SIGNIANT

Media Shuttle

SAML Configuration

October 2017

Revision 2.0

Table of Contents

Overview

Media Shuttle supports SAML authentication allowing you to authenticate your users with your own directory services, such as Active Directory, LDAP and Identity as a Service (IaaS) providers like Okta, OneLogin, Centrify, and Azure Active Directory B2C.

Media Shuttle supports both native authentication and SAML (Security Assertion Markup Language) 2.0 Web Browser Single Sign-On form-based authentication. Either of these mechanisms can be configured to operate on any given portal, or be combined on the same portal.

Media Shuttle's SAML support allows you to:

- Improve password policy enforcement - You can maintain and set your own password policies.
- Reduce risk regarding passwords in SaaS products – No passwords are not stored by Media Shuttle.
- Automate expiry of credentials - When you remove a portal member from your directory service, they immediately lose access to Media Shuttle.
- Simplify onboarding – SAML authentication allows you to automatically add new members to Media Shuttle.

Media Shuttle provides two configuration options: You can create a single SAML configuration for all portals, or configure per-portal authentication policies to segment access to your Media Shuttle portal.

Media Shuttle native authentication requires the user's email address and password. This password is managed by the user and is the same for all Media Shuttle portals, regardless of their ownership.

With SAML authentication, the user is redirected to the Identity Provider for authentication. After successfully authenticating, the user is directed back to the Media Shuttle portal. The user is tied to Media Shuttle by the email address returned by the Identity Provider.

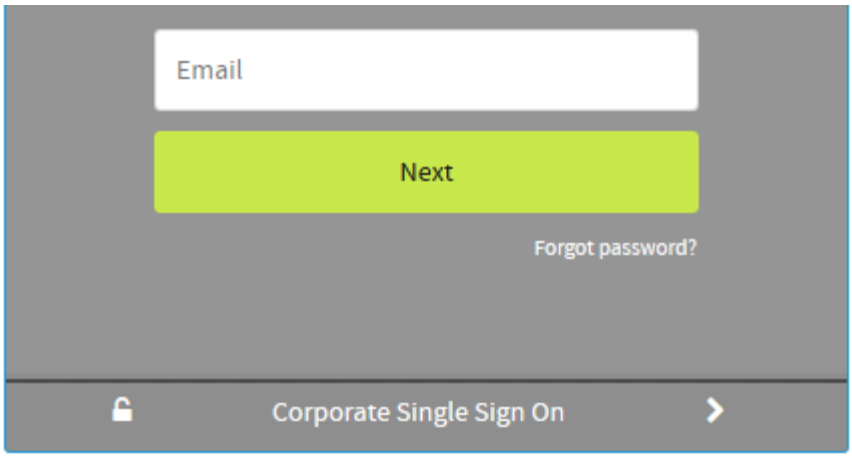
A single trust relationship is established between a given Media Shuttle account and an Identity Provider. This enables multiple portals within a single account to use SAML authentication without per portal Identity Provider configuration.

When portals have both Media Shuttle native authentication and SAML authentication enabled, specific email domains may be configured such that corporate users will only be permitted to authenticate via the SAML corporate directory.

In SAML terms, Media Shuttle is known as the **Service Provider** (SP) or **Relaying Party**, and the SAML authentication service is known as the **Identity Provider** (IdP) or **Claims Provider**. The Service Provider makes a request to the Identity Provider, and the Identity Provider returns a response which includes assertions, or claims concerning the identity of the person who successfully authenticated. In the Media Shuttle case, the assertion of interest is the user's email address.

End User Experience

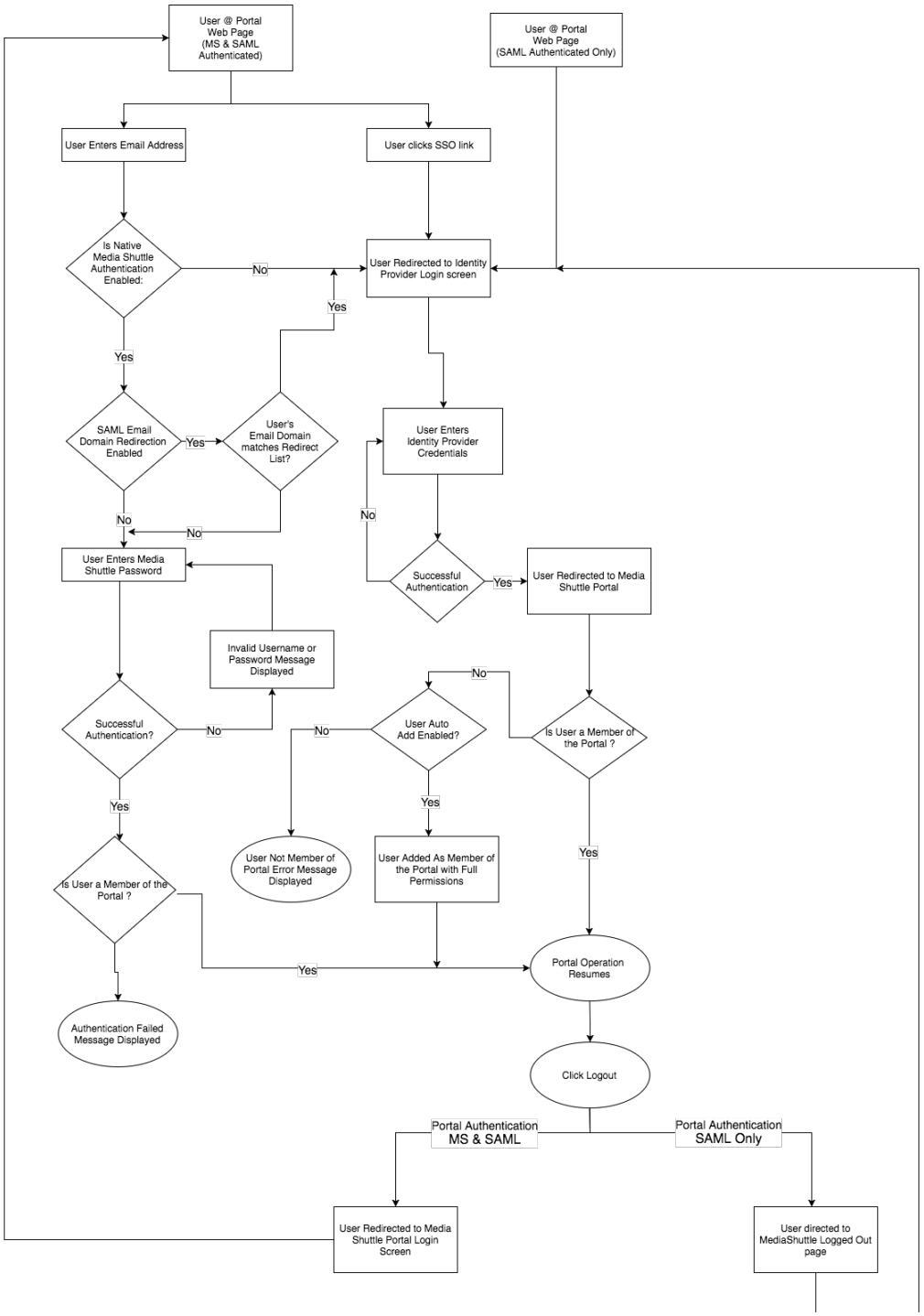
When logging in to a Media Shuttle portal with SAML authentication, users may either enter their email address, or click the **Corporate Single Sign On** link at the bottom to be forwarded directly to the SAML Identity Provider.



Note: If the user already has a valid Single Sign-On authentication token, then the login process is bypassed, and the user is taken directly into the portal.

