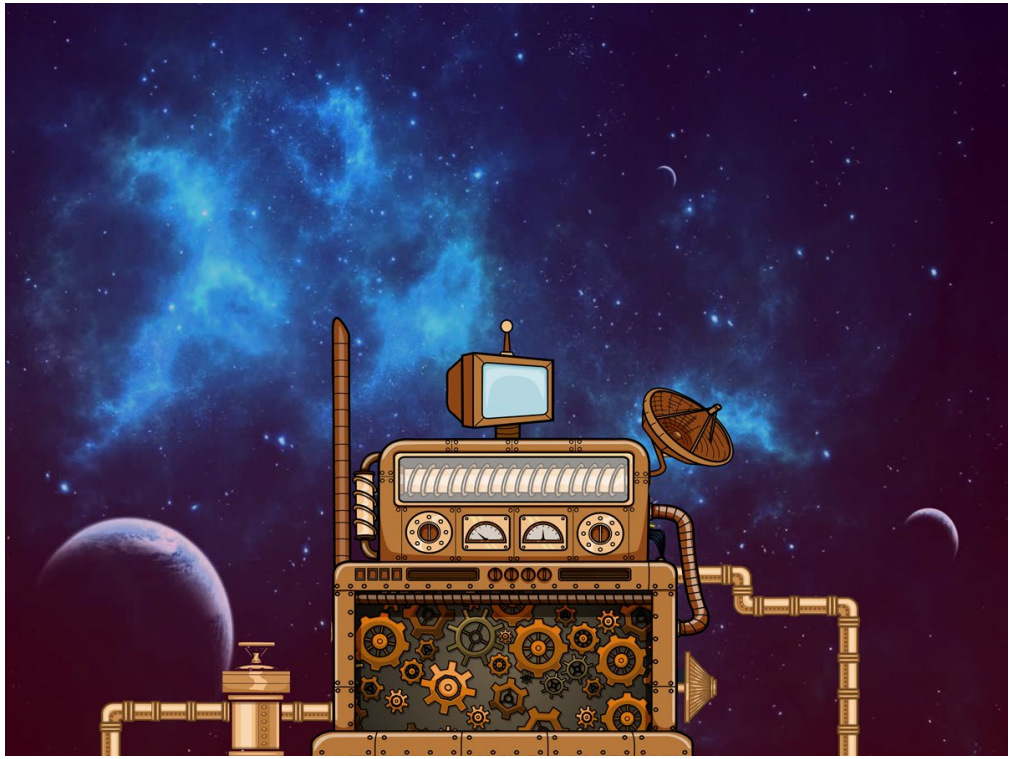
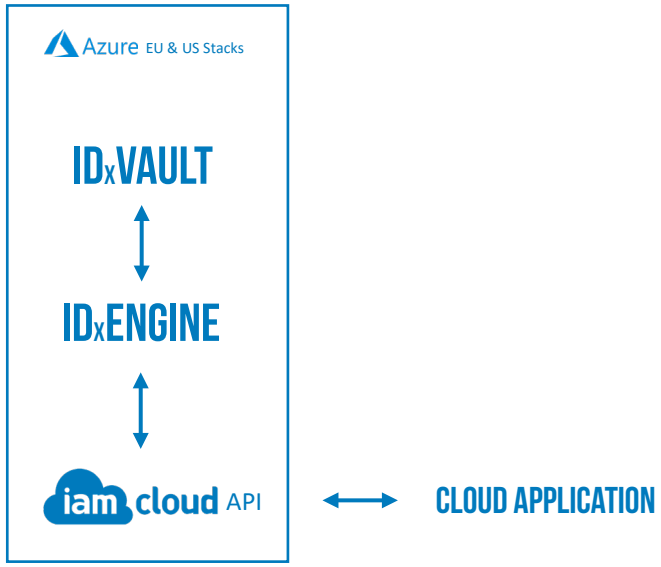

iam cloud
IDx
The Identity Exchange

CONTENTS



IAM Cloud – Software Cogs for your Cloud Machine

ARCHITECTURE SUMMARY



IAM Cloud Agent
IAM Cloud's sync agent is typically installed on a domain control server, or a member server if no password sync is required. The Agent syncs the data you decide between Active Directory (or other on-prem applications) and the IAM Cloud API. The sync agent runs as a lightweight service on the server and encrypts all outgoing traffic before transferring over HTTPS.

