

STARTING MARCH 15, 2026

TLS CERTIFICATE AUTHORITIES UPDATE

Databricks is updating trusted TLS CAs for public-facing websites & API endpoints

WHAT'S CHANGING?



TLS CERTIFICATE MIGRATION

- **New Trusted CAs** — Databricks is migrating certificates for public-facing websites and API endpoints to new Certificate Authorities.
- **Security & Reliability** — This ensures continued compliance with industry best practices and improved resilience.
- **Gradual Rollout** — The update will begin rolling out gradually starting March 15, 2026.

[Sign Up to the newsletter](#)

 [Databricks.news](#)

Find more databricks tips @

[dailydatabricks.tips](#)

NEW CAS

[Sign Up to the newsletter](#)

 Databricks.news

Find more databricks tips @

[dailydatabricks.tips](#)

NEW CERTIFICATE AUTHORITIES

Databricks certificates are being migrated to these trusted CAs

- 1 Let's Encrypt**
Free, automated, and open CA trusted globally
- 2 Google Trust Services**
Google's publicly trusted Certificate Authority
- 3 AWS Certificate Manager**
Amazon's managed public & private certificates
- 4 DigiCert**
Enterprise-grade digital certificate provider



CHECK YOUR CLIENT CONNECTIVITY

You are NOT impacted if:

You use a supported browser or a client that already trusts the root and intermediate certificates from all four CAs.

Test your connectivity with these URLs:

ⓘ Let's Encrypt delta-sharing.westus.azuredatabricks.net

ⓘ Google Trust help.databricks.com

ⓘ AWS Cert Manager community.databricks.com

ⓘ DigiCert nvirginia.cloud.databricks.com

If you see "**Your connection is not private**" or "**certificate verify error**", you need to update your configuration.

ARE YOU IMPACTED?

[Sign Up to the newsletter](#)

 Databricks.news

Find more databricks tips @

dailydatabricks.tips

WHAT YOU NEED TO DO

- 1 **Test Connectivity** – Visit the test URLs on the previous slide using your client to check if connections succeed without errors.
- 2 **Update Trust Store** – If your clients don't trust all four CAs, update them to trust the root and intermediate certificates from all providers.
- 3 **Don't Pin to One CA** – If your clients are set to use only one CA, reconfigure them to trust all four to avoid interruptions.
- 4 **Need Help?** – Contact your Databricks account team for assistance with verifying or updating your client certificates.

ACTION REQUIRED



[Sign Up to the newsletter](#)

 [Databricks.news](#)

Find more databricks tips @

[dailydatabricks.tips](#)

WANT MORE TIPS?

FOLLOW FOR DAILY
DATABRICKS TIPS

SIGN UP TO THE NEWSLETTER



dailydatabricks.tips