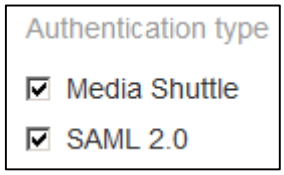
- If the portal is configured for both Media Shuttle native authentication, and SAML authentication, then the user can log in with their email address and password.
- If the portal is enabled for SAML authentication only, the user will be redirected to the SAML identity provider.
- IT administrators can also create a list of email domains that require users to authenticate with a SAML Identity Provider even if native authentication is allowed for other users.

Portal Authentication Flow

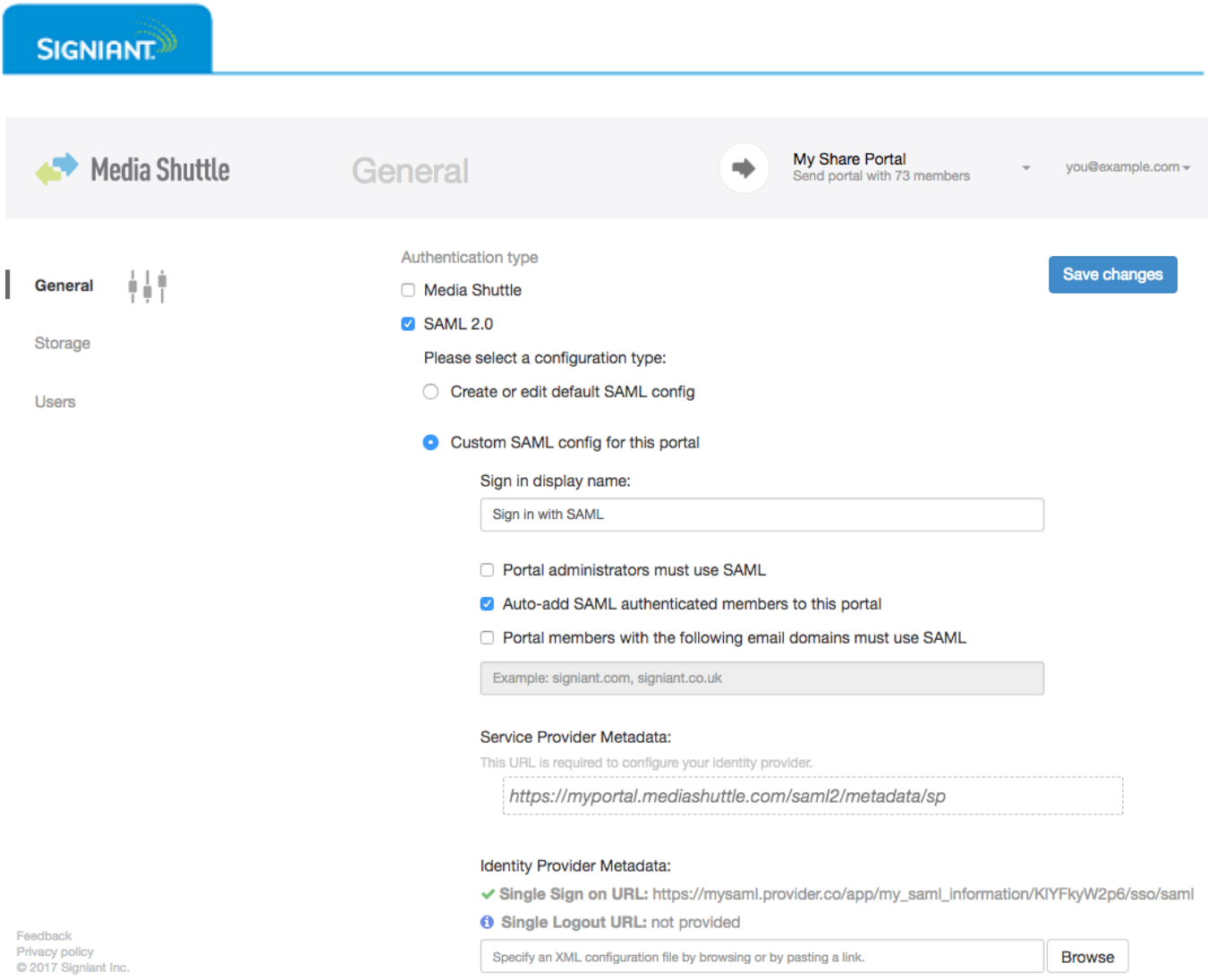


Configuration Steps

Media Shuttle portal security is configured through the IT administration console at `https://manage.mediashuttle.com`. On the General tab, when the Security is specified as *Login is required*, Media Shuttle and/or SAML authentication can be enabled.



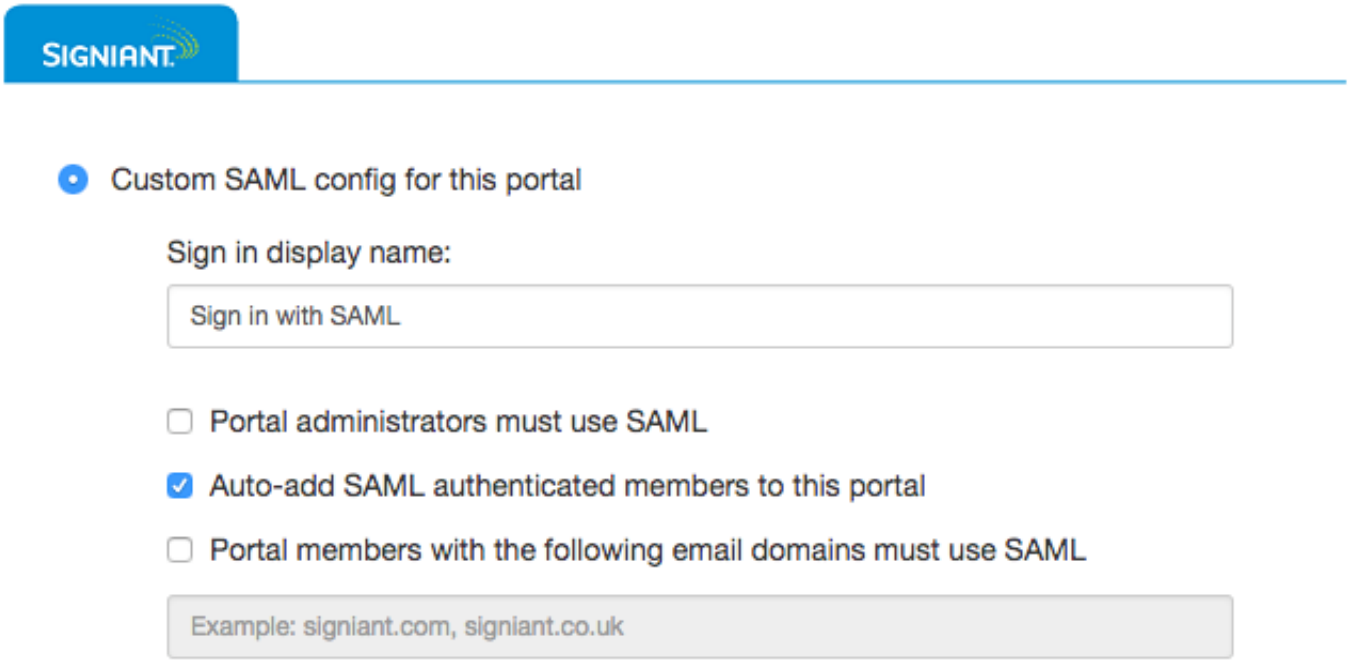
When SAML has been configured for any portal in an account, the same configuration will be used for all SAML enabled portals across the entire account. Once the initial SAML configuration has been completed, including the metadata exchange with the Identity Provider, you can enable **SAML 2.0** in the Authentication type menu.



The **Sign in display name** allows you to customize the Single Sign On link displayed on the portal login box.

Each portal may be individually configured as to whether users should be automatically added as members of the portal if they are not already listed once they successfuly authenticate with SAML. When users are automatically added, they are given full permissions applicable to that portal.

If only limited permissions are desired, automatic user addition is not possible, and the users must be manually added as a member of the portal with the desired permission levels.



