SSL/TLS System Variables

Reference list of system variables related to TLS configuration, such as `ssl_cipher`, `ssl_crl`, and `have_ssl`, used to manage and monitor encryption settings.

The system variables listed on this page relate to encrypting data during transfer between servers and clients using the Transport Layer Security (TLS) protocol. Often, the term Secure Sockets Layer (SSL) is used interchangeably with TLS, although strictly speaking the SSL protocol is the predecessor of TLS and is no longer considered secure.

For compatibility reasons, the TLS system variables in MariaDB still use the `ssl_` prefix, but MariaDB only supports its more secure successors. For more information on SSL/TLS in MariaDB, see Secure Connections Overview.

Variables

`have_openssl`

- Description: This variable shows whether the server is linked with OpenSSL ↗ rather than MariaDB's bundled TLS library, which might be wolfSSL ↗ or yaSSL ↗ .
  - I this system variable shows `YES` , the server is linked with OpenSSL.
  - See TLS and Cryptography Libraries Used by MariaDB for more information about which libraries are used on which platforms.
- Scope: Global

- Dynamic: No

`have_ssl`

- Description: This variable shows whether the server supports using TLS to secure connections.
  - If the value is `YES`, then the server supports TLS, and TLS is enabled.
  - If the value is `DISABLED`, then the server supports TLS, but TLS is not enabled.
  - If the value is `NO`, then the server was not compiled with TLS support, so TLS cannot be enabled.
  - When TLS is supported, check the have_openssl system variable to determine whether the server is using OpenSSL or MariaDB's bundled TLS library. See TLS and Cryptography Libraries Used by MariaDB for more information about which libraries are used on which platforms.
- Scope: Global
- Dynamic: No

`ssl_ca`

- Description: Defines a path to a PEM file that should contain one or more X509 certificates for trusted Certificate Authorities (CAs) to use for TLS. This system variable requires that you use the absolute path, not a relative path. This system variable implies the ssl option.
  - See Secure Connections Overview: Certificate Authorities (CAs) for more information.
- Command line: `--ssl-ca=file_name`
- Scope: Global
- Dynamic: No
- Data Type: `file name`

`ssl_capath`

- Description: Defines a path to a directory that contains one or more PEM files that should each contain one X509 certificate for a trusted Certificate Authority (CA) to use for TLS. This system variable requires that you use the absolute path, not a relative path. The directory specified by this variable needs to be run through the openssl rehash command. This system variable implies the ssl option.
  - See Secure Connections Overview: Certificate Authorities (CAs) for more information.
- Command line: `--ssl-capath=directory_name`
- Scope: Global
- Dynamic: No
- Data Type: `directory name`

`ssl_cert`

- Description: Defines a path to the X509 certificate file to use for TLS. This system variable requires that you use the absolute path, not a relative path. This system variable implies the ssl option.
- Command line: `--ssl-cert=name`
- Scope: Global
- Dynamic: No
- Data Type: `file name`
- Default Value: None

`ssl_cipher`

- Description: List of permitted ciphers or cipher suites to use for TLS. Besides cipher names, if MariaDB was compiled with OpenSSL, this variable could be set to "SSLv3" or "TLSv1.2" to allow all SSLv3 or all TLSv1.2 ciphers. Note that the TLSv1.3 ciphers cannot be excluded when using OpenSSL, even by using this system variable. See Using TLSv1.3 for details. This system variable implies the ssl option.
- Command line: `--ssl-cipher=name`
- Scope: Global

- Dynamic: No
- Data Type: `string`
- Default Value: None

`ssl_crl`

- Description: Defines a path to a PEM file that should contain one or more revoked X509 certificates to use for TLS. This system variable requires that you use the absolute path, not a relative path.
  - See Secure Connections Overview: Certificate Revocation Lists (CRLs) for more information.
  - This variable is only valid if the server was built with OpenSSL. If the server was built with wolfSSL ↗ or yaSSL ↗, then this variable is not supported. See TLS and Cryptography Libraries Used by MariaDB for more information about which libraries are used on which platforms.
- Command line: `--ssl-crl=name`
- Scope: Global
- Dynamic: No
- Data Type: `file name`
- Default Value: None

