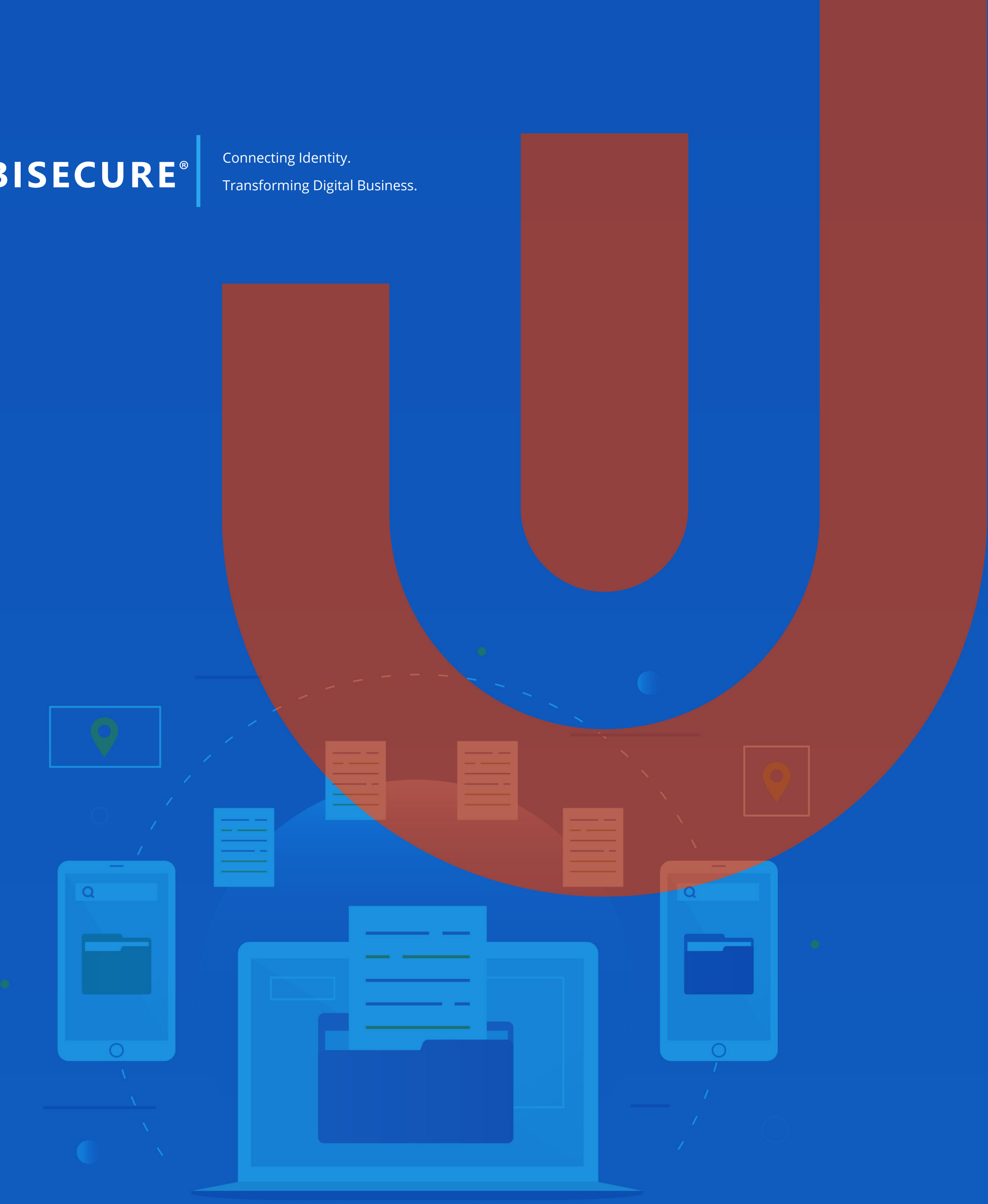
UBISECURE®

Connecting Identity.
Transforming Digital Business.



Migrating from RSA's Access Manager to Ubisecure's Identity Platform

Identity and Access Management beyond RSA (ClearTrust) Access Manager End-of-Life

Contents

Migration from RSA to Ubisecure 3

High-level options for migration 3

- Migrating all users at once 4

- Gradual migration 4

Which method is better for enterprise use cases? 5

User-friendly migration considerations 5

User-driven federation 6

Directory User Mapping 7

Tips and Tricks 7

Get in touch 8

Migration from RSA to Ubisecure

In March 2017, RSA announced that its Identity and Access Management (IAM) suite, 'RSA Access Manager' (and previously known as ClearTrust), would reach end-of-life (EOL) status in June 2021. As of this writing, this leaves RSA customers with just one year in which to migrate to another IAM platform.

For those planning their migration now, the timetable will be concentrated but certainly achievable. Much has happened in the world since RSA acquired its IAM suite in August 2001 and the world has moved towards the standardisation and unification of digital identities.

