5.0.0 to 5.1.0

Tip: Scroll left/right to view the entire table below.

IS 5.0.0 to 5.1.0 | IS 5.1.0 to 5.2.0

MultiExcerpt named '**configs**' was not found

The page: **Upgrading WSO2 Identity Server** was found, but the multiexcerpt named '**configs**' was not found. Please check/update the page name used in the 'multiexcerpt-include macro.

API changes: Click here to view the steps..

MultiExcerpt named '**apis**' was not found

The page: **Upgrading WSO2 Identity Server** was found, but the multiexcerpt named '**apis**' was not found. Please check/update the page name used in the 'multiexcerpt-include macro.

Recommended: See the WSO2 IS 5.1.0 migration guide for more information.

Note that the following files located in the `<IS_HOME>/repository/conf/` folder in 5.0.0 have been moved to the `<IS_HOME>/repository/conf/identity/` folder in 5.1.0 onwards:

- `provisioning-config.xml`
- `identity.xml`
- `/security/identity-mgt.properties`

5.1.0 to 5.2.0

Tip: Scroll left/right to view the entire table below.

IS 5.0.0 to 5.1.0 | IS 5.1.0 to 5.2.0

Behavioral changes: Click here to view

Due to a fix done in this release, the effective default value of the system property `org.apache.xml.security.ignoreLineBreaks` has been changed from “true” to “false”. Due to this change, you will observe line breaks in SAML responses.

However, if the SAML response consuming client applications have used a standard library such as OpenSAML and use canonicalization when processing the response, this should not cause any problems. Therefore, our recommendation is to use a standard library to process SAML responses on consuming applications.

If you have any concerns about this behavioral change or if the SAML response consuming client applications does not use canonicalization when processing the response and the client cannot be updated to do so, add the following jvm parameter to the server startup script located in the `<IS_HOME>/bin/` folder to revert back to the previous behavior.

```
-Dorg.apache.xml.security.ignoreLineBreaks=true
```

Configuration changes: Click here to view the table..

Recommended: See the WSO2 IS 5.2.0 migration guide for more information.

Note that the following new configuration files have been added from 5.2.0 onwards.

- `repository/conf/event-processor.xml`
- `repository/conf/security/Owasp.CsrfGuard.Carbon.properties`
- `repository/conf/tomcat/carbon/WEB-INF/web.xml`
- `repository/conf/identity/oidc-scope-config.xml`

Configuration File	Changes	
`oidc-scope-config.xml` file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	The following configuration file was added to enable grouping claims that are bound to a scope value in OpenID Connect (OIDC). When requesting for an OIDC token, you can specify a scope value that is bound to a set of claims in the `oidc-scope-config.xml` file. When sending that OIDC token to the userinfo endpoint, only the claims that are common to both the oidc-scope-config and the service provider claim configuration, will be returned.	
identity-mgt.properties file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	The following parameters were added: `# Whether to use hash of username when storing codes.` `# Enable this if Registry is used to store the codes and if username may contain non alphanumeric characters.` `UserInfoRecovery.UseHashedUserNames=false` `UserInfoRecovery.UsernameHashAlg=SHA-1` If you have enabled the using email address as the username option, the confirmation codes are retained after they are used, due to the special character '@' contained in the email address. To resolve this, you can set the `UserInfoRecovery.UseHashedUserNames` parameter to true so that the registry resources will be saved by **hash of**	

	username instead of the email address username which contains the '@' sign.	
	The following properties were added to support notification sending for account enabling and disabling: `Notification.Sending.Enable.Account.Disable=false` `Notification.Sending.Enable.Account.Enable=false` For more information, see User Account Locking and Account Disabling.	
	The following property was added to check if the account has been locked, at the point of authentication. `Authentication.Policy.Check.Account.Disable=false`	
`EndpointConfig.properties` file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	The following properties were replaced: **Old configuration** `identity.server.host=localhost` `identity.server.port=9443` `identity.server.serviceURL=/services/` The properties above were replaced with the following:	

	New configuration `#identity.server.serviceURL=https://localhost:9443/services/`	
entitlement.properties file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	When policy sets are used with entitlements, the default policy set cache size is 100. This may cause frequent cache eviction if there are more than 100 policies in the set. To avoid this, configure the following property. It will cause the cache size to increase depending on the policy set size for better performance. `PDP.References.MaxPolicyEntries=3000`	
`identity.xml` file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	Session data persistence is enabled by default from IS 5.2.0 onwards. `<SessionDataPersist>` `<Enable>true</Enable>` `<Temporary>true</Temporary>` `<PoolSize>0</PoolSize>` `<SessionDataCleanUp>` `<Enable>true</Enable>`	

```
        <CleanUpTimeout>20160</CleanUpTimeout>
        <CleanUpPeriod>1140</CleanUpPeriod>
    </SessionDataCleanUp>
    <OperationDataCleanUp>
        <Enable>true</Enable>
        <CleanUpPeriod>720</CleanUpPeriod>
    </OperationDataCleanUp>
</SessionDataPersist>
```

The following properties were removed:

```
<!--SessionContextCache>
    <Enable>true</Enable>
    <Capacity>100000</Capacity>
</SessionContextCache-->
```

The following property was added to the <SSOService> and <PassiveSTS> elements:

```
<SLOHostNameVerificationEnabled>true</SLOHostNameVerificationEnabled>
```

For more information on configuring hostname verification, see the info note at the bottom of the Configuring WS-Federation page.

Listeners and properties related to analytics in WSO2 Identity Server were added. For more information, see Prerequisites to Publish Statistics.

Listeners

```
<EventListener
type="org.wso2.carbon.identity.core.handler.AbstractIdent
ityMessageHandler"
name="org.wso2.carbon.identity.data.publisher.application
.authentication.impl.DASLoginDataPublisherImpl"
orderId="10" enable="false" />

<EventListener
type="org.wso2.carbon.identity.core.handler.AbstractIdent
ityMessageHandler"
name="org.wso2.carbon.identity.data.publisher.application
.authentication.impl.DASSessionDataPublisherImpl"
orderId="11" enable="false" />

<EventListener
type="org.wso2.carbon.identity.core.handler.AbstractIdent
ityMessageHandler"
name="org.wso2.carbon.identity.data.publisher.application
.authentication.AuthnDataPublisherProxy" orderId="11"
enable="true" />
```

Properties

```
<ISAnalytics>

        <DefaultValues>

            <userName>NOT_AVAILABLE</userName>


<userStoreDomain>NOT_AVAILABLE</userStoreDomain>


<rolesCommaSeperated>NOT_AVAILABLE</rolesCommaSeperated
>


<serviceprovider>NOT_AVAILABLE</serviceprovider>


<identityProvider>NOT_AVAILABLE</identityProvider>

        </DefaultValues>

    </ISAnalytics>
```

The security element was updated:

```
<!-- Security configurations-->

<Security>

    <!-- The directory under which all other KeyStore
files will be stored-->
```

```
<KeyStoresDir>${carbon.home}/conf/keystores</KeyStoresDir
>

    <KeyManagerType>SunX509</KeyManagerType>

    <TrustManagerType>SunX509</TrustManagerType>

</Security>
```

The following elements were added under the <OAuth> element:

Caching Recommendation

It is recommended to keep the OAuth2 local cache and the distributed cache disabled as it may cause out-of-memory issues. However, if you want to enable the OAuth2 local cache, you have to enable the distributed cache as well.

To enable the OAuth2 local cache and distributed cache, set the `<EnableOAuthCache>` property and `isDistributed` to true.

```
<EnableOAuthCache>true</EnableOAuthCache>
<Cache name="OAuthCache" enable="true" timeout="1" capacity="5000" isDistributed="true"/>
```

```
<OIDCCheckSessionEPUrl>${carbon.protocol}://${carbon.h
ost}:${carbon.management.port}/oidc/checksession</OIDC
CheckSessionEPUrl>

<OIDCLogoutEPUrl>${carbon.protocol}://${carbon.host}:$
{carbon.management.port}/oidc/logout</OIDCLogoutEPUrl>

<OIDCConsentPage>${carbon.protocol}://${carbon.host}:$
{carbon.management.port}/authenticationendpoint/oauth2
_consent.do</OIDCConsentPage>
```

```
<OIDCLogoutConsentPage>${carbon.protocol}://${carbon.host}:${carbon.management.port}/authenticationendpoint/oauth2_logout_consent.do</OIDCLogoutConsentPage>

<OIDCLogoutPage>${carbon.protocol}://${carbon.host}:${carbon.management.port}/authenticationendpoint/oauth2_logout.do</OIDCLogoutPage>



<EnableOAuthCache>false</EnableOAuthCache>
```

Caching Recommendation

It is recommended to keep the OAuth2 local cache and the distributed cache disabled as it may cause out-of-memory issues.
However, if you want to enable the OAuth2 local cache, you have to enable the distributed cache as well.

To enable the OAuth2 local cache and distributed cache, set the `<EnableOAuthCache>` property and `isDistributed` to true.

```
<EnableOAuthCache>true</EnableOAuthCache>

<Cache name="OAuthCache" enable="true" timeout="1"
capacity="5000" isDistributed="true"/>
```

The following elements were removed from the <OAuth><OpenIDConnect> element:

```
<IDTokenSubjectClaim>http://wso2.org/claims/givenname</IDTokenSubjectClaim>

<UserInfoEndpointClaimDialect>http://wso2.org/claims</UserInfoEndpointClaimDialect>
```

The following code was updated. To add audiences to the JWT token, use the code block below. For more information, see JWT Token Generation.

```
<OpenIDConnect>

<IDTokenBuilder>org.wso2.carbon.identity.openidconnect.DefaultIDTokenBuilder</IDTokenBuilder>
    <!-- Comment out to add Audience values to the JWT token (id_token)-->
    <!--Audiences>

<Audience>${carbon.protocol}://${carbon.host}:${carbon.management.port}/oauth2/token</Audience>
    </Audiences-->
    <!--Default value for IDTokenIssuerID, is OAuth2TokenEPUrl.If that doesn't satisfy uncomment the following config and explicitly configure the value-->

<IDTokenIssuerID>${carbon.protocol}://${carbon.host}:${carbon.management.port}/oauth2/token</IDTokenIssuerID>

  ...
```

```
</OpenIDConnect>
```

The <CacheConfig> was replaced:

```
<CacheConfig>
    <CacheManager
name="IdentityApplicationManagementCacheManager">
        <Cache name="AppAuthFrameworkSessionContextCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="AuthenticationContextCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="AuthenticationRequestCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="AuthenticationResultCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="AppInfoCache" enable="true"
timeout="1" capacity="5000" isDistributed="false" />
        <Cache name="AuthorizationGrantCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="OAuthCache" enable="false"
timeout="1" capacity="5000" isDistributed="false" />
        <Cache name="OAuthSessionDataCache" enable="false"
timeout="1" capacity="5000" isDistributed="false" />
        <Cache name="SAMLSSOParticipantCache"
enable="false" timeout="1" capacity="5000"
```

```
isDistributed="false" />
        <Cache name="SAMLSSOSessionIndexCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="SAMLSSOSessionDataCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="ServiceProviderCache" enable="true"
timeout="1" capacity="5000" isDistributed="false" />
        <Cache name="ProvisioningConnectorCache"
enable="true" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="ProvisioningEntityCache"
enable="false" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache
name="ServiceProviderProvisioningConnectorCache"
enable="true" timeout="1" capacity="5000"
isDistributed="false" />
        <Cache name="IdPCacheByAuthProperty" enable="true"
timeout="1" capacity="5000" isDistributed="false" />
        <Cache name="IdPCacheByHRI" enable="true"
timeout="1" capacity="5000" isDistributed="false" />
        <Cache name="IdPCacheByName" enable="true"
timeout="1" capacity="5000" isDistributed="false" />
    </CacheManager>
</CacheConfig>
```

• `context.xml` file stored in the `<PRODUCT_HOME>/repository/conf/tomcat/carbon/META-INF/` directory. • `context.xml` file stored in the `<PRODUCT_HOME>/repository/conf/tomcat/` directory. • `web.xml` file	The entire file was replaced.	

stored in the `<PRODUCT_HOME>/repository/conf/tomcat/carbon/WEB-INF/` directory.		

`carbon.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	The following elements were added under the <Security> tag: `<STSCallBackHandlerName>org.wso2.carbon.identity.provider.AttributeCallbackHandler</STSCallBackHandlerName>` `<XSSPreventionConfig>` `<Enabled>true</Enabled>` `<Rule>allow</Rule>` `<Patterns>` `<!--Pattern></Pattern-->` `</Patterns>` `</XSSPreventionConfig>` The following elements were removed:	

```
<!--Configurations to avoid Cross Site Request Forgery
vulnerabilities-->

<CSRFPreventionConfig>

    <!--CSRFPreventionFilter configurations that adopts
Synchronizer Token Pattern-->

    <CSRFPreventionFilter>

    <!-- Set below to true to enable the
CSRFPreventionFilter-->

    <Enabled>false</Enabled>

    <!--Url Pattern to skip application of CSRF
protection-->

    <SkipUrlPattern > (.*)(/images|/css | /js|/docs)(.*)
</SkipUrlPattern>

    </CSRFPreventionFilter>

</CSRFPreventionConfig>



<!-- Configuration to enable or disable CR and LF
sanitization filter-->

<CRLFPreventionConfig>
```

	<!--Set below to true to enable the CRLFPreventionFilter--> <Enabled>true</Enabled> </CRLFPreventionConfig	
`claim-config.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	The following claims were added. For more information on configuring these, see Configuring Users or User Account Locking and Account Disabling depending on the claim you want to configure. <Claim> <ClaimURI>http://wso2.org/claims/identity/lastLoginTime</ClaimURI> <DisplayName>Last Login</DisplayName> <!-- Proper attribute Id in your user store must be configured for this --> <AttributeID>carLicense</AttributeID> <Description>Last Login Time</Description> </Claim> <Claim>	

```
<ClaimURI>http://wso2.org/claims/identity/lastPasswordUpd
ateTime</ClaimURI>

    <DisplayName>Last Password Update</DisplayName>

    <!-- Proper attribute Id in your user store must be
configured for this -->

    <AttributeID>businessCategory</AttributeID>

    <Description>Last Password Update Time</Description>

</Claim>

<Claim>


<ClaimURI>http://wso2.org/claims/identity/accountDisabled
</ClaimURI>

    <DisplayName>Account Disabled</DisplayName>

    <!-- Proper attribute Id in your user store must be
configured for this -->

    <AttributeID>ref</AttributeID>

    <Description>Account Disabled</Description>

</Claim>
```

• `data-agent-config.xml` file stored in the `<PRODUCT_HOME>/repository/conf/data-bridge/` directory. • `event-processor.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	The file was newly added.	
`metrics-datasources.xml` file stored in	Set the `<defaultAutocommit>` property to true.	

the <PRODUCT_HOME>/repository/conf/datasources/ directory.

```
<datasource>
            <name>WSO2_METRICS_DB</name>
            <description>The default datasource used for
WSO2 Carbon Metrics</description>
            <jndiConfig>
                <name>jdbc/WSO2MetricsDB</name>
            </jndiConfig>
            <definition type="RDBMS">
                <configuration>
<url>jdbc:h2:repository/database/WSO2METRICS_DB;DB_CLOSE_
ON_EXIT=FALSE;AUTO_SERVER=TRUE</url>
                    <username>wso2carbon</username>
                    <password>wso2carbon</password>

<driverClassName>org.h2.Driver</driverClassName>
                    <maxActive>50</maxActive>
                    <maxWait>60000</maxWait>
                    <testOnBorrow>true</testOnBorrow>
                    <validationQuery>SELECT
1</validationQuery>

<validationInterval>30000</validationInterval>

<defaultAutoCommit>true</defaultAutoCommit>
                </configuration>
            </definition>
        </datasource>
```

application-authentication.xml file stored in the <PRODUCT_HOME>/repository/conf/id

```
 <AuthenticatorConfig name="EmailOTP" enabled="true">

     <Parameter
 name="GmailClientId">gmailClientIdValue</Parameter>

     <Parameter
```

`entity/` directory.	name="GmailClientSecret">gmailClientSecretValue</Parameter> <Parameter name="SendgridAPIKey">sendgridAPIKeyValue</Parameter> <Parameter name="GmailRefreshToken">gmailRefreshTokenValue</Parameter> <Parameter name="GmailEmailEndpoint">https://www.googleapis.com/gmail/v1/users/[userId]/messages/send</Parameter> <Parameter name="SendgridEmailEndpoint">https://api.sendgrid.com/api/mail.send.json</Parameter> <Parameter name="accessTokenRequiredAPIs">Gmail</Parameter> <Parameter name="apiKeyHeaderRequiredAPIs">Sendgrid</Parameter> <Parameter name="SendgridFormData">sendgridFormDataValue</Parameter> <Parameter name="SendgridURLParams">sendgridURLParamsValue</Parameter> <Parameter name="GmailAuthTokenType">Bearer</Parameter> <Parameter name="GmailTokenEndpoint">https://www.googleapis.com/oauth2/v3/token</Parameter> <Parameter name="SendgridAuthTokenType">Bearer</Parameter>

	`` </AuthenticatorConfig> <AuthenticatorConfig name="x509CertificateAuthenticator" enabled="true"> <Parameter name="AuthenticationEndpoint">https://localhost:8443/x509-certificate-servlet</Parameter> </AuthenticatorConfig> <AuthenticatorConfig name="totp" enabled="true"> <Parameter name="encodingMethod">Base32</Parameter> <Parameter name="timeStepSize">30</Parameter> <Parameter name="windowSize">3</Parameter> <Parameter name="enableTOTP">false</Parameter> </AuthenticatorConfig> ```	
`metrics.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	The following elements were added: ``` <Metrics xmlns="http://wso2.org/projects/carbon/metrics.xml"> <Reporting> <Console> <Enabled>false</Enabled> <!-- Polling Period in seconds. This is the period for polling metrics from the metric registry and printing in the console --> ```	

```
            <PollingPeriod>60</PollingPeriod>
        </Console>

        <DAS>
            <Enabled>false</Enabled>
            <!-- Source of Metrics, which will be used to
                identify each metric sent in the streams
-->
            <!-- Commented to use the hostname
                <Source>Carbon</Source>
            -->
            <!-- Polling Period in seconds.
                This is the period for polling metrics
from the metric registry and
                sending events via the Data Publisher -->
            <PollingPeriod>60</PollingPeriod>
            <!-- The type used with Data Publisher -->
            <Type>thrift</Type>
            <!-- Data Receiver URL used by the Data
Publisher -->

<ReceiverURL>tcp://localhost:7611</ReceiverURL>
            <!-- Authentication URL for the Data Publisher
-->
            <!-- <AuthURL>ssl://localhost:7711</AuthURL>
-->
            <Username>admin</Username>
            <Password>admin</Password>
            <!-- Path for Data Agent Configuration -->

<DataAgentConfigPath>repository/conf/data-bridge/data-age
nt-config.xml</DataAgentConfigPath>
        </DAS>
```