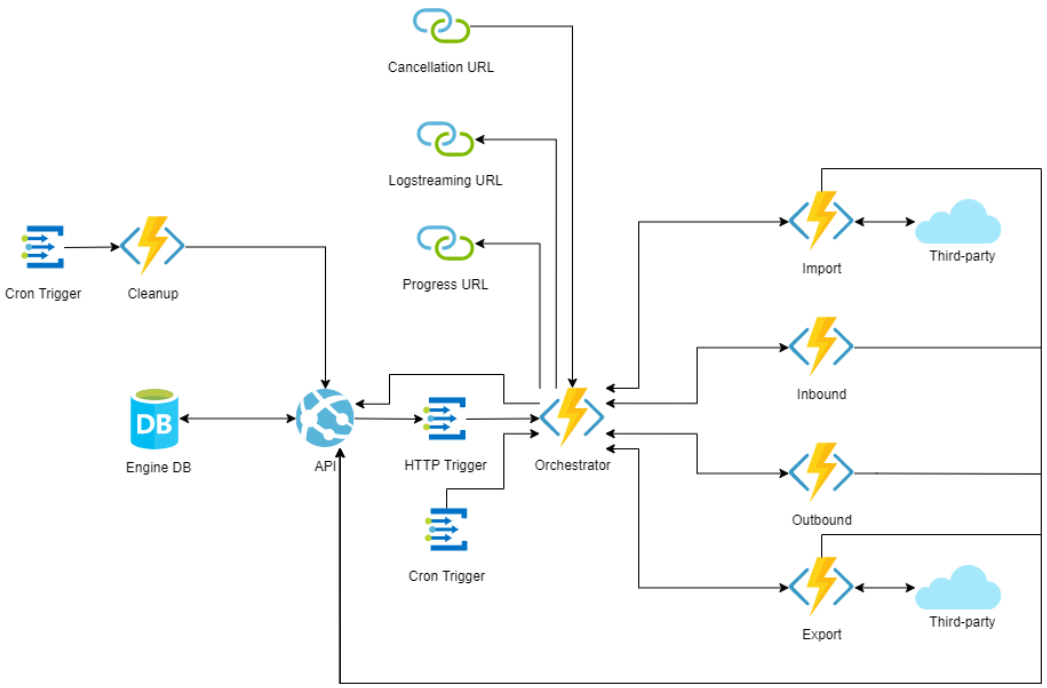
IDx Infrastructure
IDx is hosted in Microsoft Azure and is independently hosted in two regions: US and EU.
Each region runs in high-availability mode across two Azure data centers within each region for service continuity. IDx leverages a number of Azure technologies including Web Services, orchestration functions, Cosmos and event hubs to enable highly elastic service scaling to meet the needs of our customers regardless of their size from 100 to 1m users.

IAM Cloud API
IAM Cloud has a centralized API with advanced multi-layered security and permissions. It handles all inbound operation requests and is the main gateway between IDx and all peripheral services, including the IAM Cloud Agent and other SaaS applications, such as Workday, Office 365, Google, Salesforce and countless others. While most of IDx's features are set-up within a Portal, each customer tenancy has an optional API service account available to them to build their own custom integrations.

IDxEngine
The Engine is the main processing system of the IDx identity platform. It handles all main identity processes ranging from rule-based account joining, attribute creation & computation, identity changes, creations & deletions, group membership handling, and notifications. Fully rule-based, the Engine orchestrates 'if, when and how' identity information should be created, synced, changed or removed across the connected systems the identity is joined to.

