# Download an SSL certificate for your managed database in Amazon Lightsail

*Last updated: January 2, 2020*

**Important**
The certificates labeled as `rds-ca-2015` expire on March 5, 2020. We strongly recommend that you start using the certificates labeled as `rds-ca-2019` as soon as possible. For more information, see Modifying your managed database in Amazon Lightsail to use a specific certificate.

You can use Secure Socket Layer (SSL) or Transport Layer Security (TLS) from your application to encrypt a connection to a managed database in Amazon Lightsail running MySQL, or PostgreSQL. Each DB engine has its own process for implementing SSL/TLS. For more information, see Using SSL to connect to your MySQL database in Amazon Lightsail or Using SSL to connect to your PostgreSQL database in Amazon Lightsail.

**Note**
The certificates available for download are labeled for Amazon Relational Database Service (Amazon RDS), but also work for managed databases in Lightsail.

To get a certificate bundle that contains both the intermediate and root certificates, download from https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem.

To get a root certificate that works for all AWS Regions, download from one of these locations:

- https://s3.amazonaws.com/rds-downloads/rds-ca-2019-root.pem
- https://s3.amazonaws.com/rds-downloads/rds-ca-2015-root.pem

This root certificate is a trusted root entity and should work in most cases but might fail if your application doesn't accept certificate chains. If your application doesn't accept certificate chains, download the AWS Region–specific certificate from the list of intermediate certificates found later in this section.

If your application is on Microsoft Windows and requires a PKCS7 file, you can download the PKCS7 certificate bundle. This bundle contains both the intermediate and root certificates at https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.p7b.

## Intermediate certificates

You might need to use an intermediate certificate to connect to your AWS Region. If you need an intermediate certificate for a particular AWS Region, download the certificate from the following list.

- US East (Ohio)
  - CA-2019: rds-ca-2019-us-east-2.pem
  - CA-2015: rds-ca-2015-us-east-2.pem
- US East (N. Virginia)
  - CA-2019: rds-ca-2019-us-east-1.pem
  - CA-2015: rds-ca-2015-us-east-1.pem
- US West (Oregon)
  - CA-2019: rds-ca-2019-us-west-2.pem

  - CA-2015: rds-ca-2015-us-west-2.pem
- Asia Pacific (Mumbai)
  - CA-2019: rds-ca-2019-ap-south-1.pem
  - CA-2015: rds-ca-2015-ap-south-1.pem
- Asia Pacific (Seoul)
  - CA-2019: rds-ca-2019-ap-northeast-2.pem
  - CA-2015: rds-ca-2015-ap-northeast-2.pem
- Asia Pacific (Singapore)
  - CA-2019: rds-ca-2019-ap-southeast-1.pem
  - CA-2015: rds-ca-2015-ap-southeast-1.pem
- Asia Pacific (Sydney)
  - CA-2019: rds-ca-2019-ap-southeast-2.pem
  - CA-2015: rds-ca-2015-ap-southeast-2.pem
- Asia Pacific (Tokyo)
  - CA-2019: rds-ca-2019-ap-northeast-1.pem
  - CA-2015: rds-ca-2015-ap-northeast-1.pem
- Canada (Central)
  - CA-2019: rds-ca-2019-ca-central-1.pem
  - CA-2015: rds-ca-2015-ca-central-1.pem
- Europe (Frankfurt)
  - CA-2019: rds-ca-2019-eu-central-1.pem
  - CA-2015: rds-ca-2015-eu-central-1.pem
- Europe (Ireland)
  - CA-2019: rds-ca-2019-eu-west-1.pem
  - CA-2015: rds-ca-2015-eu-west-1.pem
- Europe (London)
  - CA-2019: rds-ca-2019-eu-west-2.pem
  - CA-2015: rds-ca-2015-eu-west-2.pem
- Europe (Paris)
  - CA-2019: rds-ca-2019-eu-west-3.pem
  - CA-2015: rds-ca-2015-eu-west-3.pem