`output-event-adapters.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	The following adapter configurations were added: `<adapterConfig type="http">` `  <!-- Thread Pool Related Properties -->` `  <property key="minThread">8</property>` `  <property key="maxThread">100</property>` `  <property key="keepAliveTimeInMillis">20000</property>` `  <property key="jobQueueSize">10000</property>` `  <!-- HTTP Client Pool Related Properties -->` `  <property key="defaultMaxConnectionsPerHost">50</property>` `  <property key="maxTotalConnections">1000</property>` `</adapterConfig>` `<adapterConfig type="jms">` `  <!-- Thread Pool Related Properties -->` `  <property key="minThread">8</property>` `  <property key="maxThread">100</property>` `  <property key="keepAliveTimeInMillis">20000</property>` `  <property key="jobQueueSize">10000</property>` `</adapterConfig>` `<adapterConfig type="mqtt">` `  <!-- Thread Pool Related Properties -->` `  <property key="minThread">8</property>` `  <property key="maxThread">100</property>` `  <property key="keepAliveTimeInMillis">20000</property>` `  <property key="jobQueueSize">10000</property>` `  <property key="connectionKeepAliveInterval">60</property>` `</adapterConfig>`	

```
<adapterConfig type="kafka">
    <!-- Thread Pool Related Properties -->
    <property key="minThread">8</property>
    <property key="maxThread">100</property>
    <property
key="keepAliveTimeInMillis">20000</property>
    <property key="jobQueueSize">10000</property>
</adapterConfig>

<adapterConfig type="email">
    <!-- Comment mail.smtp.user and mail.smtp.password
properties to support connecting SMTP servers which use
trust
        based authentication rather username/password
authentication -->
    <property
key="mail.smtp.from">abcd@gmail.com</property>
    <property key="mail.smtp.user">abcd</property>
    <property key="mail.smtp.password">xxxx</property>
    <property
key="mail.smtp.host">smtp.gmail.com</property>
    <property key="mail.smtp.port">587</property>
    <property
key="mail.smtp.starttls.enable">true</property>
    <property key="mail.smtp.auth">true</property>
    <!-- Thread Pool Related Properties -->
    <property key="minThread">8</property>
    <property key="maxThread">100</property>
    <property
key="keepAliveTimeInMillis">20000</property>
    <property key="jobQueueSize">10000</property>
</adapterConfig>

<adapterConfig type="ui">
    <property key="eventQueueSize">30</property>
    <!-- Thread Pool Related Properties -->
```

```
    <property key="minThread">8</property>
    <property key="maxThread">100</property>
    <property
key="keepAliveTimeInMillis">20000</property>
    <property key="jobQueueSize">10000</property>
</adapterConfig>

<adapterConfig type="websocket-local">
    <!-- Thread Pool Related Properties -->
    <property key="minThread">8</property>
    <property key="maxThread">100</property>
    <property
key="keepAliveTimeInMillis">20000</property>
    <property key="jobQueueSize">10000</property>
</adapterConfig>

<adapterConfig type="websocket">
    <!-- Thread Pool Related Properties -->
    <property key="minThread">8</property>
    <property key="maxThread">100</property>
    <property
key="keepAliveTimeInMillis">20000</property>
    <property key="jobQueueSize">10000</property>
</adapterConfig>

<adapterConfig type="soap">
    <!-- Thread Pool Related Properties -->
    <property key="minThread">8</property>
    <property key="maxThread">100</property>
    <property
key="keepAliveTimeInMillis">20000</property>
    <property key="jobQueueSize">10000</property>
    <!-- Axis2 Client Connection Related Properties -->
    <property
key="axis2ClientConnectionTimeout">10000</property>
    <property key="reuseHTTPClient">true</property>
```

	<property key="autoReleaseConnection">true</property> <property key="maxConnectionsPerHost">50</property> </adapterConfig>	
registry.xml file stored in the <PRODUCT_HOME>/repository/conf/ directory.	The following elements were added: <indexingConfiguration> <startIndexing>false</startIndexing> <startingDelayInSeconds>35</startingDelayInSeconds> <indexingFrequencyInSeconds>5</indexingFrequencyInSeconds> <!--number of resources submit for given indexing thread --> <batchSize>40</batchSize> <!--number of worker threads for indexing --> <indexerPoolSize>40</indexerPoolSize> <!-- location storing the time the indexing took place--> <lastAccessTimeLocation>/_system/local/repository/components/org.wso2.carbon.registry/indexing/lastaccesstime</lastAccessTimeLocation> <!-- the indexers that implement the indexer interface for a relevant media type/(s) --> <indexers> <indexer class="org.wso2.carbon.registry.indexing.indexer.MSExcelIndexer" mediaTypeRegEx="application/vnd.ms-excel" /> <indexer class="org.wso2.carbon.registry.indexing.indexer.MSPowerpointIndexer" mediaTypeRegEx="application/vnd.ms-powerpoint" /> <indexer	

```
class="org.wso2.carbon.registry.indexing.indexer.MSWordIndexer" mediaTypeRegEx="application/msword" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.PDFIndexer" mediaTypeRegEx="application/pdf" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.XMLIndexer" mediaTypeRegEx="application/xml" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.XMLIndexer" mediaTypeRegEx="application/(.)+\+xml" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.PlainTextIndexer" mediaTypeRegEx="application/swagger\+json" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.PlainTextIndexer" mediaTypeRegEx="application/(.)+\+json" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.PlainTextIndexer" mediaTypeRegEx="text/(.)+" />
        <indexer class="org.wso2.carbon.registry.indexing.indexer.PlainTextIndexer" mediaTypeRegEx="application/x-javascript" />
    </indexers>
    <exclusions>
        <exclusion pathRegEx="/_system/config/repository/dashboards/gadgets/swfobject1-5/.*[.]html" />
        <exclusion pathRegEx="/_system/local/repository/components/org[.]wso2[.]carbon[.]registry/mount/.*" />
    </exclusions>
</indexingConfiguration>
```

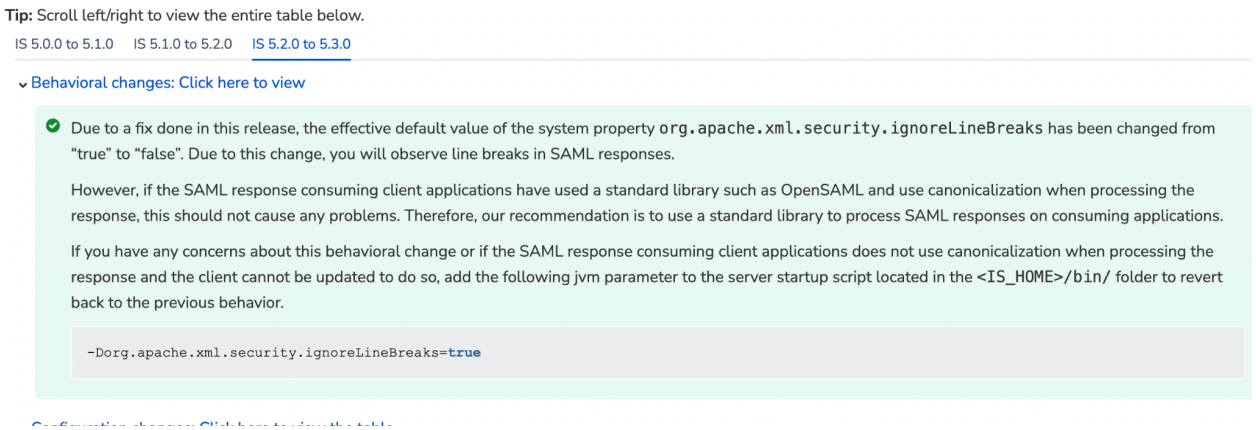
user-mgt.xml file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	The following LDAP/AD property was added: `<Property name="AnonymousBind">false</Property>`	

Recommended: See the WSO2 IS 5.2.0 migration guide for more information.

Note that the following new configuration files have been added from 5.2.0 onwards.

- `repository/conf/event-processor.xml`
- `repository/conf/security/Owasp.CsrfGuard.Carbon.properties`
- `repository/conf/tomcat/carbon/WEB-INF/web.xml`
- `repository/conf/identity/oidc-scope-config.xml`

5.2.0 to 5.3.0



Configuration File	Required	Changes

The `web.xml` file stored in the `<PRODUCT_HOME>/repository/conf/tomcat/carbon/WEB_INF` directory.	Optional	Add the following properties after the `CsrfGuardHttpSessionListener.` `<filter>` `<filter-name>CaptchaFilter</filter-name>` `<filter-class>org.wso2.carbon.identity.captcha.filter.CaptchaFilter</filter-class>` `</filter>` `<filter-mapping>` `<filter-name>CaptchaFilter</filter-name>` `<url-pattern>/samlsso</url-pattern>`

		<url-pattern>/oauth2</url-pattern> <url-pattern>/commonauth</url-pattern> <dispatcher>FORWARD</dispatcher> <dispatcher>REQUEST</dispatcher> </filter-mapping>
The `user-mgt.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	Mandatory	Add the following element under the `<Realm> <Configuration>` tag. <Property name="initializeNewClaimManager">true</Property>

The `Owasp.CsrfGuard.Carbon.properties` stored in the `<PRODUCT_HOME>/repository/conf/security/` directory.	Mandatory	Find the following line. **Old configuration** `org.owasp.csrfguard.unprotected.authiwa=%servletContext%/commonauth/iwa/*` Update the line as follows. **New Configuration** `org.owasp.csrfguard.unprotected.oauthiwa=%servletContext%/commonauth/iwa/*` Add the following property. `org.owasp.csrfguard.unprotected.mex=%servletContext%/mexut/*`

The `output-event-adapters.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	Optional	Add the following properties under the `<outputEventAdaptersConfig>` tag. `<adapterConfig type="wso2event">` `<property key="default.thrift.tcp.url">tcp://localhost:7612</property>` `<property key="default.thrift.ssl.url">ssl://localhost:7712</property>` `<property key="default.binary.tcp.url">tcp://localhost:9612</property>` `<property key="default.binary.ssl.url">ssl://localhost:9712</property>` `</adapterConfig>`
The `log4j.properties` file stored in the `<PRODUCT_HOME>/r`	Optional	Add the following property.

`epository/conf/` directory.		`log4j.logger.org.springframework=WARN`

The `identity.xml` file stored in the `<PRODUCT_HOME>/repository/conf/identity`directory.	Mandatory	Add the following event listeners as child elements under the <EventListeners> tag. `<EventListeners>` `....` `....` `<EventListener` `type="org.wso2.carbon.user.core.listener.UserOperationEventListener"` `name="org.wso2.carbon.identity.governance.listener.IdentityStoreEventListener"` `orderId="97" enable="true">` `<Property name="Data.Store">org.wso2.carbon.identity.governance.store.JDBCIdentityDataStore</Property>` `</EventListener>`

		<EventListener type="org.wso2.carbon.user.core.listener.UserOperationEventListener" name="org.wso2.carbon.identity.governance.listener.IdentityMgtEventListener" orderId="95" enable="true"/> .... </EventListeners> Add the following properties under the <OAuth> tag.

		<OIDCWebFingerEPUrl>${carbon.protocol}://${carbon.host}:${carbon.management.port}/.well-known/webfinger</OIDCWebFingerEPUrl> <!-- For tenants below urls will be modified as https://<hostname>:<port>/t/<tenant domain>/<path>--> <OAuth2DCREPUrl>${carbon.protocol}://${carbon.host}:${carbon.management.port}/identity/connect/register</OAuth2DCREPUrl> <OAuth2JWKSPage>${carbon.protocol}://${carbon.host}:${carbon.management.port}/oauth2/jwks</OAuth2JWKSPage> <OIDCDiscoveryEPUrl>${carbon.protocol}://${carbon.host}:${carbon.management.port}/oauth2/oidcdiscovery</OIDCDiscoveryEPUrl> Add the following property under the <SSOService> tag. <!--<SAMLSSOAssertionBuilder>org.wso2.carbon.identity.sso.saml

		`.builders.assertion.ExtendedDefaultAssertionBuilder</SAMLSSOAssertionBuilder>-->` Add the following properties at the top level. `<!--Recovery>` `<Notification>` `<Password>` `<Enable>false</Enable>` `</Password>` `<Username>` `<Enable>false</Enable>` `</Username>` `<InternallyManage>true</InternallyManage>` `</Notification>` `<Question>` `<Password>` `<Enable>false</Enable>` `<NotifyStart>true</NotifyStart>` `<Separator>!</Separator>` `<MinAnswers>2</MinAnswers>` `<ReCaptcha>`

		<Enable>true</Enable> <MaxFailedAttempts>3</MaxFailed Attempts> </ReCaptcha> </Password> </Question> <ExpiryTime>3</ExpiryTime> <NotifySuccess>true</NotifySucc ess> <AdminPasswordReset> <Offline>false</Offline> <OTP>false</OTP> <RecoveryLink>false</RecoveryLi nk> </AdminPasswordReset> </Recovery> <EmailVerification> <Enable>false</Enable> <LockOnCreation>false</LockOnCr eation> <Notification> <InternallyManage>true</Interna llyManage> </Notification> </EmailVerification> <SelfRegistration> <Enable>false</Enable>

```
<LockOnCreation>false</LockOnCr
eation>
    <Notification>

<InternallyManage>true</Interna
llyManage>
    </Notification>

<ReCaptcha>false</ReCaptcha>
    </SelfRegistration-->
```

Remove the following section:

```
<ISAnalytics>

        <DefaultValues>


<userName>NOT_AVAILABLE</userNa
me>


<userStoreDomain>NOT_AVAILABLE<
/userStoreDomain>


<rolesCommaSeperated>NOT_AVAILA
BLE</rolesCommaSeperated>
```

		`<serviceprovider>NOT_AVAILABLE</serviceprovider>` `<identityProvider>NOT_AVAILABLE</identityProvider>` `</DefaultValues>` `</ISAnalytics>` Add the following properties to the top level. `<ResourceAccessControl>` `<Resource context="(.*)/api/identity/user/(.*)" secured="true" http-method="all"/>` `<Resource context="(.*)/api/identity/recovery/(.*)" secured="true" http-method="all"/>` `<Resource context="(.*)/.well-known(.*)" secured="true" http-method="all"/>` `<Resource context="(.*)/identity/register(.*)" secured="true" http-method="all">` `<Permissions>/permission/admin/`

```
manage/identity/applicationmgt/
delete</Permissions>
        </Resource>
        <Resource
context="(.*)/identity/connect/
register(.*)" secured="true"
http-method="all">

<Permissions>/permission/admin/
manage/identity/applicationmgt/
create</Permissions>
        </Resource>
        <Resource
context="(.*)/oauth2/introspect
(.*)" secured="true"
http-method="all">

<Permissions>/permission/admin/
manage/identity/applicationmgt/
view</Permissions>
        </Resource>
        <Resource
context="(.*)/api/identity/enti
tlement/(.*)" secured="true"
http-method="all">

<Permissions>/permission/admin/
manage/identity/pep</Permission
s>
        </Resource>
    </ResourceAccessControl>

    <ClientAppAuthentication>
        <Application
name="dashboard"
hash="66cd9688a2ae068244ea01e70
```

		f0e230f5623b7fa4cdecb65070a09ec06452262"/> </ClientAppAuthentication> <TenantContextsToRewrite> <WebApp> <Context>/api/identity/user/v0.9</Context> <Context>/api/identity/recovery/v0.9</Context> <Context>/oauth2</Context> <Context>/api/identity/entitlement</Context> </WebApp> <Servlet> <Context>/identity/(.*)</Context> </Servlet> </TenantContextsToRewrite>

The `entitlement.properties` file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	Optional	If you are using the service provider authorization feature, add the following property to the config file. If you have any other `AttributeDesignators` configured with the number 2, use the smallest unused number instead of 2 when adding the property below. `PIP.AttributeDesignators.Designator.2=org.wso2.carbon.identity.application.authz.xacml.pip.AuthenticationContextAttributePIP`

The `email-admin-config.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	Mandatory	If you have **not** made any custom changes to this file in your previous version of WSO2 IS: • Copy the `<NEW_IS_HOME>/repository/conf/email/email-admin-config.xml` file and replace the existing one. If you **have** made custom changes to this file in your previous version: a. Locate the templates you have updated that differ from the default config file. You can use a diff tool to compare your `<OLD_IS_HOME>/repository/conf/email/email-admin-config.xml` file with the default file to identify the custom changes you have made. Note these changes/updates. b. Copy the file from `<NEW_IS_HOME>/repository/conf/em`

		`ail/email-admin-config.xml` to `<OLD_IS_HOME>/repository/conf/email/` directory and rename it to email-"admin-config-new.xml". c. For each template you have modified, do the following: d. **Note:** If you opt to migrate to the new identity management implementation, follow all the steps below. If you wish to continue with the old identity management implementation, skip steps iii and iv. i. Locate the relevant template configuration in the old `email-admin-config-new.xml` file by searching for '<configuration type="xxxxx" where "xxxxx"

		is the type at `email-admin-config.xml`. ii. Update the subject, body, and footer in the new config file with the values from the existing configuration. iii. **`[OPTIONAL]`** Update the placeholders so that they are enclosed with double braces (E.g., `{user-name} -> {{user-name}} )` iv. **`[OPTIONAL]`** Update the user's attribute related placeholders to follow the `{{user.claim.yyyy}}` format where `yyyy` is the attribute name

		(E.g., `{first-name} -> {{user.claim.givenname}}`) Delete the `<OLD_IS_HOME>/repository/conf/email/email-admin-config.xml` file and rename the `email-admin-config-new.xml` file to "email-admin-config.xml" to finish the update. For more information about this feature, see Email Templates.
The `data-agent-config.xml` filestored in the `<NEW_IS_HOME>/repository/conf/data-bridge` directory.	Mandatory	Add the following properties under the `<Agent>` `ThriftDataEndpoint` and under the `<Agent>BinaryDataEndpoint` tags.

		<!--<sslEnabledProtocols>TLSv1,TLSv1.1,TLSv1.2</sslEnabledProtocols>--> <!--<ciphers>SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES _128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,SSL _RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_ 3DES_EDE_CBC_SHA</ciphers>-->

