WSO2-2025-4494 - Mitigation steps for System REST APIs

After applying the update for WSO2-2025-4494, certificate-based authentication for System REST APIs will be disabled.

Refer to the following sections and add relevant configurations to enable it and enforce specific certificate issuer and user validations based on the use case.

- If you use certificate-based client authentication for System REST APIs without the WSO2-Identity-User header
- If you use certificate-based client authentication for System REST APIs with the WSO2-Identity-User header

Important: If you are using any of the following features on top of any of the following versions, certificate-based authentication is used internally for System REST APIs. Hence, you must follow the section Securing System REST APIs for internal usage **in addition** to the sections mentioned above.

- Features:
    - Identifier-first authentication
    - Dynamic prompts using adaptive scripts
    - Session limiter
- Product versions:
    - WSO2 Identity Server 5.7.0, 5.9.0, 5.10.0, 5.11.0
    - WSO2 Identity Server Key Manager 5.7.0, 5.9.0, 5.10.0
    - WSO2 Open Banking IAM 2.0.0
    - WSO2 Open Banking Key Manager 1.4.0, 1.5.0

If you use certificate-based client authentication for System REST APIs without the WSO2-Identity-User header

Enable certificate-based authentication for System REST APIs and configure system user thumbprint mappings as per the requirements of your use cases.

The following are example values:

- For IS 5.9.0 and above; APIM 3.0.0 and above; OB IAM 2.0.0; OB AM 2.0.0:
  `<PRODUCT_HOME>/repository/conf/deployment.toml`

```
[client_certificate_based_authentication]
enable = true

[[client_certificate_based_authentication.system_thumbprint_mapping]]
trusted_issuer =    "C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA,
emailAddress=ca@wso2.com"
cert_thumbprint =
"78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48
:22:91:98:A9:FD:47"
allowed_system_user = "admin"
```

- For IS 5.8.0 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`

```
<ClientCertBasedAuthentication enable="true">
    <SystemThumbprintMappings>
        <Mapping>
            <TrustedIssuer>C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM,
CN=RootCA, emailAddress=ca@wso2.com</TrustedIssuer>

<CertThumbprint>78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3
:77:41:1B:6D:48:22:91:98:A9:FD:47</CertThumbprint>
            <AllowedSystemUser>admin</AllowedSystemUser>
        </Mapping>
    </SystemThumbprintMappings>
</ClientCertBasedAuthentication>
```

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

Configuration	Example value(s)	Description
`trusted_issuer`	`"C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com "`	Specifies the distinguished name (DN) of the certificate issuer that is permitted. Certificates issued by other authorities will be rejected. You can retrieve the issuer name by running the following command: `openssl x509 -in <your-crt> -noout -issuer -nameopt dn_rev` **This is a mandatory configuration after applying this update.**
`cert_thumbprint`	`"78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48:22:91:98:A9:FD:47"`	Exact fingerprint of the client certificate. You can retrieve the fingerprint by running the following command: `openssl x509 -in <your-cert> -noout -fingerprint -sha256` **This is a mandatory configuration after applying this update.** If the requirement is to allow any thumbprints issued by the trusted issuer, please ensure the value is "*"
`allowed_system_user`	`"sample_system_user"`	Maps the certificate directly to a system-level user account **This is a mandatory configuration after applying this update.** If the requirement is to allow any system users who are accessing with a certificate issued by a trusted issuer and having the same thumbprint, please ensure the value is "*"

The following table outlines the different combinations of configurations and description about the applied scenario in each case.

Trusted Issuer (trusted_issuer)	**Thumbprint** (cert_thumbprint)	**Allowed System User** (allowed_system_user)	**Description**
C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com	*	*	Any certificate present in the trust store, issued by the specified Issuer, can be used by any user from the configured user stores. **If backward compatibility is required for an existing deployment, you may use this configuration. However, WSO2 strongly recommends avoiding the use of wildcards in these settings.**
C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com	*	"sample_system_user"	Any certificate in the trust store, issued by the specified Issuer, can be used by the specified user, which may also be a system user.
C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com	78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48:22:91:98:A9:FD:47	"sample_system_user"	Any certificate with a thumbprint included in the allowed list, issued by the specified Issuer, can be used by the specified users. **This configuration is the recommended approach.**
C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com	78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48:22:91:98:A9:FD:47	*	Any certificate with a thumbprint included in the allowed list, issued by the specified Issuer, can be used by any user.

If you use certificate-based client authentication for System REST APIs with the WSO2-Identity-User header

Enable certificate-based authentication for System REST APIs and configure user thumbprint mappings as per the requirements of your use cases.

