FAQ

- **Common**
  - Are WSO2 products able to integrate with external entities and provide security management services to them?
  - Do WSO2 products support cross-domain federated identity management functionality to authenticate and authorize individuals of internal and external entities into the system, determine their permissions, and control access to the resources accordingly?
  - Do WSO2 products support different user access technologies such as user credentials, biometrics, smart card, token, etc?
  - Do WSO2 products provide encryption and data integrity functionality (symmetric & asymmetric signatures) to maintain secure messaging across the platform and support various encryption and signature standards?
  - Does WSO2 Identity Server help your journey with GDPR and digital transformation?
  - Does WSO2 Identity Server support security standards and protocols such as WS-Trust, WS-Federation, WS-Policy, etc?
  - Error initializing Cipher when using a custom Key Store for Secure Vault: If you try with a custom keystore, you might encounter the following error for certain instances:
  - Do WSO2 products provide encryption and data integrity functionality to maintain secure messaging across the platform?
  - Can we store user identity, user attributes as well as Trust Level (TL) and Consent level (CL) as user data stored in the data repositories?
  - What provisioning standards does WSO2 support?
  - How can I setup WSO2 IS as a KDC?
  - How can I change the host-name of the Identity Server?
  - How to install a new feature in WSO2 Identity Server?
  - What are all the non-apache 2 licensed software in IS, if any?
  - Does the WSO2 platform provide support for mobile phone access?
  - Do we have a way to support off-line process to support off-line verification/validation of user identities?
  - Do we have SPML (Service Provisioning Markup Language) XML-based standard in the WSO2 platform?
  - How easy is it to use carbon administration console and a security monitoring tool for security based administration?
  - How can I access the XDAS audit information of the WSO2 Identity Server?
  - Why do I get the javax.net.ssl.SSLHandshakeException when running the samples?
  - Why do I get an org.apache.jasper.JasperException Java error when I am trying to access a web app?

- **SAML and SSO Support**
  - Do we support Enterprise Single Sign On (E-SSO) to enable internal desktop users to seamlessly access heterogeneous applications (including web applications)?
  - Do WSO2 products provide single-sign-on (SSO) and identity assertion features for services, applications, portal, etc across the SDP?
  - Does WSO2 Identity Server support SAML security token standard and a framework for exchanging security information?
  - Do WSO2 products provide single-sign-on (SSO) and identity assertion features for services, applications, portal, etc across the SDP?
  - What is the difference between SP-Initiated SSO and IDP-Initiated SSO? Do WSO2 products support both scenarios?
  - What are differences between SAML2 and PassiveSTS based authentication?

- **STS**
  - Do WSO2 products provide authentication services to authenticate client access to various services across platforms by supporting security tokens and STS?
  - Is it possible to have STS exposed to the external world for external clients?
  - Does a client need to make a call for each and every request to get the token from STS server, or could it be session based?

- **XACML**
  - How can I write a custom PIP extension for WSO2 IS XACML engine?
Do you support hierarchical roles in Carbon based products?
Do WSO2 products provide complex user entitlement support with XACML?
Do WSO2 products provide policy based authorization services?
Do WSO2 products provide fine grained authorization services to determine access rights for users and user groups?

Common

Are WSO2 products able to integrate with external entities and provide security management services to them?

External entities are incorporated in the following scenarios:

- Authentication - STS that issues SAML tokens + can accept SAML tokens
- OpenID Connect Provider + Relying party
- SSO IDP + relying party
- Authorization - XACML

Do WSO2 products support cross-domain federated identity management functionality to authenticate and authorize individuals of internal and external entities into the system, determine their permissions, and control access to the resources accordingly?

This can be achieved with WS-Trust (e.g., a service in WSO2 EI can be protected with a security policy to accept a security token issued by a trusted STS confirming the authentication of a user in a outside domain), XACML - PDP, PAP and PIP supported by WSO2 Identity Server. PEPs can communicate with the PDP of WSO2 Identity Server to grant authorization.

Do WSO2 products support different user access technologies such as user credentials, biometrics, smart card, token, etc?

User credentials and SAML tokens X.509 tokens are supported out of the box. Biometrics and smart card can be integrated via the custom authenticators available in the WSO2 Identity Server.

Do WSO2 products provide encryption and data integrity functionality (symmetric & asymmetric signatures) to maintain secure messaging across the platform and support various encryption and signature standards?

For Encryption/Decryption, Symmetric/Asymmetric key based encryption/decryption algorithms that are recommended in the WS-Security specification are being used.

For Digital Signature, the Identity module supports Symmetric/Asymmetric key based digital signature algorithms recommended in the WS-Security specification.

