Cheat sheet

# IFS IAM User Management

## Key concepts and definitions

| | |
|---|---|
| **Identity and Access Management (IAM)** | Access management is the process of managing a user's login and access across a wide range of applications, systems, and resources belonging to an organization. IAM services authorize user access to protected resources but delegate the authorization decisions to the applications' owners. |
| **Identity Provider (IdP)** | A system that validates the identity of a user in a federated system. The service provider (or SP; see below) uses the IdP to get the identity of the current user. |
| **Service Provider (SP)** | A system that provides a generic service to the user in a federated system. To users, a service provider is the same thing as the application they are trying to use. |
| **Federation** | An agreement (trust) between identity providers and service providers that allows for the sharing of information. It lets users of a service sign on to said service through one single identity provider. Also known as federated identity management, this is a technical implementation that enables identity information to be developed and shared among several entities and across trust domains. |
| **Security Assertion Markup Language** | SAML is an industry standard XML-based framework for communicating user authentication and attribute information. The SAML 2.0 protocol standard is leveraged by Infor applications. |
| **Single Sign On (SSO)** | A service model in which users log into one single platform that gives them automatic log-in access to multiple applications for a certain period of time. Users using this system only have to remember one set of credentials, as opposed to learning a new password for each application. |
| **Single Log Out (SLO)** | Enables a user to log out of all participating sites in a created session. The party that authenticated the user handles all logout requests and responses for participating sites. |
| **Identity Store** | User information stored across a variety of technologies, including databases, LDAP, Active Directory, etc. |
| **User Provisioning** | A set of technologies that create, modify, and de-activate user accounts and their profiles across IT infrastructure and business applications. |
| **System for Cross-domain Identity Management (SCIM)** | SCIM is a standard for automating the exchange of user identity information between identity domains, or IT systems. SCIM communicates user identity data between identity providers and service providers requiring user identity information. |
| **Just In Time (JIT)** | Process where a user account can be created on demand after successful authentication occurs. |
| **Authentication** | Authentication is the process of validating an identity, whether it be the identity of a user or, as in the Identity of Things, a device. The classic method of validation is the username/password combination. Authentication ensures that the individual is who he/she claims to be. |
| **Authorization** | The process of determining if a user has the right to access a service or perform an action or the process of giving individuals access to system objects based on their identity. |

## Resources

Product Overview | YouTube | Documentation | Education | Dev Portal | User Community

## Components Cloud Features Flags

To enable any of these features, create a customer care inquiry support incident and clearly state what features are required to be enabled and for what Infor CloudSuite tenants.

| | |
|---|---|
| **IFS Email Not Required**<br>**IFSEMAILNOTREQUIRED** | The default within IFS is that the email attribute is used to identify the user. The email attribute and username attributes are coupled so users must have an email address when being provisioned to IFS. If users do not have an email address or a different attribute other than email (UPN, Employee ID, etc.) needs to be leveraged to identify the user then this feature will decouple the email and username attributes in IFS. |
| **IFS Multiple IdP**<br>**IFSMULTIPLEIDP** | This feature will allow multiple Identity Provider (IdP) federated connections for authentication purposes. A maximum number of federations is limited to 5. |
| **Okta Activation Mode**<br>**EmanleOktaActiveModeAuthentication** | Some applications require a WS-Trust call to the IdP for secondary authentication requests. Some IdPs (ADFS, Ping Federate) support WS-Trust and can leverage the WS-Trust configuration within Federated Security and some IdPs (Okta, Azure) do not support WS-Trust. The Okta Active Mode feature was developed as a work around for those customers leveraging Okta for authentication. |
| **Azure Activation Mode**<br>**AzureADActiveAuthn** | Enable this feature when the Azure version of the WS-Trust work around for secondary authentication requests are required. It currently does not support any Azure AD accounts where MFA is enabled. |
| **Advanced WS-Trust**<br>**AdvancedWsTrust** | This feature will need to be enabled to allow WS-Trust calls to execute properly when Infor STS proxy mode has been enabled for the tenant federation. WS-Trust configuration parameters within Federated Security does not change when this feature is enabled and requires an IdP that supports WS-Trust calls (ADFS, Ping Federate). |
| **Security Access Profiles:**<br>**SecurityAccessProfiles**<br>**and**<br>**SessionSvcSecurity:**<br>**AccessProfile** | This feature will allow for the ability to add profiles to restrict a specific set of user's access to the portal by IP ranges and / or date / time ranges. It also has custom session timeout settings that can be configured per profile. |

## SSO Overview

| | |
|---|---|
| **Single Sign On (SSO) Overview** | User authentication process that authenticates the user for all the applications they have been given rights to and eliminates further password prompts. |