Back in 2001, the smooth handling of workplace identities and customer identities required two separate workflows and two separate IAM systems. Even to this date, the difference exists in some providers' IAM platforms – mainly in pricing, where segmented 'enterprise' features (e.g. high availability) command stiff premiums.

> **Ubisecure's Identity Platform offers the same competitive pricing for internal and external user digital identities, with enterprise-level reliability and scalability built-in for all. Our customers reap the benefits of our years of involvement in identity standardisation bodies and enjoy seamless, user-friendly and secure workflows.**

In this white paper, we will first guide you through the different approaches and considerations for your legacy RSA system migration. We will then finish with more detailed coverage on account linking utilising User-Driven Federation and Directory User Mapping, as well as other tips and tricks.

High-level options for migration

There are multiple ways to handle a migration project. What the best option is for your company depends on your business requirements and the exact scope of your existing RSA installation, but roughly speaking there are two main options to consider: migrating all users at once and gradual migration.

MIGRATING ALL USERS AT ONCE

Migrating all users at once distils the process down to a mass database export & import. After extracting all relevant data from the legacy system, you will then import it into the new system and reconfigure all related applications for all users in one go.

This means that you switch all of the system's identities to a new system during a certain maintenance window, which is usually when there is a minimal traffic flow to your applications, e.g. overnight on Christmas Day. In many cases, after the change is done, users won't even notice the difference. Since Ubisecure's Identity Platform has full API coverage, the user interfaces will not need to change; functionality is simply integrated into the existing application.

Here it should be kept in mind that unless the users have been very unhappy with the old system, any change is generally resisted. Resist the temptation to label the system (e.g.) "completely new", unless the users themselves have demanded a new system designed from scratch.

Migrating all users at once simplifies the planning of the project schedule, since you can do the actual data import inside a relatively small, predefined time window.

GRADUAL MIGRATION

Gradual migration or phased migration involves running the two systems (legacy and new) in parallel, migrating target applications one at a time and decommissioning the old system integrations gradually, until everything is running on the new IAM platform.

This method offers a phased approach, which gives you time to monitor a successful execution of the step by step migration process, while the services are still partly relying on the old system and running simultaneously with the new one.

This approach gives you the comfort of running two systems in parallel, enabling any migration issues to be handled by business priorities instead of technical ones, but naturally at the cost of delaying the completion of the migration, that will in turn accrue (e.g.) license fees from the legacy system.

Which method is better for enterprise use cases?

Migrating all users at once is the better fit for 'pure enterprise' systems, meaning they only handle internal users and have not been partially migrated to modern platforms. However, due to its short time window for changeover, there might be delays and strains on the budget if something goes wrong during that time. In comparison, gradual migration smears the risk temporally due to its gradual progress, particularly if there is a huge amount of data to be imported.

On the other hand, gradual migration can be more complicated to plan and execute since there can be several distinct components affecting the migration, meaning the project's time frame has more potential to overrun. Although a longer timeframe also brings opportunities, as the migration can serve as a bridge to merge internal and external IAM databases, and even to update the user attributes. You must think carefully about the synchronisation between the old and the new systems which are in operation at the same time. Therefore, a tried and tested compromise is to do the migration at the application level instead of at the database level. This means that one, or a tightly defined group of, business-critical application(s) will be migrated all together in the first phase. Then, later on, the other applications can be migrated piecemeal or in groups.

User-friendly migration considerations

External users typically tolerate less interruptions and changes in their usual workflow than internal users, who can even be retrained on systems if needs be. In order to help the migration project to progress smoothly, consider the following tips:

→ Always transfer existing customer credentials where possible. The chances are that you can import most of the user attributes from the legacy system to the new IAM system. However, sensitive information such as passwords and SSNs are stored in a hash format. This is not a problem if your RSA Access Manager database is configured to use one of the strong cryptographic hash algorithms that Ubisecure's Identity Platform supports.

→ Always transfer existing customer account links where possible. Sometimes your system has a link to log in via another trusted party's service, such as Office 365 or a social account login. Another case is where, during the authentication process, another service returns one or more attributes to enrich the user data. You should preserve these links to the new service during the migration project.

- Test and audit the access control logic thoroughly. Both pre-testing and post-testing are essential parts of migration projects. Typically, an enterprise has at least a testing environment in addition to a production environment. Establish the test environment before the production environment and utilise it in the pre-testing stage by migrating integrations one at a time to it. It is also important to test the environment after (and possibly during) the migration to see that everything is working as planned, including all possible ways to authenticate.

In order to ensure consistency, critical attributes should be transferred atomically if migrating from a live system to another. One potential common pitfall is that the old IAM system does not support the secure hashes that the new system does. If this is the case then there's no magic bullet – you simply cannot transfer all attributes without resetting the passwords as, by definition, one-way hashes are irreversible.

An alternative to a system-wide password reset is to ask the users to re-register their accounts to the new system. In many cases, some of the identity attribute fields can be refilled (e.g. when the invitation is initiated from a CRM system). Then most of the fields could be pre-filled, and the user is required to just verify that everything is correct, accept the terms of use and define a new password. Then the migration is complete and the user can start using the new IAM platform immediately.

