

***External Partner – SAML 2.0 Integration Guide***

*Version 2.1*

*May 11, 2015*

*CIO Security Architecture*

Table of Contents

[1.0 Introduction 3](#_Toc360198952)

[2.0 SAML 2.0 – SSO Configuration 3](#_Toc360198953)

[3.0 Service Provider (SP) Integration Details 3](#_Toc360198954)

[4.0 Accenture (IdP) Integration Details 5](#_Toc360198955)

[Accenture Staging (Development/Staging) 5](#_Toc360198956)

[Accenture Production 6](#_Toc360198957)

[5.0 Appendix A: Example Claims 7](#_Toc360198958)

# 1.0 Introduction

This document’s purpose is to provide key information regarding the integration points between Accenture’s Identity Provider SAML connection component and a third party Service Provider (Resource Partner).

# 2.0 SAML 2.0 – SSO Configuration

The SAML 2.0 protocol allows for two ways for an end user to initiate the login process:

* SP-initated (Service Provider initiated): meaning the end user first browses to the third party Service Provider’s web application URL. If the user is not yet authenticated, the Service provider would create an AuthnRequest to the Identity Provider (IdP), in this case Accenture.
* IdP initiated (Identity Provider initiated): meaning the end user first browses to the Accenture Identity Provider’s login URL. The user will submit their login credentials and the IdP will then redirect the user to the Service Provider’s endpoint URL.

*Note: For the SP-initiated use case, if the Service Provider chooses to sign the AuthnRequest, they will need to share their signing certificate’s public key with Accenture for the initial configuration (this is so Accenture can verify the signature on the AuthnRequest).*

*Note: For the IDP-initiated use case, Accenture’s SSO system does not currently support RelayState in the IDP-initiated login scenario so if you require RelayState please use SP-initiated login instead.*

 The Accenture team generally expects the SP-initiated login method to be used by default. If the Service Provider wishes to use the IdP-initiated method, they should communicate this to the Accenture team during the initial integration process to ensure both parties are aware of this.

# 3.0 Service Provider (SP) Integration Details

In order to start the integration with Accenture, you will need to provide the following details to your Accenture application team contact (the Accenture app team will then provide these details to the CIO Security Integration team via a “Federation Form”).

Required information for each environment the Service Provider wants to integrate with Accenture (integrations typically require both Staging and Production integrations):

