|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | |  |  | | PwC IT  Identity and Access Management (IdAM)  Application Integration Guide |
|  |  |

|  |
| --- |
|  |
| **Document Status:** Published  **Date & Version:** 06 May 2016; version 2.20  **Review Date:** N/A  **Authors:** PwC IT  **Data Classification:** DC1 |



Table of contents

[1 Management summary 1](#_Toc438555545)

[1.1 Global User Authentication 1](#_Toc438555546)

[1.2 Global Directory Service 2](#_Toc438555547)

[2 Service architecture 3](#_Toc438555548)

[2.1 Logical architecture 3](#_Toc438555549)

[2.2 Consumer interfaces 9](#_Toc438555550)

[2.3 Service Supported Protocols 9](#_Toc438555551)

[3 Feature sets 10](#_Toc438555552)

[3.1 Features 10](#_Toc438555553)

[4 Service request processes 12](#_Toc438555554)

[4.1 Request a new application integration or a new application / service account 12](#_Toc438555555)

[4.2 Request support for incident or problem 12](#_Toc438555556)

[4.3 Request an enhancement 12](#_Toc438555557)

[5 Integration methods 13](#_Toc438555558)

[5.1 Global LDAP integration 13](#_Toc438555559)

[5.2 External and Internal Authentication (Federation) 13](#_Toc438555560)

[5.3 SharePoint 21](#_Toc438555561)

[5.4 Microsoft .NET application using WIF 22](#_Toc438555562)

[6 Appendix A – Single URL (deprecated) 26](#_Toc438555563)

[7 Appendix B – IdAM EndPoints 28](#_Toc438555564)

[8 Appendix C – Login Page Customization 31](#_Toc438555565)

[8.1 Customisation template 33](#_Toc438555566)

[9 Appendix D – IBM Domino Application Integration 34](#_Toc438555567)

[10 Appendix D - Glossary 35](#_Toc438555568)

[11 Appendix E – Document Revisions 36](#_Toc438555569)

Table of figures

[Figure 1: Global Internal User Authentication Service Authentication flow 3](#_Toc450055742)

[Figure 2: End user interaction with Global Internal User Authentication Service 4](#_Toc450055743)

[Figure 3: Global External User Authentication Service Authentication flow 5](#_Toc450055744)

[Figure 4: End user interaction with Global External User Authentication Service 6](#_Toc450055745)

[Figure 5: Global Identity Broker User Authentication Service Authentication flow 7](#_Toc450055746)

[Figure 6: End user interaction with Global Identity Broker User Authentication Service 8](#_Toc450055747)

[Figure 7: Session Management and SSO experience 18](#_Toc450055748)

[Figure 8: Broker login page (not customizable) 20](#_Toc450055749)

[Figure 9: Default login page 21](#_Toc450055750)

[Figure 10: Fully customised login page 21](#_Toc450055751)

[Figure 11: Single URL integration flow diagram 27](#_Toc450055752)

[Figure 12: Fully customised login page 33](#_Toc450055753)

# Management summary

The following section is intended to describe the different components of the service. Further sections below will go into detail around the architecture, feature sets, request processes, and integration methods.

## Global User Authentication

PwC IT’s Global User Authentication Service will allow PwC to leverage industry standard authentication / authorization protocols of SAML 2, WS-Fed, and X509 to provide a uniform mechanism for External and Internal Users to provide secure entry into collaborative SharePoint sites, as well as most applications that support SAML or WS-Fed authentication.

The service only supports applications that can consume SAML, WS-Fed, OAuth and OpenID Connect tokens for authentication. SAML is an industry standard and the most widely used Protocol for authentication users to cloud services such as Google, Microsoft, and IBM.

### Internal User Authentication Service

The Global Internal User Authentication Service uses a combination of products to provide seamless and secure authentication for PwC staff.

Internal users will authenticate to the Global Internal User Authentication Service using a mixture of authentication methods:

* PwC issued Client Certificate – x509 Certificate installed on PwC workstations and managed iOS Devices
* Forms Based – GUID and Password if a valid Client Certificate is not found
* Multi-Factor – Either Certificate or GUID and Password as first factor, plus a One-Time Password (OTP) for second factor using Soft Token from Entrust Identity Guard.

The authentication method and [federation protocol](#_Service_Supported_Protocols) used will be determined by the application design and the application security requirements.

Upon authentication, users will be issued an identity token, which can then be used to access applications for authorization

### External User Authentication Service

The Global External User Authentication Services uses a similar combination of products to provide secure authentication to our external users.

External users can authenticate to the Global External User Authentication Service using a mixture of authentication methods:

* Single Factor – Username(SMTP Email address) and Password
* Multi-Factor – Username (SMTP Email address) and Password, plus security questions
* Dual-Factor – Username (SMTP Email Address) and Password, plus a One-Time Password (OTP) via Short Messaging Service (SMS) or E-Mail

The authentication method and [federation protocol](#_Service_Supported_Protocols) used will be determined by the application design and the application security requirements.

During the authentication process, users will be prompted to accept PwC’s IdAM Terms and Acceptance before they can access applications. It is a one-time user experience, unless there are changes to the Terms and Acceptance which would require the user to reaccept.

Upon authentication, users will be issued an identity token, which can then be used to access applications for authorization.

### Identity Broker Authentication Service

The Global Identity Broker Authentication Service is a “Single Identity” Provider Cloud Solution that abstracts and incorporates the Internal and External User Authentication Services. It is the default integration service for all applications. The core feature of the Identity Broker is its abstraction to the backend Identity Providers and enables PwC to integrate with more Identity Providers than just the globally hosted ones. For example, the Identity Broker can be configured to integrate with Client Identity Providers that provide an SSO experience for our clients from their local network.

Furthermore, the SaaS solution has several non-functional benefits, such as:

1. Being up to date with the latest version, which improves agility.
2. Geolocation Load balancing across 4 global data centers, which provides faster response times and high availability.
3. Automatic disaster recovery if a data center goes down.

The authentication process for Internal and External Authentication is simplified to a common page in which users can authenticate using an internal or external email address depending on the application they accessed. The Identity Broker will redirect the user to the Internal or External Authentication service based on the user type. The user will be authenticated with their supplied credentials (single factor, multi-factor, dual-factor, certificate) and then be redirected to the requested application.

## Global Directory Service

PwC IT has deployed multiple directory environments – one for Internal users and applications and one for External users and applications. Both directories are virtualized under a Virtual Directory to provide a single consolidated view and access point.

* The Internal directory environment contains accounts for all PwC staff, partners, and contractors that have been on boarded.
* The External directory environment contains non-PwC staff accounts (e.g., vendors and clients). Accounts in the External directory are created via a registration process, in which authorized PwC staff register external users. The External user then completes the registration process by setting up multi-factor information. This is required of all users during initial registration.
* The Virtual Directory (VIS) provides all data already contained in the existing Internal and External directory environments as well as the legacy Oracle Enterprise Directory.

# Service architecture

## Logical architecture

The following diagrams depict the various components that make up the PwC IT Global Internal and External Authentication Service.

### Internal User Authentication

The diagram displayed below depicts the authentication flow process through the Global Internal User Authentication Service.