Does WSO2 Identity Server help your journey with GDPR and digital transformation?

WSO2 Identity and Access Management (IAM) helps address the new requirements of GDPR by providing customer data privacy, a self care portal to enable customer rights defined in the GDPR and full scale consent life-cycle management. The WSO2 IAM solution also supports secure identity provisioning across systems.
Does WSO2 Identity Server support security standards and protocols such as WS-Trust, WS-Federation, WS-Policy, etc?
Yes. Throughout the WSO2 product stack, WS-Trust, WS-Policy and a few other WS-* standards are supported. We currently do not have complete support for WS-Federation (only the Passive profile is supported).

Error initializing Cipher when using a custom Key Store for Secure Vault: If you try with a custom keystore, you might encounter the following error for certain instances:

```
Exception in thread "main" org.wso2.ciphertool.CipherToolException: Error initializing Cipher at
org.wso2.ciphertool.CipherTool.handleException(CipherTool.java:861) at
org.wso2.ciphertool.CipherTool.initCipher(CipherTool.java:202) at
org.wso2.ciphertool.CipherTool.main(CipherTool.java:80) Caused by:
java.security.InvalidKeyException: Wrong key usage at
javax.crypto.Cipher.init(DashoA13..) at
javax.crypto.Cipher.init(DashoA13..) at
org.wso2.ciphertool.CipherTool.initCipher(CipherTool.java:200) ...
```

You can analyze the public certificates of the two jks's - In default wso2carbon.jks, the KeyUsage is KeyUsage [DigitalSignature Non_repudiation Key_Encipherment Data_Encipherment] - In the custom.jks, the KeyUsage is KeyUsage [DigitalSignature Key_Encipherment] Since the custom key store's certificate does not have 'Data_Encipherment' it can't use the Ciphertool and encrypt data for secure vault. So you may have to generate a new key store with at least a Self signed certificate.

Do WSO2 products provide encryption and data integrity functionality to maintain secure messaging across the platform?
For Encryption/Decryption, Symmetric/Asymmetric key based encryption/decryption algorithms that are recommended in the WS-Security specification are being used.
For Digital Signature, the Identity module supports Symmetric/Asymmetric key based digital signature algorithms recommended in the WS-Security specification.

Can we store user identity, user attributes as well as Trust Level (TL) and Consent level (CL) as user data stored in the data repositories?
A user store includes the user identity and user attributes. TL and CL are not stored directly. But role/user are stored there. Role permission model is hierarchical (permissions are inherited from parent and/or grandparent(s) unless it has been overridden at the child-level). With this permission model, the permissions can be given either to a specific user or a user role (a user role may have multiple users in it).

What provisioning standards does WSO2 support?
SPML was there for more than a decade but never became a main stream provisioning standard - mostly because this is very much biased to SOAP.
SPML (now at version 2.0) was originally developed for the enterprise provisioning market. While many Identity
Management vendors support sending and accepting SPML requests, few vendors of the target systems support SPML as their “API” for provisioning. As a result, most integrations from IAM vendors still use the API provided by the vendor (and those APIs vary greatly from vendor to vendor).

SCIM is a relatively new standard put forward by Ping Identity, Google, and Salesforce.

The SCIM specification is designed to make managing user identity in cloud-based applications and services easier. The specification suite seeks to build upon experience with existing schemas and deployments, placing specific emphasis on simplicity of development and integration, while applying existing authentication, authorization, and privacy models.

Coming from the lessons of SPML, the first S of SCIM is important: It’s designed to be simple. SCIM doesn’t try to cover every provisioning situation; rather, it just covers the most common use cases and as a result is much simpler than SPML. It can handle creation, update, and deletion of users and groups; search; XML and JSON representations; and SAML binding for just-in-time provisioning.

SCIM has a common user schema, so name-value pairs (e.g., first name, last name, email address) mean the same thing regardless of which SaaS vendor you’re provisioning to, and this schema can be extended if necessary to handle specific identity or service-provider requirements. It uses a RESTful API, which makes it easier to integrate into existing cloud services. And SCIM has been designed to be fast for the service provider to implement.

Unlike with SPML, the industry itself has been developing this specification based on practical experience. Salesforc e.com, Cisco, Google, Ping Identity, Technology Nexus, and UnboundID, among others, are committed to its success.

WSO2 supports SCIM specification with its Charon implementation.

For more information, see:
- The following blog posts for details on WSO2 Charon.
- SCIM Simplifies Cloud Service Identity Provisioning
- Move over SPML, Hello SCIM

How can I setup WSO2 IS as a KDC?