If re-registration, or even a password reset, cannot be tolerated, the only course of action is to write and use a custom tool in order to keep using the old hashes (information security should be carefully considered here!). The old passwords can be stored as custom attributes and do not have to follow any pre-defined formats.

User-driven federation

The basic idea of user-driven federation is to let an end user link their existing third-party system credentials to your online service. This allows users to use an authentication method they already own, instead of the traditional new username and password combination. The concept is called BYOI (**Bring Your Own Identity**).

The user could link a business account, such as an Office 365 account, or a social media account, such as a LinkedIn account. If necessary, the linking can be verified by using a strong authentication method, like Bank ID, to get a verified social identity. From the user perspective, it is a manual linking of two authentication methods provided by different sources that do not even need to have common trusted attributes. The Ubisecure Identity Platform will transparently handle the mapping of attributes between the identity providers. The end user can do the account linking either by first signing in using the existing local account or by registering a new local account while being signed into an existing third-party identity provider.

This linking enables the user to sign in using their Office 365 credentials and transparently utilise features such as SSO (**Single Sign-On**) just like when signing in with their enterprise credentials.

Directory User Mapping

Directory User Mapping is quite similar to User-Driven Federation. The major difference is that it does not require or enable the user to do the mapping between user accounts themselves but, instead, offers an automatic account linking based on an automated query to a third-party user repository. The user can sign into a service using their existing credentials for a different service. The third-party credentials are not shared with your internal service.

Tips and Tricks

An IAM system migration is a relatively big project that potentially introduces a lot of new things to the end users. Some users can be resistant to big changes, so it is a good idea to communicate in advance that users should expect a system update on given dates. Focus on the positive side and possibilities that the new solution provides. Here are some tips and tricks on how to make the introduction of the new solution frictionless.

— THINK OF IT AS A DATA CLEANSING

This is a good time to re-validate and re-verify user attributes to maintain data quality. You could show all the relevant attributes to the user on the first login with the new system, and let the users correct any stale or missing fields themselves.

— RE-ATTESTATION OF USER RIGHTS

An IAM migration project is the perfect time for re-approval of access to services. A situation where the job role of an existing user has changed, or they have left the company, often requires modifications in the access credential configurations.

Here, a **delegated user management** facility can considerably help the task – where the customer or partner organisation's main user manages the access rights and authorisations of company employees. There are several benefits in this approach such as increased data accuracy, decreased security risks of abandoned accounts and credential sharing, and reduced operational costs for your enterprise. Find out more about Delegated Authority **here**.

— INCREASE SECURITY AND REGULATORY COMPLIANCE

There are many business-driven factors to purchase a new IAM system, such as increased security and help complying with regulations. You get better hashing and encryption algorithms for passwords and other sensitive information and you can choose from the latest and best authentication methods. Self-service portals let users view and manage their own account information, which is necessary for compliance with regulations such as GDPR and saves organisations considerable amounts of time (and therefore money).

— ADD USABILITY AND CONVENIENCE

As mentioned before, users can be resistant to big changes. To soften the introduction of the new system, increase usability and convenience. This can be achieved, for example, by planning easy-to-use workflows provided by the new IAM system and using login with an email address instead of user ID or log in with (verified) social identities.

— MAINTAIN ALL THINGS THAT IMPACT BROWSER HEURISTICS ON FORM FILLINGS

This includes hostnames, field names, page elements etc. Use any existing browser cookies for discovery where possible.

Get in touch

To find out more about how to migrate from RSA Access Manager to the Ubisecure Identity Platform, deployed in your region as SaaS, private cloud, or on-premise software, contact us.

ubisecure.com/contact

UK: +44 1273 957 613
Finland: +358 46 712 1100
Sweden: +46 70 603 34 83
Germany: +49 89 20190980

About Ubisecure

Ubisecure provides feature rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS, Cloud, or on-premises software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

Ubisecure's Right to Represent is a representation governance solution offering a fast and easy way to assert and verify an individual's mandated rights to electronically represent their company, including financial, signatory, or other authority. Ubisecure's widely used Delegated Authority solution allows individuals and organisations to manage which users and organisations can act on their behalf to dramatically reduce costly, time consuming and delay-prone manual workflows.

Ubisecure is accredited by the GLEIF to issue Legal Entity Identifiers (LEI) under its RapidLEI brand. RapidLEI is a cloud-based service that automates the issuance and registration of these highly assured organisation identifiers.

UBISECURE®

www.ubisecure.com
sales@ubisecure.com

UBISECURE UK
The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK
UK: +44 1273 957 613

UBISECURE FINLAND
Vaisalantie 2
FI- Espoo, 02130
Finland
FI: +358 9 251 77250

UBISECURE SWEDEN
Blekholmstorget 30 F
111 64 Stockholm
Sweden
SE: +46 70 603 34 83

UBISECURE DACH
Franz-Joseph-Str. 11
80801 Munich
Germany
DE: +49 89 20190980