Figure 1: Global Internal User Authentication Service Authentication flow

The diagram below depicts the end user interaction with the Global Internal User Authentication service via a web browser.



Figure 2: End user interaction with Global Internal User Authentication Service

### External User Authentication

The External User Authentication service provides single-, dual-, and multi-factor authentication. The integration method is to use SAML and OFIS.



Figure 3: Global External User Authentication Service Authentication flow

The diagram below depicts the end user interaction with the Global External User Authentication service via a web browser.



Figure 4: End user interaction with Global External User Authentication Service

### Identity Broker User Authentication

The Identity Broker User Authentication is a cloud based service that provides a single entry point for Internal and External users and various authentication methods.



Figure 5: Global Identity Broker User Authentication Service Authentication flow

The diagram below depicts the end user interaction with the Global Identity Broker User Authentication service via a web browser.



Figure 6: End user interaction with Global Identity Broker User Authentication Service

## Consumer interfaces

The IdAM Service has many interfaces depending on the action that is required. The following table details the various systems and their interfaces.

| Component | Interface | Description |
| --- | --- | --- |
| AD | LDAPS | Secure LDAP interface to allow applications to read and write to the AD (internal and external are separate directories) |
| Virtual Directory | LDAPS | Secure LDAP interface to allow applications to read, write or authenticate users to the consolidated view of the Internal and External Active Directories via standard LDAP functionality. |
| External Authentication | HTTPS | Secure open standards interface to allow users to authenticate to an Identity Provider via User Name and Password, and receive a token which can be used for accessing applications. |
| Internal Authentication | HTTPS | Secure open standards interface to allow users to authenticate to an Identity Provider, via a PwC certificate, and receive a token which can be used for accessing applications. |
| GUM | HTTPS | Secure web application to register external users (single/bulk) for external authentication, password, security questions reset, and external user self-service password change. These functionalities are also available through an API (SOAP). |

## Service Supported Protocols

The IdAM Service supports various industry standard federation protocols. It is up to the application team to determine which protocol best suits their needs. The following table details the various supported protocols and their versions.

| Protocol | Version |
| --- | --- |
| SAML | 2.0 |
| WS-Fed | 1.2 |
| WS-Trust | 1.4 |
| OAuth | 2.0 |
| OpenID Connect | 1.0 |

# Feature sets

## Features

### Single Factor Login

Both the Global Internal and Global Identity Broker Authentication Services provide capabilities for users to authenticate with a single set of credentials. For Internal User login, both services require the user’s Client Certificate for login, however, the Identity Broker Service requires the user to supply their PwC email address first (this can be avoided in consecutive login attempts should the user enable the “Remember Me” checkbox). For External User login, the Identity Broker service requires the user’s email address and password as credentials.

### Multi-Factor (MFA) Login

Both the Global Internal and Global Identity Broker Authentication Services provide capabilities for users to authenticate with a multiple set of factors. The Identity Broker allows applications to be configured for MFA using One Time Passwords (OTP) that can be sent to the user through an SMS text & through email or it can be configured for MFA using Knowledge Based Answers (KBA). The Internal Authentication service allows applications to be configured for MFA using Soft-Token OTPs that are generated through a Smart application.

### Certificate Login

The Internal Authentication Service’s primary authentication method is through the use of Client Certificates installed on the Users’ Workstation. Once the certificate is recognized by an application, the user is automatically authenticated and redirected back to the application without ever having to enter any credentials.

### I forgot My Password

The Identity Broker Authentication service provides a way for users to reset their password through the “Forgot your Password” link in the login page. Users will be requested to verify themselves by answering a KBA question and then an email with a temporary password will be sent.

### Change Password

Whenever a new External User attempts to access the Identity Broker or if an existing External User attempts to reset their password using a temporary password, the user will be redirected to a change Password page. During this process, the user must provide their temporary password as well as create a new password while conforming to the password character restrictions.

In a case where an External User’s password has expired, they will be redirected to the change Password page. Similarly, they must provide the expired password as well as create a new password while conforming to the password character restrictions.

### Terms & Conditions

As part of OGC’s Data Privacy and Risk requirements, External Users must now accept PwC’s IdAM Terms and Acceptance agreement when attempting to access the IdAM services. Users will only be required to accept it once, and on any future logins when there are changes to the Terms and Acceptance content.

### Step-Up Login

Step-Up Login prevents users that authenticated to a less secure application using only a single factor such as an email and password (Basic Authentication) to SSO into a more secure application that requires a second factor (Strong Authentication). Users are required to re-authenticate with the required set of factors when switching between Strong Authentication and Basic Authentication.

### Single Sign-On (SSO)

SSO is a process which allows users to access multiple applications without having to re-authentication multiple times. This is achieved in the IdAM by the use of Identity tokens.

### Register Single User

GUM has the capability for Administrators to register an External User by filling out the user’s information through a web interface.

External users can also self-register through Active Directory Web Services (ADWS) v3.

### Register Bulk Users

GUM also has the capability for Administrators to register bulk External Users by filling out the user’s information through a web interface. The user creation is not immediate as there are back end batch processes that must execute at periodic intervals for data synchronization.

### Register Users via API Call

In addition the existing manual User Registration services GUM provides, applications can now use API calls to register single or bulk External Users.

### Password Reset

In cases where an External User cannot reset a password themselves, Administrators can use the GUM web interface to reset a password and email an automatically generated temporary password. When the user attempts to login with the temporary password, they will be prompted to change their password to proceed forward.

### Knowledge Based Answer (KBA) Reset

In cases where the user requires to reset their KBA’s, Administrations can use the GUM web interface to reset the KBA’s. When the user attempts to login after a reset, they will be prompted to set their new KBA’s to proceed forward.

### Client Federation

Both the Global Internal and Global Identity Broker Authentication services use Federation at their core which allows users to possess a single user identity and use it to authenticate against multiple applications. User information is sent to Clients applications by the IdAM service through Identity Claims.

### Member Firm Federation

Member firms interested in using their user’s existing identity can do so by configuring an Identity Provider-Replying Party relationship with External Authentictation Services.

### Custom Login Pages

Applications can customize the shared login pages to match application/site style (e.g., CSS, colours, graphic images). Refer to [Custom Login Pages](#_Custom_login_pages) & [Appendix A](#_Appendix_A_–) for examples and integration information.

### 3.1.17 Requesting Dynamic Groups

Dynamic Groups are user groups in AD, comprised of accounts which are included automatically if part of the defined criteria and filtering selections of a requested Group. A Dynamic Group can be requested from IdAM, which can include all the needed users from a particular firm, territory, or application. To request a Dynamic Group, please submit an IdAM Integration Request Form.  
  
**For example** – [*All External Users in UK, With a Last Active Date of 1 Day Ago or less, and Federated User = True*.]   
This example set of criteria, or ‘filters’, will allow for a group to be dynamically populated with all the members who fit the criteria.

### 3.1.18 External Self-Registered (IA1) Users

External user accounts can be created by a PwC contact, or users can create an IA1-level account themselves. Users who do not have a PwC account are able to access the Self-Registration wizard from the Login Pages. There is a “Self-Registration” hyperlink placed in the bottom footer area of the application Login Page.