The `claim-config.xml` file stored in the `<NEW_IS_HOME>/repository/conf/` directory	Mandatory	Replace the following attribute found under the `<Claim>` `<ClaimURI>`http://wso2.org/claims/locality> tag. Replace this attribute: <AttributeID>localityName</AttributeID> with this: <AttributeID>local</AttributeID> Modify the following claims as follows. <Claim> <ClaimURI>http://wso2.org/claims/userid</ClaimURI> <DisplayName>User ID</DisplayName> <AttributeID>scimId</AttributeID> <Description>Unique ID of the

```
user</Description>
  <ReadOnly/>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/externalid</ClaimURI>
  <DisplayName>External User ID</DisplayName>

<AttributeID>externalId</AttributeID>
  <Description>Unique ID of the user used in external systems</Description>
  <ReadOnly/>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/created</ClaimURI>
  <DisplayName>Created Time</DisplayName>

<AttributeID>createdDate</AttributeID>
  <Description>Created timestamp of the user</Description>
  <ReadOnly/>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/modified</ClaimURI>
  <DisplayName>Last Modified Time</DisplayName>
```

```
<AttributeID>lastModifiedDate</
AttributeID>
  <Description>Last Modified
timestamp of the
user</Description>
  <ReadOnly/>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/location</ClaimURI>

<DisplayName>Location</DisplayN
ame>

<AttributeID>location</Attribut
eID>

<Description>Location</Descript
ion>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/formattedName</ClaimURI>
  <DisplayName>Name - Formatted
Name</DisplayName>

<AttributeID>formattedName</Att
ributeID>
  <Description>Formatted
Name</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
```

```
s/middleName</ClaimURI>
  <DisplayName>Middle
Name</DisplayName>

<AttributeID>middleName</Attrib
uteID>
  <Description>Middle
Name</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/honorificPrefix</ClaimURI>
  <DisplayName>Name - Honoric
Prefix</DisplayName>

<AttributeID>honoricPrefix</Att
ributeID>
  <Description>Honoric
Prefix</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/honorificSuffix</ClaimURI>
  <DisplayName>Name - Honoric
Suffix</DisplayName>

<AttributeID>honoricSuffix</Att
ributeID>
  <Description>Honoric
Suffix</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/userType</ClaimURI>
```

```
  <DisplayName>User
Type</DisplayName>

<AttributeID>userType</Attribut
eID>
  <Description>User
Type</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/preferredLanguage</ClaimURI>
  <DisplayName>Preferred
Language</DisplayName>

<AttributeID>preferredLanguage<
/AttributeID>
  <Description>Preferred
Language</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/local</ClaimURI>

<DisplayName>Local</DisplayName
>

<AttributeID>local</AttributeID
>

<Description>Local</Description
>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
```

```
s/timeZone</ClaimURI>
  <DisplayName>Time
Zone</DisplayName>

<AttributeID>timeZone</Attribut
eID>
  <Description>Time
Zone</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/emails.work</ClaimURI>
  <DisplayName>Emails - Work
Email</DisplayName>

<AttributeID>workEmail</Attribu
teID>
  <Description>Work
Email</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/emails.home</ClaimURI>
  <DisplayName>Emails - Home
Email</DisplayName>

<AttributeID>homeEmail</Attribu
teID>
  <Description>Home
Email</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/emails.other</ClaimURI>
```

```
  <DisplayName>Emails - Other
Email</DisplayName>

<AttributeID>otherEmail</Attrib
uteID>
  <Description>Other
Email</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/phoneNumbers</ClaimURI>
  <DisplayName>Phone
Numbers</DisplayName>

<AttributeID>phoneNumbers</Attr
ibuteID>
  <Description>Phone
Numbers</Description>

<RegEx>^([a-zA-Z0-9_\.\-])+\@((
[a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]
{2,4})+$</RegEx>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/phoneNumbers.home</ClaimURI>
  <DisplayName>Phone Numbers -
Home Phone Number</DisplayName>

<AttributeID>homePhone</Attribu
teID>
  <Description>Home
Phone</Description>
</Claim>
<Claim>
```

```
<ClaimURI>http://wso2.org/claims/phoneNumbers.work</ClaimURI>
  <DisplayName>Phone Numbers - Work Phone Number</DisplayName>

<AttributeID>workPhone</AttributeID>
  <Description>Work Phone</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/phoneNumbers.fax</ClaimURI>
  <DisplayName>Phone Numbers - Fax Number</DisplayName>

<AttributeID>fax</AttributeID>
  <Description>Fax Number</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/phoneNumbers.pager</ClaimURI>
  <DisplayName>Phone Numbers - Pager Number</DisplayName>

<AttributeID>pager</AttributeID>
  <Description>Pager Number</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
```

```
s/phoneNumbers.other</ClaimURI>
  <DisplayName>Phone Numbers -
Other</DisplayName>

<AttributeID>otherPhoneNumber</
AttributeID>
  <Description>Other Phone
Number</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/gtalk</ClaimURI>
  <DisplayName>IM -
Gtalk</DisplayName>

<AttributeID>imGtalk</Attribute
ID>
  <Description>IM -
Gtalk</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/skype</ClaimURI>
  <DisplayName>IM -
Skype</DisplayName>

<AttributeID>imSkype</Attribute
ID>
  <Description>IM -
Skype</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/photos</ClaimURI>
```

```
<DisplayName>Photo</DisplayName
>

<AttributeID>photos</AttributeI
D>

<Description>Photo</Description
>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/photourl</ClaimURI>
  <DisplayName>Photo
URIL</DisplayName>

<AttributeID>photoUrl</Attribut
eID>
  <Description>Photo
URL</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/thumbnail</ClaimURI>
  <DisplayName>Photo -
Thumbnail</DisplayName>

<AttributeID>thumbnail</Attribu
teID>
  <Description>Photo -
Thumbnail</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
```

```
s/addresses</ClaimURI>

<DisplayName>Address</DisplayNa
me>

<AttributeID>addresses</Attribu
teID>

<Description>Address</Descripti
on>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/addresses.formatted</ClaimURI
>
  <DisplayName>Address -
Formatted</DisplayName>

<AttributeID>formattedAddress</
AttributeID>
  <Description>Address -
Formatted</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/streetaddress</ClaimURI>
  <DisplayName>Address -
Street</DisplayName>

<AttributeID>streetAddress</Att
ributeID>
  <Description>Address -
Street</Description>

<DisplayOrder>5</DisplayOrder>
```

```
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/addresses.locality</ClaimURI>
  <DisplayName>Address - Locality</DisplayName>

<AttributeID>localityAddress</AttributeID>
  <Description>Address - Locality</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/groups</ClaimURI>

<DisplayName>Groups</DisplayName>

<AttributeID>groups</AttributeID>

<Description>Groups</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/identity/verifyEmail</ClaimURI>
  <DisplayName>Verify Email</DisplayName>

<AttributeID>manager</AttributeID>
```

```
  <Description>Temporary claim
to invoke email verified
feature</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/identity/askPassword</ClaimUR
I>
  <DisplayName>Ask
Password</DisplayName>

<AttributeID>postOfficeBox</Att
ributeID>
  <Description>Temporary claim
to invoke email ask Password
feature</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/identity/adminForcedPasswordR
eset</ClaimURI>
  <DisplayName>Force Password
Reset</DisplayName>

<AttributeID>departmentNumber</
AttributeID>
  <Description>Temporary claim
to invoke email force password
feature</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/entitlements</ClaimURI>
```

		<DisplayName>Entitlements</DisplayName> <AttributeID>entitlements</AttributeID> <Description>Entitlements</Description> </Claim> <Claim> <ClaimURI>urn:scim:schemas:core:1.0:roles</ClaimURI> <DisplayName>Roles</DisplayName> <AttributeID>roles</AttributeID> <Description>Roles</Description> <DisplayOrder>5</DisplayOrder> <SupportedByDefault /> <MappedLocalClaim>http://wso2.org/claims/role</MappedLocalClaim> </Claim> <Claim> <ClaimURI>http://wso2.org/claims/x509Certificates</ClaimURI> <DisplayName>X509Certificates</DisplayName>

```
<AttributeID>x509Certificates</
AttributeID>

<Description>X509Certificates</
Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/identity/failedPasswordRecove
ryAttempts</ClaimURI>
  <DisplayName>Failed Password
Recovery Attempts</DisplayName>

<AttributeID>postalCode</Attrib
uteID>
  <Description>Number of
consecutive failed attempts
done for password
recovery</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claim
s/identity/emailVerified</Claim
URI>
  <DisplayName>Email
Verified</DisplayName>
  <!-- Proper attribute Id in
your user store must be
configured for this -->

<AttributeID>postalAddress</Att
ributeID>
  <Description>Email
```

```
Verified</Description>
</Claim>
<Claim>

<ClaimURI>http://wso2.org/claims/identity/failedLoginLockoutCount</ClaimURI>
  <DisplayName>Failed Lockout Count</DisplayName>
  <!-- Proper attribute Id in your user store must be configured for this -->

<AttributeID>employeeNumber</AttributeID>
  <Description>Failed Lockout Count</Description>
</Claim>
```

Remove the following claim.

```
<Claim>


<ClaimURI>http://wso2.org/claims/identity/lastLoginTime</ClaimURI>

  <DisplayName>Last Login</DisplayName>
```

```
  <!-- Proper attribute Id in
your user store must be
configured for this -->


<AttributeID>carLicense</Attrib
uteID>

  <Description>Last Login
Time</Description>

</Claim>
```

Add the following claim.

```
<ClaimURI>http://wso2.org/claim
s/identity/lastLogonTime</Claim
URI>

<DisplayName>Last
Logon</DisplayName>

<!-- Proper attribute Id in
your user store must be
configured for this -->

<AttributeID>carLicense</Attrib
uteID>

<Description>Last Logon
Time</Description>

</Claim>
```

		Replace the following attribute from under the <Claim> <ClaimURI> http://wso2.org/claims/challengeQuestion1 </ClaimURI> tag. `Replace this attribute:` `<AttributeID>localityName</AttributeID>` `with this:` `<AttributeID>firstChallenge</AttributeID>` Replace the following attribute from under the the <Claim> <ClaimURI> http://wso2.org/claims/challengeQuestion2 </ClaimURI> `Replace this attribute:`

		<AttributeID>localityName</AttributeID> with this: <AttributeID>secondChallenge</AttributeID> Modify this claim as follows: <Claim> <ClaimURI>http://wso2.org/claims/active</ClaimURI> <DisplayName>Active</DisplayName> <AttributeID>active</AttributeID> <Description>Status of the account</Description> </Claim>

The `catalina-server.xml` file stored in the `<PRODUCT_HOME>/repository/conf/tomcat/` directory.	Mandatory	Add the following valves under the `<Host>` tag. `<!-- Authentication and Authorization valve for the rest apis and we can configure context for this in identity.xml -->` `<Valve className="org.wso2.carbon.identity.auth.valve.AuthenticationValve"/>` `<Valve className="org.wso2.carbon.identity.authz.valve.AuthorizationValve"/>` `<Valve className="org.wso2.carbon.identity.context.rewrite.valve.TenantContextRewriteValve"/>`
The `carbon.xml` file stored in the `<PRODUCT_HOME>/repository/conf/` directory.	Optional	Add the following properties after the `</Security>` tag. `<HideMenuItemIds>`

		<HideMenuItemId>identity_mgt_emailtemplate_menu</HideMenuItemId> <HideMenuItemId>identity_security_questions_menu</HideMenuItemId> </HideMenuItemIds>
The carbon.xml file stored in the <PRODUCT_HOME>/repository/conf/ directory.	Mandatory	Add the following property to the config file. <HideMenuItemIds> <HideMenuItemId>claim_mgt_menu</HideMenuItemId> <HideMenuItemId>identity_mgt_emailtemplate_menu</HideMenuItemId> <HideMenuItemId>identity_security_questions_menu</HideMenuItemId> </HideMenuItemIds> Update the following property value to 5.3.0.

		`<Version>5.3.0</Version>`
The `application-authentication.xml` file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	Mandatory	Add the following property under the `<Extensions>` tag. `<AuthorizationHandler>org.wso2.carbon.identity.application.authz.xacml.handler.impl.XACMLBasedAuthorizationHandler</AuthorizationHandler>`
The `application-authentication.xml` file stored in the `<PRODUCT_HOME>/repository/conf/identity/` directory.	Optional	If you are using the mobile connect authenticator feature, add the following element under the `<AuthenticatorConfigs>` tag. `<AuthenticatorConfig name="MobileConnectAuthenticator" enabled="true">` `<Parameter name="MobileConnectKey">mobileConnectClientId</Parameter>` `<Parameter name="MobileConnectSecret">mobi`

		leConnectClientSecret</Parameter> </AuthenticatorConfig>

Recommended: See the WSO2 IS 5.3.0 migration guide for more information.

5.3.0 to 5.4.0

Configuration changes: Click here to view the table..

Configuration File	Changes
carbon.xml file stored in the <IS_HOME>/repository/conf folder.	Change the version property value to 5.4.0. <Version>5.4.0</Version>
identity-event.properties file stored in the <IS_HOME>/rep	Add the following property. account.lock.handler.notification.manageInternally=true

`ository/conf/identity` folder.	more information about the account.lock.handler.notification.manageInternally property: The property given above allows you to enable or disable sending emails via the WSO2 Identity Server when an account is locked or unlocked.

`identity.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Add the following property within the `<SessionDataCleanUp>` tag. `<DeleteChunkSize>50000</DeleteChunkSize>` more information about the DeleteChunkSize property: In a production environment, there is a possibility for a deadlock/database lock to occur when running a session data cleanup task in high load scenarios. To mitigate this, the property given above was introduced to clean data in chunks. Configure this property with the required chunk size. For more information, see Deployment Guidelines in Production. Remove the following property found within the `<OperationDataCleanUp>` tag. `<CleanUpPeriod>720</CleanUpPeriod>` more information about the CleanUpPeriod property:

	WSO2 IS 5.3.0 had two separate tasks for session data cleanup and operation data cleanup. This is now combined and done through one task. Therefore the property given above is no longer needed. You can still configure the `<CleanUpPeriod>` property within the `<SessionDataCleanUp>` tag to specify the cleanup period for the combined task. Change the default value of the following property from 300 to 0. You can skip this step if you have already configured the `<TimestampSkew>` property with your own value. `<TimestampSkew>0</TimestampSkew>` More information about the TimestampSkew property: The property given above specifies the maximum tolerance limit for the clock skewed between the sender and recipient. The default value was changed to 0 as the best practice is to assume that the sender and recipient clocks are synchronized

	and are in the same time stamp. Configure this accordingly if the clocks are not in the same timestamp. Add the following JWT bearer grant type within the `<SupportedGrantTypes>` tag. `<SupportedGrantType>` `<GrantTypeName>urn:ietf:params:oauth:grant-type:jwt-bearer</GrantTypeName>` `<GrantTypeHandlerImplClass>org.wso2.carbon.identity.oauth2.grant.jwt.JWTBearerGrantHandler</GrantTypeHandlerImplClass>` `<GrantTypeValidatorImplClass>org.wso2.carbon.identity.oauth2.grant.jwt.JWTGrantValidator</GrantTypeValidatorImplClass>` `</SupportedGrantType>` More information about the JWT bearer grant type The JWT bearer grant type is supported out-of-the-box with WSO2 IS 5.4.0.

For more information, see Configuring JWT Grant Type in the ISConnectors documentation.

Update the `<EmailVerification>` code block with the following code.

The properties shown below at line numbers 3,8,9,10 & 11 were added in 5.4.0.

This step is optional.

```
<EmailVerification>
    <Enable>false</Enable>
    <ExpiryTime>1440</ExpiryTime>
    <LockOnCreation>true</LockOnCreation>
    <Notification>

<InternallyManage>true</InternallyManage>
    </Notification>
    <AskPassword>
        <ExpiryTime>1440</ExpiryTime>

<PasswordGenerator>org.wso2.carbon.user.mgt.
```

```
common.DefaultPasswordGenerator</PasswordGen
erator>

    </AskPassword>

</EmailVerification>
```

Update the following property found within the `<SelfRegistration>` tag to true.

This step is optional.

```
<LockOnCreation>true</LockOnCreation>
```

Add the following properties within the `<SelfRegistration>` tag.

This step is optional.

```
<VerificationCode>

  <ExpiryTime>1440</ExpiryTime>

</VerificationCode>
```

Add the following properties within the `<Server>` tag.

```
<AuthenticationPolicy>


<CheckAccountExist>false</CheckAccountExis
t>

</AuthenticationPolicy>
```

Change the default values within the `<CacheManager>` tag.

- **If you have already configured all the properties** within the `<CacheManager>` tag with your own values, skip this step.

- **If you have only configured some properties** within the `<CacheManager>` tag with your own values,
  replace the properties that are not been changed/configured with the relevant default values shown below.

- **If you have not configured or changed any of the properties** within the `<CacheManager>` tag with your own values,
  copy the entire code block below and replace the `<CacheManager>` tag in the `identity.xml` file with the code block given below.

```
<CacheManager
name="IdentityApplicationManagementCacheMana
ger">

    <Cache
name="AppAuthFrameworkSessionContextCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="AuthenticationContextCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="AuthenticationRequestCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="AuthenticationResultCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="AppInfoCache"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>

    <Cache name="AuthorizationGrantCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="OAuthCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>
```

```
    <Cache name="OAuthScopeCache"
enable="true"  timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="OAuthSessionDataCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="SAMLSSOParticipantCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="SAMLSSOSessionIndexCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="SAMLSSOSessionDataCache"
enable="true" timeout="300" capacity="5000"
isDistributed="false"/>

    <Cache name="ServiceProviderCache"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>

    <Cache name="ProvisioningConnectorCache"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>

    <Cache name="ProvisioningEntityCache"
enable="true" timeout="900" capacity="5000"
isDistributed="false"/>

    <Cache
name="ServiceProviderProvisioningConnectorCa
```

```
che" enable="true"  timeout="900"
capacity="5000" isDistributed="false"/>

    <Cache name="IdPCacheByAuthProperty"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>

    <Cache name="IdPCacheByHRI"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>

    <Cache name="IdPCacheByName"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>

</CacheManager>
```

Add the following property within the `<CacheManager>` tag if it does not already exist.

```
<Cache name="OAuthScopeCache" enable="true"
timeout="300" capacity="5000"
isDistributed="false"/>
```

Add the following properties within the `<OAuth>` tag. The code comments explain the usage and applicable values for the properties.

```
<!-- Specify the Token issuer class to be
used.

Default:
org.wso2.carbon.identity.oauth2.token.Oauth
TokenIssuerImpl.

Applicable values:
org.wso2.carbon.identity.oauth2.token.JWTTo
kenIssuer-->


<!--<IdentityOAuthTokenGenerator>org.wso2.c
arbon.identity.oauth2.token.JWTTokenIssuer<
/IdentityOAuthTokenGenerator>-->



<!-- This configuration is used to specify
the access token value generator.

Default:
org.apache.oltu.oauth2.as.issuer.UUIDValueG
enerator

Applicable values:
org.apache.oltu.oauth2.as.issuer.UUIDValueG
enerator,


org.apache.oltu.oauth2.as.issuer.MD5Generat
or,
```

```
org.wso2.carbon.identity.oauth.tokenvaluege
nerator.SHA256Generator -->


<!--<AccessTokenValueGenerator>org.wso2.car
bon.identity.oauth.tokenvaluegenerator.SHA2
56Generator</AccessTokenValueGenerator>-->



<!-- This configuration is used to specify
whether the Service Provider tenant domain
should be used when generating

access token.Otherwise user domain will be
used.Currently this value is only supported
by the JWTTokenIssuer. -->


<!--<UseSPTenantDomain>True</UseSPTenantDom
ain>-->
```

Add the following properties related to token persistence within the `<OAuth>` tag.

```
<TokenPersistence>

    <Enable>true</Enable>

    <PoolSize>0</PoolSize>
```

```
    <RetryCount>5</RetryCount>

</TokenPersistence>
```

Add the following property within the `<OpenIDConnect>` tag.

```
<SignJWTWithSPKey>false</SignJWTWithSPKey>
```

Replace the `<OAuth2RevokeEPUrll>` property with the following.

```
<OAuth2RevokeEPUrl>${carbon.protocol}://${carbon.host}:${carbon.management.port}/oauth2/revoke</OAuth2RevokeEPUrl>
```

Add the following event listener within the `<EventListeners>` tag. Uncomment this listener if you are using SCIM 2.0.

```


<!-- Uncomment the following event listener if SCIM2 is used. -->

<!--EventListener type="org.wso2.carbon.user.core.listener.UserOperationEventListener"
```

	`` name = "org.wso2.carbon.identity.scim2.common.listener.SCIMUserOperationListener" orderId = "93" enable = "true" /--> ``` Add the following properties within the `<ResourceAccessControl>` tag. These properties specify the access levels and permissions for the SCIM 2.0 resources.

```
<Resource context="(.*)/scim2/Users"
secured="true" http-method="POST">

<Permissions>/permission/admin/manage/identi
ty/usermgt/create</Permissions>

</Resource>

<Resource context="(.*)/scim2/Users"
secured="true" http-method="GET">

<Permissions>/permission/admin/manage/identi
ty/usermgt/list</Permissions>

</Resource>

<Resource context="(.*)/scim2/Groups"
secured="true" http-method="POST">

<Permissions>/permission/admin/manage/identi
```

```
</Resource>

<Resource context="(.*)/scim2/Users/(.*)"
secured="true" http-method="GET">


<Permissions>/permission/admin/manage/identi
ty/usermgt/view</Permissions>

</Resource>

<Resource context="(.*)/scim2/Users/(.*)"
secured="true" http-method="PUT">


<Permissions>/permission/admin/manage/identi
ty/usermgt/update</Permissions>

</Resource>

<Resource context="(.*)/scim2/Users/(.*)"
secured="true" http-method="PATCH">


<Permissions>/permission/admin/manage/identi
ty/usermgt/update</Permissions>

</Resource>

<Resource context="(.*)/scim2/Users/(.*)"
secured="true" http-method="DELETE">
```

```
<Permissions>/permission/admin/manage/identi
ty/usermgt/delete</Permissions>

</Resource>

<Resource context="(.*)/scim2/Groups/(.*)"
secured="true" http-method="GET">


<Permissions>/permission/admin/manage/identi
ty/rolemgt/view</Permissions>

</Resource>

<Resource context="(.*)/scim2/Groups/(.*)"
secured="true" http-method="PUT">


<Permissions>/permission/admin/manage/identi
ty/rolemgt/update</Permissions>

</Resource>

<Resource context="(.*)/scim2/Groups/(.*)"
secured="true" http-method="PATCH">


<Permissions>/permission/admin/manage/identi
ty/rolemgt/update</Permissions>

</Resource>
```

```
<Resource context="(.*)/scim2/Groups/(.*)"
secured="true" http-method="DELETE">


<Permissions>/permission/admin/manage/identi
ty/rolemgt/delete</Permissions>

</Resource>

<Resource context="(.*)/scim2/Me"
secured="true"    http-method="GET">


<Permissions>/permission/admin/login</Permis
sions>

</Resource>

<Resource context="(.*)/scim2/Me"
secured="true" http-method="DELETE">


<Permissions>/permission/admin/manage/identi
ty/usermgt/delete</Permissions>

</Resource>

<Resource context="(.*)/scim2/Me"
secured="true"    http-method="PUT">


<Permissions>/permission/admin/login</Permis
sions>
```

```
</Resource>

<Resource context="(.*)/scim2/Me"
secured="true"   http-method="PATCH">


<Permissions>/permission/admin/login</Permis
sions>

</Resource>

<Resource context="(.*)/scim2/Me"
secured="true" http-method="POST">


<Permissions>/permission/admin/manage/identi
ty/usermgt/create</Permissions>

</Resource>

<Resource
context="/scim2/ServiceProviderConfig"
secured="false" http-method="all">

    <Permissions></Permissions>

</Resource>

<Resource context="/scim2/ResourceType"
secured="false" http-method="all">

    <Permissions></Permissions>

</Resource>
```

```
<Resource context="/scim2/Bulk"
secured="true"  http-method="all">


<Permissions>/permission/admin/manage/identi
ty/usermgt</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/(.*)"
secured="true" http-method="all">


<Permissions>/permission/admin/manage/identi
ty/applicationmgt</Permissions>

</Resource>
```