Sample values are as follows:

- For IS 5.9.0 and above; APIM 3.0.0 and above; OB IAM 2.0.0; OB AM 2.0.0 : `<PRODUCT_HOME>/repository/conf/deployment.toml`

```
[client_certificate_based_authentication]
enable = true

[[client_certificate_based_authentication.user_thumbprint_mapping]]
trusted_issuer = "C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA,
emailAddress=ca@wso2.com"
cert_thumbprint =
"78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48
:22:91:98:A9:FD:47"
allowed_username = ["admin", "user@tenant.com"]
```

- For IS 5.8.0 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`

```
<ClientCertBasedAuthentication enable="true">
    <UserThumbprintMappings>
        <Mapping>
            <TrustedIssuer>C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM,
CN=RootCA, emailAddress=ca@wso2.com</TrustedIssuer>

<CertThumbprint>78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3
:77:41:1B:6D:48:22:91:98:A9:FD:47</CertThumbprint>
            <AllowedUsername>admin</AllowedUsername>
            <AllowedUsername>user@tenant.com</AllowedUsername>
        </Mapping>
    </UserThumbprintMappings>
</ClientCertBasedAuthentication>
```

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

Configuration	Example value(s)	Description
`[client_certificate_based_authentication] enable`	`true`	Use this configuration to enable mTLS-based Authentication for System REST APIs. **If you are using mTLS-based authentication for System REST APIs, this is a mandatory configuration after applying this update.**
`trusted_issuer`	`"C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com "`	Specifies the distinguished name (DN) of the certificate issuer that is permitted. Certificates issued by other authorities will be rejected. You can retrieve the issuer name by running the following command: `openssl x509 -in <your-crt> -noout -issuer -nameopt dn_rev` **This is a mandatory configuration after applying this update.**
`cert_thumbprint`	`"78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48:22:91:98:A9:FD:47"`	Exact fingerprint of the client certificate. You can retrieve the fingerprint by running the following command: `openssl x509 -in <your-cert> -noout -fingerprint -sha256` **This is a mandatory configuration after applying this update.** If the requirement is to allow any thumbprints issued by the trusted issuer, please ensure the value is "*"

Configuration	Example value(s)	Description
`allowed_username`	`["admin", "user@tenant.com"]`	The user(s) mapped to this certificate for login **This is a mandatory configuration after applying this update.** If the requirement is to allow any users who are accessing with a certificate issued by a trusted issuer and having the same thumbprint, please ensure the value is "`[*]`"

The following table outlines the different combinations of configurations and description about the applied scenario in each case.

Trusted Issuer (`trusted_issuer`)	**Thumbprint** (`cert_thumbprint`)	**Allowed Username** (`allowed_username`)	Description
`C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com`	*	`[*]`	Any certificate that is available in the trust store can be used by any user within the user stores. **If backward compatibility is required for an existing deployment, you may use this configuration. However, WSO2 strongly recommends avoiding the use of wildcards in these settings.**
`C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com`	*	`["admin", "user@tenant.com"]`	Any certificate that is available in the trust store can be used by the specified users.
`C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com`	`"78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48:22:91:98:A9:FD:47"`	`["admin", "user@tenant.com"]`	Any certificate with a thumbprint included in the allowed list can be used by the specified users. **This is the recommended configuration pattern.**

Trusted Issuer (trusted_issuer)	**Thumbprint** (cert_thumbprint)	**Allowed Username** (allowed_username)	**Description**
C=AU, ST=Northern, L=Colombo, O=WSO2, OU=IAM, CN=RootCA, emailAddress=ca@wso2.com	"78:9B:25:49:5A:A6:DA:74:9C:F7:A8:90:CE:B9:21:EA:EC:C7:22:2A:B3:77:41:1B:6D:48:22:91:98:A9:FD:47"	[*]	Any certificate with a thumbprint included in the allowed list can be used by any user.

Securing System REST APIs for internal usage

Some features use mTLS internally, and in order to continue to function properly, you need to add a system user thumbprint mappings using the public key that is used in the WSO2 Product.

User thumbprint mapping requires Issuer DN & thumbprint. You may use the commands to extract this information from the public certificate of the private key configured in the keystore pointed in the WSO2 product.

- You can retrieve the issuer name of the public certificate by running the following command:

```
openssl x509 -in <wso2_internal_certificate> -noout -issuer -nameopt
dn_rev
```

- You can retrieve the thumbprint of the public certificate by running the following command:

```
openssl x509 -in <wso2_internal_certificate> -noout -fingerprint -sha256
```

For the following versions:

- WSO2 Identity Server 5.9.0, 5.10.0, 5.11.0
- WSO2 Identity Server Key Manager 5.9.0, 5.10.0
- WSO2 Open Banking IAM 2.0.0

1. If not already enabled, enable certificate-based authentication for System REST APIs by adding the following config to `<PRODUCT_HOME>/repository/conf/deployment.toml`

```
[client_certificate_based_authentication]
enable = true
```

2. Then add a user thumbprint mapping using the extracted data above.

```
[[client_certificate_based_authentication.system_thumbprint_mapping]]
trusted_issuer = <DN_of_WSO2_internal_certificate>
cert_thumbprint = "<Thumbprint_of_WSO2_internal_certificate>"
allowed_system_user = "*"
```

For the following versions:

- WSO2 Identity Server 5.7.0
- WSO2 Identity Server Key Manager 5.7.0
- WSO2 Open Banking Key Manager 1.4.0, 1.5.0

Enable certificate-based authentication for System REST APIs by adding the following config to `<PRODUCT_HOME>/repository/conf/identity/identity.xml`

```
<ClientCertBasedAuthentication enable="true">
    <SystemThumbprintMappings>
        <Mapping>

<TrustedIssuer>{DN_of_wso2_internal_certificate}</TrustedIssuer>

<CertThumbprint>{Thumbprint_of_WSO2_internal_certificate}</CertThumbprin
t>
            <AllowedSystemUser>*</AllowedSystemUser>
        </Mapping>
        <Mapping>
            ...
        </Mapping>
    </SystemThumbprintMappings>
</ClientCertBasedAuthentication>
```