External Users are able to register themselves at the PwC Self-Registration portal. Users who self-register are placed in the Identity Assurance (IA) Level 1, known as IA1. For application owners who desire to allow IA1 users access into their application – please indicate so when completing the IdAM Integration Request Form. Please comply with all relevant security guidelines and standards for external application access.

**Setting up an Application for IA1 User level access**

Please contact the IdAM Team to enable your application for ESR access. If you are integrating for the first time, this option can be requested in the IdAM Integration Request Form. Please visit the IdAM Requests Portal to submit a new IdAM Integration request form.

# Service request processes

## Request a new application integration or a new application / service account

Please raise a new request by adding a new item to the IdAM Integration Requests Portal here:

<https://pwcit.pwcinternal.com/sites/products/idam/Lists/IdAM%20Integration%20Request%20Form%20%20Online/AllItems.aspx>

If you do not know all the requested information when you start a new item, you will be able to update your request by editing the item you create at later time or date.

For more details on the IdAM services, processes, and reference guides, please visit our [IdAM Spark page](https://pwc-spark.com/groups/pwc-itonecommunity/projects/identity-and-access-management-idam-programme).

## Request support for incident or problem

For issues around integration activities, please contact the IdAM Service Manager, **Marty Coker,** at [marty.coker@us.pwc.com](file:///C:/Users/mcoker001/Documents/SharePoint%20Drafts/marty.coker@us.pwc.com).

If you encounter an issue with the production service, please contact your territory IT Service Desk to create a ticket to be escalated to the PwC IT Global Service Desk (GSD) for investigation.

## Request an enhancement

Enhancement requests should be submitted to PwC IT IdAM Requests@Americas-US. The request should include the following information:

* Application or Line of Service (LoS) requesting enhancement
* Detailed description of the enhancement and associated use cases
* Business sponsor
* Technical lead – business side

# Integration methods

## Global LDAP integration

The IdAM solution provides three LDAPs interfaces for consuming applications.

1. Virtual Directory
2. Internal Active Directory
3. External Active Directory
4. Oracle Enterprise Directory Server

The integration to all three follows the same basic process – a request to the IdAM Service Manager mentioned in [*Section 4, Service Management Processes*](#_Service_management_processes)*,* followed by integration of the consuming application.

**All consuming applications are required to use the Virtual Directory interface –** with onlycertain exceptions (e.g., applications that require Windows Accounts to run services).

To use any account, the application must comply with the following requirements:

* Access approved via the Service Management processes
* Secure password storage (i.e., encrypted)
* Use of secure objects when referencing the password (i.e., .NET SecureString Class)
* Practice to never share password

### Global LDAP directory schema

The virtual directory exposes and aggregate schema which is a combination of both the IntUsers and ExtUsers Forest schemas as well as Oracle Enterprise Directory. Information about Active Directory’s base schema can be found here:

<http://technet.microsoft.com/en-us/library/cc773309(v=ws.10).aspx>

In addition to the standard Active Directory Person objects and attributes, which can be found [here](http://msdn.microsoft.com/en-us/library/windows/desktop/ms683895(v=vs.85).aspx) for reference, the AD schema has been extended to include PwC specific attributes. Schema extensions that have been made within the Forest will be available through VIS .

## External and Internal Authentication (Federation)

Applications can be configured to use the External or Internal Authentication services through Claims-based Login.

Both the Internal and External IdAM Services contain various SAML/WS-Fed Identity Providers (IdP) Applications will trust only OFIS as their IdP. The other IdPs are trusted by OFIS. The sections below provide examples of consuming these services.

### Identity Provider (IdP) End Points

The following tables provide a list of OFIS endpoints.

Identity Broker Development

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://fedsvc-dev.pwc.com/ofisd/ |
| Entity Identifier | ofis:pwc:broker:d |
| Federation Metadata URL | https://fedsvc-dev.pwc.com/ofisd/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://fedsvc-dev.pwc.com/ofisd/public/SignOut.aspx |
| Certificate Thumbprint | 2EE148D651630AACC591C806B5A5370090671F5A |

Identity Broker Staging

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://fedsvc-stage.pwc.com/ofiss/ |
| Entity Identifier | ofis:pwc:broker:s |
| Federation Metadata URL | https://fedsvc-stage.pwc.com/ofiss/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://fedsvc-stage.pwc.com/ofiss/public/SignOut.aspx |
| Certificate Thumbprint | 2EE148D651630AACC591C806B5A5370090671F5A |

The Internal and External Staging Authentication [End Points](#_Appendix_B_–_1) are only to be used in cases where using the Identity Broker is not an option.

Identity Broker Production

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://fedsvc.pwc.com/ofis/ |
| Entity Identifier | ofis:pwc:broker |
| Federation Metadata URL | https://fedsvc.pwc.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://fedsvc.pwc.com/ofis/public/SignOut.aspx |
| Certificate Thumbprint | 2EE148D651630AACC591C806B5A5370090671F5A |

The Internal and External Production Authentication [End Points](#_Appendix_B_–_1) are only to be used in cases where using the Identity Broker is not an option.

### Offered claims

The following table lists the claim descriptors that are sent to an application in the SAML/WS-Fed assertion.

|  |  |  |  |
| --- | --- | --- | --- |
| Claim Name | Claim Type | Availability | |
| Immutable ID  *(ObjectID of AD User Object)* | http://schemas.microsoft.com/liveid/federation/2008/05/immutableid  (e.g. HgiFbvcDrUpELcQ6B4IxGA==) | | Int / Ext |
| Authentication Instant  *(Time of User Authentication)* | http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant  (e.g. 2016-05-03T11:21:46.862Z) | | Int / Ext |
| Authentication Method  *(Login Method via SAML Context Class)* | http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod  (e.g. urn:oasis:names:tc:SAML:2.0:ac:classes:X509) | | Int / Ext |
| Role  *(Group(s) a User Belongs to Global AD)* | http://schemas.microsoft.com/ws/2008/06/identity/claims/role | | Int / Ext |
| Windows Account Name  *(PPI for External Users and AD User SID for Internal Users)* | http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname | | Int / Ext |
| EmployeeID  *(Employee ID)* | http://schemas.pwc.com/identity/claims/employeeid  (e.g. 00300823264) | | Internal |
| LineofService  *(LoS information)* | http://schemas.pwc.com/identity/claims/lineofservice  (e.g. US – IFS) | | Internal |
| OfficePhone  *(Office Phone)* | http://schemas.pwc.com/identity/claims/officephone  (e.g. +1 (813) 348-7000) | | Internal |
| Locality  *(City)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality (e.g. Austin) | | Internal |
| StateorProvince  *(State or Province)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince  (e.g. TX) | | Internal |
| AuthLevel  *(Method of Authentication – CERT, PWD, MFA)* | http://schemas.pwc.com/identity/claims/authlevel | | Int/Ext |
| Cloud Email  *(Google Cloud Email Address)* | http://schemas.pwc.com/identity/claims/cloudemailaddress  (e.g. rsmith021@pwc.com) | | Internal |
| Employee Type  *(Identifies Employee or Visitor)* | http://schemas.pwc.com/identity/claims/employeetype | | Internal |
| Middle Name  *(Middle Name)* | http://schemas.pwc.com/identity/claims/middlename | | Internal |
| Organization  *(PwC Territory)* | corchttp://schemas.pwc.com/identity/claims/organization  (e.g. US) | | Int / Ext |
| PwC GUID  *(PwC/Notes GUID)* | http://schemas.pwc.com/identity/claims/pwcguid  (e.g. rsmith021) | | Internal |
| PwCUserType  *(Identifies Internal or External)* | http://schemas.pwc.com/identity/claims/pwcusertype | | Int / Ext |
| Common Name  *(Common Name)* | http://schemas.xmlsoap.org/claims/commonname | | Int / Ext |
| Country  *(2-Letter Country Code)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country  (e.g. GB) | | Int / Ext |
| E-Mail Address  *(Email Address)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress  (e.g. robert.a.smith@us.pwc.com) | | Int / Ext |
| Given Name  *(First Name)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | | Int / Ext |
| Name  *(Full Name)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name  (e.g. Robert A Smith) | | Int / Ext |
| Name ID  *(SAML Name Identifier)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier | | Int / Ext |
| PPID  *(Private Personal Identifier)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier  (e.g. 1000345787) | | Int / Ext |
| PwC Identity Assurance Level  *(Numerical Value Depicting How an Account was Created)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/pwcidentityassurancelevel  (Self-Registered [1] or PwC Staff Registered Account [2]) | | External |
| Surname  *(Last Name)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | | Int / Ext |
| User Principal Name  *(User Principal Name in AD)* | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn  (e.g. rsmith21@intusersstg.glblintstg.ad.pwcinternal.com) | | Int / Ext |

