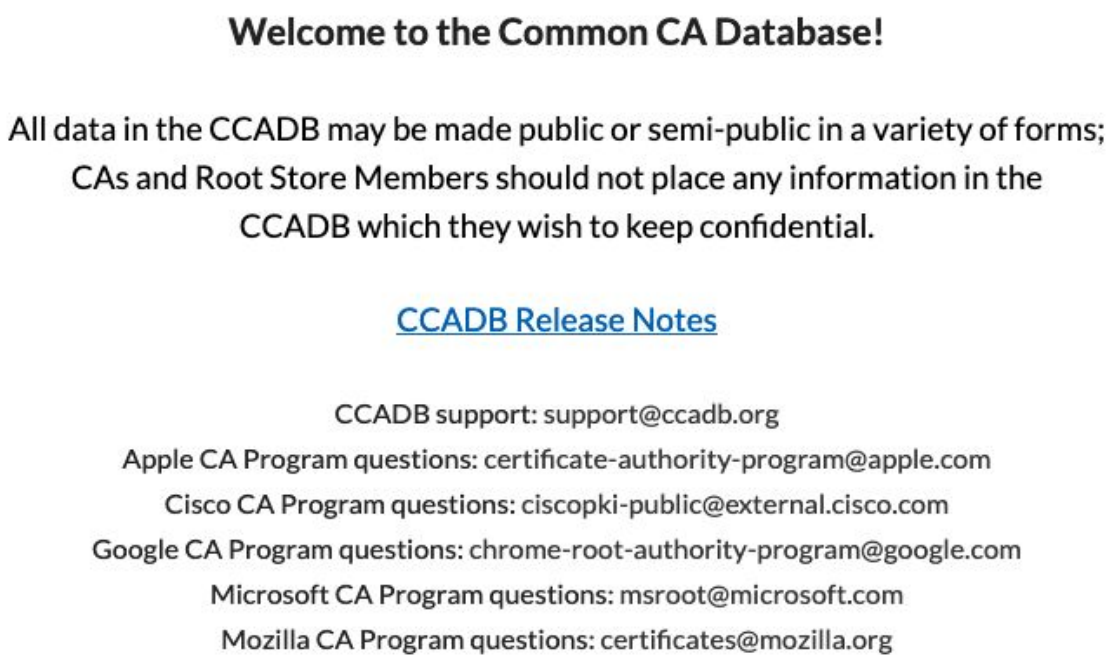
CCADB News - CABF F2F March 2021

CCADB Release Notes

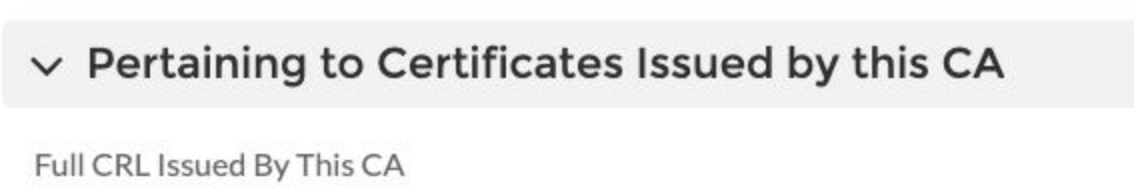
Added a link on the CCADB home page called CCADB Release Notes, which indicates the date when a significant change was made to CCADB Production, starting in November 2020.



Full CRL Issued By This CA

Added a section to root and intermediate certificate pages called ‘Pertaining to Certificates Issued by this CA’. There is currently one field in the new section:

- Full CRL Issued By This CA
    - Enter the URL to the full CRL for certificates issued by this CA.



Proposal under discussion in mozilla.dev.security.policy to add another field to this section called '**JSON Array of Partitioned CRLs Issued By This CA**'.

- When there is no full CRL for certificates issued by this CA, provide a JSON array whose elements are URLs of partial CRLs that when combined are the equivalent of a full CRL.
  - Example:
    [
    "http://cdn.example/crl-1.crl",
    "http://cdn.example/crl-2.crl"
    ]

We intend to update the API to add this new field, so that CAs can automate updates to this field for the intermediate certificates in their CA hierarchies.

API for Updating Intermediate Certificate Records

Digicert separately commissioned the creation of AddUpdateIntermediateCert API. If you would like to use this API, contact Kathleen to set up OAuth for your CA.

