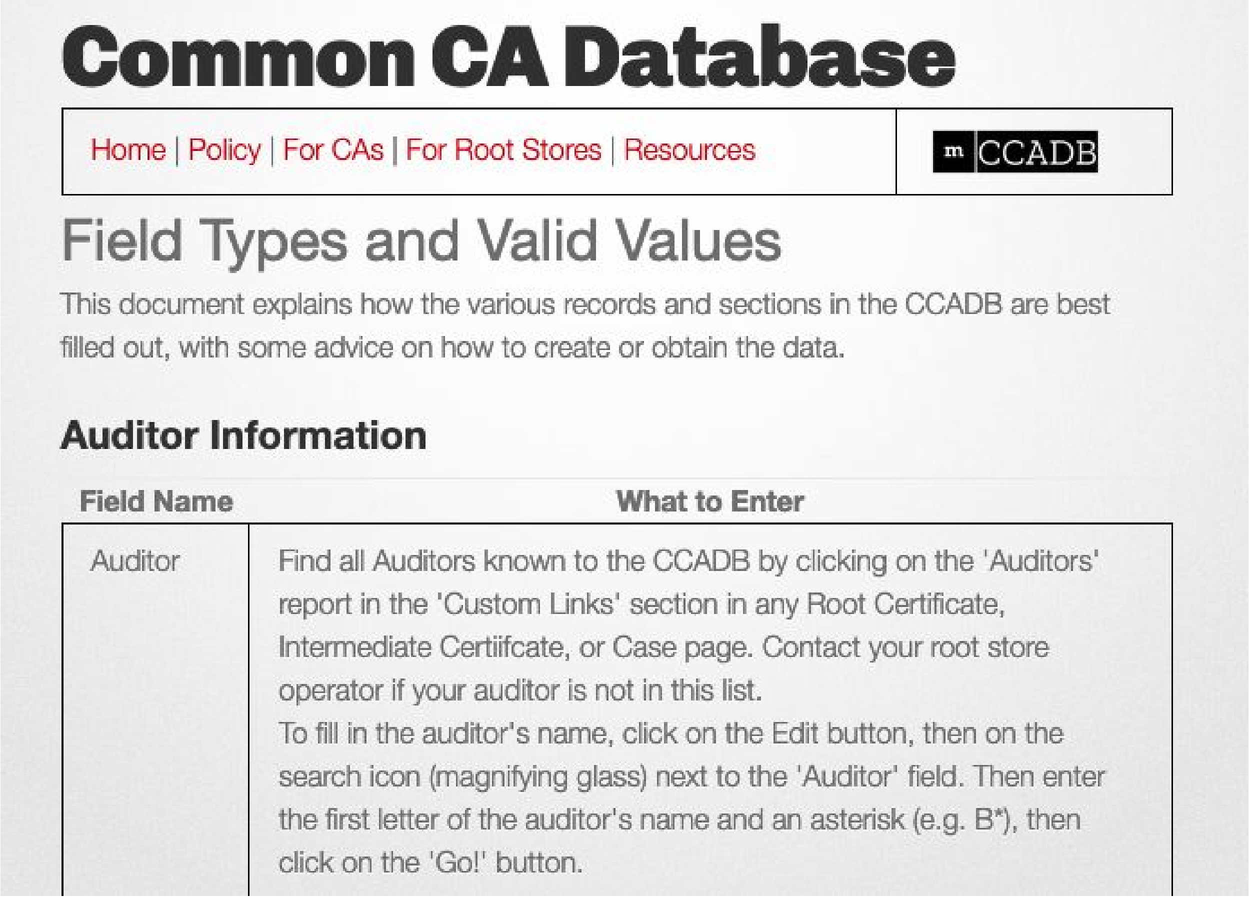
Instructions: The intermediate certificates listed below have a failed Audit Letter Validation (ALV) result. Please check the intermediate certificate to make sure it's SHA-256 Fingerprint is correctly listed in the corresponding audit statements. If you do not agree with the ALV results, add comments to the ‘Standard Audit ALV Comments’ or ‘BR Audit ALV Comments’ fields in the intermediate certificate record.