|  |  |
| --- | --- |
| Federation Service URL(Partner Endpoint URL) | *<Please provide the endpoint URL where you want Accenture to send the authenticated user SAML token>* |
| Federation Service URI(Partner URI) | *<Please provide the URI, EntityID (unique identifier) for your Federation Service.>**Note: It is preferred that this value contains the vendor name (not Accenture’s) since this is supposed to be a unique identifier for the vendor system. Acceptable formats include URNs (like urn:federation:vendorABC) or URLs (https:// sso.vendordomain.com).* |
| SAML 2.0 Protocol Binding:* POST
* Artifact
 | *<Please indicate which SAML protocol binding you wish to use: POST or Artifact >* |
| Name ID claim format & value | *<Format: If you want Accenture to provide a certain NameID claim format, please indicate that here, otherwise we will use the following format as a default: urn:oasis:names:tc:SAML:1.1:nameid-format:string**Value: The default value will be User Principal Name, please indicate if you wish to use something else (sample value: EnterpriseID@accenture.com, john.c.doe@accenture.com)>* |
| Additional claims/assertions you require | *<Format: If you want Accenture to provide additional claims in a specific format, please indicate that here, otherwise we will use the following format as a default: urn:oasis:names:tc:SAML:2.0:attrname-format:basic**Available claims you may choose from:*[*https://federation-sts.accenture.com/schemas/claims/1/careertrackcode*](https://federation-sts.accenture.com/schemas/claims/1/careertrackcode)[*https://federation-sts.accenture.com/schemas/claims/1/careertrackdescription*](https://federation-sts.accenture.com/schemas/claims/1/careertrackdescription)[*http://schemas.xmlsoap.org/claims/CommonName*](http://schemas.xmlsoap.org/claims/CommonName)[*https://federation-sts.accenture.com/schemas/claims/1/companydescription*](https://federation-sts.accenture.com/schemas/claims/1/companydescription)[*https://federation-sts.accenture.com/schemas/claims/1/countrycode*](https://federation-sts.accenture.com/schemas/claims/1/countrycode)[*https://federation-sts.accenture.com/schemas/claims/1/countrydescription*](https://federation-sts.accenture.com/schemas/claims/1/countrydescription)[*https://federation-sts.accenture.com/schemas/claims/1/displayname*](https://federation-sts.accenture.com/schemas/claims/1/displayname)[*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress*](http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress)[*https://federation-sts.accenture.com/schemas/claims/1/enterpriseid*](https://federation-sts.accenture.com/schemas/claims/1/enterpriseid)[*https://federation-sts.accenture.com/schemas/claims/1/geographicunit*](https://federation-sts.accenture.com/schemas/claims/1/geographicunit)[*https://federation-sts.accenture.com/schemas/claims/1/geographicunitcode*](https://federation-sts.accenture.com/schemas/claims/1/geographicunitcode)[*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname*](http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname)[*https://federation-sts.accenture.com/schemas/claims/1/middleinitial*](https://federation-sts.accenture.com/schemas/claims/1/middleinitial)[*https://federation-sts.accenture.com/schemas/claims/1/jobfamilydescription*](https://federation-sts.accenture.com/schemas/claims/1/jobfamilydescription)[*https://federation-sts.accenture.com/schemas/claims/1/location*](https://federation-sts.accenture.com/schemas/claims/1/location)[*https://federation-sts.accenture.com/schemas/claims/1/memberof*](https://federation-sts.accenture.com/schemas/claims/1/memberof)[*https://federation-sts.accenture.com/schemas/claims/1/metrocity*](https://federation-sts.accenture.com/schemas/claims/1/metrocity)[*https://federation-sts.accenture.com/schemas/claims/1/msexchimaddress*](https://federation-sts.accenture.com/schemas/claims/1/msexchimaddress)[*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name*](http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name)[*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier*](http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier)[*https://federation-sts.accenture.com/schemas/claims/1/nonaccenturenumber*](https://federation-sts.accenture.com/schemas/claims/1/nonaccenturenumber)[*https://federation-sts.accenture.com/schemas/claims/1/peoplekey*](https://federation-sts.accenture.com/schemas/claims/1/peoplekey)[*https://federation-sts.accenture.com/schemas/claims/1/personnelnumber*](https://federation-sts.accenture.com/schemas/claims/1/personnelnumber)[*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname*](http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname)[https://federation-sts.accenture.com/schemas/claims/1/*telephonenumber*](https://federation-sts.accenture.com/schemas/claims/1/telephonenumber)[*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn*](http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn)*\*additional claims may be available upon request**\*\*for sample claim values please refer to* [*Appendix A*](#_Appendix_A) *>* |
| Signing certificate public key | *<If your federation service will sign the AuthnRequest, please provide your signing certificate’s public key>* |
| Metadata file or URL | *<Please provide the metadata file or URL for the environment you want to integrate with Accenture>* |
| Application URL(If doing SP-Initiated login) | *<Please provide the Application URL (hosted on your side), which an end user can access to initiate the login process for your application>* |

# 4.0 Accenture (IdP) Integration Details

The following section contains the integration details for both the Accenture Staging and Accenture Production environments.