IDxVault
The Vault is the main cloud-based repository of users. Encrypted at rest, the Vault is a highly-secure user repository. Manageable through the IAM Cloud Portal, the Vault allows admins to view and interact with their users' identities.

ENGINE ARCHITECTURE



Many IT systems have a concept of import and export, but with the Engine we created a 4-process system (import, inbound, outbound, export) that gives IDx powerful on-the-fly processing capabilities during provisioning and synchronization while optimizing processing performance.

Application Repository
Between an Application's data and the IDx Vault data exists a connecting space called the Application Repository. The Application Repository is "our" representation of the Application's data. There are many benefits of this model, most especially performance. Having a local representation of an application's data means significantly faster processing times.

Import
Import pulls data from the third-party application and brings the data into our Application Repository.

Inbound
Inbound syncs pull data from the Application Repository and renders it in the Vault. Identities can be made up of attributes imported from multiple different applications eg: 'email address' may come from Active Directory whereas 'job title' may come from an HR system.

Outbound
Outbound is the reverse of an Inbound. Authoritative data from our Vault is passed into the Application Repository.

Export
When the Application Repository is updated by an outbound sync from the Vault, it joins an Export queue to the third-party application.

Attribute Mapper
Attributes can be mapped and computed on the fly using IDx attribute mappers. Attribute mappers govern the flow of attributes and enable the creation of a new attributes, e.g. by concatenating two other attributes together or simply coordinating a direct 1-1 mapping.

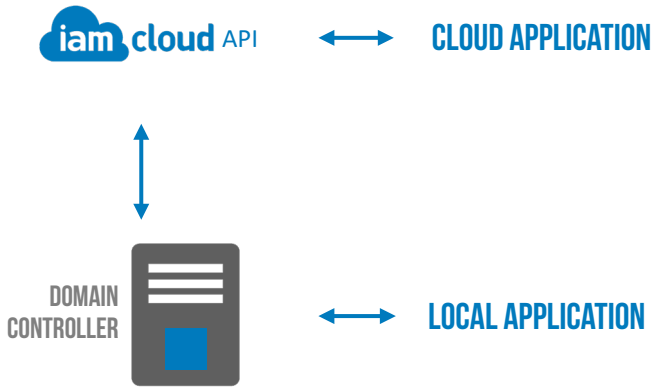
Filters Framework
On each of the Import, Inbound, Outbound and Export process there is a Filters Framework that allows for processes to take place at that point in time. Filters apply to the whole identity and are applied conditionally based on customizable rules with an almost infinite amount of flexibility and power.

Global Code Repository
Attribute Mappers and Filters can both be configured by XML for simple requirements, but IAM Cloud is built around a Global Code Repository which – among many purposes - allows the creation and use of advanced C#-based functions for Mappers & Filters.

Orchestrator
The Orchestrator is a central task handler which coordinates all IDx sync and processing activities as well as logging. While some functions are real-time or queue-based, others can be schedule to future points in time. A typical example of this is an account deletion, which you might not want to happen immediately but be scheduled to take place in e.g. 3 months instead.

Logstream (coming soon)
The Logstream is an incredibly powerful logging system that captures the full scope of identity and attribute activities for all your users in real-time. You can see everything, and you'll be able to export the Logstream to a third-party SIEM service.

IDxCONNECT



IDx is a global identity exchange hosted in the cloud that allows you to connect & sync identities between different systems.

Typical use cases
- Join your HR system to your identity directory (AD, Okta, OneLogin, Azure AD).
- Connect your Student Information System to Office 365.
- Sync your ERP system with your Active Directory.
- Link your CRM to your custom app or database.
- Connect a local user repository database to Active Directory or the cloud
- Connect any compatible system to any other or join several together at once.

