



## WSO2-2025-4494 - Use case 2

*You have clients that use mTLS to connect to the WSO2 products for transport-level security, but don't use certificate-based authentication for System REST APIs or SOAP services.*

---

If you are not using certificate-based authentication, disable it by following the sections below.

### **Part A: Validate and disable certificate-based authentication for System REST APIs**

If you are using one of the following versions, you need to update the product to disable certificate-based authentication for System REST APIs.

- WSO2 API Manager 3.0.0, 3.1.0, 3.2.0, 3.2.1, 4.0.0, 4.1.0
- WSO2 Identity Server 5.9.0, 5.10.0, 5.11.0
- WSO2 Identity Server as Key Manager 5.9.0
- WSO2 Open Banking AM 2.0.0
- WSO2 Open Banking IAM 2.0.0

For other products, if the following configuration is available, no further action is required. If it's missing, add it to secure the System REST APIs.

- For IS 6.0.0 and above; APIM 4.2.0 and above:

```
<PRODUCT_HOME>/repository/conf/deployment.toml
```

```
[event.default_listener.client_certificate_authentication_handler]
enable = false
```

- For IS 5.8.0 and below; IS KM 5.7.0 and below; APIM 2.6.0 and below; OB KM 1.5.0 and below; OB AM 1.5.0 and below:

```
<PRODUCT_HOME>/repository/conf/identity/identity.xml
```

```
under <EventListeners>
```

```
<EventListener id="client_certificate_authentication_handler"
type="org.wso2.carbon.identity.core.handler.AbstractIdentityMessageHandler"
name="org.wso2.carbon.identity.auth.service.handler.impl.ClientCertificateBasedAuthenticationHandler"
orderId="10"
enable="false"/>
```



## Part B: Validate and disable certificate-based authentication for SOAP services

WSO2 API Manager and WSO2 Open Banking AM products are not affected with this use case, since certificate-based authentication for SOAP services capability is not available in those products.

For the other products, if you have the below configuration, the certificate-based authentication for SOAP services is enabled.

- For IS 5.9.0 and above; IS KM 5.9.0 and above; OB IAM 2.0.0:

<PRODUCT\_HOME>/repository/conf/deployment.toml

```
[admin_console.authenticator.mutual_ssl_authenticator]
enable = true
```

- For IS 5.8.0 and below; IS KM 5.7.0 and below; OB KM 1.5.0 and below:

<PRODUCT\_HOME>/repository/conf/security/authenticators.xml under  
<Authenticators>

```
<Authenticator name="MutualSSLAuthenticator">
  <Priority>5</Priority>
  <Config>
    ...
  </Config>
</Authenticator>
```

Verify if you have any use cases that require certificate-based authentication for SOAP services. If you do not have any use cases, disable certificate-based authentication for SOAP services by changing the configuration as follows.

- For IS 5.9.0 and above; IS KM 5.9.0 and above; OB IAM 2.0.0:

<PRODUCT\_HOME>/repository/conf/deployment.toml

```
[admin_console.authenticator.mutual_ssl_authenticator]
enable = false
```

- For IS 5.8.0 and below; IS KM 5.7.0 and below; OB KM 1.5.0 and below:

<PRODUCT\_HOME>/repository/conf/security/authenticators.xml under  
<Authenticators>

```
<Authenticator name="MutualSSLAuthenticator" disabled="true">
  <Priority>5</Priority>
  <Config>
    ...
  </Config>
</Authenticator>
```