### Session management

There are two types of timeouts that impact session management:

1. IDP/STS Web SSO**.**  This is a global setting that cannot be set per Application/Relying Party in OFIS.
2. Token Lifetime, set to **60 minutes by default**. This can be set to a different value per Application/Relying Party in OFIS

Authentication to the IDP/STS **is not** validated upon each access (i.e., mouse click) within the application; only when the application timeout occurs, does the user get redirected back to the IdP/STS to check their session. If they are redirected within the 20-minute window, they will experience SSO back into the site. If they are over the 20 minutes, then they will be forced to re-authenticate.

The diagram below depicts the end user experience for SSO depending on time elapsed when accessing a SharePoint application.



Figure 7: Session Management and SSO experience

**Note:** SharePoint introduces another variable/setting for session management, LogonTokenCacheExpirationWindow. This setting is SharePoint specific anddoes not change how the IdAM IDP/STS works, but does impact end user experience as to when they are required to re-authenticate.

Please click on the following link to review a well written document on SharePoint and OFIS session management:

<http://msdn.microsoft.com/en-us/library/hh446526.aspx>

#### Identity Management Service cookies

The following is a list of all the cookies that are issued by Global IdAM Service:

| Cookie | Name | Purpose | Duration | |
| --- | --- | --- | --- | --- |
| Federation | ofisORIG\_RPURN | A session token that identifies what application URN the user attempted to access. | | Entire Session |
| Federation | ofisRPURN | A Session token that identifies what direct Relying Party URN the user was redirected from. | | Entire Session |
| Federation | ofisQUERY\_STRING | A Session token that identifies the querystring of the request. | | Entire Session |
| Federation | ofisREMEMBER\_ME | A session token that identifies the users email address. | | Entire Session |
| Federation | ofisFED\_IDPS | A session token that contains the IdP URN the user logged in from. | | Entire Session |
| Federation | ofisFED\_SPS | A session token that contains a list of all Relying Party Application URN's the user is currently logged into. | | Entire Session |
| Federation | ofisIDP\_ASSERTION\_SUBJECT\_NAME | A Session token that identifies the user's subject name attribute/value from the IdP logged in from. | | Entire Session |
| Federation | ofisRETURN\_URL | A Session token that identifies where to redirect the user after federation has been completed. | | Entire Session |
| Federation | ofisTARGET\_URL | A session token that identifies where to redirect the user after federation has been completed. | | Entire Session |
| Federation | ofisEVENT\_SLA | A session token that identifies SLA start times of federation events. | | Entire Session |
| Federation | ofisHRD | A Persistent token that identifies HRD URN the user choose to remember during the HomeRealmDiscover process. | | 365 days |
| Federation | OFIS.ASPXAUTH | A session token that represents the Logged in user within the current ASP.NET session. | | Entire Session |
| Federation | opRP\_URL | A Session token that identifies what direct Relying Party URN the user was redirected from. | | Entire Session |
| Federation | opStsSiteCookie | A Session token that identifies where to redirect the user after federation has been completed. | | Entire Session |
| Federation | VISFedAuth | A session token that represents the Logged in user within the current ASP.NET session. | | Entire Session |

### Custom login pages

The External IdAM service provides a shared login page that all applications redirect to for authenticating users. If desired, the service has the ability to provide minor custom branding on a per application basis.

When the user is redirected to the application shared login page, the application/Relying Party ID is included in the login request. The External IdAM service can key off this ID and present a customized login page.

Note: For applications using the Identity Broker, the initial redirect page to gather the user email address is not customizable. However, the following page is customizable and adheres to the details listed above.

Below are examples of what the standard and fully customized pages look like.

Default Pages:

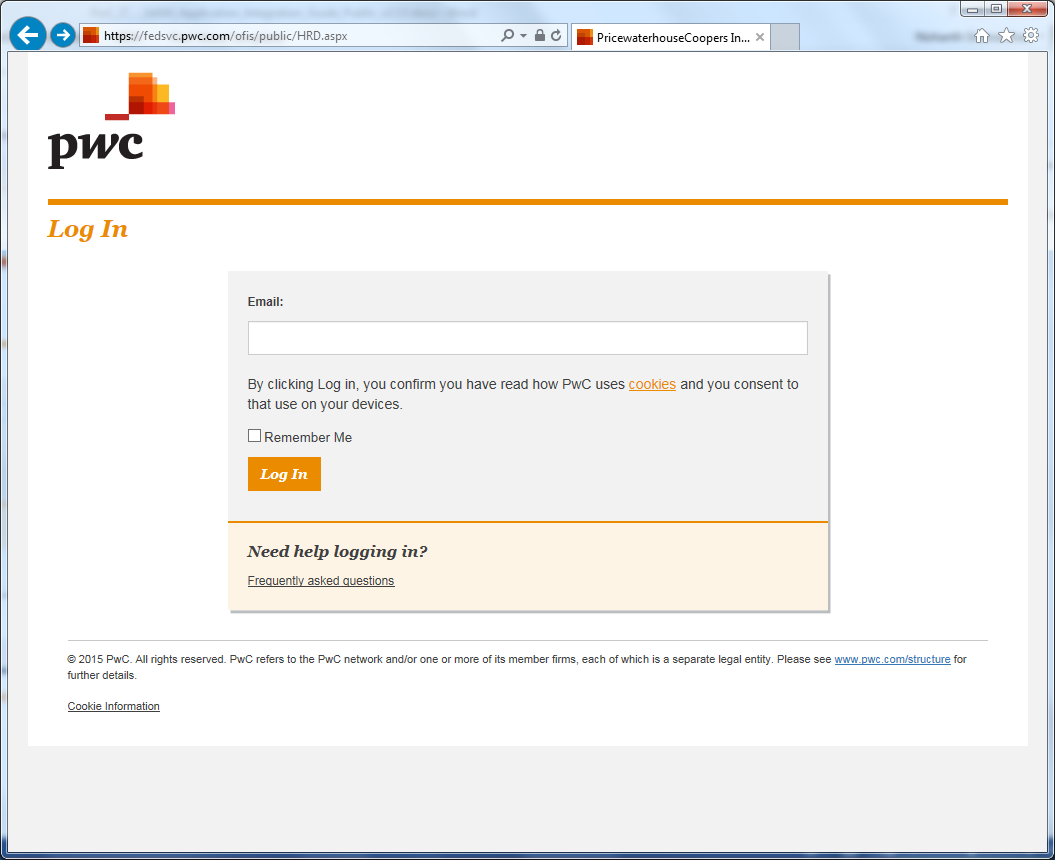


Figure 8: Broker login page (not customizable)