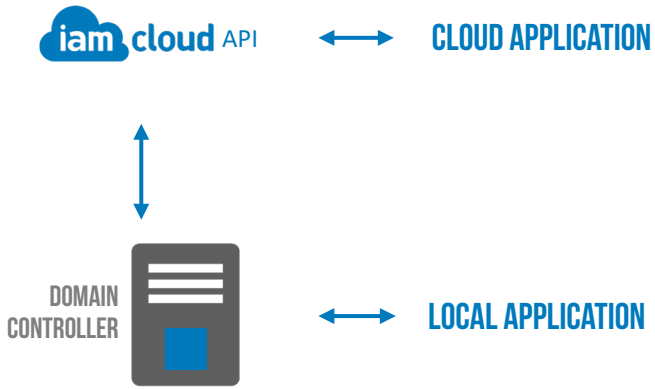
Cloud & On-prem
- IDx connects to Active Directory and other local user repositories via the IAM Cloud Agent.
- IDx connects to cloud-based applications, such as SaaS HR systems, via the IAM Cloud API.

Connector Framework
Both cloud and on-prem connectors use the same IDx 'Connector Framework' to ensure all the same functionality is available for on-prem and cloud applications. Having a unified Connector Framework also helps simplify the administration of the service by reducing potential inconsistencies and edge-cases.

IAM Cloud Agent
The IAM Cloud Agent can installed on the Domain Controller hosting Active Directory or a local member server. It uses an LDAP connection to AD, and acts as an AD listening service to catch and queue updates for scheduled synchronization. Outbound identity and attribute changes are synchronized every 15 minutes by default. The IAM Cloud Agent has a continuous heartbeat with the IAM Cloud API and listens for inbound data synchronizations. Synchronizations can be uni-directional or bi-directional, and this can be customized at the attribute level. So some attributes might be synced in one direction while others may travel in either direction. This can be customized based on the requirements of each customer.

All data, both identity and password hash (if applicable), is sent securely to the IAM Cloud API hosted in Microsoft Azure over port 443 using SSL. Within the SSL packet, all data is further encrypted using AES 256 and asymmetric algorithms for added security. IAM Cloud Agent is an outbound protocol only. Nothing – not even the IAM Cloud API – can contact the Agent, all writeback actions are coordinated through the Agent itself contacting the IAM Cloud API via its heartbeat and requesting instructions and data for any identity changes required to be written back.

IDxCONNECT



Identity Joining

'Joining' users across disparate systems is the most important process an identity service needs to undertake when it first connects to an application.

It is essential to create a 'hard' permanent join between user identities that cannot be broken by attribute changes. So if an employee, for example, changes their surname when they get married - prompting a change in email address – this should not matter to an identity system even if the email address forms part of the initial joining rules that joined the users accounts in the first place. This is how IDx works.

When we import users into our platform, the first check is to find out whether we are joining to an existing identity within IDx or creating a fresh user. If no initial hard join is present for a newly synced user, we will attempt to create a join by running customizable expression-based joining rules.

This would typically look like:

User's PayrollID in Workday matches Extension Attribute 4 in Active Directory
OR (and/or)
User's WorkdayID in Workday matches their EmployeeID in Active Directory

These follow priority order so can be processed hierarchically until they meet a condition. If they run the full set of conditions without meeting any, they need to be created in IDx. This may then trigger new provisioning flows where customers want downstream identity provisioning.

Joining rules can be customized with simple XML, but advanced joining rules can be created in C# to program advanced logic as well as potentially even call out to third party APIs to do user lookups.

IDxAUTOMATE

IDx allows you to easily create rules and actions based on different attributes, meaning you can:

- Allow different sets of attributes to flow for different groups of users
- Determine the direction of data flow between systems
- Create new attributes, such as concatenating first name + space + last name together
- Create or delete new accounts, contacts and groups
- Add or remove users from groups
- Automate your end-to-end Joiners, Movers, Leavers IT process

Identity & attribute sync cycles
By default both the IAM Cloud API and IAM Cloud Agent polls data from connected systems every 60 minutes through repeating scheduled tasks, although this can be configured to be as low as every 15 minutes. Some platforms IDx connects to have a delta concept which allows IDx to only capture any identities, groups and attributes that have changed since the last sync. For Active Directory itself, the IAM Cloud Agent has an AD listening service to capture and queue up changes.