By default, Portal Administrators are not required to log in using SAML. Once **Portal Administrators must use SAML** is enabled, Portal Administrators will only be able to log in to the management console using SAML.

If a user successfully authenticates via SAML, but they are not a member of the portal, and automatic member addition not enabled, then the following error messages is returned:

For portals where both Media Shuttle native authentication and SAML authentication options are required, it may be desired to force corporate users to always authenticate via SAML. The key benefit is that if users are removed/disabled in the corporate directory, then they immediately lose access to the portal. One or more comma separated email domains may be listed.

In establishing the trust between the Service Provider (Media Shuttle) and the Identity Provider, there are two items:

- **Identity provider metadata configuration**: This is a generic public statement by the SAML server specifying its configuration. This will tell Media Shuttle where to send the user to be authenticated. This file (or URL) is read once and the details stored within Media Shuttle. The metadata can be updated by referencing the URL/file again and selecting **Save Changes**.

- **Media Shuttle service provider metadata URL**: This lists information about Media Shuttle. Specifically, it will allow the SAML identity provider to know the request is originating from an authorized source. Additionally, it tells the SAML Identity Provider where to return the user's web browser after the authentication is complete.

Technical Details

SAML Server

The SAML server must be configured as follows:

- Protocol: SAML v2.0
- The end point is provided in the Media Shuttle SAML metadata URL, however if it must be entered separately, then the value is "`https://portals.mediashuttle.com/auth`". This is the web page to which the user's web browser will be returned after the authentication is complete.
- The Identity Provider metadata must include an HTTP-POST login service location. HTTP-Redirect services are not supported; they may be present however they will be ignored. For example:

```
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                        Location="https://company.com:9031/idp/SSO.saml2"/>
```

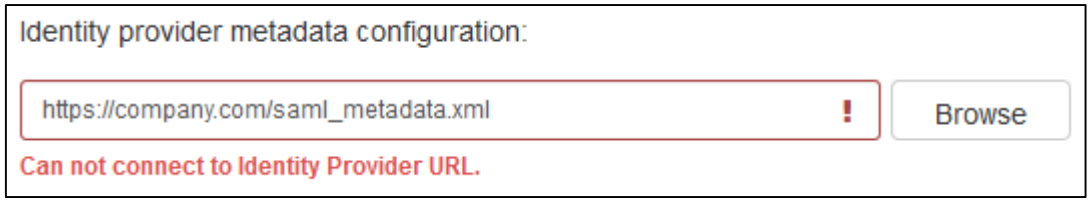
- The SAML response must contain an email address attribute. Specifically, Media Shuttle expects the following exact format:

```
<Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
  <AttributeValue>testuser@signiant.com</AttributeValue>
</Attribute>
```

Troubleshooting

Error Saving Identity Provider Metadata Configuration

When the specified metadata cannot be accessed, or is invalid, an error message is shown. For example:



If the error message is:

then the logs in the Signiant Cloud must be examined to determine the reason behind the failure. Example metadata errors:

1. Missing SingleSignOnService (could be that HTTP-Redirect was specified rather than HTTP-Post):

```
Jun 05 09:41:38 prodB-mediashuttle_i-9bc6fcca catalina.out:
com.signiant.sigcloud.exception.FederationMetadataException: Operation
extractFederationMetadata failed due to missing Federation Metadata: Federation Metadata
mandatory information missing:, SingleLogoutServiceLocation, SingleSignOnServiceLocation
```

2. Any character in the metadata preceding the `<?xml` target will result in the following error. This can occur if the SAML web server is configured for chunking. For example:

```
Aug 06 11:04:48 prodB-mediashuttle_i-8486d1d7 catalina.out: ERROR: 'The processing
instruction target matching "[xX][mM][lL]" is not allowed.'
```

3. Any whitespace (e.g. newline) between the certificate and XML tags will result in a parsing error:

```
Aug 07 06:14:05 prodB-mediashuttle_i-6709e34d catalina.out: Aug 07, 2014 1:14:05 PM
com.signiant.sigcloud.resources.FederationMetadataResource extractFederationMetadata
Aug 07 06:14:05 prodB-mediashuttle_i-6709e34d catalina.out: SEVERE: an exception occurred
extracting Federation Metadata: url=https://s3.amazonaws.com/signiant-allan-
test/adobe.saml.metadata.xml
Aug 07 06:14:05 prodB-mediashuttle_i-6709e34d catalina.out:
com.signiant.sigcloud.exception.FederationMetadataException: Operation
extractFederationMetadata failed due to invalid signing certificate: Could not parse
certificate: java.io.IOException: Incomplete data
```

4. The metadata file must be presented by the identity provider's webserver as application/xml. If it is provided as text/html, for example, the following error will occur:

```
Aug 25 15:23:47 prodB-mediashuttle_i-5075677a catalina.out: SEVERE: an exception occurred
extracting Federation Metadata: url=http://sampleidp.com/ms-saml.xml
Aug 25 15:23:47 prodB-mediashuttle_i-5075677a catalina.out:
com.signiant.sigcloud.exception.FederationMetadataException: Operation
extractFederationMetadata failed could not connect: Not Acceptable
```

Authentication Failed

If the user enters incorrect credentials on the identity provider's login web page, they are typically kept on that page until they have entered their credentials correctly. If the user is returned to the Media Shuttle web page, and the error "Authentication failed" is displayed, this is the result of one of two conditions:

1. The user entered invalid credentials; usually multiple times.
2. The SAML server is not configured in a Media Shuttle compatible fashion, and Media Shuttle is not able to interpret the SAML response.
    a. Analyse the Signiant Cloud logs to determine the exact error.

The log in the Signiant Cloud will be similar to:

```
Aug 15 08:42:15 prodA-mediashuttle_i-f2687ed8 catalina.out: Aug 15, 2014 3:42:14 PM
com.signiant.sigcloud.security.login.SamlAuthnServlet handleAuthenticationResponse

Aug 15 08:42:15 prodA-mediashuttle_i-f2687ed8 catalina.out: SEVERE:
com.signiant.sigcloud.exception.UserNotAMemberException: User with email address:
null is not a member of portal: testportal

Aug 15 08:42:15 prodA-mediashuttle_i-f2687ed8 catalina.out: Aug 15, 2014 3:42:14 PM
com.signiant.sigcloud.resources.helpers.AuthnHelper logAuthFailureEvent

Aug 15 08:42:15 prodA-mediashuttle_i-f2687ed8 catalina.out: INFO: Failed login for
user: SAML_USER for portal: 2da5b881-3c5f-48a6-ab32-ec36cad1e52b
```

These errors are typically related to:

- *handleAuthenticationResponse*
- Error processing response from IDP

Here are several examples where the returned email address attribute will not be accepted, as the format does not match that expected by Media Shuttle:

Example 1

```
<saml:AttributeStatement>
  <saml:Attribute AttributeNamespace="http://sts.corp.net/user"
                      AttributeName="EmailAddress">
    <saml:AttributeValue>
      testuser@signiant.com
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Example 2

```
<saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                       Name="email">
    <saml:AttributeValue xsi:type="xs:string"
                       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      testuser@signiant.com
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Example 3

```
<saml:AttributeStatement>
  <saml:Attribute Name="mail">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="xs:string">
      testuser@signiant.com
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

Web Browser Error


```
Mar 13 11:09:37 prodB-mediashuttle_i-76f6069e elasticbeanstalk-access_log: 10.220.21.119
(192.150.22.5, 10.220.21.119) - - [13/Mar/2015:18:09:37 +0000] "POST /auth/ HTTP/1.1" 404 725
"https://saml_idp.com/saml?fromLogin=true" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0)
Gecko/20100101 Firefox/36.0"
```

The URL used by the IDP to POST back to Media Shuttle must not contain a trailing slash.

Logging

There are no client side logs related to SAML as this authentication is handled directly between the Signiant Cloud and the SAML Identity Provider. Logging is available is the Signiant Cloud, and it is here that information will be found as to the reason behind an authentication failure. For example:

Example 1