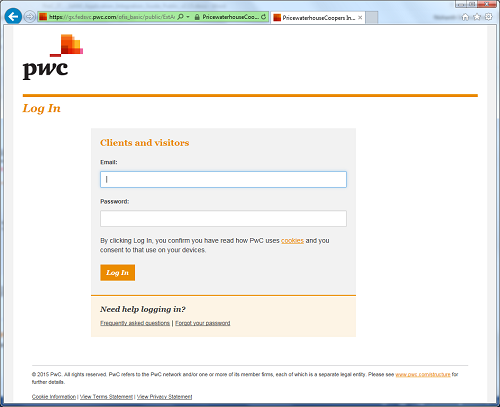


Figure 9: Default login page

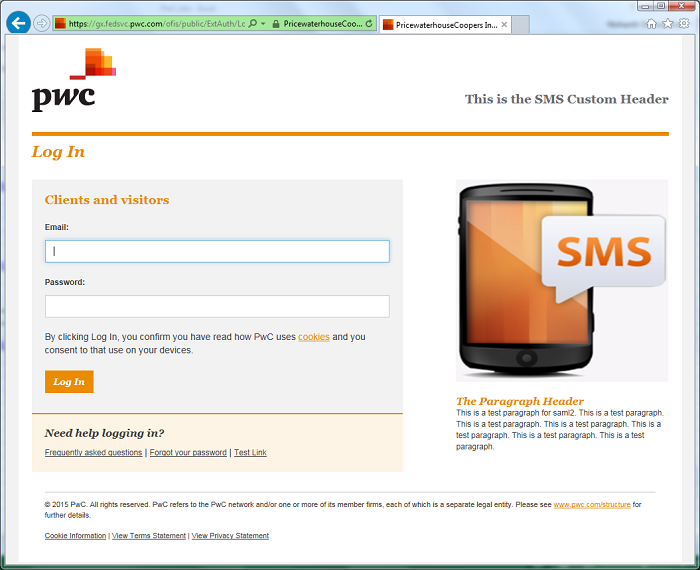


Figure 10: Fully customised login page

For more details and sample files, please see [*Appendix A, Login page customisation*](#_Appendix_C_–_1).

## SharePoint

### SharePoint Trusted Token Issuer configuration

PwC IT provides a deployment package for configuring SharePoint. To ensure you have the latest package available from PwC IT, please contact the IdAM Service Manager, Marty Coker, for latest version.

### Claims-based logout

For any application, including a SharePoint web application to participate in the SSO process, it must be able to handle the following scenarios:

* The user should be able to initiate the Single Log Out (SLO) from within the web application. The web application modified the behaviour of the standard sign-out process to send the WS-Federation wsignout message to the token issuer. This token issuer is OFIS.
* SharePoint web applications should handle WS-Federation wsignoutcleanup messages from the issuer and invalidate any security tokens for the application.

#### Current custom Claims-based Logout

To implement a successful Claims-based SLO, you must modify SharePoint to use the OFIS SLO URL.

1. Log into SharePoint as the Farm Administrator.
2. Edit …\14\TEMPLATES\CONTROLTEMPLATES\Welcome.ascx
3. Find a control called ID\_Logout and rename to ID\_Logout2 and modify the URL to be the OFIS SLO URL
4. Enter the correct OFIS SLO URL, for example, Production External: <https://fedsvc.pwc.com/ofis/public/SignOut.aspx>

**Note:** For the complete list of all SLO URLs for each environment and each instance, please see the [OFIS End Points section](#_AD_FS_End).

#### Microsoft suggested Claims-based Logout

Per the document from Microsoft (i.e., <http://msdn.microsoft.com/en-us/library/hh446525.aspx#sec19>), we may use Microsoft suggested claims-based SLO implementation instead of customizing Welcome.ascx.

There are issues related to the solution by customizing Welcome.ascx:

* It only supports a single token issuer since the AD FS SLO URL is hard coded across the entire farm.
* It is only 100% effective with SharePoint applications that use session cookies.
* SharePoint applications that use persistent cookies can have inconsistent logout experiences.

Consider the following scenario with SharePoint persistent session cookie:

A user closes the browser without clicking Sign Out, the AD FS MSISSignOut is gone since it is not a persistent cookie. When a user re-opens the browser and re-visits a SharePoint web application, does some work, and clicks Sign Out which sends wsignout message to AD FS, eventually a user will see the AD FS sign-out page. Unfortunately, the SharePoint session is still active, since AD FS doesn’t send wsignoutcleanup request to SharePoint due to missing MSISSignOut cookie.

For details about MSISSignOut cookie, refer to [*Section 5.2.2.1, Identity Management Service cookies*](#_Idenity_Management_Service).

Microsoft suggested claims-based logout implementation is based on HttpModule. The solution fixes the issues mentioned above.

The solution needs to install HttpModule for each SharePoint web application participated in Federation.

#### SharePoint FedAuth cookies

The FedAuth cookie can exist either as a persistent or in-memory cookie. After a user has successfully authenticated by any method to SharePoint, a FedAuth cookie is generated. The cookie represents the SharePoint session token. This cookie contains a reference to the SAML token that SharePoint stores in its token cache. The SAML token contains the claims issued to the user by any external identity and federation providers, and by the internal SharePoint security token service (STS).

To modify the cookie to in-memory, complete the following steps:

1. Log in to the SharePoint server as a Farm Administrator.
2. Open SharePoint 2010 Management Shell **as Administrator.**
3. Enter the following commands:

* $sts = Get-SPSecurityTokenServiceConfig
* $sts.UseSessionCookies = $true
* $sts.Update()

1. Complete an IIS reset.

**Note:** SharePoint requires persistent cookies for certain functionality, such as opening Office documents without being prompted for credentials, drop, and drag in Windows Explorer, and a few others.

## Microsoft .NET application using WIF

Windows Identity Foundation (WIF) is a set of classes and tools, an extension to the .NET Framework that enables you to use claims-based identity when developing ASP.NET or WCF applications.

This section documents only Passive federation/integration between OFIS and ASP.NET based on WS-Federation Passive protocol.

The Active Federation WS-Trust will be added in the appropriate phase, as needed.

### Federation metadata exchange

To establish the federation trust relationship, OFIS and Claims-based .NET application need to exchange federation metadata.