## Accenture Staging (Development/Staging)

|  |  |
| --- | --- |
| Federation Service URL(for both POST and Artifact) | https://federation-sts-stage.accenture.com/adfs/ls/ |
| Federation Service URI (EntityID) | urn:federation:accenture:stage |
| Federation Service Metadata URL | <https://federation-sts-stage.accenture.com/FederationMetadata/2007-06/FederationMetadata.xml> |
| Token Signing Certificate Public Key | -----BEGIN CERTIFICATE-----MIIFODCCBCCgAwIBAgIQB8xTGEwgaXnSo/Ah7bmryjANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5EaWdpQ2VydCBTSEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMTcxMjA3MDAwMDAwWhcNMjAwODA2MTIwMDAwWjB4MQswCQYDVQQGEwJVUzERMA8GA1UECBMISUxMSU5PSVMxEzARBgNVBAcTClBBUksgUklER0UxFjAUBgNVBAoTDUFjY2VudHVyZSBMTFAxKTAnBgNVBAMTIHRva2Vuc2lnbmluZy1zdGFnZS5hY2NlbnR1cmUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0bEQTypm/uAmdDN9JZJ12grbvBq7pE3IfuO+xGIxv/3IRCafv0GSD2x536G/zkzsEe5DenEK2tEbEnHWGsigqbVigpBaxm01T0HtZLSjpDGPivGcck4g4dmeG1QHlNIOGIgjw6PLTjLJg2vqTIRdD8ej8OW2wxV3e06NKBIQB8VJSES35BKvttFNFfFt+7diHSq7EbdQm+wnLK6AOA6NREHN5+EcPcEXAYNSzy0x1FNJle9DcA0AUeh/oi5vfg3yQmQ435iBXDgoE8I4BaXFSj5o5tKuV+CYeBsw6tC1pYcxIB7t/B3YJVCknLhwZMls2WwI4EA6o+tkFsEYZ/08qQIDAQABo4IB5zCCAeMwHwYDVR0jBBgwFoAUD4BhHIIxYdUvKOeNRji0LOHG2eIwHQYDVR0OBBYEFL6ULXsGl5IU7HZP6wGv5LqQZvZKMCsGA1UdEQQkMCKCIHRva2Vuc2lnbmluZy1zdGFnZS5hY2NlbnR1cmUuY29tMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwawYDVR0fBGQwYjAvoC2gK4YpaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL3NzY2Etc2hhMi1nNi5jcmwwL6AtoCuGKWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9zc2NhLXNoYTItZzYuY3JsMEwGA1UdIARFMEMwNwYJYIZIAYb9bAEBMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwCAYGZ4EMAQICMHwGCCsGAQUFBwEBBHAwbjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMEYGCCsGAQUFBzAChjpodHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRTSEEyU2VjdXJlU2VydmVyQ0EuY3J0MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggEBANiSFSuTWOGHpDZv7pQNLD6zB0Bjws/5dV+5TAdqADxvZ+Y/L5k6XmfsAJlQI6I112wUkbp31Pdf7UGucuBoU0IJkdJc2GN1fkOx/4UW44yWjwZ2qzqOOK5N2hbt6wx1e2JivJ+cUWJLOrNl9eBtyoAvkw0bevsjAPGC0IWQwqHD2t8SLpqjYB9LcW0o4wlppGJYo64y58OtVk+Eov5vwwSDiQhX2ssR2QMlHp3K+CQdYQ+JjpOhtuuctB9fDc80NlQQphj25uYYYLud67k+/sF5xh63L2TTeYU/rtxmLb/NSRyocQSGlR8TSM02FzUb0gXFkPpvuu77wkNWIuV854c=-----END CERTIFICATE----- |

## Accenture Production

*Note: Accenture’s CIO Security Integration team recommends completing a successful Staging integration before starting a Production integration.*

