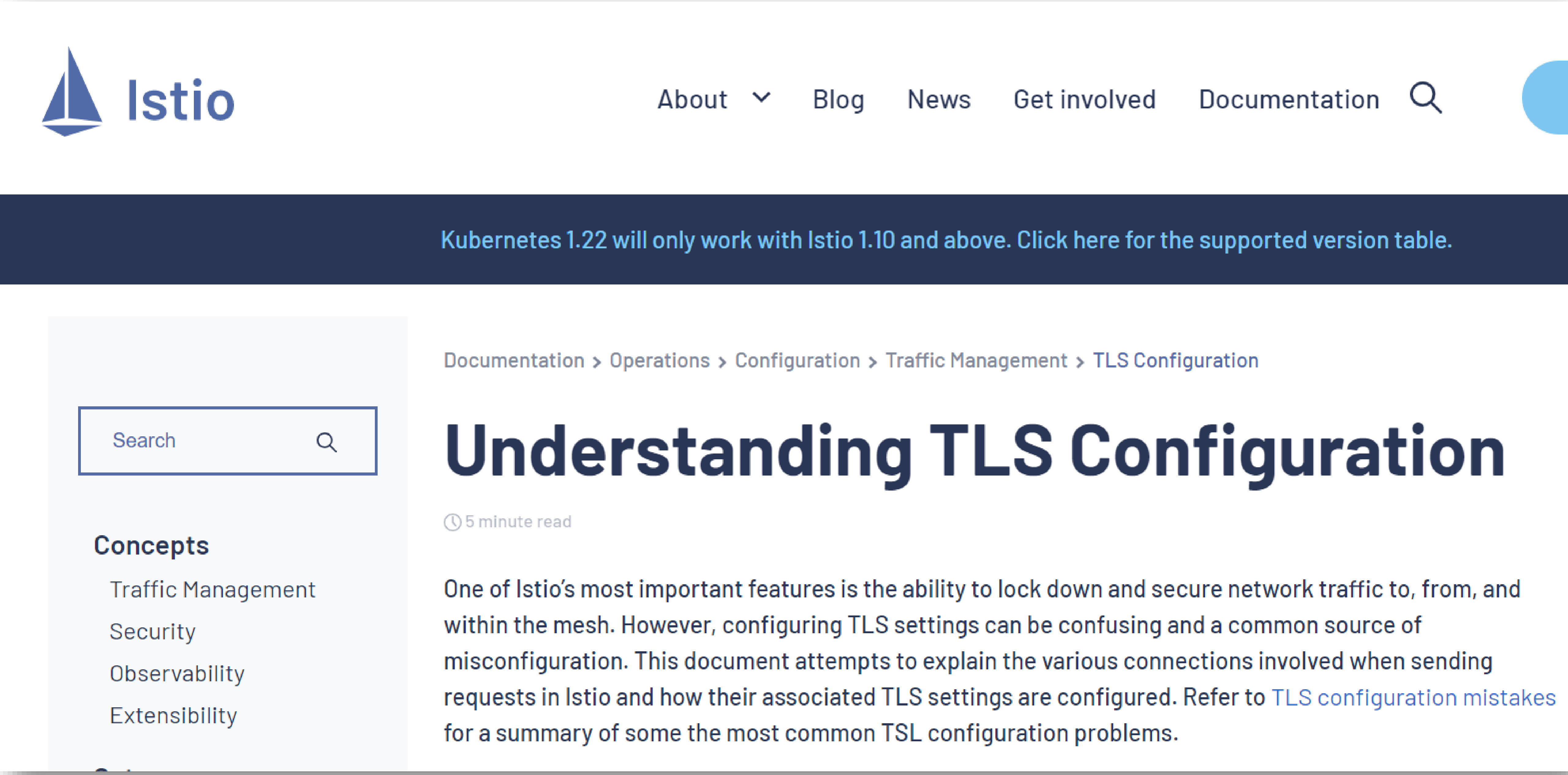
Service Mesh and Security

- Service Mesh offers a lot of built-in security features
- Handles security aspects instead of the service itself
- Should be configured, not automatic
- Learn about security features of the specific Service Mesh implementation

Service Mesh and Security

- Network security
  - Encrypt traffic using TLS
  - Restrict IP access



Kubernetes 1.22 will only work with Istio 1.10 and above. Click here for the supported version table.