A federation metadata document is an XML document that conforms to the WS-Federation 1.2 schema. Federation metadata may be imported from a file, or the partner may make the data available via https. The latter method provides the most straightforward method for creating a partnership and greatly simplifies any ongoing maintenance that may be required.

Manually creating a federation party trust requires that the Administrator supply a fair amount of information that must be obtained from the partner organization through some out of band communication. This information includes the URLs for the WS-Federation Passive protocol, one or more federation entity identifiers and, typically the X.509 Certificate used to sign and/or encrypt/decrypt any claims sent or received from the federation party.

The following table shows example federation metadata URLs. For the complete list of all URLs for each environment and each instance, please refer to the [OFIS End Points section](#_AD_FS_End).

**Note:** When Claims-based ASP .NET application defines federation identifier, it should follow the naming convention for Federated applications. Please check with the IdAM team for compliant federation identifier for your application.

The Standard Format will have four delimited fields separated by colons:

* First Delimited Field is always urn
* Second Delimited Field is the application FQDN (e.g., eldsredirect.pwcinternal.com)
* Third Delimited Field is an application code or LoS (e.g., elds)
* Fourth Delimited Field is the physical location code of the RDC or hosting location that the application resides in (e.g., deg)

### Claims-based ASP.NET configuration

For Claims-based ASP.NET application to externalize authentication and coarse-grained authorization to rely on OFIS, the web.config needs to be configured with WIF-related elements usually by tooling approach.

The following configuration setting is a basic example to show the WIF-related elements based on federation metadata exchange between OFIS and Claims-based ASP.NET application.

Items requiring changes are in **BOLD.** You will work with the PwC IT IdAM Team to determine some of these values.

In the .Net 3.5 example web.config file below, [**https://wp-stage.pwc.com/**](https://wp-stage.pwc.com/)is the application URL example, and **urn:us.wpstage.pwc.com:wp:us** is the example realm ID

<microsoft.identityModel>  
 <service>  
 <audienceUris>  
 <add value="urn:us.wp-stage.pwc.com:wp:us" />  
 </audienceUris>  
 <federatedAuthentication>  
 <wsFederation   
 passiveRedirectEnabled="true"   
 issuer=" https://fedsvc.pwc.com/ofis/"   
 realm="urn:us.wpid-stage.pwc.com:wpd:us"   
 reply="https://wp-stage.pwc.com/"   
 requireHttps="true" />  
 <cookieHandler requireSsl="true" />  
 </federatedAuthentication>  
 <applicationService>  
 <claimTypeRequired>  
 <claimType type="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" optional="true" />  
 <claimType type="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" optional="true" />  
 ….  
 </claimTypeRequired>  
 </applicationService>  
 <issuerNameRegistry type="Microsoft.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf345856ad364e35">  
 <trustedIssuers>  
 <add thumbprint="ecbf4a7c488d811b9e06f237658b8544da90262bea" name=" urn:deg.fedsvc.pwcinternal.com:ofis:deg" />  
 </trustedIssuers>  
 </issuerNameRegistry>  
 <certificateValidation certificateValidationMode="None" />  
 </service>  
 </microsoft.identityModel>

The following table is a list of primary configuration elements that are part of ASP .NET application federation metadata.

|  |  |
| --- | --- |
| Element Name | Description |
| audienceUris | Lists all the intended audience URIs that are considered valid for tokens received by this claims-based ASP .NET application |
| realm | This is a URI or URN identifying this ASP .NET application to OFIS |
| Reply | Indicates the ASP .NET application URI to which OFIS responses should be directed |
| issuer | Contains the endpoint address of OFIS to which unauthenticated requests will be redirected. |
| trustedIssuers | Maintains a list of trusted issuers, such as OFIS |
| thumbprint | The signature of an incoming token can always be verified by associating certificate thumbprint to the issuer name |

**Note:** For application’s federation metadata generation tool, if the realm and reply cannot be populated differently, one needs to manually update the generated metadata file.

The value of realm is configured differently from reply in the web.config.

<wsFederation   
 passiveRedirectEnabled="true"   
 issuer="https://deg.fedsvc.pwc.com/ofis/"   
 realm="urn:us.wpistage.pwc.com:wpd:us"   
 reply="https://wpistage.pwc.com/"   
 requireHttps="true" />

The value of realm (entityID) is same as reply (Address) in the generated metadata file.

<EntityDescriptor ID="\_06f897b4-e0a8-43fa-9147-0a4c9a86dd66" entityID="**https://wp-stage.pwc.com/**" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

<RoleDescriptor xsi:type="fed:ApplicationServiceType" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706" protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  
 <fed:ClaimTypesRequested> ....  
 <fed:TargetScopes>  
 <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">  
 <Address>https://wpid-stage.pwc.com/</Address>  
 </EndpointReference>  
 </fed:TargetScopes>  
 <fed:PassiveRequestorEndpoint>  
 <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">  
 <Address>https://wpid-stage.pwc.com/</Address>  
 </EndpointReference>  
 </fed:PassiveRequestorEndpoint>  
 </RoleDescriptor>  
</EntityDescriptor>

The metadata has to be changed as shown below in order to be consistent with web.config.

<EntityDescriptor ID="\_06f897b4-e0a8-43fa-9147-0a4c9a86dd66" entityID="**urn:us.wp-stage.pwc.com:wp:us**" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

Similarly, here is a .Net 4.5 configuration example using the same settings:

<system.identityModel>  
 <identityConfiguration>  
 <audienceUris>  
 <!-- UPDATE THE VALUE BELOW TO THE URN OF THE APPLICATION -->  
 <add value="**urn:us.wp-stage.pwc.com:wp:us**" />  
 </audienceUris>  
 <issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">  
 <trustedIssuers>  
 <!-- UPDATE THE THUMBPRINT OF THE SIGNING CERT OF YOUR IDP AND NAME/URN OF YOUR IDP IN THE 'NAME' ELEMENT -->  
 <add thumbprint="**DB27CC8C6AB01E72219992E69F3E134DED74CCFA**" name="**deg\_IdP**" />  
 </trustedIssuers>   
 </issuerNameRegistry>  
 <certificateValidation certificateValidationMode="None" />  
 <securityTokenHandlers>  
 <add type="System.IdentityModel.Services.Tokens.MachineKeySessionSecurityTokenHandler,System.IdentityModel.Services, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />  
 <remove type="System.IdentityModel.Tokens.SessionSecurityTokenHandler,System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />  
 </securityTokenHandlers>  
 </identityConfiguration>  
</system.identityModel>  
  
<system.identityModel.services>  
 <federationConfiguration>  
 <!-- UPDATE THE NAME BELOW THAT WILL BE THE COOKIE NAME USED FOR THIS APP, BE CARFULE TO MAKE SURE THIS IS UNIQUE ACROSS ALL YOUR DEPLOYMENTS -->  
 <cookieHandler requireSsl="true" name="**wpstage**" path="/" />  
 <!-- UPDATE THE ISSUER ELEMENT TO BE THE URL (NOT URN) OF YOUR IDP, THE REALM, IS THE URN OF THIS TEST APPLICATION AND THE REPLY IS THE ROOT URL OF THIS APPLICATION-->  
 <wsFederation passiveRedirectEnabled="true" issuer=" **https://deg.fedsvc.pwc.com/ofis/**" realm="**urn:us.wp-stage.pwc.com:wp:us**" reply="**https://wp-stage.pwc.com/**" requireHttps="true" />  
 </federationConfiguration>  
</system.identityModel.services>

For a detailed list of examples on how to integrate applications with IdAM servers, please refer to the [developer portal](https://fedsvc-stage.pwc.com/devportals/).