Certificate Name	SHA-256 Fingerprint	Audits Same As Parent	Mozilla Root Status	Microsoft Root Status	Standard Audit ALV Found Cert	Standard Audit ALV Comments	BR Audit ALV Found Cert	BR Audit ALV Comments

CCADB.org Website Updates

- Added CCADB Data Usage Terms
  - https://www.ccadb.org/rootstores/usage#ccadb-data-usage-terms
  - Linked to from https://www.ccadb.org/resources and pages like https://wiki.mozilla.org/CA/Included_Certificates
- Updated section 5.1 of the Common CCADB Policy to align with the BRs:
  - “**MUST**: be encoded in the document (PDF) as **text searchable**, not an image”

- Updated For CAs -> Getting Started page to align with the current UI.
- Updated homepage to replace webPKI-centric text, since there are certificates in our root stores that are for other purposes.
- Updated the For CAs -> Field Types and Valid Values page to align with the current UI, **and to explain how to find the list of auditors and locations known to the CCADB**.



Common CA Database

Field Types and Valid Values

This document explains how the various records and sections in the CCADB are best filled out, with some advice on how to create or obtain the data.

Auditor Information

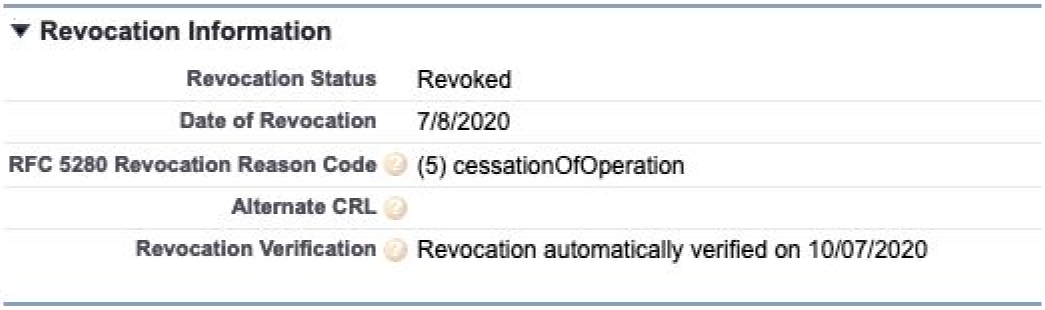
Field Name	What to Enter
Auditor	Find all Auditors known to the CCADB by clicking on the 'Auditors' report in the 'Custom Links' section in any Root Certificate, Intermediate Certiifcate, or Case page. Contact your root store operator if your auditor is not in this list. To fill in the auditor's name, click on the Edit button, then on the search icon (magnifying glass) next to the 'Auditor' field. Then enter the first letter of the auditor's name and an asterisk (e.g. B*), then click on the 'Go!' button.

PROPOSAL: Add field called Full CRL Issued By This CA

Please participate in discussion in mozilla.dev.security.policy about this.
Root store operators would like to easily find and use the URLs to the Full CRLs for things like Mozilla's CRLite. The BRs do not require CRL URLs in end-entity certificates, and many CAs use partitioned CRLs for end-entity certificates.
Proposal:

- Add field called '**Full CRL Issued By This CA**'

    - New field on intermediate certificate records which may be filled in by CAs or root store operators when the certificate signs certificates that do not contain CRL URLs or only contain URLs to partitioned CRLs.
    - This field would be included in **public-facing reports** such as http://ccadb-public.secure.force.com/ccadb/AllCertificateRecordsCSVFormat so that it can be used programmatically by root store operators, and could also be provided in crt.sh.
    - Also add this field to root certificate records, even though only root store operators can currently update root certificate records.
- Rename the current ‘Alternate CRL’ field to ‘Alternate CRL Containing This Cert’
    - This field was created because some intermediate certificates do not contain CRL URLs. (BRs now require intermediate certs to contain CRL URLs)



▼ **Revocation Information**

Revocation Status	Revoked
Date of Revocation	7/8/2020
RFC 5280 Revocation Reason Code	(5) cessationOfOperation
Alternate CRL	
Revocation Verification	Revocation automatically verified on 10/07/2020

ROADMAP

- November/December 2020
    - Upgrade to Salesforce Lightning -- this will cause some user interface changes, but we will try to keep the same page layout and flow.
    - Extend Audit Letter Validation (ALV) on intermediate certs to EV for TLS
- 2021
    - Update Case pages to use Lightning capabilities (to have better flow/interface)
    - Provide ability for CAs to preflight their new/draft audit statements on their root certs
    - Enable CAs to test new audit statements on their full CA hierarchies
    - Add Case for CAs to be able to update their non-audit information more frequently.