- Current documentation is available in GitHub, and it will be updated soon with more information about the process to set up OAuth.
  - https://github.com/mozilla/CCADB-Tools/tree/master/API_AddUpdateIntermediateCert

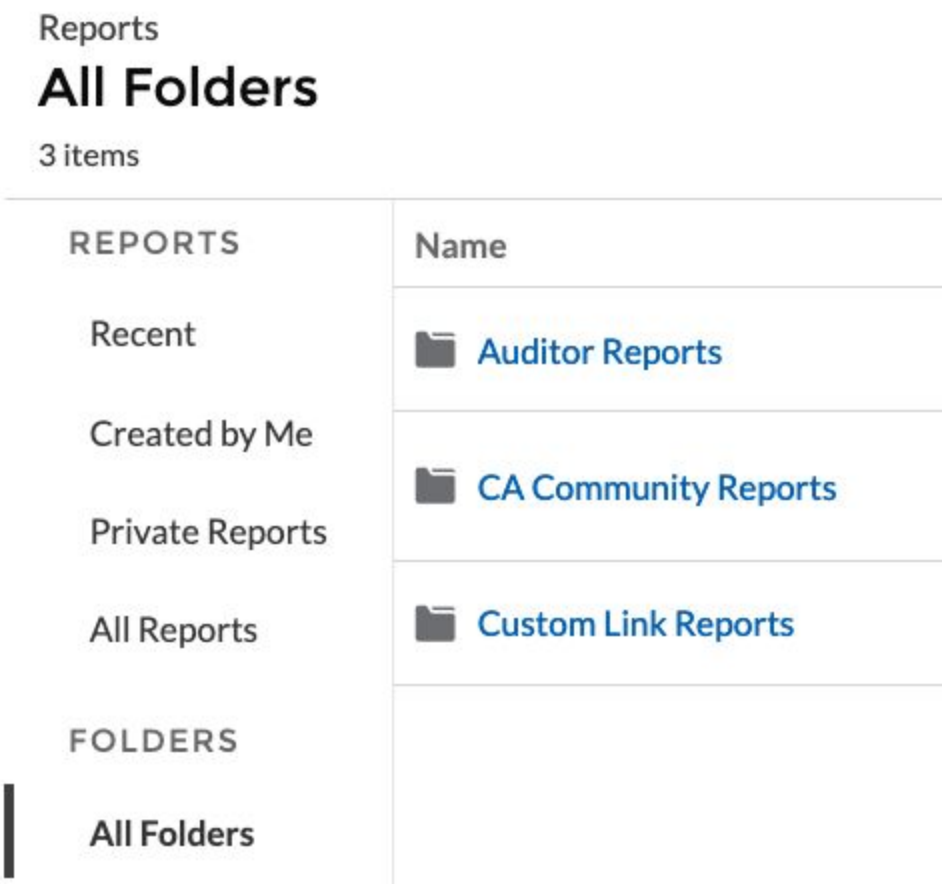
We also added an API for determining the CCADB Record ID given a cert PEM or SHA-256 Fingerprint and record type (i.e. root or intermediate certificate record). Information about this API will be added to the CCADB-Tools repository soon.

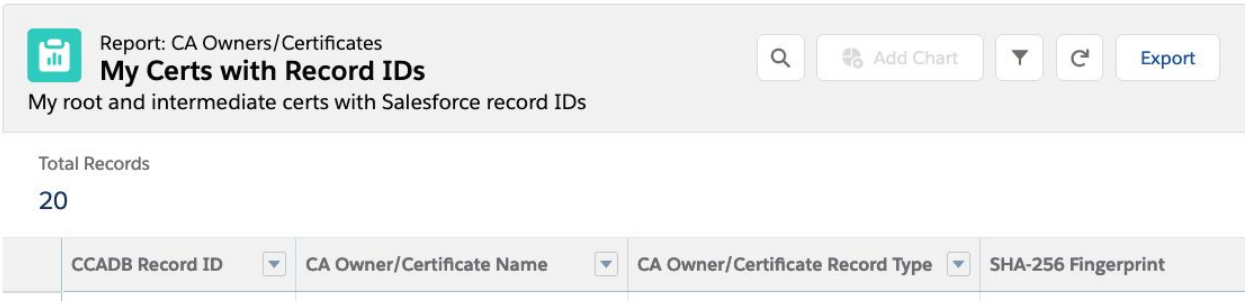
HARICA (Dimitris) used the API to update the 'Full CRL Issued By This CA' field for all of their intermediate certificate records.