However, some platforms do not have a delta concept which means a full sync needs to take place each time. This means our service needs to undertake a delta process on behalf of the application, which requires intensive computation and time. For larger environments this may require the syncs to operate less regularly to ensure new syncs aren't delayed and held-up in a queue.

Unlike attribute changes which take place in scheduled syncs, enables & disables are handled in real-time pulse data.

Passwords
IDx can securely synchronize password hashes too. This may not be important for HR/MIS <-> AD integrations, but it is very powerful for enabling identity synchronization across Active Directory instances that exist in separate AD Forests. Unlike identity and attribute changes mentioned above, password sync is handled in real-time pulses (along with enables/disables) rather than repeating scheduled tasks.

Classifications
IDxClassifications are a simple and lightweight method of grouping certain objects (users, groups and/or contacts) in order to create separate workflows for each grouping. Classifications are not essential if every user needs to follow similar rules. But they can be useful if there are different types of groups such as Employees/Contractors in companies or Staff/Students in schools, which may need to be handled in distinct ways. Objects can only belong to a single classification, and are processed on the initial inbound sync to IDx. Classifications create an integer that can be used in high-performance logic, e.g.

- Users in Classification A get provisioned into Application A only
- Users in Classification B get provisioned into Applications A & B.

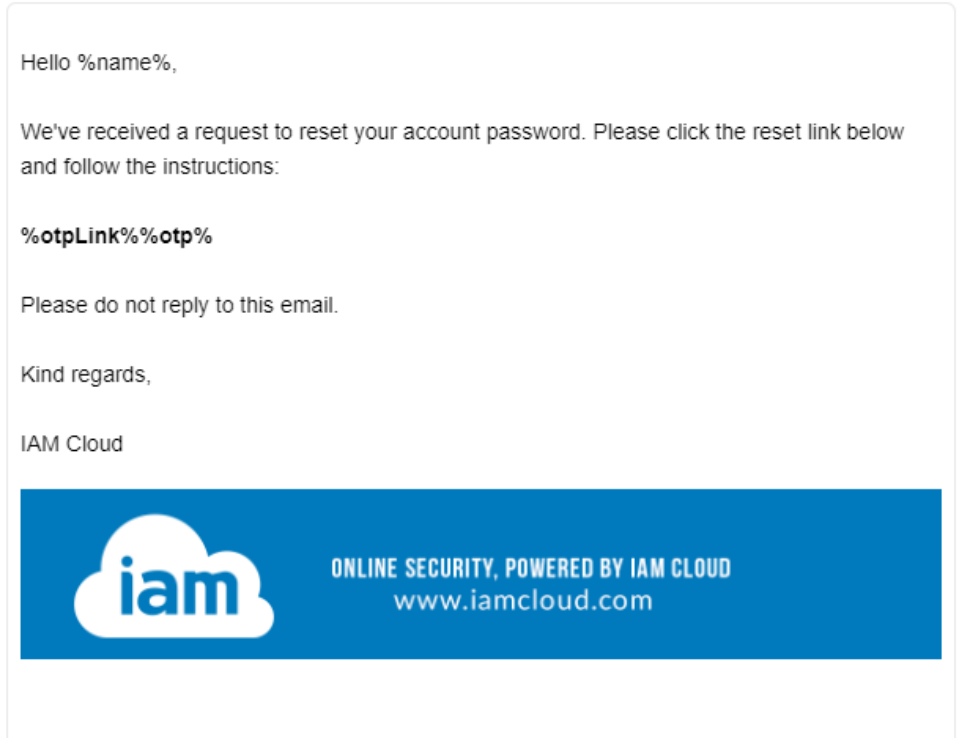
IDx classifications allow conditional evaluations to be performed ahead of time. This means for large bulk actions like provisioning thousands of users into a new application. Instead of having to evaluate a complex series of conditions each of e.g. 20,000 users - the classification integer can be used instead, which makes processing performance lightning fast.