Add the following properties within the `<TenantContextsToRewrite><WebApp>` tag.

```
<Context>/scim2</Context>

<Context>/api/identity/oauth/dcr/v1.0</Conte
xt>
```

Remove the following property found within the `<OAuth>` tag.

```
<AppInfoCacheTimeout>-1</AppInfoCacheTimeout
>

<AuthorizationGrantCacheTimeout>-1</Authoriz
ationGrantCacheTimeout>

<SessionDataCacheTimeout>-1</SessionDataCach
eTimeout>

<ClaimCacheTimeout>-1</ClaimCacheTimeout>
```

Add the following commented property within the `<OAuth>` tag.

```
<!-- True, if access token alias is stored
in the database instead of access token.

Eg.token alias and token is same when

default AccessTokenValueGenerator is used.

When JWTTokenIssuer is used, jti is used as
the token alias

Default: true.

Applicable values: true, false-->
```

```
<!--<PersistAccessTokenAlias>false</PersistA
ccessTokenAlias>-->
```

Replace the `<OAuth2DCREPUrl>` property with the property value given below.

```
<OAuth2DCREPUrl>${carbon.protocol}://${carbo
n.host}:${carbon.management.port}/api/identi
ty/oauth2/dcr/v1.0/register</OAuth2DCREPUrl>
```

Uncomment the following property and add line number 3 given below to the file.

```
<TokenValidators>

    <TokenValidator type="bearer"
class="org.wso2.carbon.identity.oauth2.valid
ators.DefaultOAuth2TokenValidator" />

    <TokenValidator type="jwt"
class="org.wso2.carbon.identity.oauth2.valid
ators.OAuth2JWTTokenValidator" />

</TokenValidators>
```

Add the following commented property to the file. You can place it after the `</EnableAssertions>`closing tag.

```
<!-- This should be true if subject
identifier in the token validation response
needs to adhere to the

following SP configuration.



- Use tenant domain in local subject
identifier. - Use user store domain in local
subject identifier.



if the value is false, subject identifier
will be set as the fully qualified username.



Default value: false



Supported versions: IS 5.4.0 beta onwards-->


<!--<BuildSubjectIdentifierFromSPConfig>true
</BuildSubjectIdentifierFromSPConfig>-->
```

Uncomment the `<UserType>` property that has the value "Federated" and comment out the `<UserType>` property that has the value "Local" as seen below.

The property can be found within the `<SAML2Grant>` tag.

```
<SAML2Grant>


<!--SAML2TokenHandler></SAML2TokenHandler-->

    <!-- UserType conifg decides whether the
SAML assertion carrying user is local user
or a federated user.

            Only Local Users can access
claims from local userstore. LEGACY users
will have to have tenant domain appended
username.

            They will not be able to access
claims from local userstore. To get claims
by mapping users with exact same username
from local

            userstore (for non LOCAL
scenarios) use mapFederatedUsersToLocal
config -->

    <!--<UserType>LOCAL</UserType>-->

    <UserType>FEDERATED</UserType>

    <!--UserType>LEGACY</UserType-->

</SAML2Grant>
```

Remove the following properties found within the `<SSOService>` tag.

This step is optional.

```
<PersistanceCacheTimeout>157680000</Persista
nceCacheTimeout>

<SessionIndexCacheTimeout>157680000</Session
IndexCacheTimeout>
```

Add the following properties to the file. You can place the code block after the `</SCIM>` closing tag.

```
<SCIM2>

    <!--Default value for UserEPUrl and
GroupEPUrl are built in following format


https://<HostName>:<MgtTrpProxyPort except
443>/<ProxyContextPath>/<context>/<path>

            If that doesn't satisfy
uncomment the following config and
explicitly configure the value-->


<!--UserEPUrl>${carbon.protocol}://${carbon.
```

```
host}:${carbon.management.port}/scim2/Users<
/UserEPUrl-->


<!--GroupEPUrl>${carbon.protocol}://${carbon
.host}:${carbon.management.port}/scim2/Group
s</GroupEPUrl-->

</SCIM2>
```

Add the following properties to the file. You can place it after the `</EnableAskPasswordAdminUI>` closing tag.

```
<EnableRecoveryEndpoint>true</EnableRecovery
Endpoint>

<EnableSelfSignUpEndpoint>true</EnableSelfSi
gnUpEndpoint>
```

Add the following properties within the `<ResourceAccessControl>` tag.

```
<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/r
egister(.*)" secured="true"
http-method="POST">


<Permissions>/permission/admin/manage/identi
ty/applicationmgt/create</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/r
egister(.*)" secured="true"
http-method="DELETE">


<Permissions>/permission/admin/manage/identi
ty/applicationmgt/delete</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/r
egister(.*)" secured="true"
http-method="PUT">


<Permissions>/permission/admin/manage/identi
ty/applicationmgt/update</Permissions>

</Resource>
```

	<Resource context="(.*)/api/identity/oauth2/dcr/v1.0/register(.*)" secured="true" http-method="GET"> <Permissions>/permission/admin/manage/identity/applicationmgt/view</Permissions> </Resource>
`oidc-scope-config.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Replace the `<Claim>` tag within the `<Scope id="openid">` tag with the following. <Claim> sub, email, email_verified, name, family_name, given_name, middle_name, nickname, preferred_username, profile, picture, website, gender, birthdate, zoneinfo, locale, updated_at, phone_number, phone_number_verified, address,street_address,country, formatted, postal_code, locality, region </Claim>

	Replace the `<Claim>` tag within the `<Scope id="address">` tag with the following. `<Claim>address,street</Claim>`
`authenticators.xml` file stored in the `<IS_HOME>/repository/conf/security` folder.	Update the parameter name of the `JITUserProvisioning` parameter to the following. `<Parameter name="JITUserProvisioningEnabled">true</Parameter>`
`web.xml` file stored in the `<IS_HOME>/repository/conf/tomcat` folder.	Add the following property under the `<session-config>` tag. `<tracking-mode>COOKIE</tracking-mode>` Add the following properties below the `<servlet-class>org.apache.jasper.servlet.JspServlet</servlet-class>` property.

	`` <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>```
`email-admin-config.xml` file stored in the `<IS_HOME>/repository/conf/email` folder.	Replace "https://localhost:9443" in all instances of the `accountrecoveryendpoint` URL with the **`{{carbon.product-url}}`** placeholder. The URL should look similiar to the URL shown in the code block below. The placeholder will retrieve the value configured in the `carbon.xml` file. You can skip this step if you have already configured this with your load balancer URL.

	`` {{carbon.product-url}}/accountrecoveryendpoint/confirmregistration.do?confirmation={{confirmation-code}}&userstoredomain={{userstore-domain}}&username={{url:user-name}}&tenantdomain={{tenant-domain}} ```
`cipher-tool.properties` file stored in the `<IS_HOME>/repository/conf` folder.	Add the following property. ``` ThirftBasedEntitlementConfig.KeyStore.Password=repository/conf/identity/identity.xml//Server/EntitlementSettings/ThirftBasedEntitlementConfig/KeyStore/Password,true ```
`cipher-text.properties` file stored in the `<IS_HOME>/repository/conf` folder.	Add the following property. ``` ThirftBasedEntitlementConfig.KeyStore.Password=[wso2carbon] ```

`claim-config.xml` file stored in the `<IS_HOME>/repository/conf` folder.	Add the following claims within the <Dialect dialectURI="http://wso2.org/claims"> tag. `<Claim>` `<ClaimURI>http://wso2.org/claims/identity/phoneVerified</ClaimURI>` `<DisplayName>Phone Verified</DisplayName>` `<!-- Proper attribute Id in your user store must be configured for this -->` `<AttributeID>phoneVerified</AttributeID>` `<Description>Phone Verified</Description>` `</Claim>` `<Claim>` `<ClaimURI>http://wso2.org/claims/department</ClaimURI>`

```
    <DisplayName>Department</DisplayName>


 <AttributeID>departmentNumber</AttributeID>

    <Description>Department</Description>

    <SupportedByDefault />

    <ReadOnly />

 </Claim>
```

Add the following claims. This new claim dialect and the claims within it are required for SCIM 2.0.

```
<Dialect
dialectURI="urn:ietf:params:scim:schemas:core:2.0"
>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:id
</ClaimURI>
        <DisplayName>Id</DisplayName>
        <AttributeID>scimId</AttributeID>
        <Description>Id</Description>
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/userid</M
appedLocalClaim>
    </Claim>
    <Claim>
```

```
<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:ex
ternalId</ClaimURI>
        <DisplayName>External Id</DisplayName>
        <AttributeID>externalId</AttributeID>
        <Description>External Id</Description>
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/externali
d</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:me
ta.created</ClaimURI>
        <DisplayName>Meta - Created</DisplayName>
        <AttributeID>createdDate</AttributeID>
        <Description>Meta - Created</Description>
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/created</
MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:me
ta.lastModified</ClaimURI>
        <DisplayName>Meta - Last
Modified</DisplayName>

<AttributeID>lastModifiedDate</AttributeID>
        <Description>Meta - Last
Modified</Description>
        <Required />
```

```
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/modified<
/MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:me
ta.location</ClaimURI>
        <DisplayName>Meta - Location</DisplayName>
        <AttributeID>location</AttributeID>
        <Description>Meta - Location</Description>
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/location<
/MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:me
ta.resourceType</ClaimURI>
        <DisplayName>Meta - Location</DisplayName>
        <AttributeID>ref</AttributeID>
        <Description>Meta - Location</Description>
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/resourceT
ype</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:me
```

```
ta.version</ClaimURI>
        <DisplayName>Meta - Version</DisplayName>
        <AttributeID>im</AttributeID>
        <Description>Meta - Version</Description>
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/im</Mappe
dLocalClaim>
    </Claim>
</Dialect>
<Dialect
dialectURI="urn:ietf:params:scim:schemas:core:2.0:
User">
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:userName</ClaimURI>
        <DisplayName>User Name</DisplayName>
        <AttributeID>uid</AttributeID>
        <Description>User Name</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/username<
/MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:name.givenName</ClaimURI>
        <DisplayName>Name - Given
Name</DisplayName>
        <AttributeID>givenName</AttributeID>
        <Description>Given Name</Description>
```

```
        <Required />
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/givenname
</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:name.familyName</ClaimURI>
        <DisplayName>Name - Family
Name</DisplayName>
        <AttributeID>sn</AttributeID>
        <Description>Family Name</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/lastname<
/MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:name.formatted</ClaimURI>
        <DisplayName>Name - Formatted
Name</DisplayName>
        <AttributeID>formattedName</AttributeID>
        <Description>Formatted Name</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/formatted
Name</MappedLocalClaim>
    </Claim>
```

```
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:name.middleName</ClaimURI>
        <DisplayName>Name - Middle Name</DisplayName>
        <AttributeID>middleName</AttributeID>
        <Description>Middle Name</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/middleName</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:name.honorificPrefix</ClaimURI>
        <DisplayName>Name - Honoric Prefix</DisplayName>
        <AttributeID>honoricPrefix</AttributeID>
        <Description>Honoric Prefix</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/honorificPrefix</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:name.honorificSuffix</ClaimURI>
        <DisplayName>Name - Honoric Suffix</DisplayName>
        <AttributeID>honoricSuffix</AttributeID>
```

```
        <Description>Honoric Suffix</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/honorific
Suffix</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:displayName</ClaimURI>
        <DisplayName>Display Name</DisplayName>
        <AttributeID>displayName</AttributeID>
        <Description>Display Name</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/displayNa
me</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:nickName</ClaimURI>
        <DisplayName>Nick Name</DisplayName>
        <AttributeID>nickName</AttributeID>
        <Description>Nick Name</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/nickname<
/MappedLocalClaim>
    </Claim>
    <Claim>
```

```
<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:profileUrl</ClaimURI>
        <DisplayName>Profile URL</DisplayName>
        <AttributeID>url</AttributeID>
        <Description>Profile URL</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/url</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:title</ClaimURI>
        <DisplayName>Title</DisplayName>
        <AttributeID>title</AttributeID>
        <Description>Title</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/title</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:userType</ClaimURI>
        <DisplayName>User Type</DisplayName>
        <AttributeID>userType</AttributeID>
        <Description>User Type</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />
```

```
<MappedLocalClaim>http://wso2.org/claims/userType<
/MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:preferredLanguage</ClaimURI>
        <DisplayName>Preferred
Language</DisplayName>

<AttributeID>preferredLanguage</AttributeID>
        <Description>Preferred
Language</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/preferred
Language</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:locale</ClaimURI>
        <DisplayName>Locality</DisplayName>
        <AttributeID>localityName</AttributeID>
        <Description>Locality</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/local</Ma
ppedLocalClaim>
    </Claim>
    <Claim>
```

```
<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:timezone</ClaimURI>
        <DisplayName>Time Zone</DisplayName>
        <AttributeID>timeZone</AttributeID>
        <Description>Time Zone</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/timeZone</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:active</ClaimURI>
        <DisplayName>Active</DisplayName>
        <AttributeID>active</AttributeID>
        <Description>Active</Description>
        <DisplayOrder>2</DisplayOrder>
        <Required />
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/active</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:emails.work</ClaimURI>
        <DisplayName>Emails - Work Email</DisplayName>
        <AttributeID>workEmail</AttributeID>
        <Description>Work Email</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />
```

```
<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+
([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/emails.wo
rk</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:emails.home</ClaimURI>
        <DisplayName>Emails - Home
Email</DisplayName>
        <AttributeID>homeEmail</AttributeID>
        <Description>Home Email</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+
([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/emails.ho
me</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:emails.other</ClaimURI>
        <DisplayName>Emails - Other
Email</DisplayName>
        <AttributeID>otherEmail</AttributeID>
        <Description>Other Email</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+
([a-zA-Z0-9]{2,4})+$</RegEx>
```

```
<MappedLocalClaim>http://wso2.org/claims/emails.other</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.mobile</ClaimURI>
        <DisplayName>Phone Numbers - Mobile Number</DisplayName>
        <AttributeID>mobile</AttributeID>
        <Description>Mobile Number</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/mobile</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.home</ClaimURI>
        <DisplayName>Phone Numbers - Home Phone Number</DisplayName>
        <AttributeID>homePhone</AttributeID>
        <Description>Home Phone</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/phoneNumbers.home</MappedLocalClaim>
    </Claim>
```

```
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.work</ClaimURI>
        <DisplayName>Phone Numbers - Work Phone Number</DisplayName>
        <AttributeID>workPhone</AttributeID>
        <Description>Work Phone</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/phoneNumbers.work</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.other</ClaimURI>
        <DisplayName>Phone Numbers - Other</DisplayName>

<AttributeID>otherPhoneNumber</AttributeID>
        <Description>Other Phone Number</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/phoneNumbers.other</MappedLocalClaim>
    </Claim>
    <Claim>
```

```
<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:ims.gtalk</ClaimURI>
        <DisplayName>IM - Gtalk</DisplayName>
        <AttributeID>imGtalk</AttributeID>
        <Description>IM - Gtalk</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/gtalk</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:ims.skype</ClaimURI>
        <DisplayName>IM - Skype</DisplayName>
        <AttributeID>imSkype</AttributeID>
        <Description>IM - Skype</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/skype</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:photos.photo</ClaimURI>
        <DisplayName>Photo</DisplayName>
        <AttributeID>photoUrl</AttributeID>
        <Description>Photo</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/photourl</MappedLocalClaim>
```

```
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:photos.thumbnail</ClaimURI>
        <DisplayName>Photo - Thumbnail</DisplayName>
        <AttributeID>thumbnail</AttributeID>
        <Description>Photo - Thumbnail</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/thumbnail</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:addresses.home</ClaimURI>
        <DisplayName>Address - Home</DisplayName>
        <AttributeID>localityAddress</AttributeID>
        <Description>Address - Home</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/addresses.locality</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:addresses.work</ClaimURI>
        <DisplayName>Address - Work</DisplayName>
        <AttributeID>region</AttributeID>
        <Description>Address - Work</Description>
        <DisplayOrder>5</DisplayOrder>
```

```
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/region</M
appedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:groups</ClaimURI>
        <DisplayName>Groups</DisplayName>
        <AttributeID>groups</AttributeID>
        <Description>Groups</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/groups</M
appedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:entitlements.default</ClaimURI>
        <DisplayName>Entitlements</DisplayName>
        <AttributeID>entitlements</AttributeID>
        <Description>Entitlements</Description>
        <DisplayOrder>5</DisplayOrder>
        <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/entitleme
nts</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.0:Us
er:roles.default</ClaimURI>
        <DisplayName>Roles</DisplayName>
        <AttributeID>roles</AttributeID>
```

	<Description>Roles</Description> <DisplayOrder>5</DisplayOrder> <SupportedByDefault /> <MappedLocalClaim>http://wso2.org/claims/role</MappedLocalClaim> </Claim> <Claim> <ClaimURI>urn:ietf:params:scim:schemas:core:2.0:User:x509Certificates.default</ClaimURI> <DisplayName>X509Certificates</DisplayName> <AttributeID>x509Certificates</AttributeID> <Description>X509Certificates</Description> <DisplayOrder>5</DisplayOrder> <SupportedByDefault /> <MappedLocalClaim>http://wso2.org/claims/x509Certificates</MappedLocalClaim> </Claim> </Dialect>
`application-authentication.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Add the following parameter within the FacebookAuthenticator tag. <!--<Parameter name="ClaimDialectUri">http://wso2.org/facebook/claims</Parameter>-->

	Add the following parameter within the relevant tags of the following authenticators: `MobileConnectAuthenticator`, `EmailOTP`, `SMSOTP` and `totp` `<Parameter name="redirectToMultiOptionPageOnFailure">false</Parameter>`
`entitlement.properties` file stored in the `<IS_HOME>/repository/conf/identity` folder.	WSO2 IS 5.4.0 introduces a set of new XACML policies that load at server startup when the `PAP.Policy.Add.Start.Enable` property is set to `true`. Therefore, when you upgrade to IS 5.4.0, follow one of the steps below depending on whether you want to add the new policies: • If you want to add the new policies on server startup, set both `PDP.Balana.Config.Enable` and `PAP.Policy.Add.Start.Enable` properties to `true`. • If you do not want to add the new policies on server startup, set both `PDP.Balana.Config.Enable` and `PAP.Policy.Add.Start.Enable` properties to `false`.

	Note If you set the `PDP.Balana.Config.Enable` property to `false`, while the `PAP.Policy.Add.Start.Enable` property is set to `true`, the server does not look for the `balana-config.xml` file on startup. This results in an error as follows because the balana-config.xml file includes functions required by the new XACML policies: `TID: [-1234] [] [2018-01-01 01:16:37,547] ERROR {org.wso2.carbon.identity.entitlement.EntitlementUtil} Error while adding sample XACML policies java.lang.IllegalArgumentException: Error while parsing start up policy`

Recommended: See the WSO2 IS 5.4.0 migration guide for more information.

5.4.0 to 5.5.0 (from older releases)

General doc

REMOVED_Upgrading From an Older Version of WSO2 IS

Note that these instructions have been tested for migration from WSO2 IS 5.0.0 to 5.6.0 only with the ORACLE and MySQL databases.

The following sections provide instructions that enable you to upgrade from older versions of WSO2 Identity Server (from version 5.0.0 onwards) to the latest version of WSO2 Identity Server. In this topic, `<OLD_IS_HOME>` is the directory that the older version of WSO2 Identity Server resides in, and `<NEW_IS_HOME>` is the directory that the latest version of WSO2 Identity Server resides in.