See Kerberos Security and follow the instructions.

How can I change the host-name of the Identity Server ?

Follow the instruction given in Deployment Guidelines in Production#Changingthehostname document.

How to install a new feature in WSO2 Identity Server ?

Follow the instructions given in Installing Features document.

What are all the non-apache 2 licensed software in IS, if any ?

Non-apache2 licenses used in IS are listed below. The licensing information can be found using the CARBON_HOME/LICENSE.txt file.

- lgpl3 [GNU LESSER GENERAL PUBLIC LICENSE Version 3]
- cpl1 [Common Public License 1.0]
- epl1 [Eclipse Public License]
- lgpl2 [Lesser GPL v2.1]
- icu [ICU License]
- sunbinary [Binary Code License Agreement]
- mit [MIT License]
- bsd [Berkeley License]
- cddl1 [Common Development and Distribution License]
Does the WSO2 platform provide support for mobile phone access?

In the mobile phone access scenarios lightweight authentication mechanisms such as sending REST like tokens from OAuth and using Mutual SSL can be considered.

Do we have a way to support off-line process to support off-line verification / validation of user identities?

No current support is available for this feature.

Do we have SPML (Service Provisioning Markup Language) XML-based standard in the WSO2 platform?

The WSO2 platform supports both SPML and SCIM (Simple Cloud Identity Management) specifications.

How easy is it to use carbon administration console and a security monitoring tool for security based administration?

The WSO2 Identity Server packages an UI based PAP component for XACML and a collection of relying party components in an easy to use, rich UI based and intuitive management console. Any security configuration can be done and the applied security policies and other viewing capabilities can be handled via this GUI based admin console.

How can I write my own custom authenticator?

Writing a Custom Local Authenticator describes how to write an authenticator, including a sample custom authenticator.

How can I access the XDAS audit information of the WSO2 Identity Server?

The audit logs of IS can be found at $IS_ROOT/repository/logs/audit.log.

Why do I get the `javax.net.ssl.SSLHandshakeException` when running the samples?

The sample applications do not have a keystore in them. Therefore, after changing the tomcat hostname you might get the error given below because the public key of the WSO2 Identity Server does not exist in the Java certificate store.

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
```

Follow the steps given below to avoid this error.

1. Generate a public key from the WSO2 carbon keystore.
   Navigate to the `<IS_HOME>epositoryesources\security` directory via your terminal and run the command given below to export the public certificate.
2. You are prompted to enter the password. The default password is `wso2carbon`. Once the command is executed you see the newly created `PubCert.cer` file in this folder.

3. Navigate to the `<JAVA_HOME>/jre/lib/security` directory via the terminal and run the following command to get the number of certificates that are currently in the certificate store.

   ```
   keytool -list -keystore cacerts
   ```

4. You are prompted to enter a password. The default password is `changeit`. Scroll up on your terminal to see the list of certificates in the store.

5. Import the WSO2 public certificate to the Java certificate store by running the command that is given below. If you are a Windows users, make sure to run the commands as an administrator.

   ```
   keytool -import -keystore cacerts -file <Certificate Path>\wso2PubCert.cer
   ```

6. You are prompted to enter a password. The default password is `changeit`. Once the command is successfully executed, you get the confirmation that the certificate is successfully imported.

   ```
   keytool -list -keystore cacerts
   ```

7. Restart your machine after the above changes.

   Now you are able to use the WSO2 IS samples.

   **Why do I get an `org.apache.jasper.JasperException` Java error when I am trying to access a web app:**

   Are you are getting the error that is given below?

   Example:
{org.apache.catalina.core.StandardContext} - Servlet
[confirmregistration.do] in web application [/accountrecoveryendpoint] threw load() exception
org.apache.jasper.JasperException: Unable to compile class for JSP:

An error occurred at line: 56 in the jsp file:
/self-registration-with-verification-confirm.jsp
'<>' operator is not allowed for source level below 1.7
53:     try {
54:         SelfRegisterApi selfRegisterApi = new SelfRegisterApi();
55:         CodeValidationRequest validationRequest = new
CodeValidationRequest();
56:         List<Property> properties = new ArrayList<>();
57:         Property tenantDomainProperty = new Property();
58:         tenantDomainProperty.setKey(MultitenantConstants.TENANT_DOMAIN);
59:         tenantDomainProperty.setValue(tenantdomain);

Follow the steps given below to overcome the error:

1. Open the <IS_HOME>/repository/conf/tomcat/web.xml file.
2. Add the following properties below the <servlet-class>org.apache.jasper.servlet.JspServlet</servlet-class> property.

