Axiom Configuration for SAML

Version 18.0.3 of the Canary suite includes additional parameters for configuring Axiom to work with SAML. These settings are not configurable via the Canary Admin; they are only available through the xml in the AxiomService.exe.admin file. Below is a sample development version of the AxiomService.exe.admin with the new settings outlined

```
    <deny />
    <basePath>C:\ProgramData\Canary Labs\Axiom</basePath>
    <samlEnabled>true</samlEnabled>
    <samlIssuer>https://jwolf.office.canarylabs.com/</samlIssuer>
    <samlIsAudienceRestricted>false</samlIsAudienceRestricted>
    <samlIDPDescriptorFileName>CanaryADFS_DeltaMetadata.xml</samlIDPDescriptorFileName>
    <samlClaimsNameIdUri>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</samlClaimsNameIdUri>
    <samlClaimsGivenNameUri>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</samlClaimsGivenNameUri>
    <samlClaimsSurNameUri>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</samlClaimsSurNameUri>
    <samlClaimsGroupsUri>http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid</samlClaimsGroupsUri>
    <samlIDPUserGroupIDs>
      <GroupID>S-1-5-21-1601490498-3659835538-1429252828-512</GroupID>
    </samlIDPUserGroupIDs>
    <samlIDPAdminGroupIDs>
      <GroupID>S-1-5-21-1601490498-3659835538-1429252828-512</GroupID>
    </samlIDPAdminGroupIDs>
    <samlCreateUserPassword>password</samlCreateUserPassword>
    <samlCreateUserDomainName />
    <samlCreateUserLdapPath />
    <samlCreateUserAdminGroup>samltestadminsgroup</samlCreateUserAdminGroup>
    <samlCreateUserUserGroup>samltestusersgroup</samlCreateUserUserGroup>
    <samlWantAssertionsSigned>false</samlWantAssertionsSigned>
    <samlCertificateValidationMode>ChainTrust</samlCertificateValidationMode>
    <samlCertificateRevocationMode>Online</samlCertificateRevocationMode>
    <samlSignAuthnRequest>false</samlSignAuthnRequest>
    <samlDetectReplayedTokens>false</samlDetectReplayedTokens>
    <samlSignatureAlgorithm>RsaSha256Signature</samlSignatureAlgorithm>
  </axiomConfig>
</configuration>
```

samlEnabled: Master control setting for saml. Default: ‘false’.
samlIssuer: Identity Provider server identifier
samlIsAudienceRestricted: If true, Axiom validates that the SAML response issuer matches the samlIssuer setting. False ignores the issuer.
samlIDPDescriptorFileName: Name of the metadata xml file to load metadata from for the identity provider. This is an xml that describes the claims offered by the identity provider. This file needs to be placed within the axiom service executable directory and the name of the file (including the extension) configured into this setting.
samlClaimsNameIdUri: Claim key (uri from the metadata file) that Axiom uses to lookup the email address of the user and then uses this to create a local or domain account for the user.
samlClaimsGivenNameUri: Claim key (uri from the metadata file) that Axiom uses to lookup the first name of the user.
samlClaimsSurNameUri: Claim key (uri from the metadata file) that Axiom uses to lookup the last name of the user.
samlClaimsGroupsUri: Claim key (uri from the metadata file) that identifies which groups the user belongs to. Axiom uses these to determine whether the user is an admin or user within Axiom.
samlIDPUserGroupIDs: List of names or SIDs of the groups that the customer has determined will be ‘users’ in Axiom. Axiom iterates through the groups returned in the saml response and searches for matches within this list. If found, then the user has ‘user’ permissions in Axiom.
samlIDPAdminGroupIDs: Names or SIDs of the groups that the customer has determined will be ‘admins’ in Axiom. Axiom iterates through the groups returned in the saml response and searches for matches within this list. If found, then the user has ‘admin’ permissions in Axiom.
samlCreateUserPassword: Password used for all accounts created by Axiom.

samlCreateUserDomainName: Active directory domain used to create the accounts. If blank, the accounts are created on the local machine.
samlCreateUserLdapPath: (only for samlCreateUserDomainName != blank) LDAP path within which the accounts will be created.
samlCreateUserAdminGroup: Accounts classified as 'Admin's are added to this group.
samlCreateUserUserGroup: Accounts classified as 'Users' are added to this group.

Added in v21.1
New URL path for Service Descriptor XML: <yourdomain>/saml2/servicemetadata.xml

Settings
samlWantAssertionsSigned: True/False - Indicates that Axiom would like the saml assertions signed from the IDP server
samlCertificateValidationMode: String – One of ['ChainTrust' = default, 'Custom', 'None', 'PeerOrChainTrust', 'PeerTrust']
samlCertificateRevocationMode: String – One of ['Online' = default, 'Offline', 'NoCheck']
samlSignAuthnRequest: True/False – Indicates the authn request from Axiom will be signed with Axiom's certificate
samlDetectReplayedTokens: True/False – Indicates that Axiom will detect if a token has been replayed. Default = true
samlSignatureAlgorithm: String – One of ['Sha1Digest', 'RsaSha1Signature', 'Sha256Digest', 'RsaSha256Signature' = default, 'Sha384Digest', 'RsaSha384Signature', 'Sha512Digest', 'RsaSha512Signature'