Before you begin

This release is a WUM-only release. This means that there are no manual patches. Any further fixes or latest updates for this release can be updated through WSO2 Update Manager (WUM).

- **If you are upgrading to use this version in your production environment**, use the WSO2 Update Manager to get the latest updates available for WSO2 IS. For more information on how to do this, see Updating WSO2 Products.

Migrating the embedded LDAP user store

It is not generally recommended to use the embedded LDAP user store that is shipped with WSO2 Identity Server in production setups. However, if migration of the embedded LDAP is required, follow the instructions below to migrate the existing WSO2 IS LDAP user store to the new version of WSO2 IS.

1. Copy the `<OLD_IS_HOME>/repository/data` folder to `<NEW_IS_HOME>/repository/data` folder.
2. Restart the server to save the changes.

Migrating the configurations

You can use one of the following approaches to migrate depending on your production evironment.

- **Migrating by updating the custom configurations**

  This approach is recommended if:

  - You have done very few configuration changes in your previous version of WSO2 IS. These configuration changes have been tracked and are easy to redo.

  Steps:

  1. If you have made configuration changes to the config files in your previous version of WSO2 IS, update the files in the `<NEW_IS_HOME>/repository/conf` folder with your own configurations.
  2. Proceed to the Migrating the data section to run the migration client.

- **Migrating by updating the new configurations in 5.5.0**

  This approach is recommended if:

  - You have done many configuration changes in your previous version of WSO2 IS.
  - These configurations have not been tracked completely and/or are difficult to redo.

  Steps:

  1. Make a copy of the `<OLD_IS_HOME>/repository/conf` folder. (Do not change the original configurations. You may use it as a backup in case there are any issues)
  2. Copy the following configuration files from the `<NEW_IS_HOME>` and paste it in the copy of the `<OLD_IS_HOME>` in the relevant path.
     - `<IS_HOME>/repository/conf/carbon.properties`
     - `<IS_HOME>/repository/conf/consent-mgt-config.xml`
  3. The sections below list out all the configuration changes from IS 5.0.0 to IS 5.5.0. You can scroll through each table and change the relevant configurations according to the features you are using.

     Note: The configuration changes listed below will not affect the existing system because these configurations are applied only at first start up and new tenant creation.

     If you want to change the configurations for the existing tenants, configure it through the management console user interface.

Migrating the custom components

Any custom OSGI bundles which were added manually should be recompiled with new dependency versions that are relevant to the new WSO2 IS version. All custom OSGI components reside in the `<OLD_IS_HOME>/repository/components/dropins` directory.

1. Get the source codes of the custom OSGI components located in the `dropins` directory.
2. Change the dependency versions in the relevant POM files according to the WSO2 IS version that you are upgrading to, and compile them. The compatible dependency versions for each release of WSO2 IS is given below.
    - WSO2 Identity Server 5.1.0
    - WSO2 Identity Server 5.2.0
    - WSO2 Identity Server 5.3.0
    - WSO2 Identity Server 5.4.0
    - WSO2 Identity Server 5.5.0
3. If you come across any compile time errors, refer to the WSO2 IS code base and make the necessary changes related to that particular component version.
4. Add the compiled JAR files to the `<NEW_IS_HOME>/repository/components/dropins` directory.
5. If there were any custom OSGI components in `<OLD_IS_HOME>/repository/components/lib` directory, add newly compiled versions of those components to the `<NEW_IS_HOME>/repository/components/lib` directory.

Tip: Scroll left/right to view the entire table below.

IS 5.0.0 to 5.1.0 | IS 5.1.0 to 5.2.0 | IS 5.2.0 to 5.3.0 | IS 5.3.0 to 5.4.0 | IS 5.4.0 to 5.5.0

MultiExcerpt named '**configs**' was not found

The page: **Upgrading WSO2 Identity Server** was found, but the multiexcerpt named '**configs**' was not found. Please check/update the page name used in the 'multiexcerpt-include macro.

› API changes: Click here to view the steps..

Recommended: See the WSO2 IS 5.1.0 migration guide for more information.

Note that the following files located in the `<IS_HOME>/repository/conf/` folder in 5.0.0 have been moved to the `<IS_HOME>/repository/conf/identity/` folder in 5.1.0 onwards:

- `provisioning-config.xml`
- `identity.xml`
- `/security/identity-mgt.properties`

4. Replace the `<NEW_IS_HOME>/repository/conf` folder with the modified copy of the `<OLD_IS_HOME>/repository/conf` folder.
5. Proceed to the Migrating the data section to run the migration client.

Migrating the data

To upgrade the version of WSO2 Identity Server, the user store database should be upgraded. Note that there are no registry schema changes between versions.

Follow the steps below as needed to complete the migration process.

Download the latest version of WSO2 Identity Server and unzip it in the `<NEW_IS_HOME>` directory.

1. Take a backup of the existing database used by the `<OLD_IS>`. This backup is necessary in case the migration causes issues in the existing database.
   Make the following database updates as indicated below.
    a. Download the migration resources and unzip it to a local directory. This folder is referred to as `<IS5.x.x_MIGRATION_TOOL_HOME>`.
    b. Copy the `org.wso2.carbon.is.migration-5.x.x.jar` and the `snakeyaml-1.16.0.wso2v1.jar` found in the `<IS5.x.x_MIGRATION_TOOL_HOME>` folder, and paste it in the `<NEW_IS_HOME>/repository/components/dropins` directory.
    c. Copy migration-resources folder to the `<NEW_IS_HOME>` root folder.
    d. Set the following property values accordingly in the `migration-config.yaml` file found in the `<NEW_IS_HOME>/migration-resources` folder. Specify the current WSO2 Identity Server version as the `currentVersion` value and specify the new version of WSO2 Identity Server that you want to migrate to, as the `migrateVersion`.

    If your current version of WSO2 Identity Server is 5.4.1, set the value of the `currentVersion` parameter to 5.4.0 in the `migration-config.yaml` instead. This is because data migration is not required when migrating from 5.4.0 to 5.4.1.

```
migrationEnable: "true"

currentVersion: "5.x.x"

migrateVersion: "5.x.x"
```

2. Copy any custom OSGI bundles that were added manually from the `<OLD_IS_HOME>/repository/components/dropins` folder and paste it in the `<NEW_IS_HOME>/repository/components/dropins` folder.
3. Copy any added JAR files from the `<OLD_IS_HOME>/repository/components/lib` folder and paste it in the `<NEW_IS_HOME>/repository/components/lib` folder.
4. Copy the `.jks` files from the `<OLD_IS_HOME>/repository/resources/security` folder and paste them in `<NEW_IS_HOME>/repository/resources/security` folder.
5. If you have created tenants in the previous WSO2 Identity Server version and if there are any resources in the `<OLD_IS_HOME>/repository/tenants` directory, copy the content to the `<NEW_IS_HOME>/repository/tenants` directory.

6 If you have created secondary user stores in the previous WSO2 IS version, copy the content in the **<OLD_IS_HOME>/repository/deployment/server/userstores** directory to the **<NEW_IS_HOME>/repository/deployment/server/userstores** directory.

Note: If your current version is 5.0.0, run the following queries on the database that is referenced in the `identity.xml` file in order to identify if there is any corrupted data.

```
SELECT * FROM IDN_OAUTH2_ACCESS_TOKEN WHERE AUTHZ_USER LIKE '% @%' AND TOKEN_STATE='ACTIVE';
SELECT * FROM IDN_OAUTH2_ACCESS_TOKEN WHERE AUTHZ_USER NOT LIKE '%@%' AND TOKEN_STATE='ACTIVE';
```

7 Start WSO2 Identity Server with the following command to perform the data migration for all components.

a. Linux/Unix:

```
sh wso2server.sh -Dmigrate -Dcomponent=identity
```

b. Windows:

```
wso2server.bat -Dmigrate -Dcomponent=identity
```

8 Once the migration is successful, stop the server and remove the following files and folders from the **<NEW_IS_HOME>/repository/components/dropins** directory.

a. `org.wso2.carbon.is.migration-5.x.x.jar`

b. `snakeyaml-1.16.0.wso2v1.jar`

c. `migration-resources` directory

Configurations

`carbon.xml` file stored in the `<IS_HOME>/repository/conf` folder.	Change the version property value to 5.5.0. `<Version>5.5.0</Version>`

application-authentication.xml file stored in the `<IS_HOME>/repository/conf/identity` folder.	Replace the following property found within the `<Extensions>` list. If you are using a custom `<StepBasedSequenceHandler>`, skip this step. `<StepBasedSequenceHandler>org.wso2.carbon.identity.application.authentication.framework.handler.sequence.impl.DefaultStepBasedSequenceHandler</StepBasedSequenceHandler>` with the one given below. `<StepBasedSequenceHandler>org.wso2.carbon.identity.application.authentication.framework.handler.sequence.impl.GraphBasedSequenceHandler</StepBasedSequenceHandler>` If you are using a custom authorization handler, see REMOVED_Migrating Custom Authorization Handlers. The OpenIDAuthenticator is no longer available. Remove the following configurations that are related to it. Remove the following property found within the `<AuthenticatorNameMappings>` tag.

```
<AuthenticatorNameMapping
name="OpenIDAuthenticator" alias="openid" />
```

Remove the whole configuration block that starts with the config given below found within the `<AuthenticatorConfigs>` tag.

```
<AuthenticatorConfig
name="OpenIDAuthenticator" enabled="true">

.....

.....

</AuthenticatorConfig>
```

Replace the `AuthenticatorConfig` block for the **`MobileConnectAuthenticator`** found within the `<AuthenticatorConfigs>` tag, with the following configuration.

```
<AuthenticatorConfig
name="MobileConnectAuthenticator"
enabled="true">

    <Parameter
name="MCAuthenticationEndpointURL">mobilecon
```

```
nectauthenticationendpoint/mobileconnect.jsp
</Parameter>

    <Parameter
name="MCDiscoveryAPIURL">https://discover.mo
bileconnect.io/gsma/v2/discovery/</Parameter
>

    <Parameter
name="redirectToMultiOptionPageOnFailure">fa
lse</Parameter>

</AuthenticatorConfig>
```

Remove the following property found within the `<AuthenticatorNameMappings>` tag. The `AuthorizationHandler` property has been removed from this file for newer versions of this product.

```
<AuthorizationHandler>org.wso2.carbon.identi
ty.application.authz.xacml.handler.impl.XACM
LBasedAuthorizationHandler</AuthorizationHan
dler>
```

`identity-event.properties` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Add the following properties that are required for Request Object Support. For more information about the feature, see Request Object Support. `module.name.11=handleRequestObject` `handleRequestObject.subscription.1=POST_REVOKE_ACESS_TOKEN` `handleRequestObject.subscription.2=POST_REVOKE_CODE` `handleRequestObject.subscription.3=POST_REVOKE_ACESS_TOKEN_BY_ID` `handleRequestObject.subscription.4=POST_REVOKE_CODE_BY_ID` `handleRequestObject.subscription.5=POST_REFRESH_TOKEN` `handleRequestObject.subscription.6=POST_ISSUE_CODE` `handleRequestObject.subscription.7=POST_ISSUE_ACCESS_TOKEN` Add the following properties to enable the user event handler used to delete user consents when users are deleted.

	`` module.name.12=user.consent.delete user.consent.delete.subscription.1=POST_DELE TE_USER user.consent.delete.receipt.search.limit=500 ```

`identity.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Remove the `<ClientAuthHandlers>` code block found within the `<OAuth>` tag. From WSO2 IS 5.5.0 onwards, client authentication is handled differently. For more information, see the introduction of the Writing A New OAuth Client Authenticator topic. `<ClientAuthHandlers>` `<ClientAuthHandler Class="org.wso2.carbon.identity.oauth2.token.handlers.clientauth.BasicAuthClientAuthHandler">` `<Property Name="StrictClientCredentialValidation">false</Property>` `</ClientAuthHandler>` `</ClientAuthHandlers>` Add the following property within the `<ScopeValidators>` tag. For more information about the XACML based scope validator, see Validating the Scope of OAuth Access Tokens using XACML Policies.

	Tip: To migrate custom scope validators, see REMOVED_Migrating Custom Scope Validators. `<ScopeValidator class="org.wso2.carbon.identity.oauth2.validators.xacml.XACMLScopeValidator"/>` Add the following property within the `<OpenIDConnect>` tag to enable the service provider wise audience configuration. For more information about this, see This feature requires a new database table that is created when running the migration script. If you do not wish to use this feature, you can set the value of the property given below to false. `<EnableAudiences>true</EnableAudiences>` Add the following property within the `<OpenIDConnect>` tag. `<LogoutTokenExpiration>120</LogoutTokenExpiration>`

Add the following property within the `<EventListeners>` tag.

```
<EventListener
type="org.wso2.carbon.user.core.listener.UserOperationEventListener"


name="org.wso2.carbon.user.mgt.listeners.UserDeletionEventListener"

                        orderId="98"
enable="false"/>
```

Add the following code block within the root tag after the `<EventListeners>` code block. For more information about this configuration, see Tracking user deletion on deleting a user.

```
<UserDeleteEventRecorders>

    <UserDeleteEventRecorder
name="org.wso2.carbon.user.mgt.recorder.DefaultUserDeletionEventRecorder"
enable="false">

        <!-- Un comment below line if you need to write entries to a separate .csv file. Otherwise this will be
```

```
            written in to a log file using a
separate appender. -->

        <!--<Property
name="path">${carbon.home}/repository/logs/d
elete-records.csv</Property>-->

    </UserDeleteEventRecorder>

</UserDeleteEventRecorders>
```

Do the following configuration changes to enable fine grained access control introduced with Identity Server 5.5.0

Remove the following property found within the `<ResourceAccessControl>` tag.

```
<Resource
context="(.*)/api/identity/user/(.*)"
secured="true" http-method="all"/>
```

Add the following set of resources within the `<ResourceAccessControl>` tag.

```
<Resource
context="(.*)/api/identity/user/v1.0/validat
e-code" secured="true" http-method="all"/>

<Resource
context="(.*)/api/identity/user/v1.0/resend-
code" secured="true" http-method="all"/>

<Resource
context="(.*)/api/identity/user/v1.0/me"
secured="true" http-method="POST"/>

<Resource
context="(.*)/api/identity/user/v1.0/me"
secured="true" http-method="GET"/>

<Resource
context="(.*)/api/identity/user/v1.0/pi-info
" secured="true" http-method="all">


<Permissions>/permission/admin/manage/identi
ty/usermgt/view</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/user/v1.0/pi-info
/(.*)" secured="true" http-method="all">


<Permissions>/permission/admin/manage/identi
ty/usermgt/view</Permissions>
```

```
    </Resource>

    <Resource
    context="(.*)/api/identity/consent-mgt/v1.0/
    consents" secured="true" http-method="all"/>

    <Resource
    context="(.*)/api/identity/consent-mgt/v1.0/
    consents/receipts/(.*)" secured="true"
    http-method="all"/>

    <Resource
    context="(.*)/api/identity/consent-mgt/v1.0/
    consents/purposes" secured="true"
    http-method="POST">


    <Permissions>/permission/admin/manage/identi
    ty/consentmgt/add</Permissions>

    </Resource>

    <Resource
    context="(.*)/api/identity/consent-mgt/v1.0/
    consents/purposes(.*)" secured="true"
    http-method="GET"/>

    <Resource
    context="(.*)/api/identity/consent-mgt/v1.0/
    consents/purposes(.+)" secured="true"
    http-method="DELETE">
```

```
<Permissions>/permission/admin/manage/identity/consentmgt/delete</Permissions>

</Resource>

<Resource context="(.*)/api/identity/consent-mgt/v1.0/consents/pii-categories" secured="true" http-method="POST">


<Permissions>/permission/admin/manage/identity/consentmgt/add</Permissions>

</Resource>

<Resource context="(.*)/api/identity/consent-mgt/v1.0/consents/pii-categories(.*)" secured="true" http-method="GET"/>

<Resource context="(.*)/api/identity/consent-mgt/v1.0/consents/pii-categories(.+)" secured="true" http-method="DELETE">


<Permissions>/permission/admin/manage/identity/consentmgt/delete</Permissions>

</Resource>

<Resource context="(.*)/api/identity/consent-mgt/v1.0/
```

```
consents/purpose-categories" secured="true"
http-method="POST">


<Permissions>/permission/admin/manage/identi
ty/consentmgt/add</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/consent-mgt/v1.0/
consents/purpose-categories(.*)"
secured="true" http-method="GET"/>

<Resource
context="(.*)/api/identity/consent-mgt/v1.0/
consents/purpose-categories(.+)"
secured="true" http-method="DELETE">


<Permissions>/permission/admin/manage/identi
ty/consentmgt/delete</Permissions>

</Resource>
```

Replace the following property found within the `<WebApp>` tag under the `<TenantContextsToRewrite>` tag.

```
<Context>/api/identity/user/v0.9/</Context>
```

	with the one given below `<Context>/api/identity/user/v1.0/</Context>` Add the following new property within the `<WebApp>` tag found under the `<TenantContextsToRewrite>` tag. `<Context>/api/identity/consent-mgt/v1.0/</Context>` Add the following code block within the root tag after the `<SSOService>` code block. This configuration specifies whether consent management should be enabled during single sign-on authentication. For more information, see Consent Management with Single-Sign-On. `<Consent>` `<!--Specify whether consent management should be enable during SSO.-->` `<EnableSSOConsentManagement>true</EnableSSOConsentManagement>`

```
    </Consent>
```

Add the following code block within the `<OAuth>` tag. This configuration is used to specify the grant types that filter claims based on user consents. The grant types given below are out-of-the-box grant types that prompt the user for consent.

```
    <!--Defines the grant types that will filter
    user claims based on user consent in their
    responses such as id_token or user info
    response.Default grant types that filter
    user claims based on user consent are
    'authorization_code' and 'implicit'.

    Supported versions: IS 5.5.0 onwards. -->



    <UserConsentEnabledGrantTypes>

        <UserConsentEnabledGrantType>


    <GrantTypeName>authorization_code</GrantType
    Name>

        </UserConsentEnabledGrantType>
```

	<UserConsentEnabledGrantType> <GrantTypeName>implicit</GrantTypeName> </UserConsentEnabledGrantType> </UserConsentEnabledGrantTypes>
`log4j.properties` file stored in the `<IS_HOME>/repository/conf` folder.	Add the following properties. log4j.logger.DELETE_EVENT_LOGGER=INFO, DELETE_EVENT_LOGFILE log4j.appender.DELETE_EVENT_LOGFILE=org.apache.log4j.FileAppender log4j.appender.DELETE_EVENT_LOGFILE.File=${carbon.home}/repository/logs/delete-event.log log4j.appender.DELETE_EVENT_LOGFILE.Append=true log4j.appender.DELETE_EVENT_LOGFILE.layout=org.apache.log4j.PatternLayout log4j.appender.DELETE_EVENT_LOGFILE.layout.ConversionPattern=%m %n log4j.appender.DELETE_EVENT_LOGFILE.threshold=INFO

	`log4j.additivity.DELETE_EVENT_LOGFILE=false`
`provisioning-config.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Remove the `<scim-providers>` and `<scim-consumers>` code blocks from the file.

Recommended: See the WSO2 IS 5.5.0 migration guide for more information.

5.5.0 to 5.6.0

Configuration File	Changes
`carbon.xml` file stored in the `<IS_HOME>/repository/conf` folder.	Change the version property value to 5.6.0. `<Version>5.6.0</Version>` Add the following new property within the `<cache>` tag. Setting this property to `true` enables local cache invalidation for clustered nodes. `<ForceLocalCache>false</ForceLocalCache>`

`axis2.xml` file stored in the `<IS_HOME>/repository/conf/axis2` folder.	Change the following property values to 5.6.0. `<parameter name="userAgent" locked="true">` `WSO2 Identity Server-5.6.0` `</parameter>` `<parameter name="server" locked="true">` `WSO2 Identity Server-5.6.0` `</parameter>`
`application-authentication.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Add the following new property within the root tag. `<AuthenticationEndpointMissingClaimsURL>/authenticationendpoint/claims.do</AuthenticationEndpointMissingClaimsURL>`
`entitlement.properties` file stored in the `<IS_HOME>/`	Add the following property. Setting this property to true will shorten the SAML JSON response format.