```
May 05 17:06:30 prodB-mediashuttle_i-8bf3c7db catalina.out: WARNING: SAML authentication
failed

May 05 17:06:30 prodB-mediashuttle_i-8bf3c7db catalina.out:
com.signiant.sigcloud.exception.ValidationException: Bad SAML authentication response status:
urn:oasis:names:tc:SAML:2.0:status:Responder

May 05 17:06:30 prodB-mediashuttle_i-8bf3c7db catalina.out:  at
com.signiant.sigcloud.exception.ValidationException.badAuthnResponse(ValidationException.java
:16)
```

Example 2

```
May 13 12:39:07 prodB-mediashuttle_i-8bf3c7db catalina.out: SEVERE: Error obtaining email
address from the SAML response.
```

Example 3

```
May 28 08:51:29 prodB-mediashuttle_i-8d40f8de catalina.out: INFO: SAML login attempt from IP
address: 192.195.66.5

May 28 08:51:29 prodB-mediashuttle_i-8d40f8de catalina.out: May 28, 2014 3:51:29 PM
com.signiant.sigcloud.security.login.SamlAuthnServlet handleAuthenticationResponse

May 28 08:51:29 prodB-mediashuttle_i-8d40f8de catalina.out: SEVERE:
com.signiant.sigcloud.exception.UserNotAMemberException: User with email address: null is not
a member of portal: abc-poc-share

May 28 08:51:29 prodB-mediashuttle_i-8d40f8de catalina.out: May 28, 2014 3:51:29 PM
com.signiant.sigcloud.resources.helpers.AuthnHelper logAuthFailureEvent

May 28 08:51:29 prodB-mediashuttle_i-8d40f8de catalina.out: INFO: Failed login for user:
SAML_USER for portal: ad0af11c-4d9f-4815-b479-737802f629dc Request/Response Capture
```

In these failure cases, often the best analysis method is to review the SAML response from the Identity Provider. Two options are:

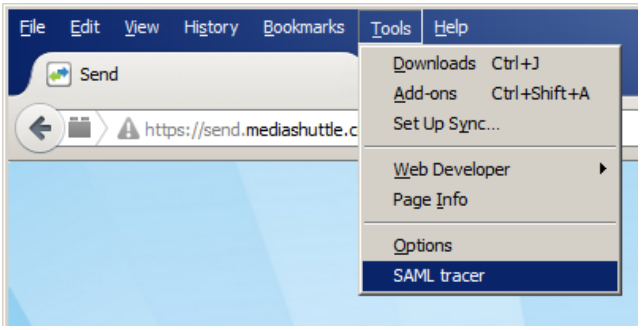
1. The Firefox add-on *SAML tracer*
2. The debugging proxy *Fiddler* (http://www.telerik.com/fiddler).

SAML tracer is recommended as it automatically decodes the response, including any necessary decryption.

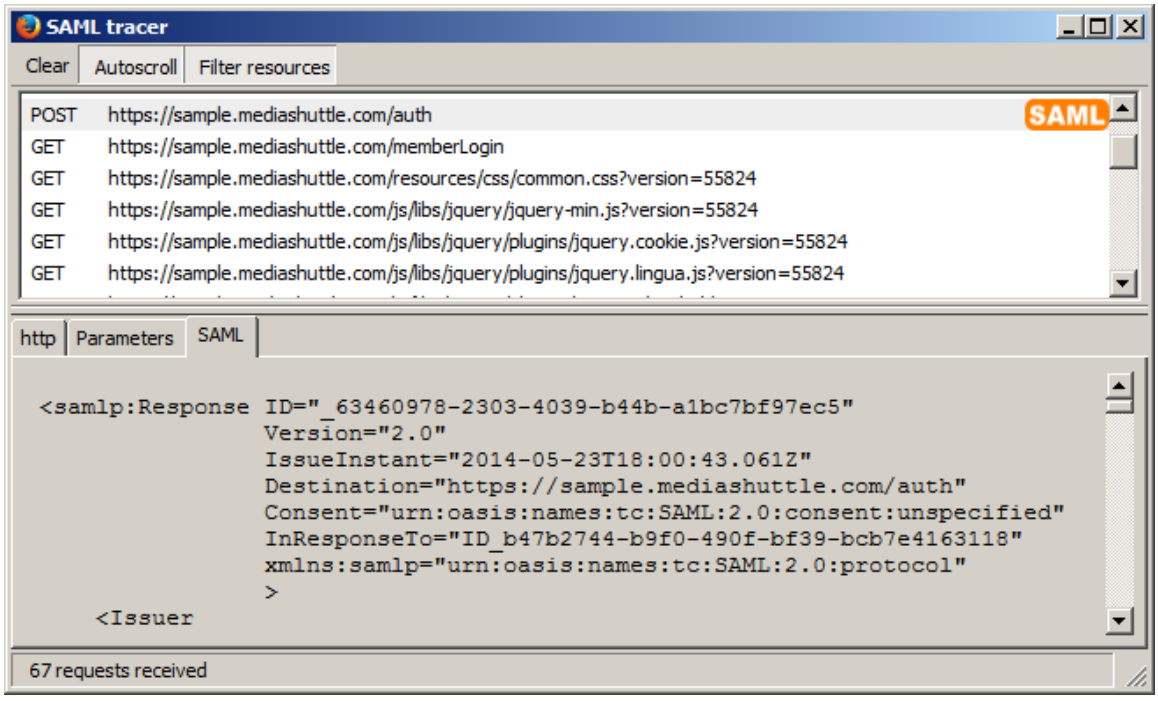
SAML tracer

SAML tracer is a Firefox plugin that helps debug SAML errors.

1. Download and install the *SAML tracer* add-on; requires browser restart.
2. Open the *SAML tracer* window:



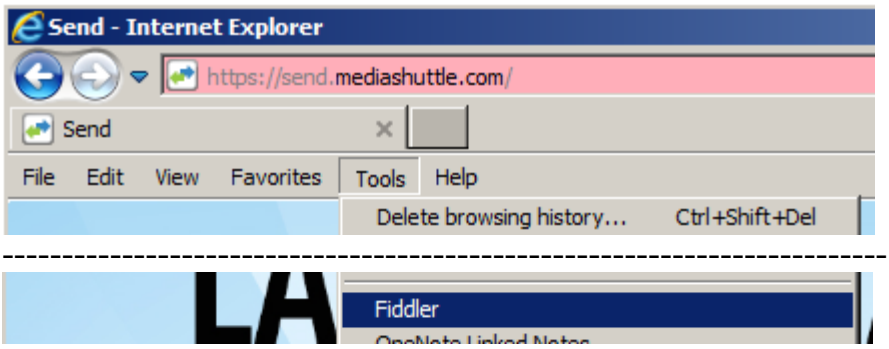
3. Go to the SAML enabled portal, select the SAML authentication mode (if native authentication is also an option), and enter a set of correct credentials.
4. Review the SAML response in the *SAML tracer* window. Select the line with the POST operation to the <Portal Prefix>.mediashuttle.com/auth URL. Then select the SAML tab. For example:



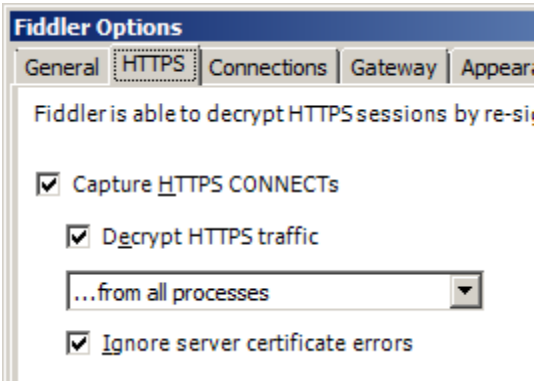
Fiddler

Fiddler can help debug SAML configuration errors.

1. Download the *Fiddler* application from http://www.telerik.com/fiddler; available for Windows only.
2. Install the *Fiddler* application.
3. Launcher the Fiddler application from the Windows Start menu, or from the Tools/Fiddler menu item within Internet Explorer.

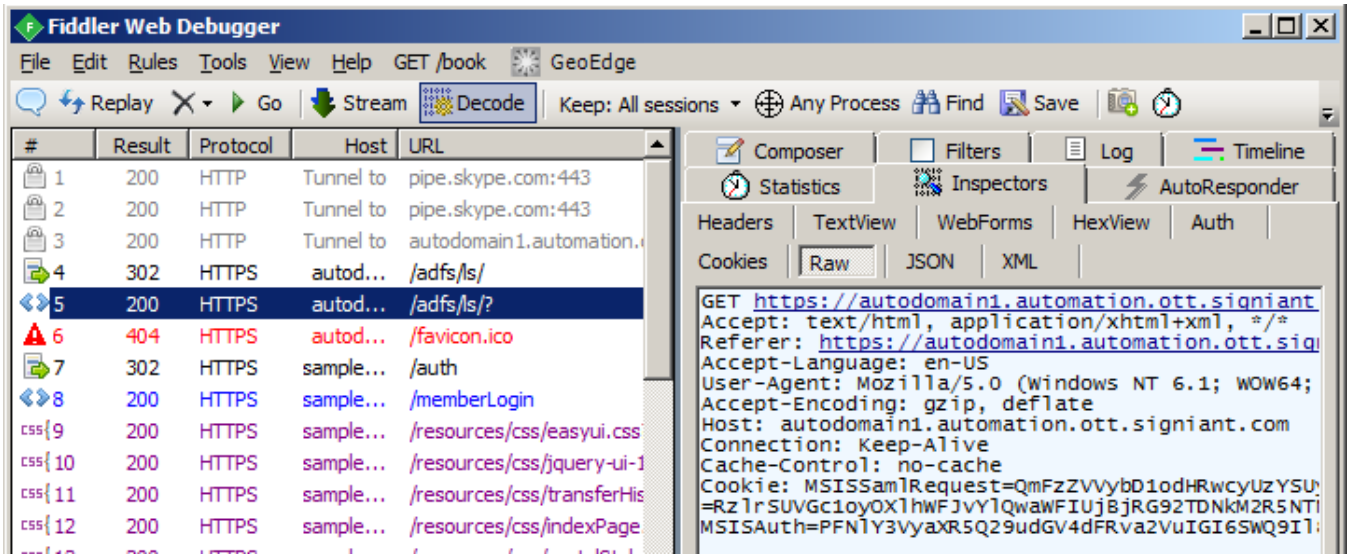


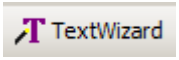
4. Enable decryption of HTTPS traffic, in the Tools/Fiddler Options menu item:



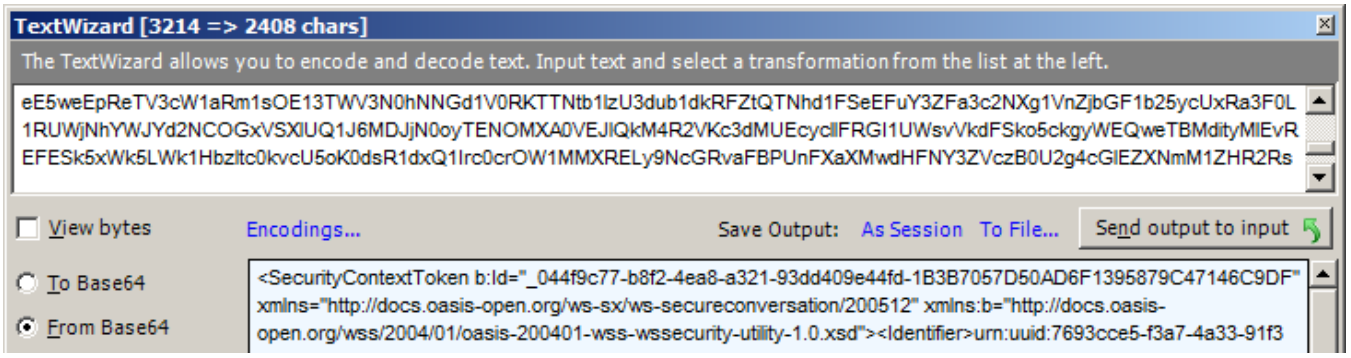
5. Go to the SAML enabled portal, select the SAML authentication mode (if native authentication is also an option), and enter a set of correct credentials.

6. In the F*iddler Web Debugger* window, locate the SAML response line which, for an ADFS server, will most likely have /adfs/ls/? in the URL:



7. Select the Inspectors tab on the right, with the Raw option.
8. Copy the Cookies information to a text editor.
9. Select the MSISAuth and MSISAuthe1 cookies. Join them together, removing the 'MSISAuth=' and 'MSISAuth1=' prefixes and the ';' suffixes.
10. Open the Fiddler Text Wizard: 

11. Take the combined text from above and copy it into the Text Wizard. Select the "From Base64" option. The resulting decoded text will be the SAML response.



12. If the output is encrypted with "SecurityContextToken", then the Firefox *SAML tracer* must be used instead of *Fiddler*.

References

What Is SAML
http://howtojboss.com/2012/08/07/saml-behind-the-wheel/

SAML 2.0 Web Browser SSO Profile
http://en.wikipedia.org/wiki/SAML_2.0#Web_Browser_SSO_Profile

SAML Standards
http:// docs.oasis-open.org/security/saml/v2.0/

Active Directory Federation Services
http://technet.microsoft.com/en-us/windowsserver/dd448613.aspx

Active Directory Federation Services Step-by-Step and How To Guides
http://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides%28v=ws.10%29.aspx

Service Provider Metadata