# Appendix A – Single URL (deprecated)

Single URL is now a deprecated feature within the External IdAM service to provide the ability for both internal and external users to access a SharePoint or .NET application using the same Internet facing URL (e.g., teamspace.pwc.com), while also maintaining different authentication methods for each user type:

* User name and password for external users
* Certificate and “invisible” login for internal users

The Global Identity Broker service now replaces the Single URL feature and is to be used for all applications that are accessed by both internal and external users. The Single URL feature is only available in Global External Authentication services to assist migrate already integrated applications.

The diagram below shows the overview of Single URL integration flow.



Figure 11: Single URL integration flow diagram

The main steps are performed as follows:

1. The user attempts to access SharePoint or .NET site in Step 1.
2. In Step 2, the Global External Authentication Service login page looks for the RememberMe cookie. If the cookie is for an Internal Email Address (ex. ..@us.pwc.com) then it goes to Step 3. If the cookie is for an External Email Address (ex. ..@gmail.com) then it goes to Step 4. If no cookie is found, then it goes to Step 5.
3. Step 3 validates the user’s Client Certificate through the Global Internal Authentication Service.
4. The user is then authenticated in Step 6 and a valid WS-Fed token is generated.
5. In Step 11, the user is redirected back to the SharePoint application.
6. If at Step 2, the user’s RememberMe cookie was for an External user then the user is redirected to the SharePoint site’s customized login page and prompted to enter their password as in Step 4.
7. In Step 8, the user is redirected back to the Global External Authentication Service where they are authenticated and a valid WS-Fed token is generated. They are then directed to Step 10.
8. If at Step 2 a valid RememberMe cookie was not found, then the user is redirected to the Global External Authentication Service where they are prompted to enter their email address.
9. Step 7 determines if the entered email address is an Internal or External Address. If it is an Internal Address then the user is directed to Step 9.
10. At Step 9, the user has been identified to be an Internal User, therefore they are redirected to the Global Internal Authentication Service Step 3.
11. If at Step 7 the email address entered is found to be an External Address, then the use is redirected to the SharePoint site’s customized login page and prompted to enter their password as in Step 4. They are then directed to Step 8.

Implementing SingleURL requires changes on both the IdAM side, as well as installing code and HTTP modules, on the SharePoint Farm or .NET application.

On the IdAM side, both the Internal & External OFIS IdP must be configured to know about the External URL end point as well as updating/creating the custom.xml file that resides on the External OFIS IdP.

# Appendix B – IdAM EndPoints

Internal Authentication Staging Europe

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://deg.fedsvc-stage.pwcinternal.com/ofis/ |
| Entity Identifier | urn:deg.fedsvc-stage.pwcinternal.com:visfed:deg |
| Federation Metadata URL | https://deg.fedsvc-stage.pwcinternal.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://deg.fedsvc-stage.pwcinternal.com/ofis/public/SignOut.aspx |
| Certificate Thumbprint | ‎5263D22EEFF44991BB1617891FB18219E4B8D9B3 |

Internal Authentication Staging US

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://us.fedsvc-stage.pwcinternal.com/ofis/ |
| Entity Identifier | urn:us.fedsvc-stage.pwcinternal.com:visfed:us |
| Federation Metadata URL | https://us.fedsvc-stage.pwcinternal.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://us.fedsvc-stage.pwcinternal.com/ofis/public/SignOut.aspx |
| Certificate Thumbprint | 5B2FDF139AC529875D14EF658217A0496D54EE7B |

External Staging – Strong Authentication

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://gx.fedsvc-stage.pwc.com/ofis/ |
| Entity Identifier | urn:federation:gx.fedsvc-stage.pwc.com:ofis:gx |
| Federation Metadata URL | https://gx.fedsvc-stage.pwc.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://gx.fedsvc-stage.pwc.com/public/SignOut.aspx |
| Certificate Thumbprint | 0FA44D103901F7402DF81FD0A973D2AFCCD7E8A7 |

External Staging – Basic Authentication

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://gx.fedsvc-stage.pwc.com/ofis\_basic/ |
| Entity Identifier | urn:federation:gx.fedsvc-stage.pwc.com:ofis\_basic:gx |
| Federation Metadata URL | https://gx.fedsvc-stage.pwc.com/ofis\_basic/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://gx.fedsvc-stage.pwc.com/ofis\_basic/public/SignOut.aspx |
| Certificate Thumbprint | 0FA44D103901F7402DF81FD0A973D2AFCCD7E8A7 |

Internal Authentication Production Europe

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://deg.fedsvc.pwcinternal.com/ofis/ |
| Entity Identifier | urn:deg.fedsvc.pwcinternal.com:visfed:deg |
| Federation Metadata URL | https://deg.fedsvc.pwcinternal.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://deg.fedsvc.pwcinternal.com/ofis/public/SignOut.aspx |
| Certificate Thumbprint | F5DBA00484F09EC2CC73BF389621DADD0DBA35F8 |

Internal Authentication Production Hong Kong

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://hkg.fedsvc.pwcinternal.com/ofis/ |
| Entity Identifier | urn:hkg.fedsvc.pwcinternal.com:visfed:hkg |
| Federation Metadata URL | https://hkg.fedsvc.pwcinternal.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://hkg.fedsvc.pwcinternal.com/ofis/public/SignOut.aspx |
| Certificate Thumbprint | F5DBA00484F09EC2CC73BF389621DADD0DBA35F8 |

Internal Authentication Production US

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://us.fedsvc.pwcinternal.com/ofis/ |
| Entity Identifier | urn:us.fedsvc.pwcinternal.com:visfed:us |
| Federation Metadata URL | https://us.fedsvc.pwcinternal.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://us.fedsvc.pwcinternal.com/ofis/public/SignOut.aspx |
| Certificate Thumbprint | F5DBA00484F09EC2CC73BF389621DADD0DBA35F8 |

External Production – Strong Authentication

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://gx.fedsvc.pwc.com/ofis/ |
| Entity Identifier | urn:federation:gx.fedsvc.pwc.com:ofis:gx |
| Federation Metadata URL | https://gx.fedsvc.pwc.com/ofis/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://gx.fedsvc.pwc.com/public/SignOut.aspx |
| Certificate Thumbprint | 086C8AEF54B3F4299828E296607553B0AAB61AAE |

External Production – Basic Authentication

|  |  |
| --- | --- |
| Parameter Name | Parameter Value |
| EndPoint URL | https://gx.fedsvc.pwc.com/ofis\_basic/ |
| Entity Identifier | urn:federation:gx.fedsvc.pwc.com:ofis\_basic:gx |
| Federation Metadata URL | https://gx.fedsvc.pwc.com/ofis\_basic/FederationMetadata/2007-06/FederationMetadata.xml |
| Signout URL | https://gx.fedsvc.pwc.com/ofis\_basic/public/SignOut.aspx |
| Certificate Thumbprint | 086C8AEF54B3F4299828E296607553B0AAB61AAE |

# Appendix C – Login Page Customization

The External IdAM framework provides the ability for application owners to customize the look and feel of the shared IdAM login pages. This is not a required option, but does provide a significantly simplified customization method. Refer to the Design Specification Document for the full customization capabilities.



