



On-boarding using external https relays (22.x.x)

September 28, 2023

Table of Contents

- 1 Management Console Communication 1
- 2 Elasticsearch Communication..... 1
- 3 Common Settings..... 1

The functionality described below can be used when an application protected by the Waratek Agent requires SSL configuration that conflicts with the configuration required by the Agent.

The implementation is based on a new feature called a 'Relay', which utilizes a separate java process, and therefore can be configured separately.

A relay can be configured for the following services :

- agent to Portal Dedicated communication
- agent to Elasticsearch communication

1 Management Console communication

The functionality for Portal Dedicated communication is enabled using the following flag :

```
com.waratek.ControllerRelay=true
```

No extra changes are required to other flags, in particular other flags that specify the connectivity to the Portal Dedicated do not need to change.

One optional parameters is also provided, for greater control of the relay:

```
com.waratek.ControllerRelayPort=<port>
```

The default value for this flag is 48080

2 Elasticsearch communication



Note : Elasticsearch communication is only supported in agents v22.2.0 or greater

The functionality for Elasticsearch communication is enabled using the following flag :

```
com.waratek.ElasticsearchRelay=true
```

One optional parameters is also provided, for greater control of the relay:

```
com.waratek.ElasticsearchRelayPort=<port>
```

The default value for this flag is 49200

3 Common settings

The settings below are common to both Portal Dedicated and Elasticsearch communication:

```
com.waratek.ControllerRelayJavaPath=<path to java executable>
```

This flag can be used to specify an alternative location of Java executable. By default, the relay will use the same J path as the application.

If the environment is utilizing custom trust store, the following flags are required :

```
com.waratek.trustStore=<path-to-truststore>  
com.waratek.trustStorePassword=<password-for-truststore>
```

If the above flags are specified then the following flag will be ignored :

```
com.waratek.ControllerSSLCertificateValidation=false
```

So in summary, these settings are mutually exclusive, i.e. if Waratek trust store is provided it will be used and in this case the relay would never disable certificate validation.