



WSO2-2025-4494 - Mitigation steps for SOAP Services

After getting this update for WSO2-2025-4494, certificate-based authentication for SOAP Services will be disabled by default.

Add the following configuration to make it enable and enforce specific certificate issuer and user validations as per the requirements of your use cases.

The following are example values:

- For IS 5.9.0 and above; OB IAM 2.0.0:

<PRODUCT_HOME>/repository/conf/deployment.toml

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

[admin_console.authenticator.mutual_ssl_authenticator.config]
allowed_issuers="DN1|DN2"

"issuer_DN1"="user01,user02"
"issuer_DN2"="*"
```

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

<PRODUCT_HOME>/repository/conf/security/authenticators.xml

```
<Authenticator
  id="mutual_ssl_authenticator"
  name="MutualSSLAuthenticator"
  disabled="false">
  <Priority>5</Priority>
  <Config>
    <Parameter name="log_client_cert_info">false</Parameter>
    <Parameter name="allowed_issuers">DN1|DN2</Parameter>
    <Parameter name="issuer_DN1">user01,user02</Parameter>
    <Parameter
name="cert_thumbprint_E2:AE:8D:6E:04">user01,user02</Parameter>
    <Parameter name="UsernameHeader">UserName</Parameter>
    <Parameter name="WhiteListEnabled">false</Parameter>
  </Config>
</Authenticator>
```



The following table describes the configuration parameters along with their meaning and possible values.

Configuration	Example value(s)	Description
allowed_issuers	"C=US, ST=California, O=Global Tech Inc, OU=Engineering, CN=Jane Smith C=GB, L=London, O=Example Services Ltd, CN=api.example.co.uk"	Specifies the distinguished names (DNs) of certificate issuers that are permitted. Certificates issued by other authorities will be rejected. This is a mandatory configuration after applying this update.

The following table outlines the configuration parameters, their description, and possible values.

Configuration	Description
"cert_thumbprint_<thumbprint_01>="user01,user02"	Any certificate with a thumbprint included in the allowed list can be used by the specified users.
"cert_thumbprint_<thumbprint_02>="*"	Any certificate with a thumbprint included in the allowed list can be used by any user within the user stores.
"issuer_<DN1>="user01,user02"	Any certificate issued by the specified Issuer can be used by the specified users.
"issuer_<DN2>="*"	Any certificate issued by the specified Issuer can be used by any user within the user stores.

You can retrieve the issuer name by running the following command:

```
openssl x509 -in <your-crt> -noout -issuer -nameopt dn_rev
```

You can retrieve the thumbprint by running the following command:

```
openssl x509 -in <your-crt> -noout -fingerprint -sha256
```