```xml
<init-param>
  <param-name>compilerSourceVM</param-name>
  <param-value>1.8</param-value>
</init-param>
<init-param>
  <param-name>compilerTargetVM</param-name>
  <param-value>1.8</param-value>
</init-param>
```

Click here to see the servlet XML property block after you added the above properties.
SAML and SSO Support

Do we support Enterprise Single Sign On (E-SSO) to enable internal desktop users to seamlessly access heterogeneous applications (including web applications)?

This not supported out of the box. But there are several extension points that can be implemented to support such capabilities.

Do WSO2 products provide single-sign-on (SSO) and identity assertion features for services, applications, portal, etc across the SDP?

WSO2 Identity Server supports SAML and SAML 2.0 web browser single sign-on profile. With this feature, WSO2 Identity Server can act as the Identity Provider in single sign-on scenarios while third party service providers can delegate user authentication to Identity Server. Also this SSO feature is supported for our entire product stack with the above mentioned security standards.

Does WSO2 Identity Server support SAML security token standard and a framework for exchanging security information?

WSO2 Identity Server supports SAML 1.0/1.1 and SAML 2.0. SAML token can be used to exchange security information using WS-trust scenarios.

When dealing with Credential Mapping it is possible to map different credentials such as User name Token, X.509 tokens, SAML tokens, Kerberos tokens, etc.

Do WSO2 products provide single-sign-on (SSO) and identity assertion features for services,
WSO2 Identity Server supports SAML and SAML 2.0 web browser single sign-on profile. With this feature, WSO2 Identity Server can act as the Identity Provider in single sign-on scenarios while third party service providers can delegate user authentication to Identity Server. Also this SSO feature is supported for our entire product stack with the above mentioned security standards.

WSO2 Identity Server supports centralized and policy based access control mechanism based on XACML. Authentication mechanism, such as username token, X.509 SAML, OAuth and kerberos can be easily plugged with the XACML access control engine.

What is the difference between SP-Initiated SSO and IDP-Initiated SSO? Do WSO2 products support both scenarios?

In SP-Initiated SSO, user tries to access a resource on SP without logging in. The service provider initiates the SSO message flow by sending authentication request to the Identity Provider (IdP).

But in IdP-Initiated flow, user loges on to IdP first and then tries to access the resource on SP. So IdP initiate the flow by sending an authentication response to the SP directly.

What are differences between SAML2 and PassiveSTS based authentication?

SAML2 enables a SSO system where users can login to multiple applications within a "trust domain". Identities of the users in the "trust domain" are managed by the identity provider/s withing the same "trust domain". So only the users whose identities are managed within the same "trust domain" can access applications withing the "trust domain".

But PassiveSTS is a cross domain authentication mechanism where users in one "trust domain" can access applications in another "trust domain". The mechanism of brokering trust between "trust domain"s is defined in the WS-Federation specification. PassiveSTS is defined under the topic "Web (Passive) Requesters" of the specification.

STS

Do WSO2 products provide authentication services to authenticate client access to various services across platforms by supporting security tokens and STS?

STS is shipped with WSO2 Identity Server. Services can be protected with a security policy to accept a token issued by STS.

Is it possible to have STS exposed to the external world for external clients?

It is possible for external users (who reside outside the domain where STS is setup) to connect to the STS and get a security token. However, in order to do so, the user store which is associated with the STS, should have these external users' data (credentials etc.) stored in there.

Does a client need to make a call for each and every request to get the token from STS server, or could it be session based?
This can be configured at the client’s end according to your requirement. For example, if the user needs to keep the token alive for the whole session, you can set up an expiry time for the token. Then the end service (ESB here) successfully authenticates this token until the specified expiration time limit is exceeded.

**XACML**

**How can I write a custom PIP extension for WSO2 IS XACML engine?**

See [Writing a Custom Policy Info Point](#).

**Do you support hierarchical roles in Carbon based products?**

Carbon products do not support hierarchical roles out of the box, but with the support of WSO2 XACML engine (feature of Identity server), we can define set of policies to cater the requirement.

**Do WSO2 products provide complex user entitlement support with XACML?**

WSO2 products support authorization through entitlement policies defined in XACML. In XACML, complex user entitlement can be defined.

**Do WSO2 products provide policy based authorization services?**

WSO2 products support centralized, policy-based authorization through entitlement policies defined in XACML.

**Do WSO2 products provide fine grained authorization services to determine access rights for users and user groups?**

To support authorization requirements, we support RBAC (Role Based Access Control) and XACML. XACML is specifically used to define fine-grained authorization policies that help align your business level security requirements with the security implementation.