Rules
Classifications excel at performing simple logic for large numbers of users. Rules exist to cover the opposite. Rules are evaluated on every single synchronization for every user who meets the Rules conditions. This means they are much more process intensive than Classifications but allows them to be incredibly granular, giving deep levels of control over user creations and deletions, attribute updates, and other processes.

Mappers
A Mapper is the mechanism used to map attributes between different systems as well as handling simple attribute logic e.g. concatenated attributes by joining several attributes like First + Last name together to create Full Name. Attribute mappers are unconditional and universal. A Full Name will always need to be processed in the same way for every user and condition.

Filters
Everything above can be considered out of the box. It's easy to set-up, it's reasonably standardized and exists to meet 95% of the requirements organizations are typically looking for in an identity system. Filters can handle the rest. Filters can call our Global Code Repository to pull custom C# sharp code during the synchronization process, enabling almost infinite flexibility in handling any kind of attribute processing, provisioning, deletion, disablement and update logic as well as a wide range of potential functionality such as custom notifications etc. Unlike the Mappers, Filters are conditional and rule-based, so they may only apply in certain conditions or for certain classifications of users.

IDxNOTIFY



IDxNotify allows Admins to create templated emails with smart-fields that can be sent on a range of triggers.

Some common use cases for our notify service are:

- Account login information sent to a new starter
- Admins notified of user creations and deletions
- New starter information send to employee's Manager
- Notices of account changes, such as an email address update or surname change.

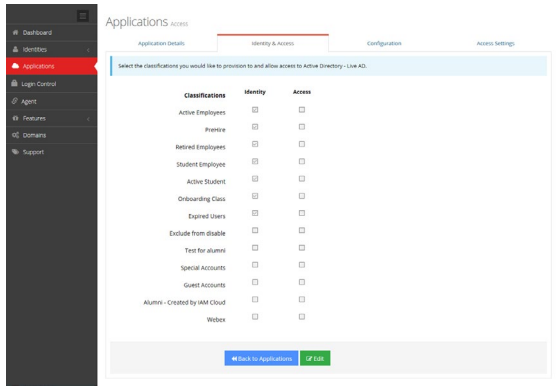
Our service also supports SMS notifications and webhooks, although these are currently created on a case-by-case basis by the IAM Cloud team on behalf of each customer.

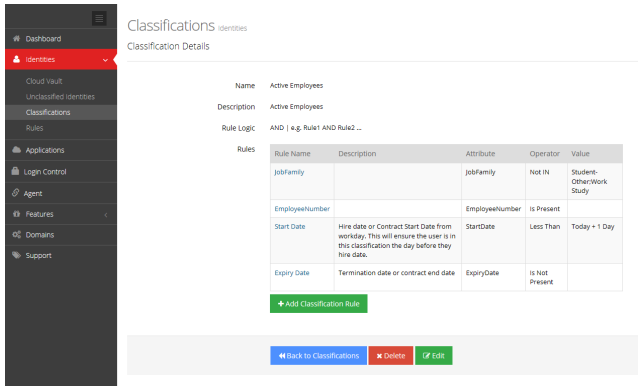
With the launch of our new Admin Console later in 2020, we hope to enable Admins to have more direct control over their notifications.

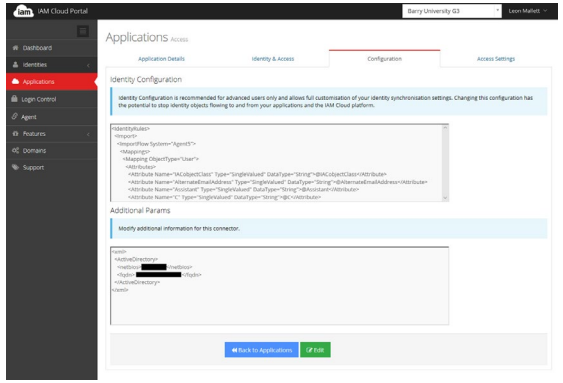
The IAM Cloud API also supports the ability for Admins to create their own custom triggers – which can be embedded in their own applications – in order to trigger IDx notifications.