`ssl_crlpath`

- Description: Defines a path to a directory that contains one or more PEM files that should each contain one revoked X509 certificate to use for TLS. This system variable requires that you use the absolute path, not a relative path. The directory specified by this variable needs to be run through the openssl rehash ↗ command.
  - See Secure Connections Overview: Certificate Revocation Lists (CRLs) for more information.
  - This variable is only supported if the server was built with OpenSSL. If the server was built with wolfSSL ↗ or yaSSL ↗, then this variable is not supported. See TLS and Cryptography Libraries Used by MariaDB for more information about which libraries are used on which platforms.
- Command line: `--ssl-crlpath=name`

- Scope: Global
- Dynamic: No
- Data Type: `directory name`
- Default Value: None

`ssl_key`

- Description: Defines a path to a private key file to use for TLS. This system variable requires that you use the absolute path, not a relative path. This system variable implies the ssl option.
- Command line: `--ssl-key=name`
- Scope: Global
- Dynamic: No
- Data Type: `string`
- Default Value: None

`ssl_passphrase`

- Description: SSL certificate key passphrase. Works similarly to the `--passout/--passin` openssl command-line parameters. The pass phrase value can be formatted as follows:
  - `pass:` *`password`* — Provide the actual *password*.
  - `env:` *`var`* — Obtain the password from the environment variable *var*.
  - `file:` *`filename`* — Read the password from the specified file *filename*. Only the first line, up to the newline character, is read from the stream.

  If `ssl_passphrase` is set, SHOW VARIABLE shows one of `file:`, `env:`, or `pass:`, and doesn't reveal sensitive data.
- Command line: `--ssl-passphrase=val`
- Scope: Global
- Dynamic: No
- Data Type: `string`
- Default Value: None

- Introduced: MariaDB 12.0

`tls_version`

- Description: This system variable accepts a comma-separated list (with no whitespaces) of TLS protocol versions. A TLS protocol version will only be enabled if it is present in this list. All other TLS protocol versions will not be permitted.
  - See Secure Connections Overview: TLS Protocol Versions for more information.
- Command line: `--tls-version=value`
- Scope: Global
- Dynamic: No
- Data Type: `enumerated`
- Default Value:
  - TLSv1.1,TLSv1.2,TLSv1.3 (<= MariaDB 10.6.15, MariaDB 10.11.5, MariaDB 11.0.3)
  - TLSv1.2,TLSv1.3 (>= MariaDB 10.6.16, MariaDB 10.11.6, MariaDB 11.0.4 and later versions)
- Valid Values: TLSv1.0,TLSv1.1,TLSv1.2,TLSv1.3
- Introduced: MariaDB 10.4.6

`version_ssl_library`

- Description: The version of the TLS library that is being used. Note that the version returned by this system variable does not always necessarily correspond to the exact version of the OpenSSL package installed on the system. OpenSSL shared libraries tend to contain interfaces for multiple versions at once to allow for backward compatibility. Therefore, if the OpenSSL package installed on the system is newer than the OpenSSL version that the MariaDB server binary was built with, then the MariaDB server binary might use one of the interfaces for an older version.
  - See TLS and Cryptography Libraries Used by MariaDB: Checking the Server's OpenSSL Version for more information.
- Scope: Global

- Dynamic: No
- Data Type: `string`
- Default Value: None

See Also

- Secure Connections Overview
- System Variables for a complete list of system variables and instructions on setting them.
- Full list of MariaDB options, system and status variables

Previous
Securing Connections for Client and Server

Next
Using TLSv1.3

Last updated 19 days ago

Was this helpful?