Login page customisation includes the following steps:

* Upon request, PwC IT sends a zip folder containing two files (File is also embedded in this document):
* “custom.xml”
* “img.png”
* Application owner edits the “custom.xml” file according to the application’s specification and within the limitations, stated below.
* Application owner replaces the “img.png” with another application-specific file of the same name and size (image size dimensions must be maintained)
* Application owner zips the updated “custom.xml” and “img.png” files into a new file, named after the application. For example “mytaxapplication.zip”
* Application owner sends the zip file to PwC IT IdAM for implementation

|  |  |  |
| --- | --- | --- |
| Element Name | Description | Value |
| appName | Specifies the application Realm/URI, the identifier used to recognize the application by the Identity Provider | Application specific  ex. **urn:us.fedsvc.pwc.com:ClaimsApp:us** |
| scheme | Specifies the color scheme for the customized login page | **tangerine**, **rose**, **orange**, **maroon**, **burgundy** or **red** |
| machineAuth | Specifies if the machineAuth cookie can be used instead of an OTP during MFA authentication | **true** or **false** |
| navType | Specifies if login will be forms based login or multifactor (SMS OTP & KBA) | **single** or **strong** |
| navUrl | Specifies the navigational URL for the authentication factor chosen in the navType element. Leave this field blank if navType is set to **single** | **~/public/ExtAuth/LoginSMS.aspx** or  **~/public/ExtAuth/ForgotPwdQuestion.aspx** |
| showImage | Specifies to show or hide the image listed in the **imagePath** location | **true** or **false** |
| showHeading | Specifies to show or hide the header listed in the **header** value | **true** or **false** |
| showParagraph | Specifies to show or hide the paragraph listed in the **paragraph** & **paraHeader** value | **true** or **false** |
| showLink | Specifies to show or hide the link listed in the **linkText** & **LinkAddress** values | **true** or **false** |
| paragraph | The paragraph explains the purpose and function of the application. | Blob of text  Character limit: |
| paraHeader | The paragraph header specifies the title for the **paragraph** description. | Line of text |
| imagePath | Specifies the path to the custom image to display on the customized login page | **../../App\_Themes/Base/**<image name>  ex. **../../App\_Themes/Base/**sms.png |
| header | This header specifies the name of the application, which appears at the very top right of the page. | Line of text  ex. **ClientConnect** |
| linkText | Specifies a link that can be displayed on the customized login page | Link Text  Ex. **Yahoo** |
| linkAddress | Specifies the link URL associated with the **linkText** value | **http://**<address>  ex. **https://www.yahoo.com** |



Figure 12: Fully customised login page

## Customisation template

All customisations are made in the custom.xml file. Here is a template showing all possible values:

Basic Auth Example:

<app>  
 <appName>urn:wsfed:d</appName>  
 <scheme>tangerine</scheme>  
 <machineAuth>false</machineAuth>  
 <navType>single</navType>  
 <navUrl></navUrl>  
 <showImage>false</showImage>  
 <showHeading>true</showHeading>  
 <showParagraph>true</showParagraph>  
 <showInternalLogin>false</showInternalLogin>  
 <showLink>true</showLink>  
 <paragraph>This application (wsfed) is sourced at the Identity Broker and is using for testing purposes.</paragraph>  
 <paraHeader>The is the Identity Broker (wsfed) App</paraHeader>  
 <imagePath>../../App\_Themes/Base/img-clientconnect.png</imagePath>  
 <header>WSFED Test Application</header>  
 <linkText>Test Link</linkText>  
 <linkAddress>http://www.yahoo.com</linkAddress>  
</app>

Strong Auth Example:

<app>  
 <appName>urn:saml2</appName>  
 <scheme>tangerine</scheme>  
 <machineAuth>true</machineAuth>  
 <navType>strong</navType>  
 <navUrl>~/public/ExtAuth/LoginSMS.aspx</navUrl>  
 <showImage>true</showImage>  
 <showHeading>true</showHeading>  
 <showParagraph>true</showParagraph>  
 <showInternalLogin>false</showInternalLogin>  
 <showLink>true</showLink>  
 <paragraph>This is a test paragraph for saml2. This is a test paragraph. This is a test paragraph. This is a test paragraph. This is a test paragraph. This is a test paragraph. This is a test paragraph.</paragraph>  
 <paraHeader>The Paragraph Header</paraHeader>  
 <imagePath>../../App\_Themes/Base/sms.png</imagePath>  
 <header>This is the SMS Custom Header</header>  
 <linkText>Test Link</linkText>  
 <linkAddress>http://www.yahoo.com</linkAddress>  
 </app>

# Appendix D – IBM Domino Application Integration

Refer to the attached document to configure a Domino based application with IdAM.



# Appendix D - Glossary

Listed below are acronyms and their definitions, as depicted in this document.

|  |  |
| --- | --- |
| Acronym | Definition |
| AD | Active Directory |
| ADWS | Active Directory Web Services |
| CSS | Cascading Style Sheets |
| FQDN | Fully Qualified Domain Name |
| GUID | Globally Unique Identifier |
| GUM | Group and User Management |
| OFIS | Optimal Federation Identity Services |
| IdAM | Identity and Access Management |
| IdP | Identity Provider |
| IT | Information Technology |
| KBA | Knowledge Based Answers |
| LDAP | Lightweight Directory Access Protocol |
| LDAPS | LDAP over SSL |
| LoS | Line of Service |
| MFA | Multi-Factor Authentication |
| OTP | One Time Password |
| RDC | Regional Data Center |
| SaaS | Software as a Service |
| SLO | Single Log Out |
| SMS | Short Messaging Service |
| SMTP | Simple Mail Transfer Protocol |
| SSO | Single Sign On |
| STS | Secure Token Service |
| VIS | Virtual Identity Server |
| WCF | Windows Communication Foundation |
| WIF | Windows Identity Foundation |
| XML | Extensible Markup Language |

# Appendix E – Document Revisions

Described below are the various iterations in the development of this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Contributor |
| 9 September 2015 | 2.13 | Major Updates for Internal and External Auth. Included Identity Broker. | Nishanth Sivananthan |
| 9 December 2015 | 2.14 | Added Domino IdAM Integration | Nishanth Sivananthan |
| 21 December 2015 | 2.15 | New integration request process changed to IdAM Integration Requests Portal | David Winter |
| 22 December 2015 | 2.15 | New application / service account request process changed to IdAM Integration Requests Portal | David Winter |
| 11 January 2016 | 2.17 | Added update Domino IdAM Integration Document | Nishanth Sivananthan |
| 11 January 2016 | 2.18 | Dev Broker endpoints as we now onboard apps into the Dev Broker environment | Nishanth Sivananthan |
| 21 April 2016 | 2.19 | Dynamic groups and External Self Registration details added to Section 3 | Ray Fernandez |
| 06 May 2016 | 2.20 | Updated Claims chart in Section 5.2.2 | John Yee |
|  |  |  |  |