- Scripts that were written by Dimitris are available here: https://github.com/HARICA-official/ccadb-ca-tools

There is a new CCADB report called 'My Certs with Record IDs' for CAs:

- 'More' tab -> 'Reports' tab -> 'All Folders' along the left column -> 'CA Community Reports -> 'My Certs with Record IDs'
- AddUpdateIntermediateCert API requires the 'CCADB Record ID' if you are updating an existing record



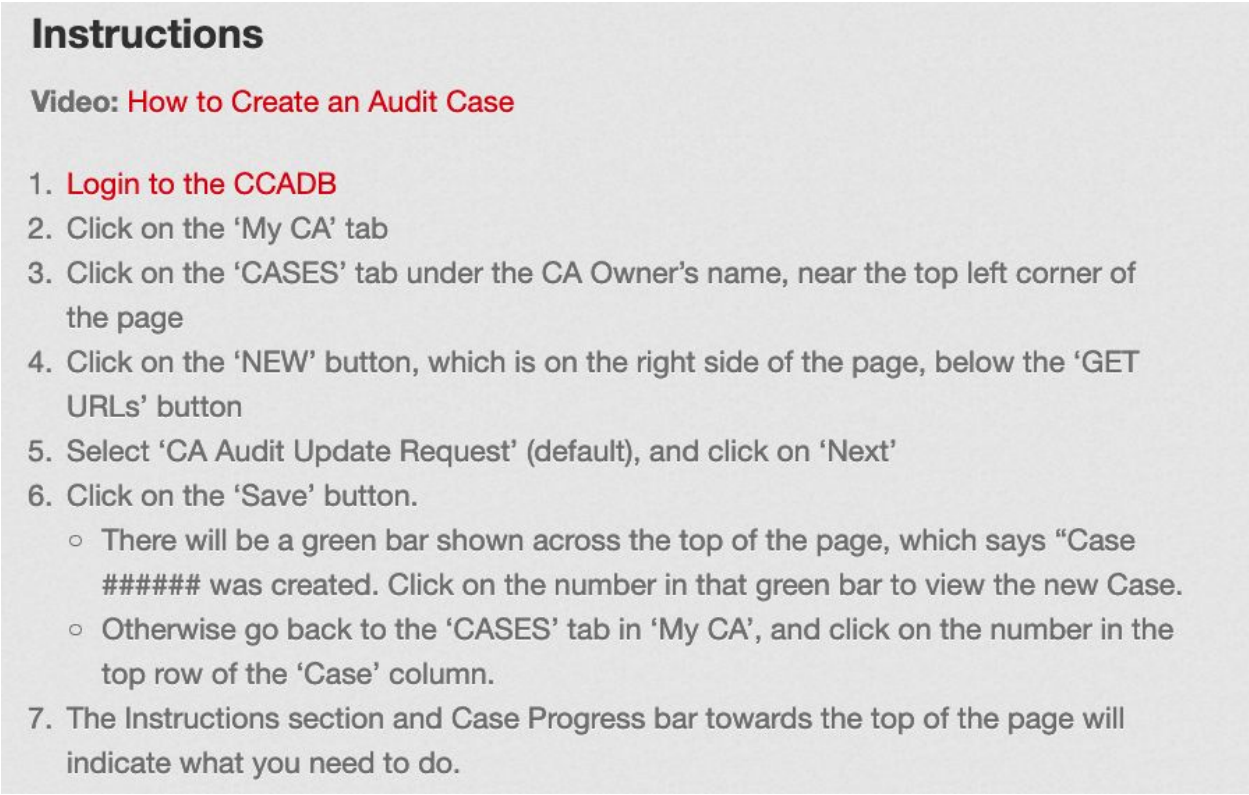


Migrated to newer “Lightning” interface

The CCADB has been migrated to Salesforce’s newer interface called “Lightning”, which was launched in 2014. In spring of 2019 Salesforce announced that they will no longer be adding features to their older interface called “Classic”.

- Differences between the Lightning(new) and Classic(old) interfaces
- Updated https://www.ccadb.org/cas/ pages to match the new interface

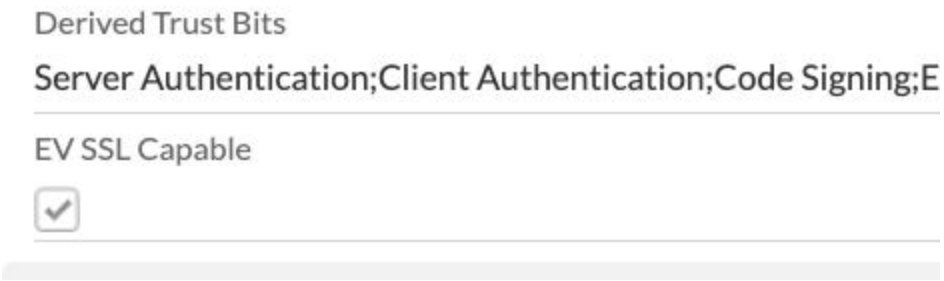
- Updated Video: “How to create an Audit Case”, which is available in Audit Case Instructions here: https://www.ccadb.org/cas/updates#instructions