```
<?xml version="1.0" encoding="utf-8"?>
<EntityDescriptor       ID="_F90ADBFBBAD1F2C794B9FF904E4FF7A3"
                  entityID="mediashuttle"
                     xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
                    WantAuthnRequestsSigned="true">

  <KeyDescriptor use="signing">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>
          MIIEGTCCAwGgAwIBAgIJAOGkExYjrM6bMA0GCSqGSIb3DQEBBQUAMIGiMQswCQYDVQQG
          EwJDQTEQMA4GA1UECAwHT250YXJpbzEPMA0GA1UEBwwGT3R0YXdhMRYwFAYDVQQKDA1T
          aWduaWFudCBJbmMuMRkwFwYDVQQLDBBtZWRpYXNodXR0bGUuY29tMRkwFwYDVQQDDBBt
          ZWRpYXNodXR0bGUuY29tMSIwIAYJKoZIhvcNAQkBFhNkZXZvcHNAc2lnbmlhbnQuY29t
          MB4XDTEyMDYwNjE1NTI1MFoXDTMyMDYwMTE1NTI1MFowgaIxCzAJBgNVBAYTAkNBMRAw
          DgYDVQQIDAdPbnRhcmlvMQ8wDQYDVQQHDAZPdHRhd2ExFjAUBgNVBAoMDVNpZ25pYW50
          IEluYy4xGTAXBgNVBAsMEG1lZGlhc2h1dHRsZS5jb20xGTAXBgNVBAMMEG1lZGlhc2h1
          dHRsZS5jb20xIjAgBgkqhkiG9w0BCQEWE2R1dm9wc0BzaWduaWFudC5jb20wggEiMA0G
          CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDIo2ND7CTh6D+QcZm+fBzf7d7vN0VrLVPc
          s3PlClzjLfmAuUc4+OEotg6ei6mjWpCTmDhuT64S2BVf5AQ4QYpDk3+sJodYEluVryJM
          cZKW8uGn/3fWEVasriyG5SS3IgiLZfgA6zuJEfPCVM9MrR/2rYitExSrZshfuw2bYT5m
          iPplaQ4HRLYUDh1WxL2DH/ML5fXujTcRqufJO4XSsIhFkBWUnWNE7WKJ4TeSJBeImIJP
          W8PKB2IsKW1sV6ramxE/0R9Nqc+g5kltbCS+RwcYiXkK298m6ALZNBr6fiG+HbqObRX6
          ZBnYVrzM0yj5o3gWNHcDSe39tuj3kjIs1o1ZAgMBAAGjUDBOMB0GA1UdDgQWBBTuYndN
          FXZu5NTPDhmDqQylHUEbeDAfBgNVHSMEGDAWgBTuYndNFXZu5NTPDhmDqQylHUEbeDAM
          BgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQCG81lGuNPlNfJqp6nYNvx96DJg
          oLaTyepQHk3RPvjrwC2pN5f1DzrzB+EgAL8npqkz9epFKBS/xPDZ+QvT4q7Zx3rNxvsi
          eQYLl35NuFxKJ1bAuYI1tCZcM0ZNvuoPwEDNR1Ld/5cN8+hqlcn27t5AfYVTcQamBoqn
          vedsyM3xA4IxwOCI1hChaJ91fGGHpFCYpATRPTWj4e10nKHNbm7wo0p3jaOxyambk0SJ
          yMZ9jxdfOi+ct59XXPmx7yBblS3pY3wRINMYkEA7Wmpbkq35dsBwFjrufOl3Kfn+EdxH
          egwF0KoTGpaJF6wHQk2foPuXwQMKLTi65znGIcMXtlNt
        </X509Certificate>
      </X509Data>
    </KeyInfo>
  </KeyDescriptor>

