


## Configure security for the Elastic Stack

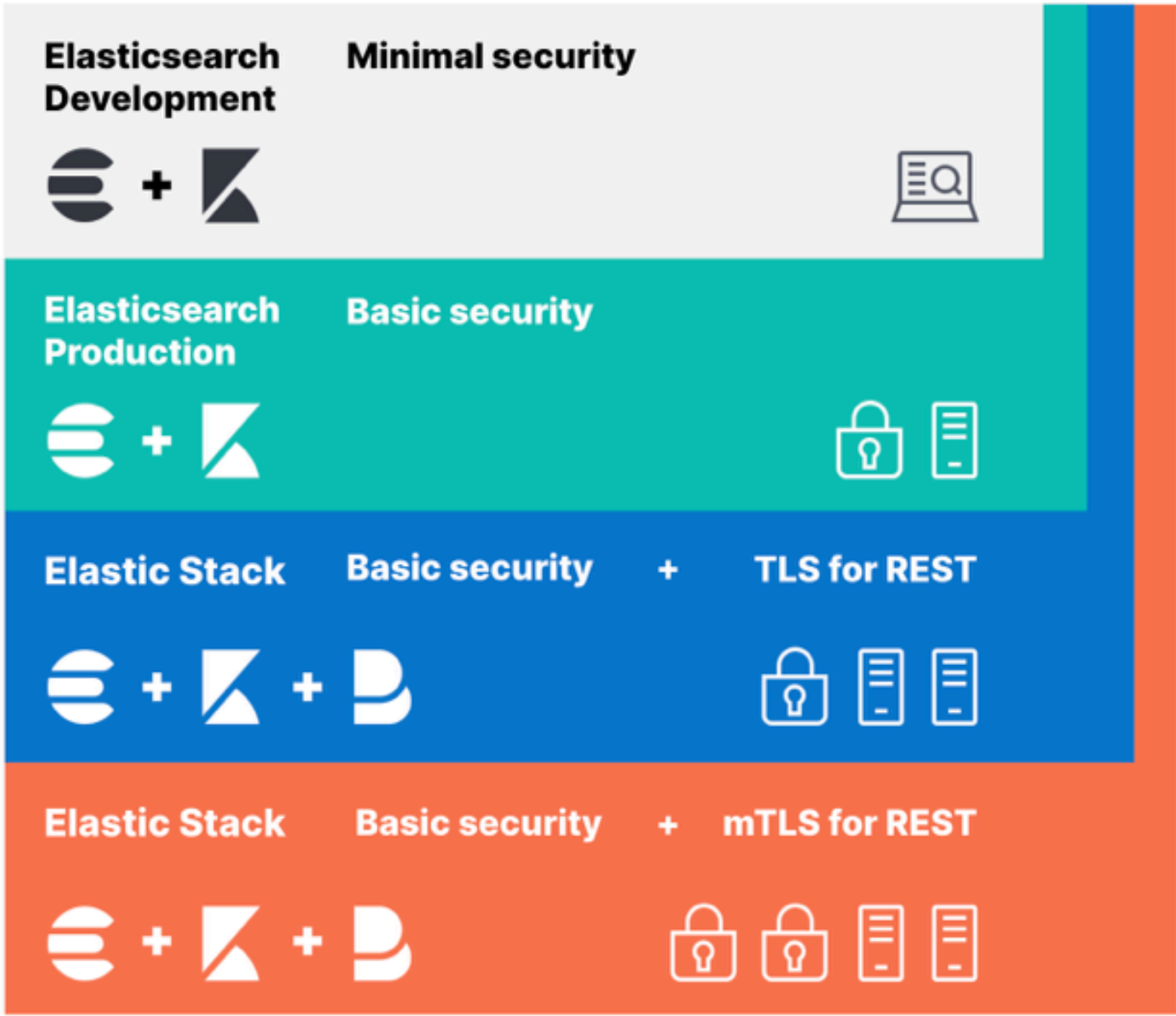
Security needs vary depending on whether you're developing locally on your laptop or securing all communications in a production environment. Because security needs vary, the following scenarios provide options for configuring the Elastic Stack.

TIP

Each subsequent scenario builds on the previous one so that you can add additional security by building on the existing layer.


These scenarios don't cover every situation, but provide a framework for securing Elasticsearch and the Elastic Stack based on typical use cases.

### Elastic Security Layers



#### Minimal security (Elasticsearch Development)

If you want to set up Elasticsearch on your laptop and start developing, this scenario is for you. This configuration prevents unauthorized access to your local cluster by setting up passwords for the built-in users. You also configure password authentication for Kibana.