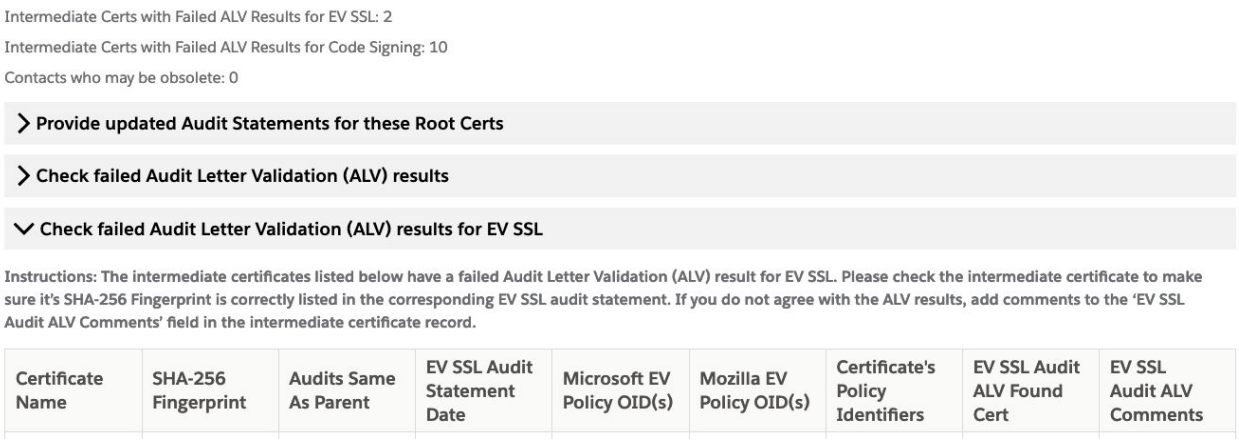
Extended ALV to EV SSL audits for intermediate certificates

Extended automated Audit Letter Validation (ALV) to EV SSL audits for intermediate certificates.

- Added ‘EV SSL Capable’ checkbox to the bottom of the ‘Certificate Data’ section on intermediate certificate records. The value of this checkbox is automatically determined based on the certificate content and root store values, and may not be changed manually. For example, for CAs in Mozilla’s program, the value is determined as described here: https://wiki.mozilla.org/CA/EV_Processing_for_CAs#EV_TLS_Capable



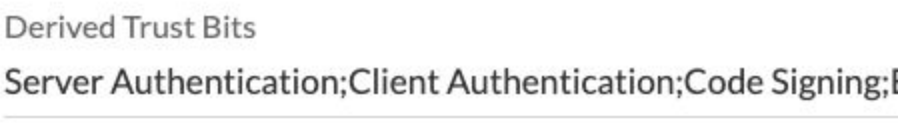
- Added CA home page Task list item called ‘Intermediate Certs with Failed ALV Results for EV SSL’.
    - When it is non-zero, click on the ">" next to ‘Check failed Audit Letter Validation (ALV) results for EV SSL’, which is below the Summary section. Then click on the link in the 'Certificate Name' column.



Extended ALV to Code Signing audits for intermediate certificates

Extended automated Audit Letter Validation (ALV) to Code Signing audits for intermediate certificates.

- If the ‘Derived Trust Bits’ field contains “Code Signing”, then the certificate’s SHA-256 fingerprint must be found in the corresponding code signing audit statements. The ‘Derived Trust Bits’ field contents are automatically determined based on certificate content and root store values, and may not be changed manually.



- Added CA home page Task list item called ‘Intermediate Certs with Failed ALV Results for Code Signing’.
    - When it is non-zero, click on the ">" next to ‘Check failed Audit Letter Validation (ALV) results for Code Signing’, which is below the Summary section. Then click on the link in the 'Certificate Name' column.

Intermediate Certs with Failed ALV Results for Code Signing: 10

Contacts who may be obsolete: 0

> **Provide updated Audit Statements for these Root Certs**

> **Check failed Audit Letter Validation (ALV) results**

> **Check failed Audit Letter Validation (ALV) results for EV SSL**

Check failed Audit Letter Validation (ALV) results for Code Signing

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

Certificate Name	Audits Same As Parent	Code Signing Audit Statement Date	Derived Trust Bits	Code Signing Audit ALV Found Cert	Code Signing Audit ALV Comments

2021 ROADMAP

- **[Done]** Extend ALV to Code Signing audits for intermediate certs.
- **[In Progress]** Extend Root Inclusion Cases to Apple
- Add Case Type for CAs to be able to update non-audit information more frequently on root certs (CP/CPS, contact info, test websites, full CRLs, etc.)
- Enable CAs to test new audit statements on full CA hierarchies
- Make it easier for CAs to preflight new (draft) audit statements; e.g. a form
- Update Case pages to have better flow/interface