  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                       Location="https://sample.mediashuttle.com/auth" />

  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>

  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                            Location="https://portals.mediashuttle.com/auth"
                               index="0"
                           isDefault="true"/>
</SPSSODescriptor>
</EntityDescriptor>
```

SIGNIANT

Identity Provider Metadata

```
<md:EntityDescriptor entityID="company.com"
                cacheDuration="PT1440M"
                          ID="gacY_sH36-ShRuCv5FFJZoj_G28"
                    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#gacY_sH36-ShRuCv5FFJZoj_G28">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>
        DIYfXT/SjK66puECDSsMQzgKN3k=
      </ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    J05WhHJhXu3+ojvqf30pMy4dla4ke0gL1+mKjX34Jilv+Id4S3/3V0gX/mXyzyQQ/DMV6eWMhiM4w2gGLUZ
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
        MIIFFDCCA/ygAwIBAgIETCEqLDANBgkqhkiG9w0BAQUFADCBsTELMAkGA
      </ds:X509Certificate>
    </ds:X509Data>
    <ds:KeyValue>
      <ds:RSAKeyValue>
        <ds:Modulus>
           tfcd+5Sj8LEOK5IoLw/eBaSx0E2bnHjireNI8Yag8hHfkLtarg7rRapUMKFxm4HD5o3reiPxEn9JPZ
        </ds:Modulus>
        <ds:Exponent>AQAB</ds:Exponent>
      </ds:RSAKeyValue>
    </ds:KeyValue>
  </ds:KeyInfo>
</ds:Signature>

<md:IDPSSODescriptor WantAuthnRequestsSigned="true"
                  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

<md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>
        MIIFFDCCA/ygAwIBAgIETCEqLDANBgkqhkiG9w0BAQUFADCBsTELMAkGA1UEBhMCVVMxFjAUBgNVBAoT
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>

<md:NameIDFormat>
  urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</md:NameIDFormat>
```

```
<md:SingleSignOnService Location="https://company.com:9031/idp/SSO.saml2"
                         Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>

<md:SingleSignOnService Location="https://company.com:9031/idp/SSO.saml2"
                         Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                        Location="https://company.com:9031/idp/SLO.saml2"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                        Location="https://company.com:9031/idp/SLO.saml2"/>

<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                      Name="email"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>

<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                      Name="lastname"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>

<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                      Name="firstname"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>

</md:IDPSSODescriptor>
<md:ContactPerson contactType="administrative"/>
</md:EntityDescriptor>
```

Example SAML Login Request (XML)

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                            xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    AssertionConsumerServiceURL="https://portals.mediashuttle.com/auth"
                    Destination="https://domain.signiant.com/adfs/ls/"
                              ID="ID_04455b10-d5b0-45d6-bf73-4e0c75f4815e"
                   IssueInstant="2014-05-13T15:47:19.110Z"
                ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                        Version="2.0">

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  https://sample.mediashuttle.com/
</saml:Issuer>

<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo>
    <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#WithComments" />
    <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <dsig:Reference URI="#ID_04455b10-d5b0-45d6-bf73-4e0c75f4815e">
      <dsig:Transforms>
        <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </dsig:Transforms>
      <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <dsig:DigestValue>fWDPVjiGLFE0KnULmewrzqQiT6I=</dsig:DigestValue>
    </dsig:Reference>
  </dsig:SignedInfo>

<dsig:SignatureValue>
  jWfS6XSmx+DNUIMeFG65/P/h/RjseV3fUPyZ5jMI0W8YtqwcG+rWIHm5brJXP3TzE/Lvp3Uk1o2Z
  dgQjACZiDlXLORw/hCv33+eoyrM2fZkkxcEQtL47jmmfESPEp2BjaB9L8qKaa4IhZn6ZZoQtpov+
  aenhJ8oQLuc+vGAOTnvjrpvT/Q/tEHjYYNrYdxD2Xlv8oK2ovMBVaW9A3Uvj15Lvg5En15rukfu2
  JZAJBbxOb23DWLUpLFolyKB1vppvRht21qMp9gTbMHJDEKnhK7okW1RkJlyweS6gaxq6DVBJn1Rz
  fZmD2Zi3RTIcf1zLXAOcjB21z2nr6VqnFoaLpA==
</dsig:SignatureValue>

<dsig:KeyInfo>
  <dsig:KeyValue>
    <dsig:RSAKeyValue>
      <dsig:Modulus>
        yKNjQ+wk4eg/kHGZvnwc3+3e7zdFay1T3LNz5Qpc4y35gLlHOPjhKLYOnoupo1qQk5g4bk+uEtgV
        X+QEOEGKQ5N/rCaHWBJbla8iTHGSlvLhp/931hFWrK4shuUktyIIi2X4AOs7iRHzwlTPTK0f9q2I
        rRMUq2bIX7sNm2E+Zoj6ZWkOB0S2FA4dVsS9gx/zC+X17o03EarnyTuF0rCIRZAVlJ1jRO1iieE3
        kiQXiJiCT1vDygdiLCltbFeq2psRP9EfTanPoOZJbWwkvkcHGIl5CtvfJugC2TQa+n4hvh26jm0V
        +mQZ2Fa8zNMo+aN4FjR3A0nt/bbo95IyLNaNWQ==
      </dsig:Modulus>
      <dsig:Exponent>AQAB</dsig:Exponent>
    </dsig:RSAKeyValue>
  </dsig:KeyValue>
</dsig:KeyInfo>

</dsig:Signature>
<samlp:NameIDPolicy AllowCreate="true"
                          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />
</samlp:AuthnRequest>
```