|  |  |
| --- | --- |
| Federation Service URL(for both POST and Artifact) | https://federation-sts.accenture.com/adfs/ls/ |
| Federation Service URI (EntityID) | urn:federation:accenture |
| Federation Service Metadata URL | <https://federation-sts.accenture.com/FederationMetadata/2007-06/FederationMetadata.xml> |
| Token Signing Certificate Public Key | -----BEGIN CERTIFICATE-----MIIFLDCCBBSgAwIBAgIQBmsDsVA/AjTIVErbkbPUxjANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5EaWdpQ2VydCBTSEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMTcxMjA3MDAwMDAwWhcNMjAwODA2MTIwMDAwWjByMQswCQYDVQQGEwJVUzERMA8GA1UECBMISUxMSU5PSVMxEzARBgNVBAcTClBBUksgUklER0UxFjAUBgNVBAoTDUFjY2VudHVyZSBMTFAxIzAhBgNVBAMTGnRva2Vuc2lnbmluZy5hY2NlbnR1cmUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAygJlefadCrrx6h23Df3ZOeoK6thKzVS0BpefWVpUfhQNpk6eVWv8f9Ld3b4zT0vFS0s0lhmJW2Ih43UCC3zochS42WCTuqMxYJV/FU7M6rzp0kMm3wfjDCyV6StcDLEZorlWKSLAMlxMurc98zMOCQSWpxMqzWvdCSv4PhEWsjx4JOeIjPbHcJYFatuaUEkScFA6EYuOt1agz9kXo4Iw+Klk+oOmWm2JpXI+z8Gk+0Xo8sX+BNOT6GsJ9WoW9ZDvQYTHEMuJJBLE4f59VXz/JIbOW5OtgW1HFMbqDuRZYm4tbxuM8mS4J9+QfVU/BokwneM2FWYp2+0t+vw5ed3skQIDAQABo4IB4TCCAd0wHwYDVR0jBBgwFoAUD4BhHIIxYdUvKOeNRji0LOHG2eIwHQYDVR0OBBYEFAvhxkEmbq3PlgvpxhUmdnDVX440MCUGA1UdEQQeMByCGnRva2Vuc2lnbmluZy5hY2NlbnR1cmUuY29tMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwawYDVR0fBGQwYjAvoC2gK4YpaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL3NzY2Etc2hhMi1nNi5jcmwwL6AtoCuGKWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9zc2NhLXNoYTItZzYuY3JsMEwGA1UdIARFMEMwNwYJYIZIAYb9bAEBMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwCAYGZ4EMAQICMHwGCCsGAQUFBwEBBHAwbjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMEYGCCsGAQUFBzAChjpodHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRTSEEyU2VjdXJlU2VydmVyQ0EuY3J0MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggEBAESGew8pOF/yGV5JQ1f/C9SXDthsWA5rbG0iam9WQuOIbb7kFc0jXOqjki1cS/MSIN69PQ0Vs6dLkyf1qSafhsMqdMVLVw2G1IlMF4JkDNtKsXTpU5r6W6Qzs3zc5+BwpCdu8qg6sQ0qbpwHxcI6bJYoM911LRVv46YQV5gmWeyANJNqnFoYj4f+H0PgE/QY4ADmimCsx0pX5fh5IFFkY7V7tutMZh1HkBgqaQVSWIXxRnGSm7tpDWdonmkmFZ5HEK56ZN5ujwTvWqWWgtcvxlRSylJ1oQ9gdkYD7sKYWOfeUFzia8lJEcLUeu5YUxT1mBCkXMUu3TPSqJoVgvefkSo=-----END CERTIFICATE----- |

# 5.0 Appendix A: Example Claims

This table contains sample dummy data for the types of claims (assertions) that Accenture can provide about our authenticated users.

|  |  |  |
| --- | --- | --- |
| Claim Name | Sample Employee | Sample Contractor |
| *CommonName* | *john.m.doe* | *john.a.smith* |
| *companydescription* | *Accenture LLP* | *Accenture LLP* |
| *countrycode* | *US* | *US* |
| *countrydescription* | *USA* | *USA* |
| *displayname* | *Doe, John* | *Smith, John* |
| *emailaddress* | *john.m.doe@accenture.com* | *john.a.smith@accenture.com* |
| *enterpriseid* | *john.m.doe* | *john.a.smith* |
| *geographicunit* | *United States* | *United States* |
| *geographicunitcode* | *USA* | *USA* |
| *givenname* | *John* | *John* |
| *middleinitial* | *M.* | *A.* |
| *jobfamilydescription* | *Analyst* | *Analyst* |
| *location* | *Chicago GS 180 LaSalle* | *Chicago GS 161 Clark St* |
| *memberof* | *CIO.Security.Integration* | *CIO.Security.Contractors* |
| *metrocity* | *CI* | *CI* |
| *name* | *john.m.doe* | *john.a.smith* |
| *nonaccenturenumber* | *NA* | *N0559019* |
| *peoplekey* | *840576* | *840577* |
| *personnelnumber* | *10806211* | *NA* |
| *surname* | *Doe* | *Smith* |
| *telephonenumber* | *+1 312-013-5430* | *+1 312-013-5431* |
| *upn* | *john.m.doe@accenture.com* | *john.a.smith@accenture.com* |