`repository/conf/identity` folder.	`JSON.Shorten.Form.Enabled=false`

`identity.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Add the following properties within the `<JDBCPersistenceManager><SessionDataPersist>` tag. These configurations are relevant for cleaning temporary authentication context data after each authentication flow. `<TempDataCleanup>` `<!-- Enabling separated cleanup for temporary authentication context data -->` `<Enable>true</Enable>` `<!-- When PoolZize > 0, temporary data which have no usage after the authentication flow will be deleted immediately` `When PoolZise = 0, data will be deleted only by the scheduled cleanup task-->` `<PoolSize>20</PoolSize>` `<!-- All temporary authentication context data older than CleanUpTimeout value are considered as expired` `and would be deleted during cleanup task -->` `<CleanUpTimeout>40</CleanUpTimeout>`

```
    </TempDataCleanup>
```

Add the following property within the `<OAuth>` tag for OAuth key hashing. For more information, see Setting Up OAuth Token Hashing.

```
    <!-- This should be true if the oauth keys
    (consumer secret, access token, refresh token
    and authorization code) need to be
    hashed,before storing them in the database. If
    the value is false, the oauth keys will be
    saved in a plain text format.

    By default : false.

    Supported versions: IS 5.6.0 onwards.

       -->

    <EnableClientSecretHash>false</EnableClientSec
    retHash>
```

Tip: Use a fresh server to enable hashing.

Add the following configurations within the `<EventListeners>` tag.

```
<!-- Audit Loggers -->

<!-- Old Audit Logger -->

<EventListener
type="org.wso2.carbon.user.core.listener.UserO
perationEventListener"


name="org.wso2.carbon.user.mgt.listeners.UserM
gtAuditLogger"

                        orderId="0"
enable="false"/>

<!-- New Audit Loggers-->

<EventListener
type="org.wso2.carbon.user.core.listener.UserO
perationEventListener"


name="org.wso2.carbon.user.mgt.listeners.UserM
anagementAuditLogger"

                        orderId="1"
enable="true"/>

<EventListener
type="org.wso2.carbon.user.core.listener.UserM
anagementErrorEventListener"
```

```
name="org.wso2.carbon.user.mgt.listeners.UserMgtFailureAuditLogger"
                        orderId="0"
enable="true"/>
```

Add the following properties related to the validitating JWT based on JWKS capability. For more information, see Validating JWT based on JWKS.

```
<!-- JWT validator configurations -->
<JWTValidatorConfigs>
    <Enable>true</Enable>
    <JWKSEndpoint>

<HTTPConnectionTimeout>1000</HTTPConnectionTimeout>

<HTTPReadTimeout>1000</HTTPReadTimeout>
        <HTTPSizeLimit>51200</HTTPSizeLimit>
    </JWKSEndpoint>
</JWTValidatorConfigs>
```

If you are using SCIM 1.1, disable the following SCIM 2.0 event listener.

```
<EventListener
type="org.wso2.carbon.user.core.listener.UserO
perationEventListener"


name="org.wso2.carbon.identity.scim2.common.li
stener.SCIMUserOperationListener"

                        orderId="93"
enable="false"/>
```

If you are using SCIM 2.0, disable the following SCIM 1.1 event listener (this listener is disabled by default in 5.6.0).

```
<EventListener
type="org.wso2.carbon.user.core.listener.UserO
perationEventListener"


name="org.wso2.carbon.identity.scim.common.lis
tener.SCIMUserOperationListener"

                        orderId="90"
enable="false"/>
```

`oidc-scope-config.xml` file stored in the `<IS_HOME>/repository/conf/identity` folder.	Append the values "upn" and "groups" to the comma separated list within the `<Scope id="openid"><Claim>` element. `<Claim>` `sub,email,email_verified,name,family_name,given_name,middle_name,nickname,preferred_username,upn,groups,profile,picture,website,gender,birthdate,zoneinfo,locale,updated_at,phone_number,phone_number_verified,address,street_address,country,formatted,postal_code,locality,region` `</Claim>` These are MP-JWT supported claims. The MP-JWT 1.0 specification has introduced two claims; namely "upn" and "groups", which are mandatory to generate a JWT token that is supported by the MicroProfile JWT authentication framework.
catalina-server.xml file stored in the `<IS_HOME>/repository/conf/tomcat` folder.	Disable the following properties by setting the relevant properties to false to avoid displaying unneccessary information.

	<!--Error pages --> <Valve className="org.apache.catalina.valves.ErrorRep ortValve" showServerInfo="false" showReport="false"/>

claim-config.xml file stored in the <IS_HOME>/repository/conf/ folder.	Add the following claims within the <Dialect dialectURI="http://wso2.org/claims"> dialect tag. ``` <Claim> <ClaimURI>http://wso2.org/claims/userprincipal</ClaimURI> <DisplayName>User Principal</DisplayName> <AttributeID>uid</AttributeID> <Description>User Principal</Description> </Claim> <Claim> <ClaimURI>http://wso2.org/claims/extendedRef</ClaimURI> <DisplayName>Extended Ref</DisplayName> <!-- Proper attribute Id in your user store must be configured for this --> <AttributeID>extendedRef</AttributeID> <Description>Extended Ref</Description> ```

```
    </Claim>

    <Claim>


    <ClaimURI>http://wso2.org/claims/extendedDispl
    ayName</ClaimURI>

        <DisplayName>Extended Display
    Name</DisplayName>

        <!-- Proper attribute Id in your user
    store must be configured for this -->


    <AttributeID>extendedDisplayName</AttributeID>

        <Description>Extended Display
    Name</Description>

    </Claim>

    <Claim>


    <ClaimURI>http://wso2.org/claims/costCenter</C
    laimURI>

        <DisplayName>Cost Center</DisplayName>

        <!-- Proper attribute Id in your user
    store must be configured for this -->

        <AttributeID>costCenter</AttributeID>
```

```
        <Description>Cost Center</Description>

    </Claim>

    <Claim>


    <ClaimURI>http://wso2.org/claims/extendedExter
    nalId</ClaimURI>

        <DisplayName>Extended External
    ID</DisplayName>

        <!-- Proper attribute Id in your user
    store must be configured for this -->


    <AttributeID>extendedExternalId</AttributeID>

        <Description>Extended External
    ID</Description>

    </Claim>
```

Add the following claims within the `<Dialect dialectURI="http://wso2.org/oidc/claim">` dialect tag.

```
<Claim>

    <ClaimURI>upn</ClaimURI>

    <DisplayName>User Principal</DisplayName>

    <AttributeID>uid</AttributeID>

    <Description>The user principal
name</Description>

    <DisplayOrder>11</DisplayOrder>

    <SupportedByDefault />


<MappedLocalClaim>http://wso2.org/claims/userp
rincipal</MappedLocalClaim>

</Claim>

<Claim>

    <ClaimURI>groups</ClaimURI>

    <DisplayName>User Groups</DisplayName>

    <AttributeID>role</AttributeID>

    <Description>List of group names that have
been assigned to the principal. This typically
will require a mapping at the application
```

```
container level to application deployment
roles.</Description>

    <DisplayOrder>12</DisplayOrder>

    <SupportedByDefault />


<MappedLocalClaim>http://wso2.org/claims/role<
/MappedLocalClaim>

</Claim>
```

Add the following claims within the `<Dialect dialectURI="urn:ietf:params:scim:schemas:core:2.0:User">` dialect tag.

```
<Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.
0:User:emails</ClaimURI>
    <DisplayName>Emails</DisplayName>
    <AttributeID>mail</AttributeID>
    <Description>Email Addresses</Description>
    <DisplayOrder>5</DisplayOrder>
    <SupportedByDefault />

<RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+
\.)+([a-zA-Z0-9]{2,4})+$</RegEx>

<MappedLocalClaim>http://wso2.org/claims/email
address</MappedLocalClaim>
</Claim>
<Claim>

<ClaimURI>urn:ietf:params:scim:schemas:core:2.
0:User:phoneNumbers</ClaimURI>
    <DisplayName>Phone Numbers</DisplayName>
```

```
        <AttributeID>phoneNumbers</AttributeID>

        <Description>Phone Numbers</Description>

        <DisplayOrder>5</DisplayOrder>

        <SupportedByDefault/>


    <RegEx>^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+
    \.)+([a-zA-Z0-9]{2,4})+$</RegEx>


    <MappedLocalClaim>http://wso2.org/claims/phone
    Numbers</MappedLocalClaim>

    </Claim>

    <Claim>


    <ClaimURI>urn:ietf:params:scim:schemas:core:2.
    0:User:photos</ClaimURI>

        <DisplayName>Photo</DisplayName>

        <AttributeID>photos</AttributeID>

        <Description>Photo</Description>

        <DisplayOrder>5</DisplayOrder>

        <SupportedByDefault />
```

```
<MappedLocalClaim>http://wso2.org/claims/photo
s</MappedLocalClaim>

</Claim>

<Claim>


<ClaimURI>urn:ietf:params:scim:schemas:core:2.
0:User:addresses</ClaimURI>

    <DisplayName>Address</DisplayName>

    <AttributeID>addresses</AttributeID>

    <Description>Address</Description>

    <DisplayOrder>5</DisplayOrder>

    <SupportedByDefault />


<MappedLocalClaim>http://wso2.org/claims/addre
sses</MappedLocalClaim>

</Claim>
```

Replace the following property values within the urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber claim URI.

```
<Claim>

<ClaimURI>urn:ietf:params:scim:schemas:extensi
on:enterprise:2.0:User:employeeNumber</ClaimUR
I>

    <DisplayName>Employee Number</DisplayName>

<AttributeID>extendedExternalId</AttributeID>

    <Description>Employee Number</Description>

    <Required />

    <DisplayOrder>1</DisplayOrder>

    <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/exten
dedExternalId</MappedLocalClaim>

</Claim>
```

Replace the following property values within the urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:costCenter claim URI.

```
<Claim>

<ClaimURI>urn:ietf:params:scim:schemas:extens
ion:enterprise:2.0:User:costCenter</ClaimURI>
    <DisplayName>Cost Center</DisplayName>
    <AttributeID>costCenter</AttributeID>
    <Description>Cost Center</Description>
    <Required />
    <DisplayOrder>1</DisplayOrder>
    <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/cost
Center</MappedLocalClaim>
</Claim>
```

Replace the following property values within the `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager.$ref` claim URI.

```
<Claim>

<ClaimURI>urn:ietf:params:scim:schemas:extensi
on:enterprise:2.0:User:manager.$ref</ClaimURI>
    <DisplayName>Manager - home</DisplayName>
    <AttributeID>extendedRef</AttributeID>
    <Description>Manager - home</Description>
    <Required />
    <DisplayOrder>1</DisplayOrder>
    <SupportedByDefault />

<MappedLocalClaim>http://wso2.org/claims/exten
dedRef</MappedLocalClaim>
</Claim>
```

Replace the following property values within the `urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager.displayName` claim URI.

```
<Claim>


<ClaimURI>urn:ietf:params:scim:schemas:extensi
on:enterprise:2.0:User:manager.displayName</Cl
aimURI>

    <DisplayName>Manager - Display
Name</DisplayName>


<AttributeID>extendedDisplayName</AttributeID>

    <Description>Manager - Display
Name</Description>

    <Required />

    <DisplayOrder>1</DisplayOrder>

    <SupportedByDefault />


<MappedLocalClaim>http://wso2.org/claims/exten
dedDisplayName</MappedLocalClaim>

</Claim>
```

Add the following claims within the root tag. This new claim dialect and the claims within it are required for eiDAS.

For more information, see eIDAS SAML Attribute Profile Support via WSO2 Identity Server.

```
<Dialect
dialectURI="http://eidas.europa.eu/attributes/naturalperson">
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier</ClaimURI>
        <DisplayName>Person Identifier</DisplayName>
        <AttributeID>scimId</AttributeID>
        <Description>Person Identifier</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/userid</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName</ClaimURI>
        <DisplayName>Current Family Name</DisplayName>
        <AttributeID>sn</AttributeID>
        <Description>Current Family Name</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/lastname</MappedLocalClaim>
    </Claim>
```

```
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName</ClaimURI>
        <DisplayName>Current Given Name</DisplayName>
        <AttributeID>givenName</AttributeID>
        <Description>Current Given Name</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/givenname</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/DateOfBirth</ClaimURI>
        <DisplayName>Date of birth</DisplayName>
        <AttributeID>dateOfBirth</AttributeID>
        <Description>Date of birth</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/dob</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalperson/BirthName</ClaimURI>
        <DisplayName>Birth Name</DisplayName>
        <AttributeID>uid</AttributeID>
        <Description>Birth Name</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
```

```
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/username</Mapp
edLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalpers
on/PlaceOfBirth</ClaimURI>
        <DisplayName>Place of Birth</DisplayName>
        <AttributeID>country</AttributeID>
        <Description>Place of Birth</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/country</Mappe
dLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalpers
on/CurrentAddress</ClaimURI>
        <DisplayName>Current Address</DisplayName>
        <AttributeID>localityAddress</AttributeID>
        <Description>Current Address</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/addresses</Map
pedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/naturalpers
on/Gender</ClaimURI>
```

```
        <DisplayName>Gender</DisplayName>
        <AttributeID>gender</AttributeID>
        <Description>Gender</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/gender</Mapped
LocalClaim>
    </Claim>
</Dialect>
<Dialect
dialectURI="http://eidas.europa.eu/attributes/legalpers
on">
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson
/LegalPersonIdentifier</ClaimURI>
        <DisplayName>Legal Person
Identifier</DisplayName>
        <AttributeID>extendedExternalId</AttributeID>
        <Description>Legal Person
Identifier</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/extendedExtern
alId</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson
/LegalName</ClaimURI>
        <DisplayName>Legal Person Name</DisplayName>
        <AttributeID>extendedDisplayName</AttributeID>
        <Description>Legal Person Name</Description>
```

```
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/extendedDisplayName</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress</ClaimURI>
        <DisplayName>Legal Person Address</DisplayName>
        <AttributeID>localityAddress</AttributeID>
        <Description>Legal Person Address</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/addresses</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson/VATRegistrationNumber</ClaimURI>
        <DisplayName>VAT Registration
Number</DisplayName>
        <AttributeID>im</AttributeID>
        <Description>VAT Registration
Number</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/im</MappedLocalClaim>
    </Claim>
```

```
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson
/TaxReference</ClaimURI>
        <DisplayName>Tax Reference</DisplayName>
        <AttributeID>postalcode</AttributeID>
        <Description>Tax Reference</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/postalcode</Ma
ppedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson
/D-2012-17-EUIdentifier</ClaimURI>
        <DisplayName>EU Identifier</DisplayName>
        <AttributeID>externalId</AttributeID>
        <Description>EU Identifier</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/externalid</Ma
ppedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson
/LEI</ClaimURI>
        <DisplayName>LEI</DisplayName>
        <AttributeID>extendedRef</AttributeID>
        <Description>LEI</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
```

```
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/extendedRef</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson/EORI</ClaimURI>
        <DisplayName>Economic Operator Registration and Identification</DisplayName>
        <AttributeID>departmentNumber</AttributeID>
        <Description>Economic Operator Registration and Identification</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/department</MappedLocalClaim>
    </Claim>
    <Claim>

<ClaimURI>http://eidas.europa.eu/attributes/legalperson/SEED</ClaimURI>
        <DisplayName>System for Exchange of Excise Data Identifier</DisplayName>
        <AttributeID>nickName</AttributeID>
        <Description>System for Exchange of Excise Data Identifier</Description>
        <Required/>
        <DisplayOrder>1</DisplayOrder>
        <SupportedByDefault/>

<MappedLocalClaim>http://wso2.org/claims/nickname</MappedLocalClaim>
```

	`` </Claim> <Claim> <ClaimURI>http://eidas.europa.eu/attributes/legalperson/SIC</ClaimURI> <DisplayName>Standard Industrial Classification</DisplayName> <AttributeID>nickName</AttributeID> <Description>Standard Industrial Classification</Description> <Required/> <DisplayOrder>1</DisplayOrder> <SupportedByDefault/> <MappedLocalClaim>http://wso2.org/claims/nickname</MappedLocalClaim> </Claim> </Dialect> ```

Recommended: See the WSO2 IS 5.6.0 migration guide for more information.

5.6.0 to 5.7.0

`carbon.xml` file stored in the `<IS_HOME>/repository/conf` directory.	Change the version property value to 5.7.0. ``` <Version>5.7.0</Version> ```

`axis2.xml` file stored in the `<IS_HOME>/repository/conf/axis2` directory.	Change the following property values to 5.7.0. `<parameter name="userAgent" locked="true">` `WSO2 Identity Server-5.7.0` `</parameter>` `<parameter name="server" locked="true">` `WSO2 Identity Server-5.7.0` `</parameter>`
application-authentication.xml file stored in the `<IS_HOME>/repository/conf/identity` directory.	Under `<Extensions>`, do the following changes to enable adaptive authentication: - Change the value of `<StepBasedSequenceHandler>` from `org.wso2.carbon.identity.application.authentication.framework.handler.sequence.impl.DefaultStepBasedSequenceHandler` to `org.wso2.carbon.identity.application.authentication.framework.handler.sequence.impl.GraphBasedSequenceHandler`. - Change the value of `<StepHandler>` from `org.wso2.carbon.identity.application.authentication.f`

	ramework.handler.step.impl.DefaultStepHandler to org.wso2.carbon.identity.application.authentication.framework.handler.step.impl.GraphBasedStepHandler.
	Add the following configuration under <AuthenticatorConfigs>: `<AuthenticatorConfig name="IdentifierExecutor" enabled="true">` `<Parameter name="ValidateUsername">false</Parameter>` `</AuthenticatorConfig>`
identity.xml file stored in the <IS_HOME>/repository/conf/identity directory.	Add the following configuration under <OAuth>: `<!-- Token cleanup feature config to clean IDN_OAUTH2_ACCESS_TOKEN table-->` `<TokenCleanup>` `<!--If true old access token cleaning feature is enabled -->` `<EnableTokenCleanup>true</EnableTokenCleanup>` `<!--If true old access token retained in audit table -->` `<RetainOldAccessToken>true</RetainOldAccessToken>`

	`</TokenCleanup>` This configuration is required to clean the `IDN_OAUTH2_ACCESS_TOKEN` table.
	Under `<OAuth>`, change the value of `<OAuth2DCREPUrl>` from `${carbon.protocol}://${carbon.host}:${carbon.management.port}/api/identity/oauth2/dcr/v1.0/register` to `${carbon.protocol}://${carbon.host}:${carbon.management.port}/api/identity/oauth2/dcr/v1.1/register`. This reflects the DCR version update.
	Do the following changes under <SupportedResponseTypes> to replace the deprecated `TokenResponseTypeHandler` class: - Change `<SupportedResponseType><ResponseTypeHandlerImplClass>org.wso2.carbon.identity.oauth2.authz.handlers.TokenResponseTypeHandler</ResponseTypeHandlerImplClass>` to `<SupportedResponseType><ResponseTypeHandlerImplClass>org.wso2.carbon.identity.oauth2.authz.handlers.AccessTokenResponseTypeHandler</ResponseTypeHandlerImplClass>`. - Change `<SupportedResponseType><ResponseTypeHandlerImplClass>org.wso2.carbon.identity.oauth2.authz.handlers.TokenResponseTypeHandler</ResponseTypeHandlerImplClass>` to `<SupportedResponseType><ResponseTypeHandlerImplClass>org.wso2.carbon.identity.oauth2.authz.handlers.IDTokenResponseTypeHandler</ResponseTypeHandlerImplClass>`. - Change `<SupportedResponseType><ResponseTypeHandlerImplClass>`

	`org.wso2.carbon.identity.oauth2.authz.handlers.TokenResponseTypeHandler</ResponseTypeHandlerImplClass>` to `<SupportedResponseType><ResponseTypeHandlerImplClass>org.wso2.carbon.identity.oauth2.authz.handlers.IDTokenTokenResponseTypeHandler</ResponseTypeHandlerImplClass>`.
	Under `<SSOService>`, add the following SAML2 artifact validity period configuration: `<SAML2ArtifactValidityPeriodInMinutes>4</SAML2ArtifactValidityPeriodInMinutes>`
	Under `<SCIM>`, add the following configuration that allows you to get all the details of a user from SCIM endpoint if necessary: `<ShowAllUserDetails>false</ShowAllUserDetails>`