Example SAML Login Response (XML)

```
<samlp:Response
           ID="_445ccef1-bd01-4db3-9070-00f647cec462"
       Version="2.0"
  IssueInstant="2014-05-13T13:42:26.698Z"
   Destination="https://portals.mediashuttle.com/"
       Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  http://DOMAIN.SIGNIANT.COM/adfs/services/trust</Issuer>

<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>

<Assertion  ID="_0edfeecb-d4b9-4c05-94b1-87f481fbef5f"
  IssueInstant="2014-05-13T13:42:26.698Z"
       Version="2.0"
         xmlns="urn:oasis:names:tc:SAML:2.0:assertion">

<Issuer>http://DOMAIN.SIGNIANT.COM/adfs/services/trust</Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <ds:Reference URI="#_0edfeecb-d4b9-4c05-94b1-87f481fbef5f">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <ds:DigestValue>eBqiql2K1DeMs9E9dma0xmX8f5Q=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>
  XYH8aMT83V8x2UKiuq8nmq6fJHUwh9tPgITOecz04ZPtkyIFxd35trwT52apask0E7NKVAV5YLwhAQTMWIXN0n37
  kK8u+vH8NhOvtc/vWFjtP9xJtfpV3z5Bpr+DicotcJQtdYrVOTPp/hi4VFGVsvltGgOKP8wWKoqgSpYIxW+0XAa+
  GGjU3R1/02xdh+Kxu2jSSEh7KVVHfJczaBBcnWNpdqQGW34pi/o9mIAfFt84JdDL6XDA9s5gmQtYEq57mefnWu7C
  y1KhMn280oSfehXX/IrjLw+Ul6O83COuGlGk4NkP7+lhtlykdBT75VcDeLuzT0buE+UarPB2r6ELw==
</ds:SignatureValue>

<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <ds:X509Data>
    <ds:X509Certificate>
      MIIDCjCCAfKgAwIBAgIQItadkVa/169JQ50mMowjrjANBgkqhkiG9w0BAQsFADBBMT8wPQYDVQQDEzZBREZTI
      FNpZ25pbcgLSBBVVRPRE9NQUlOMS5BVVRPTUFUSU9OLk9UVC5TSUdOSUFOVC5DT00wHhcNMTMxMDIyMTcyNzU
      A2WhcNMTQxMDIyMTyNzA2WjBBMT8wPQYDVQQDEzZBREZTIFNpZ25pbmcgLSBBVVRPRE9NQUlOMS5BVVRPTUFUS
    </ds:X509Certificate>
  </ds:X509Data>
</KeyInfo>
</ds:Signature>
```

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
    mDRQfjMoWYFpeu5DCWD6kbJlAlNyrYXzXgMT/PVF3pk=
  </NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData NotOnOrAfter="2014-05-13T13:47:26.698Z"
                             Recipient="https://sample.mediashuttle.com/"/>
  </SubjectConfirmation>
</Subject>

<Conditions NotBefore="2014-05-13T13:42:26.695Z" NotOnOrAfter="2014-05-13T14:42:26.695Z">
  <AudienceRestriction>
    <Audience>https://sample.mediashuttle.com/</Audience>
  </AudienceRestriction>
</Conditions>

<AttributeStatement>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
    <AttributeValue>testuser@signiant.com</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn">
    <AttributeValue>testuser@signiant.com </AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/claims/CommonName">
    <AttributeValue>testuser</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
    <AttributeValue>Test User</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
    <AttributeValue>Test</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
    <AttributeValue>User</AttributeValue>
  </Attribute>
  <Attribute Name="http://schemas.microsoft.com/ws/2008/06/identity/claims/role">
    <AttributeValue>Domain Users</AttributeValue>
  </Attribute>
</AttributeStatement>

<AuthnStatement AuthnInstant="2014-05-13T13:42:13.933Z"
                SessionIndex="_0edfeecb-d4b9-4c05-94b1-87f481fbef5f">
<AuthnContext>
  <AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
  </AuthnContextClassRef>
</AuthnContext>

</AuthnStatement>
</Assertion>
</samlp:Response>
```

Example SAML Logout Request (XML)

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                     xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
                    Destination="https://nesssignant123.okta.com/app/ness3_mediashuttle_1/ex
                    k1wxebn5KlYFkyW2p6/slo/saml"
                    ID="ID_e27221c7-a676-4c08-a293-74b725749767"
                    IssueInstant="2017-10-02T17:35:34.690Z"
                    Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">mediashuttle</saml:Issuer>
  <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <dsig:SignedInfo>
      <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#WithComments" />
      <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <dsig:Reference URI="#ID_e27221c7-a676-4c08-a293-74b725749767">
        <dsig:Transforms>
          <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
/>
          <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/></dsig:Transforms>
        <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <dsig:DigestValue>qyGGdpf8RXUQKVNIYnS/I9CXlm0=</dsig:DigestValue>
      </dsig:Reference>
    </dsig:SignedInfo>

<dsig:SignatureValue>us5i0b5L9ib3lKGjNQHhSUScRhJ4RnGMy/2fVswObRPn8KX38vLHSpxBhTRADCkB5d5WMUpa
j8A7IYdI1ENl3t24biy6BsDgb1GiCP/p2aORoEEQFFIX5Qk8yW9PCcpzdqXLTA4ZnVq9tMcdbszrFjOm8rCteSQnCml3B
yfj1YrvdIAXwr8lLXFeRuxnsASoBXCyGC1U3glAZtp7uvOHXDQiHzgkULiidcTFnIONdVAQT5vyHm+oJ20baQuLIjrocC
8oPo4CcswIybgAmZlJZYXsyJtSdujp25iKvIpjI4/FtOx7Se0tR3aDoCEU98byUVUbdKUA6BrV9hqeAXarvQ==</dsig:
SignatureValue>
    <dsig:KeyInfo>
      <dsig:KeyValue>
        <dsig:RSAKeyValue>

<dsig:Modulus>yKNjQ+wk4eg/kHGZvnwc3+3e7zdFay1T3LNz5Qpc4y35gLlHOPjhKLYOnoupo1qQk5g4bk+uEtgVX+Q
EOEGKQ5N/rCaHWBJbla8iTHGSlvLhp/931hFWrK4shuUktyIIi2X4AOs7iRHzwlTPTK0f9q2IrRMUq2bIX7sNm2E+Zoj6
ZWkOB0S2FA4dVsS9gx/zC+X17o03EarnyTuF0rCIRZAVlJ1jRO1iieE3kiQXiJiCT1vDygdiLCltbFeq2psRP9EfTanPo
OZJbWwkvkcHGIl5CtvfJugC2TQa+n4hvh26jm0V+mQZ2Fa8zNMo+aN4FjR3A0nt/bbo95IyLNaNWQ==</dsig:Modulus
>
          <dsig:Exponent>AQAB</dsig:Exponent>
        </dsig:RSAKeyValue>
      </dsig:KeyValue>
    </dsig:KeyInfo>
  </dsig:Signature>
  <saml:NameID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
               Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">prasanth.paleti@ness.com</saml:NameID>
  <samlp:SessionIndex>ID_8f42fe8f-dd1c-49c1-b0ba-4e3204e92bd1</samlp:SessionIndex>
</samlp:LogoutRequest>
```

Example SAML Logout Response (XML)

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                       Destination="https://portals.mediashuttle.com/auth"
                       ID="id177846804976077833171291"
                       InResponseTo="ID_e27221c7-a676-4c08-a293-74b725749767"
                       IssueInstant="2017-10-02T17:35:35.094Z"
                       Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">http://www.okta.com/exk1wxebn5KlYFkyW2p6</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="#id177846804976077833171291">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/></ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <ds:DigestValue>zVkCaOJTYrh/x61Ynb1M9FiZhioiQRsHyjX6ocekOik=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>rmVAVDgGHwru5M4+V0jefivk0e1a5Ss1Q6m605y4pg23IHpxXehJ5Ull0uCf8ZHYoQ6zTNubI+
YKu7MU2DgBA4qn4ZsNFPEtrAaLFpqOazLqGofqDSCFLkgfxFb2N0UfIQzN+ewnwzqRiAAU3UfZN0ckU52d7R7rR7o6ay3
nigSD9lt/niHILsUxUu9bFFHYNelXC+qCevCs/vf1yYFv4Ax68aXcz0f7E+c7k4DlsC+6YQam7SsgI5bv829hQI1jfE+a
4Nx+m1svINGlO5n2RcoyYO3s+nkD49J1CMXETNInHQybMXoyY8vIS+ETjgom4Ujep6Pej4NteoAI8c26Dw==</ds:Sign
atureValue>
    <ds:KeyInfo>
      <ds:X509Data>