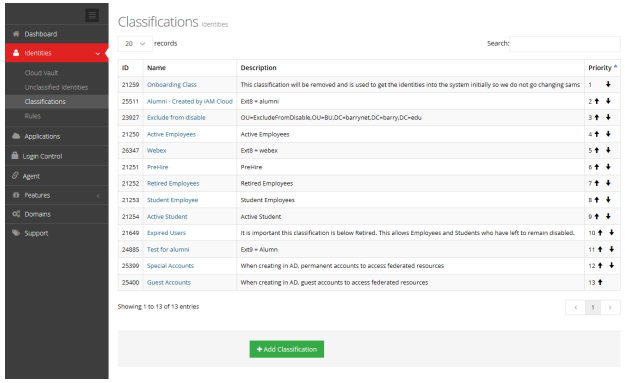
Email notifications support full HTML customization to personalize the appearance of the email, and can be sent from your own preferred email address.

IDxMANAGE









IAM Cloud has a central web portal that allows Admins to control the configuration and on-going management of the IDx service.

Vault
Users live in the Vault. From a single screen you can search and browse all your user identities and groups. From here you can access and update your users' profile data.

Classifications & Rules
Creating classifications and rules is simple in the Portal. Together classifications and rules allow admins to create conditional automation flows for provisioning and other identity processes.

Applications
IDx has complex customizable schemas for integrating with third-party applications. Typically written in XML, these can be edited within the Applications Centre of our portal.

Audit History (coming soon)
Our new powerful logging system is coming soon and it will allow Admins to view a full granular audit history of every process that has taken place with every identity and group. In time this will be available within our Portal as well as integrating with third-party data lakes and SIEM services. Using websockets you can see what the Engine is doing for you in real time. This means if a sync is running, it will create a websocket URL that can be obtained from the API and allow you to connect and see the real-time stream for your sync. This is perfect for monitoring the IDx sync performance and making sure things are smooth or highlighting any objects that may need to re-run.

END-TO-END SECURITY

IDx is a powerful IT tool to help save time, reduce manual effort and error, speed-up employee/user onboarding, and increase your organization's IT security.

- The IAM Cloud API and IAM Cloud Agent encrypts all data in transit and transfers data over 256bit HTTPS (TLS 1.2). At-rest data is held in encrypted data storage, and only keep data physically located in data-centers appropriate to each customer's regional data residency laws. So all our EU-based customers have data stored exclusively in data centers physically located with in the European Union, all our North American customers are served by data centers in the USA.
- IAM Technology Group Ltd are ISO 27001 compliant. ISO27001 is the global information security standard and our compliance covers our entire company, back-end systems, and front-end technology.
- IAM Technology Group runs a highly-secure development environment and software platform. Every single surface has a combination of conditional access policies and MFA security. IAM Technology Group does not work with third-party contractors or offshore development companies. All our operations are handled in-house with vetted and high-trust employees.
- Automated provisioning saves time and money. Automated deprovisioning does too, but it also substantially improves security by automatically removing access to users who've left the organization. In fact automated deprovisioning is one of the standards of ISO27001 compliance.
- IDx only runs on Microsoft Azure technology that has approval for use in US Federal Government.
- IDx is approved on the UK Government G-Cloud Procurement Platform.

MORE THAN TECHNOLOGY

IAM Cloud is fully supported. For no extra charge, all our customers receive a 24*7*365 service, which includes:

- Full on-boarding support, including help with integration, configuration & federation.
- Access to our customer knowledgebase
- Access to our ticketing system
- Full extended business hours support
- Availability and support SLAs, including 99.9% service up-time
- Support by telephone, email, web tickets and web conference
- Optional quarterly service reviews
- Prioritized critical support for urgent issues

IDxFAQ

How does integration and onboarding work?
Identity integration is not to be taken lightly. Configuration errors can have real-world impacts. We believe we have pretty much mastered the process of safe phased-integration. This is the IDx recommended integration process:

Phase 1 (Sandbox mode): All changes are created in a sandbox environment only. A daily report is generated which allows Admins to check that changes are expected and good. This normally lasts a week or until confidence is reached to move to next phase, allowing for any final config tweaks that may be required throughout the process.