Add the following configuration that is introduced to support filtering roles when you have configured a service provider role mapping:

```
<!--

        This configuration is used to filter the SP configured
role mappings. If the property value is,



        true : If SP role mappings are configured, returns only
the mapped SP roles. If SP role mappings are not

        configured returns all the mapped local roles.



        false : If SP role mappings are configured, returns
mapped SP roles for the mapped roles and the local mapped

        roles for others. If SP role mappings are not
configured returns all the mapped local roles.



        Default - false.

    -->



   <!--SPRoleManagement>
```

```
<ReturnOnlyMappedLocalRoles>false</ReturnOnlyMappedLocalRoles>

    </SPRoleManagement-->
```

Add the following configuration that allows you to customize the default user interfaces displayed at the time of just-in-time provisioning:

```
<JITProvisioning>

<UserNameProvisioningUI>/accountrecoveryendpoint/register.do</UserNameProvisioningUI>

<PasswordProvisioningUI>/accountrecoveryendpoint/signup.do</PasswordProvisioningUI>

</JITProvisioning>
```

Add the following configuration to include post authentication handlers introduced via JIT provisioning improvements:

```
<!-- Post Authentication handlers for JIT provisioning,
association and for handling subject identifier -->

<EventListener
type="org.wso2.carbon.identity.core.handler.AbstractIdentityHand
ler"


name="org.wso2.carbon.identity.application.authentication.framew
ork.handler.request.impl.JITProvisioningPostAuthenticationHandle
r"

                        orderId="20" enable="true"/>

<EventListener
type="org.wso2.carbon.identity.core.handler.AbstractIdentityHand
ler"


name="org.wso2.carbon.identity.application.authentication.framew
ork.handler.request.impl.PostAuthAssociationHandler"

                        orderId="25" enable="true"/>

<EventListener
type="org.wso2.carbon.identity.core.handler.AbstractIdentityHand
ler"


name="org.wso2.carbon.identity.application.authentication.framew
```

	ork.handler.request.impl.PostAuthenticatedSubjectIdentifierHandler" orderId="30" enable="true"/>

Do the following changes under `<ResourceAccessControl>`: - To reflect the changes introduced via security advisory WSO2-2018-0462, replace the following set of resources

```
<Resource context="(.*)/api/identity/user/v1.0/validate-code"
secured="true" http-method="all"/>

<Resource context="(.*)/api/identity/user/v1.0/resend-code"
secured="true" http-method="all"/>

<Resource context="(.*)/api/identity/user/v1.0/me"
secured="true" http-method="POST"/>

<Resource context="(.*)/api/identity/user/v1.0/me"
secured="true" http-method="GET"/>




<Resource
context="(.*)/api/identity/consent-mgt/v1.0/consents/purposes"
secured="true" http-method="POST">

<Resource
context="(.*)/api/identity/consent-mgt/v1.0/consents/pii-categor
ies" secured="true" http-method="POST">

<Resource
context="(.*)/api/identity/consent-mgt/v1.0/consents/purpose-cat
egories" secured="true" http-method="POST">
```

```
<Resource context="(.*)/scim2/Users" secured="true"
http-method="POST">

<Resource context="(.*)/scim2/Groups" secured="true"
http-method="POST">

<Resource context="/scim2/Bulk" secured="true"
http-method="all">
```

with the following:

```
<Resource
context="(.*)/api/identity/user/v1.0/validate-code(.*)"
secured="true" http-method="all">


<Permissions>/permission/admin/manage/identity/identitymgt</Per
missions></Resource>

<Resource context="(.*)/api/identity/user/v1.0/resend-code(.*)"
secured="true" http-method="all"/>

<Resource context="(.*)/api/identity/user/v1.0/me(.*)"
secured="true" http-method="POST"/>

<Resource context="(.*)/api/identity/user/v1.0/me(.*)"
secured="true" http-method="GET"/>
```

```
<Resource
context="(.*)/api/identity/consent-mgt/v1.0/consents/purposes(.
*)" secured="true" http-method="POST"/>

<Resource
context="(.*)/api/identity/consent-mgt/v1.0/consents/pii-catego
ries(.*)" secured="true" http-method="POST"/>

<Resource
context="(.*)/api/identity/consent-mgt/v1.0/consents/purpose-ca
tegories(.*)" secured="true" http-method="POST"/>




<Resource context="(.*)/scim2/Users(.*)" secured="true"
http-method="POST"/>

<Resource context="(.*)/scim2/Groups(.*)" secured="true"
http-method="POST"/>

<Resource context="(.*)/scim2/Bulk(.*)" secured="true"
http-method="all"/>
```

- Replace `<Resource context="(.*)/api/identity/recovery/(.*)"`

	secured="true" http-method="all"/> with the following resource: `<Resource context="(.*)/api/identity/recovery/(.*)" secured="true" http-method="all">` `<Permissions>/permission/admin/manage/identity/identitymgt</Permissions>` `</Resource>` This introduces changes done with regard to access permission for account recovery endpoint. - Add the following resource that allows using /api/identity/auth/ to retrieve data from authentication endpoint itself instead of obtaining via the URL: `<Resource context="(.*)/api/identity/auth/(.*)" secured="true" http-method="all"/>` - To reflect the DCR version upgrade, replace the following set of resources

```
<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/register(.*)"
secured="true" http-method="POST">


<Permissions>/permission/admin/manage/identity/applicationmgt/cr
eate</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/register(.*)"
secured="true" http-method="DELETE">


<Permissions>/permission/admin/manage/identity/applicationmgt/de
lete</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/register(.*)"
secured="true" http-method="PUT">


<Permissions>/permission/admin/manage/identity/applicationmgt/up
date</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.0/register(.*)"
secured="true" http-method="GET">
```

```
<Permissions>/permission/admin/manage/identity/applicationmgt/vi
ew</Permissions>

</Resource>
```

with the following:

```
<Resource
context="(.*)/api/identity/oauth2/dcr/v1.1/register(.*)"
secured="true" http-method="POST">


<Permissions>/permission/admin/manage/identity/applicationmgt/cr
eate</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.1/register(.*)"
secured="true" http-method="DELETE">


<Permissions>/permission/admin/manage/identity/applicationmgt/de
lete</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.1/register(.*)"
secured="true" http-method="PUT">
```

```
<Permissions>/permission/admin/manage/identity/applicationmgt/update</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/oauth2/dcr/v1.1/register(.*)"
secured="true" http-method="GET">


<Permissions>/permission/admin/manage/identity/applicationmgt/view</Permissions>

</Resource>
```

Add the following property that was introduced to restrict federated user association done via the `UserProfileAdmin` admin service:

```
<!--

This property restricts federated user association done
through UserProfileAdmin admin service.

Would not affect associations done through provisioning

-->

<EnableFederatedUserAssociation>false</EnableFederatedUserAsso
ciation>
```

	Under `<TenantContextsToRewrite> <WebApp>`, replace `<Context>/api/identity/oauth2/dcr/v1.0/</Context>` with `<Context>/api/identity/oauth2/dcr/v1.1/</Context>` to reflect the DCR version upgrade.
	Under `<AdaptiveAuth><EventPublisher>`, replace `<receiverURL>`http://localhost:8280/`>` with the following configuration: `<ReceiverURL>https://localhost:8280/</ReceiverURL>` `<BasicAuthentication>` `<Enable>true</Enable>` `<Username>admin</Username>` `<Password>admin</Password>` `</BasicAuthentication>` This introduces the default configurations for event publisher.

	Under `<AdaptiveAuth>`, add the following configurations introduced to support external analytics calls in adaptive authentication: `<MaxTotalConnections>20</MaxTotalConnections>` `<MaxTotalConnectionsPerRoute>20</MaxTotalConnectionsPerRoute>` `<!--Timeouts in milliseconds-->` `<!--Default configs for timeouts-->` `<!--<HTTPConnectionTimeout>5000</HTTPConnectionTimeout>-->` `<!--<HTTPReadTimeout>5000</HTTPReadTimeout>-->` `<!--<HTTPConnectionRequestTimeout>5000</HTTPConnectionRequestTimeout>-->` `<!--End of default configs for timeouts-->` `<!--<RefreshInterval>500</RefreshInterval>-->` `<!--End of timeouts in milliseconds-->` `<!--<PromptOnLongWait>false</PromptOnLongWait>-->`

	<!--Timeout in milliseconds for the waiting external calls--> <LongWaitTimeout>10000</LongWaitTimeout>
`carbon.xml` file stored in the `<IS_HOME>/repository/conf` directory.	Add the following configuration that introduces parameters related to Carbon Crypto Service, which is a crypto framework used inside Carbon products: <!-- Configurations related to Carbon Crypto Service which is a crypto framework used inside Carbon products. --> <CryptoService> <Enabled>true</Enabled> <!-- The crypto provider which is used for internal data encryption and decryption --> <InternalCryptoProviderClassName>org.wso2.carbon.crypto.provider.KeyStoreBasedInternalCryptoProvider</InternalCryptoProviderClassName>

```
 <!--

   The crypto provider which is used for the crypto needs
which come when communicating with external parties.

   e.g. Signing, Decrypting.

 -->


<ExternalCryptoProviderClassName>org.wso2.carbon.core.encrypt
ion.KeyStoreBasedExternalCryptoProvider</ExternalCryptoProvid
erClassName>

 <!--

   The list of key resolvers which will be used based on the
context when handling crypto with external parties.

   e.g. Resolving the public key of an external entity.

 -->

 <KeyResolvers>

    <KeyResolver
className="org.wso2.carbon.crypto.defaultProvider.resolver.Co
ntextIndependentKeyResolver" priority="-1"/>

 </KeyResolvers>
```

```
  </CryptoService>
```

Under <Security>, add the following keystore parameters introduced to encrypting/decrypting internal data:

```
  <!--

    The KeyStore which is used for encrypting/decrypting
  internal data.

    This block is read by Carbon Crypto Service.

  -->

  <InternalKeyStore>

    <!-- Keystore file location-->


  <Location>${carbon.home}/repository/resources/security/wso2ca
  rbon.jks</Location>

    <!-- Keystore type (JKS/PKCS12 etc.)-->

    <Type>JKS</Type>

    <!-- Keystore password-->

    <Password>wso2carbon</Password>
```

	<!-- Private Key alias--> <KeyAlias>wso2carbon</KeyAlias> <!-- Private Key password--> <KeyPassword>wso2carbon</KeyPassword> </InternalKeyStore>
`log4j.properties` file stored in the `<IS_HOME>/repository/conf` directory.	Add the following lines that include the properties introduced to support masking sensitive information in your logs: # Log masking configuration. Please uncomment the following log4j property, if you need to mask any # information in your carbon logs. # When enabled, the logs will be matched with the provided patterns and masked . # The 'path-to-masking-patterns' path should be an absolute file path to a properties file. This file should contain # the patterns that should be checked for masking as key value pairs. (mask-name=masking-regex-pattern) # If this file cannot be found, wso2-log-masking.properties file will be used as default. If the following

```
# configuration is not enabled, no masking process will be
applied.

#log4j.appender.CARBON_CONSOLE.maskingPatternFile=path-to-m
asking-patterns




# Log masking configuration. Please uncomment the following
log4j property, if you need to mask any

# information in your carbon logs.

# When enabled, the logs will be matched with the  provided
patterns and masked .

# The 'path-to-masking-patterns' path should be an absolute
file path to a properties file. This file should contain

# the patterns that should be checked for masking as key
value pairs. (mask-name=masking-regex-pattern)

# If this file cannot be found, wso2-log-masking.properties
file will be used as default. If the following

# configuration is not enabled, no masking process will be
applied.

#log4j.appender.CARBON_LOGFILE.maskingPatternFile=path-to-m
asking-patterns
```

Recommended: See the WSO2 IS 5.7.0 migration guide for more information.

5.7.0 to 5.8.0

Configuration File	Changes
`carbon.xml` file stored in the `<IS_HOME>/repository/conf` directory.	The version property value has been changed to 5.8.0. `<Version>5.8.0</Version>` **Why?** This property indicates the version of WSO2 IS.
`axis2.xml` file stored in the `<IS_HOME>/repository/conf/axis2` directory.	The following property values have been changed to 5.8.0. `<parameter name="userAgent" locked="true">` `WSO2 Identity Server-5.8.0` `</parameter>` `<parameter name="server" locked="true">`

	WSO2 Identity Server-5.8.0 </parameter> The following property has been added. <parameter name="forceIncludeNullElements">false</parameter> **Why?** Enabling this property forces elements that have the `@IgnoreNullElement` annotation to be returned as well even though the value is null. The default value for this property is 'false'.
Endpointconfig.properties file stored in the `<IS_HOME>/repository/conf/iden`	The following property has been added. mutualSSLManagerEnabled=true **Why?**

`tity` directory.	Enabling this property allows the `MutualSSLManager` to initialize the keystores. If it is set to 'false', the `MutualSSLManager` will not initialize the keystore.
`application-authentication.xml` file stored in the `<IS_HOME>/repository/conf/identity` directory.	The following property has been added to the following authenticators under the relevant tags. • BasicAuthenticator - <AuthenticatorConfig name="BasicAuthenticator" enabled="true"> • BasicAuthRequestPathAuthenticator - `<AuthenticatorConfig name="BasicAuthRequestPathAuthenticator" enabled="true">` `<Parameter name="AuthMechanism">basic</Parameter>` **Why?** This property is used to help identify the authentication mechanism used by the authenticator.

	The following parameters were added under the `<AuthenticatorConfig name="EmailOTP" enabled="true">` tag. `<Parameter name="EMAILOTPAuthenticationEndpointURL">emailotpauthenticationendpoint/emailotp.jsp</Parameter>` `<Parameter name="EmailOTPAuthenticationEndpointErrorPage">emailotpauthenticationendpoint/emailotpError.jsp</Parameter>` `<Parameter name="EmailAddressRequestPage">emailotpauthenticationendpoint/emailAddress.jsp</Parameter>` **Why?** The following parameters make the Email OTP URLs configurable.
	The `totp` authenticator configurations were uncommented and the following parameters have been added under the `<AuthenticatorConfig name="totp" enabled="true">` tag.

	``<Parameter name="Issuer">WSO2</Parameter>``` ```<Parameter name="UseCommonIssuer">true</Parameter>``` **Why?** The added parameters make the `totp` issuer configurable instead of showing the domain name.
	The following parameter has been removed from the totp authenticator as it is redundant. ```<Parameter name="redirectToMultiOptionPageOnFailure">false</Parameter>```

	The following property has been added under the `<ApplicationAuthentication>` tag. `<!--Similar to the 'AuthenticationEndpointQueryParams' above, the following section defines the parameters that should be included/excluded in the redirection responses from authentication framework. These parameters may be generated internally from the framework, handlers or authenticators. The filtered parameters will be available via the REST API for authentication framework. "removeOnConsumeFromAPI" defines whether to make the filtered parameters unavailable from the API on the first consumption. -->`  `<AuthenticationEndpointRedirectParams action="exclude" removeOnConsumeFromAPI="true">`  `<AuthenticationEndpointRedirectParam name="loggedInUser"/>`  `</AuthenticationEndpointRedirectParams>`

`captcha-config.properties` file stored in the `<IS_HOME>/repository/conf/identity` directory.	The following properties have been added. ``` #reCaptcha failed redirect urls #recaptcha.failed.redirect.urls= ``` **Why?** The properties listed above allow configuring the list of URLs that can be used for redirection when reCaptcha fails.
`scim2-schema-extension.config` file stored in the <IS_HOME>/repository/conf/ directory.	The urn:ietf:params:scim:schemas:extension:enterprise:2.0:User attribute name has been changed from what is reflected in the 5.7.0 code block to the configuration shown in the 5.8.0 code block. **5.7.0** ``` "attributeURI":"urn:ietf:params:scim:schemas:extension :enterprise:2.0:User", ```

	`"attributeName":"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",` **5.8.0** `attributeURI":"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",` `"attributeName":"urn:ietf:params:scim:schemas:extension:enterprise:2.0:User"` **Why?** This change is done in order to comply with the SCIM2 specification. For more details, see behavioral change #1 in the behavioral changes table given above.
`identity-event.properties` file stored in the `<IS_HOME>/repository`	The password policy error message has been modified as follows. `passwordPolicy.errorMsg='Password pattern policy violated. Password should contain a digit[0-9], a lower case letter[a-z], an upper case letter[A-Z], and one of !@#$%&* characters'`

`/conf/identity` directory.	The following handlers have been added. ``` module.name.17=SAMLLogoutHandler SAMLLogoutHandler.subscription.1=SESSION_TERMINATE SAMLLogoutHandler.enable=true # To delete registration code in database once the user deletion module.name.18=confirmationCodesInvalidate confirmationCodesInvalidate.subscription.1=POST_DELETE_USER ``` **Why?** These handlers are introduced to support the cross-protocol logout feature and for migration of existing data publishers to event handlers that subscribe to authentication events. For more information about migrating existing data publishers to

	event handlers, see see Migrating Data Publishers on the Migration doc.
	The following properties were added. `module.name.14=analyticsLoginDataPublisher` `analyticsLoginDataPublisher.subscription.1=AUTHENTICATION_STEP_SUCCESS` `analyticsLoginDataPublisher.subscription.2=AUTHENTICATION_STEP_FAILURE` `analyticsLoginDataPublisher.subscription.3=AUTHENTICATION_SUCCESS` `analyticsLoginDataPublisher.subscription.4=AUTHENTICATION_FAILURE` `analyticsLoginDataPublisher.enable=false` `module.name.15=analyticsSessionDataPublisher` `analyticsSessionDataPublisher.subscription.1=SESSION_CREATE`

```
analyticsSessionDataPublisher.subscription.2=SESSION_UPDATE



analyticsSessionDataPublisher.subscription.3=SESSION_TERMINATE

analyticsSessionDataPublisher.enable=true



module.name.13=authenticationAuditLogger

authenticationAuditLogger.subscription.1=AUTHENTICATION_STEP_SUCCESS

authenticationAuditLogger.subscription.2=AUTHENTICATION_STEP_FAILURE

authenticationAuditLogger.subscription.3=AUTHENTICATION_SUCCESS

authenticationAuditLogger.subscription.4=AUTHENTICATION_FAILURE

authenticationAuditLogger.subscription.5=SESSION_TERMINATE
```

	authenticationAuditLogger.enable=true" module.name.16=failLoginAttemptValidator failLoginAttemptValidator.subscription.1=AUTHENTICATION_STEP_FAILURE failLoginAttemptValidator.enable=true **Why?** The properties listed above are added to support the event listeners that were added for migrating data publishers to event handlers. For more details, see behavioral change #3 in the behavioral changes table given above.
`identity.xml` file stored in the `<IS_HOME>/repository/conf/iden`	The following property has been added to the `IntrospectionDataProvider` interface. <Introspection> <EnableDataProviders>false</EnableDataProviders>

`tity` directory.	`</Introspection>` **Why?** This property is used to inject additional data to the introspection response.
	The default `CleanUpPeriod` value has been modified to 1440. `<CleanUpPeriod>1440</CleanUpPeriod>`
	The default value of the following property has been changed from false to **true**. `<SignJWTWithSPKey>true</SignJWTWithSPKey>` **Why?** For details about this change, see behavioral change #2 in the behavioral changes table given above.

	The following property has been added under the `<SessionDataPersist>` tag. `<UserSessionMapping>` `  <Enable>true</Enable>` `</UserSessionMapping>` **Why?** This property enables terminating all the active sessions of a user during password reset, user deletion, and username renaming.