IMPORTANT

The minimal security scenario is not sufficient for [production mode](#) clusters. If your cluster has multiple nodes, you must enable minimal security and then [configure Transport Layer Security \(TLS\)](#) between nodes.

[Set up minimal security](#)

#### Basic security (Elasticsearch Production)


This scenario builds on the minimal security requirements by adding transport Layer Security (TLS) for communication between nodes. This additional layer requires that nodes verify security certificates, which prevents unauthorized nodes from joining your Elasticsearch cluster.

Your external HTTP traffic between Elasticsearch and Kibana won't be encrypted, but internode communication will be secured.

[Set up basic security](#)

#### Basic security plus secured HTTPS traffic (Elastic Stack)

This scenario builds on the one for basic security and secures all HTTP traffic with TLS. In addition to configuring TLS on the transport interface of your Elasticsearch cluster, you configure TLS on the HTTP interface for both Elasticsearch and Kibana.

NOTE

If you need mutual (bidirectional) TLS on the HTTP layer, then you'll need to configure mutual authenticated encryption.




You then configure Kibana and Beats to communicate with Elasticsearch using TLS so that all communications are encrypted. This level of security is strong, and ensures that any communications in and out of your cluster are secure.

[Set up basic security plus HTTPS traffic](#)






### On this page


- [Minimal security \(Elasticsearch Development\)](#)
- [Basic security \(Elasticsearch Production\)](#)
- [Basic security plus secured HTTPS traffic \(Elastic Stack\)](#)

#### Most Popular

-  [Get Started with Elasticsearch](#)
-  [ELK for Logs & Metrics](#)
-  [Intro to Kibana](#)

#### Recommended for you

-  [Search API | Elasticsearch](#)
-  [Query string query | Elasticsearch](#)
-  [Mapping | Elasticsearch](#)
-  [Reindex API | Elasticsearch](#)
-  [Install Elasticsearch with Docker | Elasticsearch](#)

+ Elasticsearch Guide: **7.12** (current) 

+ [What is Elasticsearch?](#)

+ [What's new in 7.12](#)

+ [Quick start](#)

+ [Set up Elasticsearch](#)

+ [Upgrade Elasticsearch](#)

+ [Index modules](#)

+ [Mapping](#)

+ [Text analysis](#)

+ [Index templates](#)

+ [Data streams](#)

+ [Ingest pipelines](#)

+ [Search your data](#)

+ [Query DSL](#)

+ [Aggregations](#)

+ [EQL](#)

+ [SQL access](#)

+ [Scripting](#)

+ [Data management](#)

+ [ILM: Manage the index lifecycle](#)

+ [Autoscaling](#)

+ [Monitor a cluster](#)

+ [Frozen indices](#)

+ [Roll up or transform your data](#)

+ [Set up a cluster for high availability](#)

+ [Snapshot and restore](#)

- [Secure the Elastic Stack](#)

- [Configuring security](#)

+ [Set up minimal security](#)

+ [Set up basic security](#)

+ [Set up basic security plus HTTPS](#)

+ [Encrypting communications in an Elasticsearch Docker Container](#)

+ [Enabling cipher suites for stronger encryption](#)

+ [Security files](#)

+ [FIPS 140-2](#)

+ [User authentication](#)

+ [User authorization](#)

+ [Enable audit logging](#)

+ [Restricting connections with IP filtering](#)

+ [Cross cluster search, clients, and integrations](#)

+ [Operator privileges](#)

+ [Troubleshooting](#)

+ [Limitations](#)

+ [Watch for cluster and index events](#)

+ [Command line tools](#)

+ [How to](#)

+ [Glossary](#)

+ [REST APIs](#)

+ [Migration guide](#)

+ [Release notes](#)

+ [Dependencies and versions](#)

#### PRODUCTS & SOLUTIONS

- [Enterprise Search](#)
- [Observability](#)
- [Security](#)
- [Elastic Stack](#)
- [Elasticsearch](#)
- [Kibana](#)
- [Logstash](#)
- [Beats](#)
- [Subscriptions](#)
- [Pricing](#)

#### COMPANY

- [Careers](#)
- [Board of Directors](#)
- [Contact](#)

#### RESOURCES

- [Documentation](#)
- [What is the ELK Stack?](#)
- [What is Elasticsearch?](#)
- [Migrating from Splunk](#)
- [Compare AWS Elasticsearch](#)
- [US Public Sector](#)

#### Subscribe to our newsletter

Email address

Sign up

#### Follow Us

- 
- 
- 
- 