Phase 2 (Semi-automatic mode): We move to the live environment but create a sign-off checkpoint that prevents any changes being made until the Admin gives approval. This would normally be done daily. Once approval is granted, the changes can pass through into the live system. This phase also normally takes a week, or until confidence is reached to move to the next phase.

Phase 3 (Go live): Full automation is switched on. Project goes live. Everyone cheers and goes for a coffee (or other preferred beverage).

How quick is the onboarding process?
From placing an order, we'll be able to start the integration process within 2-3 days. Configuration will normally take 1-3 weeks depending on the level of complexity of the project. The above phased-integration would then begin which normally takes about two weeks.

What support can we expect?
IDx is a fully supported platform. Our team will help with the onboarding project, installation of our sync client, we'll collaborate with you on setting up the right configurations to meet your needs, and provide ongoing support, guidance and troubleshooting.

We provide full hands-on business hours support 7am-10pm (+0 UTC), and 24/7/365 critical support.

What are your support SLAs?
Yes. Critical issues have a 1-hour response SLA.
High = 4 hours. Medium = 8 hours. Low = 24 hours.

Is IAM Cloud GDPR compliant?
Yes, of course. We are also ISO27001 compliant (the international equivalent to SOC 2 in the USA). We take data security and privacy seriously and undertake frequent security tests and audits to ensure our continued performance and compliance.

IAM TECHNOLOGY GROUP
TRUSTED BY 1000s OF ORGANIZATIONS OF ALL SIZES AND SECTORS

>1 MILLION USERS

>1000 ORGANIZATIONS

GEELY
COMMONWEALTH ENGINEERS, INC.
BACARDI
BAUSCH+LOMB See better. Live better.
United Learning The best in everyone
IMPAQ
The Royal Society of Medicine
coop
University of Bedfordshire
Save the Children
H&S HEALTH AND SAFETY AUTHORITY
ANA AMERICAN NURSES ASSOCIATION
ROYAL VETERINARY COLLEGE
STARWOOD RETAIL PARTNERS
Barry University
MIAMI-DADE COUNTY
HRG Healthcare Resource Group
NHS
UNITED NATIONS UNIVERSITY
MAERSK
UMASS LOWELL
Berkshire Health Systems
SAFRAM
MC WANE
SIERRA NEVADA
Mosaic
VISITING NURSE SERVICE OF NEW YORK
müller
The Highland Council Comhairle na Gaidhealtachd
American Red Cross
ENGIE
Virgin
StanleyBlack&Decker
PINE REST Foundation
WesBanco
GUILD HALL SCHOOL
Snohomish County Washington
The Growth Company
AUTOGLASS
alfa accountants en adviseurs

IAM TECHNOLOGY GROUP LTD

Worldwide Partner of the Year award from Microsoft in the education sector.

Technology **Fast 500**
2016 EMEA **WINNER**
Deloitte.

One of the fastest growing tech companies in Europe, Middle East and Africa.

Microsoft Partner
Gold Messaging
Silver Cloud Platform
Silver Cloud Productivity

Microsoft Gold Partner certification which shows our technical competency in their technology.

International Association of Microsoft Channel Partners ™
Cloud Partner Award 2015
FINALIST - EMEA Region

A leading Microsoft Cloud partner in Europe, Middle East and Africa

HM Government
G-Cloud
Supplier

Approved G-Cloud vendor, pre-certified to sell to the UK Government & Public Sector

Information Security Management System
ISO 27001
Certified

Certified ISO 27001 compliant – the international information security standard.