Configure TLS protocol

You can change TLS protocols to improve the security of your Redis Enterprise cluster and databases. The default settings are in line with industry best practices, but you can customize them to match the security policy of your organization.

Configure TLS protocol

The communications for which you can modify TLS protocols are:

- **Control plane** - The TLS configuration for cluster administration.
- **Data plane** - The TLS configuration for the communication between applications and databases.
- **Discovery service (Sentinel)** - The TLS configuration for the discovery service.

You can configure the TLS protocols with the `rladmin` commands shown here or with the REST API.

**Warning**: After you set the minimum TLS version, Redis Enterprise Software does not accept communications with TLS versions older than the specified version.

TLS support depends on the operating system. You cannot enable support for protocols or versions that aren’t supported by the operating system running Redis Enterprise Software. In addition, updates to the operating system or to Redis Enterprise Software can impact protocol and version support.

To illustrate, version 6.2.8 of Redis Enterprise Software removed support for TLS 1.0 and TLS 1.1 on Red Hat Enterprise Linux 8 (RHEL 8) because that operating system does not enable support for these versions by default.

If you have trouble enabling specific versions of TLS, verify that they're supported by your operating system and that they're configured correctly.

**Note**: TLSv1.2 is generally recommended as the minimum TLS version for encrypted communications. Check with your security team to confirm which TLS protocols meet your organization’s policies.

**Control plane**

To set the minimum TLS protocol for the control plane:

- **Default TLS Protocols**: TLSv1.0
  
  **Syntax**: `rladmin cluster config min_control_TLS_version <TLS_Version>`
  
  **TLS versions available**:
  
  - For TLSv1-1
  - For TLSv1.1 - 1.1
  - For TLSv1.2 - 1.2

  For example:

  `rladmin cluster config min_control_TLS_version 1.2`

**Data plane**

To set the minimum TLS protocol for the data path:
- Default TLS Protocols: TLSv1.0

- Syntax: `rladmin cluster config min_data_TLS_version <TLS_Version>`

- TLS versions available:
  - For TLSv1 - 1
  - For TLSv1.1 - 1.1
  - For TLSv1.2 - 1.2

For example:

```
rladmin cluster config min_data_TLS_version 1.2
```

For your changes to take effect on the discovery service, restart the service with this command:

```
supervisorctl restart sentinel_service
```

**Discovery service**

To enable TLS for the discovery service:

- Default: Allows both TLS and non-TLS connections

- Syntax: `rladmin cluster config sentinel_ssl_policy <ssl_policy>`

- **ssl_policy values available:**
  - allowed - Allows both TLS and non-TLS connections
  - required - Allows only TLS connections
  - disabled - Allows only non-TLS connections

For example:

```
rladmin cluster config sentinel_ssl_policy required min_data_TLS_version 1.2
```

For your changes to take effect on the discovery service, restart the service with this command:

```
supervisorctl restart sentinel_service
```

**Updated:** April 15, 2022