	The following event listeners have been removed. ``` <EventListener type="org.wso2.carbon.identity.core.handler.AbstractIdentityMessageHandler" name="org.wso2.carbon.identity.data.publisher.application.authentication.impl.DASLoginDataPublisherImpl" orderId="10" enable="true"/> <EventListener type="org.wso2.carbon.identity.core.handler.AbstractIdentityMessageHandler" name="org.wso2.carbon.identity.data.publisher.application.authentication.impl.DASSessionDataPublisherImpl" orderId="11" enable="true"/> <EventListener type="org.wso2.carbon.identity.core.handler.AbstractIdentityMessageHandler" name="org.wso2.carbon.identity.captcha.validator.FailLoginAttemptValidator" orderId="10" enable="true"/> ``` **Why?**

	From WSO2 IS 5.8.0 onwards, data publishers are migrated to act as event handlers that subscribe to authentication events. Hence, the event listeners listed above have been removed by default. For more details, see behavioral change #3 in the behavioral changes table given above.
	The following property has been added. `<FilterUsersAndGroupsOnlyFromPrimaryDomain>false</FilterUsersAndGroupsOnlyFromPrimaryDomain>` **Why?** Enabling this property filters users or groups only from the PRIMARY user store, regardless of the Users and Groups endpoints. If it is set to 'false' it filters users or groups across all user stores.

	The following property has been added. `<MandateDomainForUsernamesAndGroupNamesInResponse>false</MandateDomainForUsernamesAndGroupNamesInResponse>` **Why?** Enabling this property prepends the "PRIMARY/" prefix to the user name and role name (group name) that belongs to the PRIMARY user store, in the SCIM2 response regardless of the Users and Groups endpoint. When it is set to 'false', the "PRIMARY/" prefix will not be prepended. For more details, see behavioral change #4 in the behavioral changes table given above.
	The following property has been added. `<MandateDomainForGroupNamesInGroupsResponse>false</MandateDomainForGroupNamesInGroupsResponse>` **Why?** Enabling this property in the Groups endpoints prepends the "PRIMARY/" prefix to the role name (group name) that

	belongs to the PRIMARY user store. When it is set to 'false', the "PRIMARY/" prefix will not be prepended. For more details, see behavioral change #4 in the behavioral changes table given above.
	The following properties have been added under the `<Server>` tag. `<!--This configuration is used to define the Service Provider name regex in DCR and IdentityApplicationManagementService-->` `<!--<ServiceProviders>-->` `<!--<SPNameRegex>^[a-zA-Z0-9._-]*$</SPNameRegex>-->` `<!--</ServiceProviders>-->`
	The following properties have been added under the `<OAuth>` tag. `<!-- If enabled, resident Idp entity id will be honoured as the issuer location in OpenId Connect Discovery -->`

```
<UseEntityIdAsIssuerInOidcDiscovery>true</UseEntityIdAsIssuerInOidcDiscovery>
```

The UMA grant type has been added as a supported grant type under the `<SupportedGrantTypes>` tag.

```
<!-- Supported versions: IS 5.7.0 onwards.-->

<SupportedGrantType>

<GrantTypeName>urn:ietf:params:oauth:grant-type:uma-ticket</GrantTypeName>

<GrantTypeHandlerImplClass>org.wso2.carbon.identity.oauth.uma.grant.UMA2GrantHandler</GrantTypeHandlerImplClass>

<GrantTypeValidatorImplClass>org.wso2.carbon.identity.oauth.uma.grant.GrantValidator</GrantTypeValidatorImplClass>

</SupportedGrantType>
```

	The following properties have been added under the `<OAuth>` tag. `<!-- Configurations for JWT bearer grant. Supported versions: IS 5.8.0 onwards. -->` `<JWTGrant>` `<!-- Validate issued at time (iat) of JWT token. The validity can be set using 'IATValidity' configuration.` `Default value is 'true'.` `-->` `<EnableIATValidation>true</EnableIATValidation>` `<!-- Reject the JWT if the iat of JWT is pass a certain time period. Time period is in minutes.` `'EnableIATValidation' configuration should be set to 'true' in order to make use of the validity`

```
                period.

                Default value is '30' minutes.

                -->

    <IATValidityPeriod>30</IATValidityPeriod>

</JWTGrant>
```

The following properties have been added under the `<OpenIDConnect>` tag.

```
<!-- Add tenant domain to 'realm' claim of ID Token-->

<AddTenantDomainToIdToken>false</AddTenantDomainToIdTo
ken>

<!-- Add userstore domain to 'realm' claim of ID
Token-->

<AddUserstoreDomainToIdToken>false</AddUserstoreDomain
ToIdToken>
```

	The following properties have been added under the `<OAuth>` tag. `<!--Configuration provides the ability to renew the access token and the refresh token(where applicable) per each token request and revoke previously available active token for a matching clientid, user and scopes combination.` `Not applicable for refresh token grant type and when when self-contained access tokens are used.` `Default value : false` `Supported versions : IS 5.8.0 onwards -->` `<!--<RenewTokenPerRequest>true</RenewTokenPerRequest>--->` `<!--By enabling this property, in a logout request if the opbs cookie or a valid session does not exist instead of showing the invalid request error page the user will be redirected to the successfully logged out page of the IS or if a valid id_token_hint and a valid post_logout_redirect_uri is available user will be redirected to the post_logout_redirect_uri-->`

```
<HandleAlreadyLoggedOutSessionsGracefully>false</Handl
eAlreadyLoggedOutSessionsGracefully>
```

The following properties have been added under the `<SSOService>` tag.

```
<ArtifactResolutionEndpoint>${carbon.protocol}://${car
bon.host}:${carbon.management.port}/samlartresolve</Ar
tifactResolutionEndpoint>

<SAMLECPEndpoint>${carbon.protocol}://${carbon.host}:$
{carbon.management.port}/samlecp</SAMLECPEndpoint>
```

Why?

These properties allow adding the Artifact URL as a Resident IDP property in the WSO2 IS management console.

	The following properties have been added under the <SCIM2> tag. `<!--<ComplexMultiValuedAttributeSupportEnabled>true</ComplexMultiValuedAttributeSupportEnabled>-->` `<!--<EnableFilteringEnhancements>true</EnableFilteringEnhancements>-->` **Why?** The `<EnableFilteringEnhancements>` property was introduced for the purpose of applying filtering enhancements for SCIM2 filter results. Enabling this ensures that the Eq filter strictly checks for a string match (in this case cross user store search should not be performed). This configuration also enforces consistency on the filtered attribute formats in the response when filtering is done via different endpoints. e.g. Users and Groups endpoints.

	The following properties have been added under the `<Recovery>` tag. `<ReCaptcha>` `<Password>` `<Enable>false</Enable>` `</Password>` `<Username>` `<Enable>false</Enable>` `</Username>` `</ReCaptcha>` `<CallbackRegex>${carbon.protocol}://${carbon.host}:${carbon.management.port}/authenticationendpoint/login.do</CallbackRegex>` **Why?**

	This configuration block is used to enable ReCaptcha verification for password recovery and username recovery.
	The following property have been added under the `<SelfRegistration>` tag. `<CallbackRegex>${carbon.protocol}://${carbon.host}:${carbon.management.port}/authenticationendpoint/login.do</CallbackRegex>` **Why?** This property enables configuring a regex pattern for the callback URLs of the account recovery and self registration APIs. The callbackURL included in the requests is then validated with the configured regex pattern.

	The following new event listener has been added under the `<EventListeners>` tag. `<EventListener type="org.wso2.carbon.identity.core.handler.AbstractIdentityHandler"` `name="org.wso2.carbon.identity.data.publisher.oauth.listener.OAuthTokenIssuanceLogPublisher"` `orderId="12" enable="false">` `<Property name="Log.Token">false</Property>` `</EventListener>` `<EventListener type="org.wso2.carbon.user.core.listener.UserOperationEventListener"` `name="org.wso2.carbon.identity.mgt.listener.UserSessionTerminationListener"`

```
                        orderId="85" enable="true"/>



  <EventListener
  type="org.wso2.carbon.user.core.listener.UserOperation
  EventListener"


  name="org.wso2.carbon.user.mgt.listeners.UserClaimsAud
  itLogger"

                        orderId="9" enable="false"/>
```

Why?

`AbstractIdentityHandler` - Enabling this listener logs the audit data for OAuth token issuance and token introspection. Adding this property allows you to disable logging, else if this property is not present in the configuration file, logging is enabled by default. For more information about auditing, see OAuth Transaction Logs .

`UserOperationEventListener` - This event listener is used to support session termination at the point renaming the username.

`UserOperationEventListener` - This event listener allows adding claims to the audit logs.

The following caches have been added under the `<CacheManager name="IdentityApplicationManagementCacheManager">` tag.

```
<Cache name="JWKSCache" enable="true" timeout="300"
capacity="5000" isDistributed="false"/>

<Cache name="ServiceProviderCache.ID" enable="true"
timeout="900" capacity="5000"
isDistributed="false"/>

<Cache name="ServiceProvideCache.InboundAuth"
enable="true"  timeout="900" capacity="5000"
isDistributed="false"/>
```

Why?

`JKWSCache` - This property has been added to support JWKS Endpoint Cache invalidation.

`ServiceProviderCache.ID` and `ServiceProvideCache.InboundAuthKey` - These two

	properties have been added in order to cache the service provider against the ID and inboundAuth. If these new properties is not present in the configuration file, the configuration value of the `ServiceProviderCache` is applied for these caches.

	The following resources have been added under the <ResourceAccessControl> tag.

```
<Resource
context="(.*)/api/identity/config-mgt/v1.0/search(.*)"
secured="true" http-method="GET">

<Permissions>/permission/admin/manage/identity/configm
gt/list</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource-ty
pe" secured="true" http-method="POST">

<Permissions>/permission/admin/manage/identity/configm
gt/add</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource-ty
pe" secured="true" http-method="PUT">

<Permissions>/permission/admin/manage/identity/configm
gt/update</Permissions>

</Resource>
```

```
<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource-ty
pe/(.*)" secured="true" http-method="GET"/>

<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource-ty
pe/(.*)" secured="true" http-method="DELETE">

<Permissions>/permission/admin/manage/identity/configm
gt/delete</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource/(.
*)" secured="true" http-method="POST">

<Permissions>/permission/admin/manage/identity/configm
gt/add</Permissions>

</Resource>

<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource/(.
*)" secured="true" http-method="PUT">
```

```
<Permissions>/permission/admin/manage/identity/configmgt/update</Permissions>

</Resource>

<Resource context="(.*)/api/identity/config-mgt/v1.0/resource/(.*)/(.*)" secured="true" http-method="GET"/>

<Resource context="(.*)/api/identity/config-mgt/v1.0/resource/(.*)/(.*)" secured="true" http-method="DELETE">

<Permissions>/permission/admin/manage/identity/configmgt/delete</Permissions>

</Resource>

<Resource context="(.*)/api/identity/config-mgt/v1.0/resource/(.*)/(.*)" secured="true" http-method="POST">

<Permissions>/permission/admin/manage/identity/configmgt/add</Permissions>

</Resource>
```

```
<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource/(.
*)/(.*)" secured="true" http-method="PUT">



<Permissions>/permission/admin/manage/identity/configm
gt/update</Permissions>


</Resource>


<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource/(.
*)/(.*)/(.*)" secured="true" http-method="GET"/>


<Resource
context="(.*)/api/identity/config-mgt/v1.0/resource/(.
*)/(.*)/(.*)" secured="true" http-method="DELETE">



<Permissions>/permission/admin/manage/identity/configm
gt/delete</Permissions>


</Resource>
```

Why?

These resources control access to the configuration management resources in WSO2 IS.

	The resource context `/scim2/ResourceType` to `/scim2/ResourceTypes` found under the `<ResourceAccessControl>` tag has been modified as shown below. `<Resource context="/scim2/ResourceTypes" secured="false" http-method="all">` **Why?** This change is done in order to comply with the SCIM2 specification .
	The following resource found under the `<ResourceAccessControl>` tag has been removed. `<Resource context="(.*)/api/identity/auth/(.*)" secured="true" http-method="all"/>` **Why?** This change has been made in order to remove protection for the `/api/identity/auth/v1.2/authenticate` API. This is because the API itself authenticates the user.

The following resources have been added under the <ResourceAccessControl> tag.

```
<Resource
context="(.*)/api/identity/auth/v1.2/data(.*)"
secured="true" http-method="all"/>

<Resource
context="(.*)/api/identity/auth/v1.2/context(.*)"
secured="true" http-method="all"/>

<Resource
context="(.*)/api/identity/template/mgt/v1.0.0/(.*)"
secured="true" http-method="all"/>

<Resource
context="(.*)/api/identity/user/v1.0/update-username
(.*)" secured="true" http-method="PUT">

<Permissions>/permission/admin/manage/identity/userm
gt/update</Permissions>

</Resource>
```

Why?

	These resources have been added to secure the `update-username` API.

	The following properties have been added under the `<Server>` tag..

```
<!--Intermediate certificate validation for
certificate based requests-->

<IntermediateCertValidation enable="false">

    <IntermediateCerts>

        <!--Add intermediate certificate CN. Multiple
<CertCN> elements can be used for multiple
certificates.-->

        <CertCN>localhost</CertCN>

    </IntermediateCerts>

    <ExemptContext>

        <!--Add exemptable context paths. Multiple
<Context> elements can be used for multiple
contexts.-->

        <Context>scim2</Context>

    </ExemptContext>

</IntermediateCertValidation>
```

```
<!--This is the separator that use to separate
multiple roles in the role claim value coming from IDP
side-->

<FederatedIDPRoleClaimValueAttributeSeparator>,</Feder
atedIDPRoleClaimValueAttributeSeparator>

<!--This configuration is used for X509 Certificate
based authentication. -->

<!--<X509>-->

<!--During ssl termination at LB, the X509 certificate
is passed over the HTTP header. This configuration

        provides the facility to configure HTTP
request header name which is configured at LB.  -->

<!--<X509RequestHeaderName>X-SSL-CERT</X509RequestHead
erName>-->

<!--</X509>-->

<!-- This configuration specifies the claims that
should be logged to "audit.log" upon changes. -->

<!--<LoggableUserClaims>-->
```

```
<!--<LoggableUserClaim>http://wso2.org/claims/identity
/accountLocked</LoggableUserClaim>-->

<!--<LoggableUserClaim>http://wso2.org/claims/role</Lo
ggableUserClaim>-->

<!--</LoggableUserClaims>-->

<!--Configuration Store properties-->

<ConfigurationStore>

    <!--Set an upper limit to the database call
queries. Configuration store uses dynamic query
generation,

        specially for searching resources. This
property will prevent any unwanted errors due to too
large queries.

        Default value is the maximum packet size for
MySQL 5.7 in bytes.-->

    <MaximumQueryLength>4194304</MaximumQueryLength>

</ConfigurationStore>
```

`jaas.conf` file stored in the `<IS_HOME>/repository/conf/identity` directory.	The value of the following property value has been corrected from 'tfalse' to 'false'. `useKeyTab=false`
`Webapp-classloading-environments.xml` file stored in the `<IS_HOME>/repository/conf/` directory.	The following ExclusiveEnvironment has been added under the `<Classloading>` tag. `<ExclusiveEnvironments>` `<ExclusiveEnvironment>` `<Name>CXF3</Name>` `<Classpath>${carbon.home}/lib/runtimes/cxf3/*.jar;${carbon.home}/lib/runtimes/cxf3/</Classpath>` `</ExclusiveEnvironment>` `</ExclusiveEnvironments>`

`carbon.xml` file stored in the `<IS_HOME>/repository/conf` directory.	The following properties related to the tenant deletion feature have been added under the `<Server> <Tenant>` tag. `<!-- Flag to enable or disable tenant deletion. By default tenant deletion is enabled-->` `<TenantDelete>true</TenantDelete>` `<!-- Configurations related to listener invocation by tenant admin service-->` `<ListenerInvocationPolicy>` `<!-- Flag to enable or disable listener invocation on tenant delete. This is disabled by default-->` `<InvokeOnDelete>false</InvokeOnDelete>` `</ListenerInvocationPolicy>`
	The following property has been added under the `<Server>` tag.

	<!--EnablePasswordTrim>false</EnablePasswordTrim-->
	The following property has been added. <ForceLocalCache>true</ForceLocalCache> **Why?** Enabling this property forces all the caches to behave as local caches. It is required to enable this in order to have cache invalidation in between the IS nodes in a clustered enviornment. For more details, see behavioral change #5 in the behavioral changes table given above.
`claim-config.xml` file stored in the `<IS_HOME>/repository/conf` directory.	The AttributeID of the http://wso2.org/claims/resourceType claim has been modified to "resourceType". <AttributeID>resourceType</AttributeID>

	The RegEx of the http://wso2.org/claims/phoneNumbers claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`
	The RegEx of the `urn:scim:schemas:core:1.0:phoneNumbers` claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`
	The AttributeID of the claim `urn:ietf:params:scim:schemas:core:2.0:meta.resourceType` claim has been modified to "resourceType" instead of "userType". `<AttributeID>resourceType</AttributeID>`

	Why? The value "Ref" is reserved in open LDAPs for referrals. Therefore, this attributeID was modified to avoid the errors when using Active Directory open LDAPs.
	The RegEx of the `urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers` claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`
	The Regex of the `urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.mobile` claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`

	The RegEx of the `urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.home` claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`
	The RegEx of the `urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.work` claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`
	The RegEx of the `urn:ietf:params:scim:schemas:core:2.0:User:phoneNumbers.other` claim has been modified as follows. `<RegEx>^\s*(?:\+?(\d{1,3}))?[-. (]*(\d{3})[-. )]*(\d{3})[-. ]*(\d{4})(?: *x(\d+))?\s*$</RegEx>`

	Why?The default regular expression values for phone numbers were modified in the claim-config.xml file in order to recognize US and Canadian numbers with the extension code as well.
`log4j.properties` file stored in the `<IS_HOME>/repository/conf` directory.	The following properties have been added. `log4j.logger.TRANSACTION_LOGGER=INFO, TRANSACTION_LOGGER` `log4j.appender.TRANSACTION_LOGGER=org.apache.log4j.FileAppender` `log4j.appender.TRANSACTION_LOGGER.File=${carbon.home}/repository/logs/transaction.log` `log4j.appender.TRANSACTION_LOGGER.Append=true` `log4j.appender.TRANSACTION_LOGGER.layout=org.apache.log4j.PatternLayout` `log4j.appender.TRANSACTION_LOGGER.layout.ConversionPattern=[%d] - %m %n`

```
log4j.appender.TRANSACTION_LOGGER.threshold=INFO

log4j.additivity.TRANSACTION_LOGGER=false




# Appender config to put correlation Log.

log4j.logger.correlation=INFO, CORRELATION

log4j.additivity.correlation=false

log4j.appender.CORRELATION=org.apache.log4j.RollingFileAppender

log4j.appender.CORRELATION.File=${carbon.home}/repository/logs/${instance.log}/correlation.log

log4j.appender.CORRELATION.MaxFileSize=10MB

log4j.appender.CORRELATION.layout=org.apache.log4j.PatternLayout

log4j.appender.CORRELATION.Threshold=INFO
```

	`` log4j.appender.CORRELATION.layout.ConversionPattern=%d {yyyy-MM-dd HH:mm:ss,SSS}|%X{Correlation-ID}|%t|%m%n ```
`user-mgt.xml` file stored in the `<IS_HOME>/repository/conf` directory.	The following properties have been added under the `<UserManager> <Realm> <Configuration>` tag. ``` <!-- Enable username claim retrieve from the UM_USER_NAME in JDBC datasources --> <OverrideUsernameClaimFromInternalUsername>t rue</OverrideUsernameClaimFromInternalUserna me ```

	The following property has been under under the `JDBCUserStoreManager` configuration block. `<Property name="LeadingOrTrailingSpaceAllowedInUserName">false</Property>` The value of the `<UserNameListFilter>` property under the `ReadOnlyLDAPUserStoreManager` configuration block has been modified to the value given below. `(&(objectClass=person)(!(sn=Service)))` The value of the `<UserNameListFilter>` property under the `ActiveDirectoryUserStoreManager` and `ReadWriteLDAPUserStoreManager` configuration blocks has been modified as follows. `(&(objectClass=user)(!(sn=Service)))` The following property has been added under the `ActiveDirectoryUserStoreManager` and the `ReadWriteLDAPUserStoreManager` configuration blocks.

	``<Property name="StartTLSEnabled">false</Property>```

Recommended: See the WSO2 IS 5.8.0 migration guide for more information.