



Enabling DNSSEC for a .LB Domain

A practical guide for Registrars

Purpose

The .LB Registry supports DNSSEC. This guide explains how a Registrar can enable DNSSEC for a particular domain after receiving the required DS record information from the Registrant or the domain's DNS/hosting provider.

DNSSEC establishes a chain of trust between the parent zone and the DNSSEC-signed domain. The Registrar's role is to enter the DS record information supplied for the domain into the Registry.

Step by Step Process

1. Obtain the DNSSEC Information

Before making any change in the Registry, the Registrant or their DNS/hosting provider must first enable DNSSEC on the domain's authoritative DNS service and provide the Registrar with the DS record information.

The Registrar needs the following four values:

Field	Description
Key Tag	Numeric identifier of the DNSSEC key.
Algorithm	DNSSEC signing algorithm used by the domain.
Digest Type	Hash algorithm used to create the DS digest.
Digest	The hexadecimal digest value associated with the DNSSEC key.

Important: Enter the DS values exactly as provided by the Registrant or DNS/hosting provider.



Enabling DNSSEC for a .LB Domain

A practical guide for Registrars

2. Open the Domain in the Registry

Log in to the Registry as a Registrar and open the domain for which DNSSEC is to be enabled.

On the Domain Summary page, locate the OPTIONS menu on the right side and click DS Records.

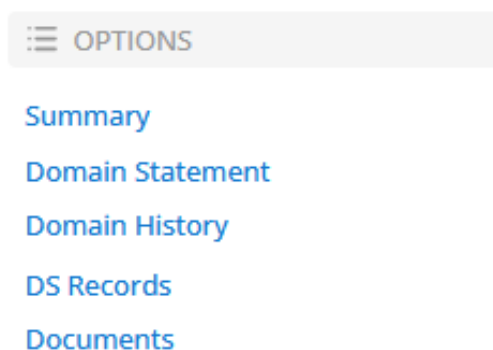


Figure 1 – Select DS Records from the domain OPTIONS menu.

3. Add the DS Record

On the DS Records page, enter the values supplied by the Registrant or DNS/hosting provider. Make sure that the selected Algorithm and Digest Type match the supplied DS record.

- Key Tag – Enter the numeric key tag.
- Algorithm – Select the matching DNSSEC algorithm.
- Digest Type – Select the matching digest type.
- Digest – Paste the complete hexadecimal digest.

Click ADD DS RECORD. If more than one DS record was supplied, add each required DS record separately.

After it is added, the DS record will appear in the table showing its Key Tag, Algorithm, Digest Type, Digest and Date.



Enabling DNSSEC for a .LB Domain

A practical guide for Registrars

	Key Tag	Algorithm	Digest Type	Digest	Date	Added By (Login)	Modify
☐	33628	ECDsa/P-256 SHA-256(No.13)	SHA-256(No.2)	67e5ef4cf60e7c36f91ab13b8d627d0313703db91a1c331cc9630ce67ba14899	2026 Feb 6 11:06	Saad Itani (saad_itani)	
☐	33628	ECDsa/P-256 SHA-256(No.13)	SHA-384(No.4)	fcf6869d34f6285522615dbf75a5a4aac78b8274770c7dec092cffe0eb690ecb653d2c74c4a43d9b3d3812809555b1	2026 Feb 6 11:06	Saad Itani (saad_itani)	

[DELETE](#)

Figure 2 – Example: DS records successfully added for LBDR.ORG.LB.

4. Confirm DNSSEC on the Domain Summary Page

After the DS records have been added, return to the Domain Summary page. In the DNSSEC section, the Registrar can confirm that DNSSEC is set to Yes, review the DS Records associated with the domain, and check the DNSSEC Status. In the LBDR.ORG.LB example below, the status shows “DNSSEC Valid and not expired”.

DNSSEC	Yes
DS Records	33628 ECDsa/P-256 SHA-256(No.13) SHA-256(No.2) 67e5ef4cf60e7c36f91ab13b8d627d0313703db91a1c331cc9630ce67ba14899 33628 ECDsa/P-256 SHA-256(No.13) SHA-384(No.4) fcf6869d34f6285522615dbf75a5a4aac78b8274770c7dec092cffe0eb690ecb653d2c74c4a43d9b3d3812809555b1
DNSSEC Status	DNSSEC Valid and not expired

Figure 3 – LBDR.ORG.LB Domain Summary showing DNSSEC enabled and valid.

5. Allow the Registry Change to Be Published

After the DS record is added, allow time for the Registry change to be published in the appropriate parent zone and for DNS caches to update.

6. Verify DNSSEC Online

After publication, verify the domain using an online DNSSEC validation service. These tools analyze the DNSSEC chain of trust and help identify missing or incorrect DS/DNSKEY relationships.

DNSViz – <https://dnsviz.net/>

Verisign DNSSEC Debugger – <https://dnssec-debugger.verisignlabs.com/>

Enter the domain name in either tool, then run the analysis. A correctly configured domain should show a valid DNSSEC chain of trust without validation errors.



Enabling DNSSEC for a .LB Domain

A practical guide for Registrars

Registrar Workflow at a Glance

1. Registrant/DNS provider enables DNSSEC.
2. Registrant/DNS provider supplies the DS information.
3. Registrar opens the domain in the Registry.
4. Registrar selects DS Records.
5. Registrar enters Key Tag, Algorithm, Digest Type and Digest.
6. Registrar clicks ADD DS RECORD.
7. After publication, Registrar verifies the domain using DNSViz or Verisign DNSSEC Debugger.

Warning: Only add a DS record after DNSSEC has been enabled on the domain's authoritative DNS service, and always use the exact DS information supplied for that domain.