Documentation > Operations > Configuration > Traffic Management > TLS Configuration

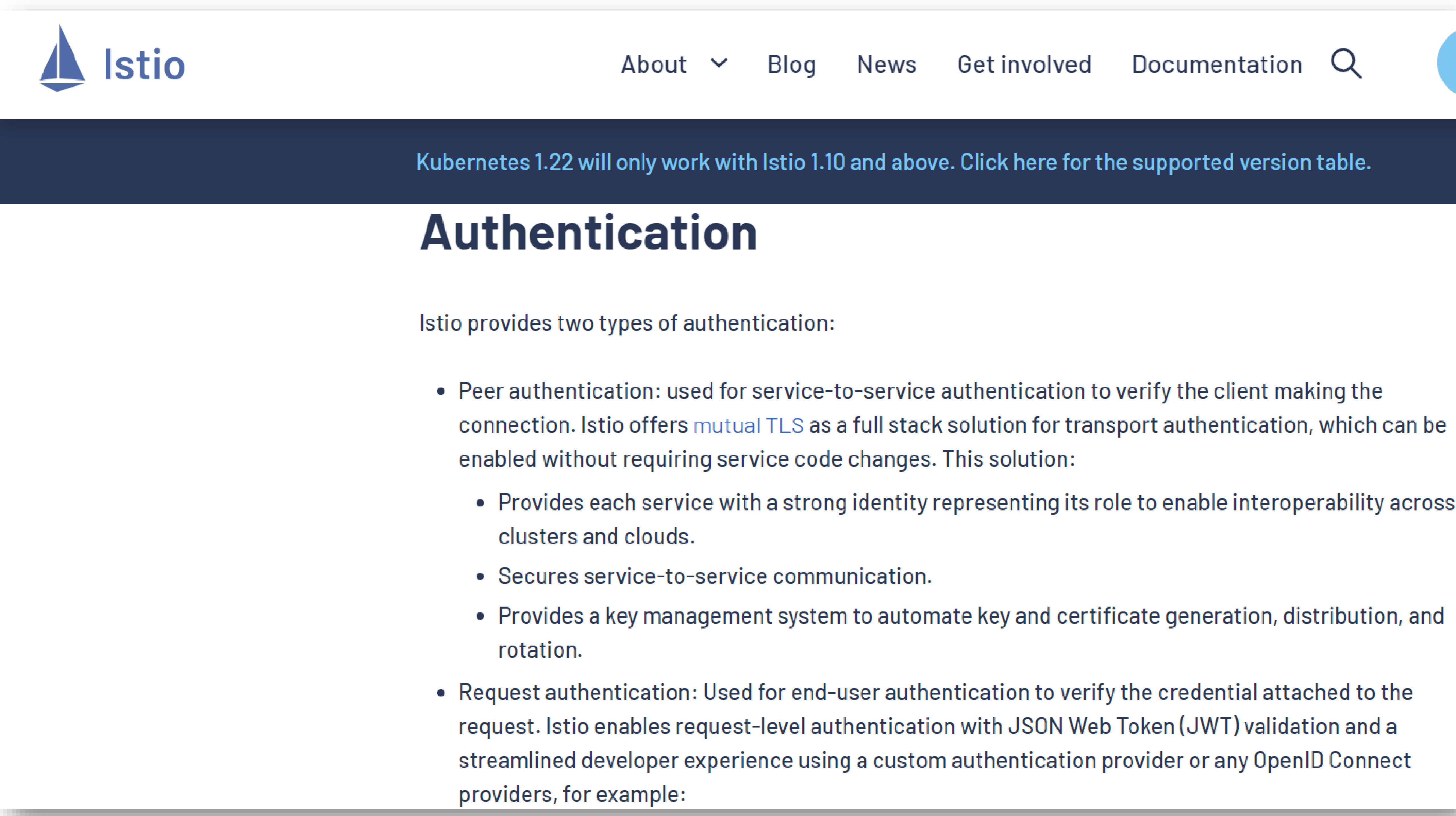
Understanding TLS Configuration

5 minute read

One of Istio's most important features is the ability to lock down and secure network traffic to, from, and within the mesh. However, configuring TLS settings can be confusing and a common source of misconfiguration. This document attempts to explain the various connections involved when sending requests in Istio and how their associated TLS settings are configured. Refer to TLS configuration mistakes for a summary of some the most common TSL configuration problems.

Service Mesh and Security

- Identity security
    - Validate certificate
    - Integrate with identity providers using OAuth
    - Integrate Role Based Access Control (RBAC)



Kubernetes 1.22 will only work with Istio 1.10 and above. Click here for the supported version table.

Authentication

Istio provides two types of authentication:

- Peer authentication: used for service-to-service authentication to verify the client making the connection. Istio offers mutual TLS as a full stack solution for transport authentication, which can be enabled without requiring service code changes. This solution:
  - Provides each service with a strong identity representing its role to enable interoperability acros clusters and clouds.
  - Secures service-to-service communication.
  - Provides a key management system to automate key and certificate generation, distribution, and rotation.
- Request authentication: Used for end-user authentication to verify the credential attached to the request. Istio enables request-level authentication with JSON Web Token (JWT) validation and a streamlined developer experience using a custom authentication provider or any OpenID Connect providers, for example:

Service Mesh and Security

- Logging
  - Extensive logging & audit trail
  - Documents every access to the service
    - Including identity
  - Provides a lot of data to be used for security analysis

Service Mesh and Security

- Check the actual features offered by the implementation you choose
- Offload security aspects to the service mesh
- Utilize the built-in logging