<ds:X509Certificate>MIIDrjCCApagAwIBAgIGAV5Sbl35MA0GCSqGSIb3DQEBBQUAMIGXMQswCQYDVQQGEwJVUzETM
BEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxGDAWBgNVBAMMD25lc3NzaWduaWFudDEyMzEcMBoGCSqGSIb3
DQEJARYNaW5mb0Bva3RhLmNvbTAeFw0xNzA5MDUxNDI0MThaFw0yNzA5MDUxNDI1MThaMIGXMQsw
          CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzEN
MAsGA1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxGDAWBgNVBAMMD25lc3NzaWduaWFu
dDEyMzEcMBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALBMxyMNZBrOQwrpO5SpHQrNFY3oXA1jWhNNEm7zXuxbzM83Tux6feaITHh/zCep
          0syz0frr2AZ37jlE1akE6nl7F7UTOL6YbDQPM4PfuBqeo6GEjwzzDUw7Kf92/CnElbfkVkQCKP+X
98CSITYe3SM/jX5S4PhyyHdU84YLuwjtMn8SCjh/229zPst1WyRwNsQPJ6azYInAKEYDG74xLQWr
nBUKSJgMpI0aBFM2sRjGhkbjqlrNuJkQpMtTAg7dLECXYtJBqVd9SqrUGDjYG79Fu4LtIWpTviWi
Mz/07g8yU5yo4qrA48Hqe0ApL09uOKNpO59alMSoTkb4BvI6opsCAwEAATANBgkqhkiG9w0BAQUF
          AAOCAQEAsEsMYMIW9Y0VuNMorzdMAa8+9mFgaPx8kkTAYIjbaHK4hkcClFQTue8DCZ3SlpOdmkQd
2s5VgWKse4qkabuNSclxwRtRCPCB+Vyn5mEHACI7zJLNvuI/v5PJLiXavnwA5Jo7H0JlfX8V+PKn
6nu6XalFOCfHDBbRqWBsG5CESLx4enNF3ip3EGzSQzlRYMCNIlGcIwViREhB1fhHjHrKYZs//82u
Sv/HNPxGp1pWXuNjbHn++09FtIheuO7CHnyMw0dTl3ee2QOfZuZSxQO7av/lLuFo0tBJArwqwcy9
          R0+VEHcvTtefFq3qyIcuhTIk/xwyF3ZzmM2tVGhzr+wYRA==
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></saml2p:Status>
</saml2p:LogoutResponse>
```

Required Aspects

1. Destination - represents the location that made the initial request. If this is not present or wrong the response will be invalid. This is set to our authentication URL as we used Signed requests.

2. Recipient - represents where the assertion is being sent. Again our authentication URL is awaiting this SAML response.

3. Audience - represents the intended audience. This can be set to multiple locations as it can be used for multiple as but we should be present here.

4. Name must be returned equal to:

   http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

   and the value has to be an email address for our portal account lookup since we only permit the use of email addresses in our login.

ADFS Sample Configuration

Stage 1: Configure the AD FS 2.x Identity Provider Metadata URL in Media Shuttle

1. Launch the Manage Interface for your Account and go to the General page.
2. Enable the "SAML 2.0" option in the "Login is required" section. This is for Send and Submit Portals
    a. Note : “SAML 2.0 option is directly available on the Share Portals.
3. Type the metadata URL of your AD FS 2.x server in the "Identity Provider Metadata configuration" field (eg. https://<FQDN_of_your_ActiveDirectoryFederationService>/FederationMetadata/2007-06/FederationMetadata.xml). Or you can browse to the XML file and select it
4. Copy the Media Shuttle Service Provider Metadata URL that is provided (i.e., https://portals.mediashuttle.com/saml2/metadata/sp). This is required for the AD FS 2.x Relying Party Trust configuration step.
5. Click Save Changes.

Stage 2: Configure the Media Shuttle Relying Party Trust configuration in AD FS 2.x

Note: You will be required to input the URL of your Media Shuttle portal at several stages of this process. This URL must adhere to the following format: https://sample.mediashuttle.com/

Launch the AD FS 2.x Management Console.

1. Go to AD FS 2.x > Trust Relationships > Relying Party Trusts.
2. Select 'Add Relying Party Trust' from the Action menu to launch the Add Relying Party Trust Wizard. Click Start.
3. Select the option to 'Import data about the relying party published online'.
4. Input the Media Shuttle Service Provider Metadata URL from Stage 1, and click Next.
5. Enter your Media Shuttle portal name as the display name. Click Next.
6. Select the option to 'Permit all users...'. Click Next.
7. Click Next to complete the wizard
8. Enable the checkbox to 'Open the Edit Claim Rules dialog'. Click Close.
9. On the Issuance Transform Rules tab, click the 'Add Rule' button and select 'Send Claims using a Custom Rule'. Click Next.
10. In the Claim Rule Name field, type "<Your Media Shuttle portal name> Custom Claim".

11. In the Custom Rule field, copy and paste the following custom rule.

```
c1:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] &&
c2:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]
     => add(
                    store = "_OpaqueIdStore",
                    types = ("https://sample.mediashuttle.com/internal/sessionid"),
                    query = "{0};{1};{2};{3};{4}",
                    param = "useEntropy",
                    param = c1.Value,
                    param = c1.OriginalIssuer,
                    param = "",
                    param = c2.Value);
```

Replace *https://sample.mediashuttle.com* with the URL of your Media Shuttle portal.

12. Click Finish.
13. Click the 'Add Rule' button and select 'Transform an Incoming Claim'. Click Next.
14. In the Claim Rule Name field, type "<Your Media Shuttle portal name> Claim Transform".
15. In the Incoming Claim Type field, type "https://sample.mediashuttle.com /internal/sessionid", replacing *https://sample.mediashuttle.com* with the URL of your Media Shuttle portal. Note: This must exactly match the "types" parameter from the Custom Rule you entered in Step 11, above.
16. In the Outgoing Claim Type field, select the "Name ID" option.
17. In the Outgoing Name ID Format field, select the "Transient Identifier" option.
18. Select the Pass Through All Claim Values option, then Click Finish.
19. Click the 'Add Rule' button and select 'Send LDAP Attributes as Claims'. Click Next.
20. In the Claim Rule Name field, type "<Your Media Shuttle portal name> LDAP Attributes".
21. In the Attribute Store field, select the Active Directory option.
22. In the LDAP Mapping fields, specify the following mappings:

LDAP Attribute	Outgoing Claim Type
E-Mail-Addresses	E-Mail Address
User-Principal-Name	UPN
SAM-Account-Name	Common Name
Display-Name	Name
Given-Name	Given Name
Surname	Surname
Token Groups - Unqualified Names	Role

23. Click Finish.
24. Click Apply, then Click OK to close the Edit Claim Rules dialog.
25. Select your portal in the Relying Party Trusts list, then select 'Properties' from the Action menu.
26. Go to the Advanced tab.
27. In the Secure Hash Algorithm field, select the "SHA-1" option. Click Apply. Click OK.

Centrify

1. In Admin Portal, click Apps and Add Web Apps.
2. Click Custom.
3. On the Custom tab, next to the SAML application click Add.
4. In the Add Web App screen, click Yes to add the application. Admin Portal adds the application.
5. In your SAML app, go to Application Settings.
6. Click on "Upload SP Metadata". Enter the Assertion Consumer Service URL as provided by SP which is `https://portals.mediashuttle.com/saml2/metadata/sp`
7. The links under Identity Provider Info, i.e. Identity Provider Sign-in URL , Identity Provider Error URL and Identity Provider SAML Meta data URL are links for you to put in your SAML app.
8. You may click "Download Identity Provider SAML Meta data" and upload in your SAML application.
9. Go to "User access" and select the roles can access the app. Click save to save all changes.

To modify the SAML response, you may need to edit the script under "Advanced" tab, please find following sample for your reference:

```
setAttribute('emailaddress', LoginUser.Get('mail'));
```