transmit security

TECHNICAL WHITE PAPER

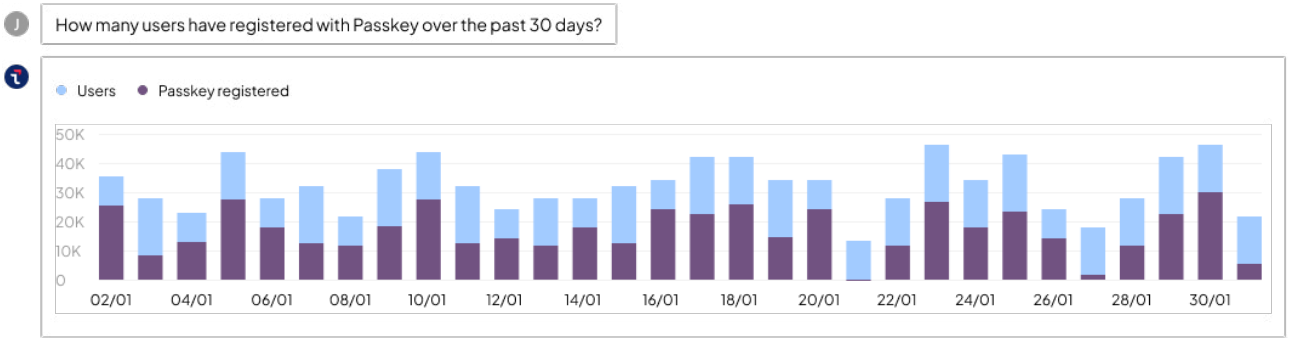
Identity Management Migration Guide

Why Migrate to Transmit Security Identity Management

Legacy identity solutions lack the scale, agility and speed to prevent today's rapidly-evolving fraud while supporting millions of customers. By necessity, organizations are migrating customer identity and access management (CIAM) to the cloud and unifying their identity stack to optimize security and customer experience (CX). In doing so, a primary concern is migrating identities, a topic covered in this guide. But first, why migrate to Transmit Security?

Transmit Security Identity Management Service improves visibility, analytics and control with a cloud-native, scalable user store and dynamic management portal. Event-driven identity services secure and simplify user journeys — from enrollment, authentication and authorization to fraud detection, orchestration and decisioning. User-friendly APIs make it easy to integrate at any point in the identity lifecycle.

Transmit Security services include the industry's first Conversational Analytics tool that works much like ChatGPT, enabling you to query your own data to receive instant insights about end users, devices, risk/trust events, attack types and more. As shown in the image below, you can ask for any type of chart or graph that's easy to comprehend. With instant analytics, you can rapidly adapt to emerging trends, strengthen security and simplify CX.



Unified user profiles, threat intelligence and other data provide holistic, contextual information that further strengthens behavioral biometrics, device fingerprinting, anomaly detection and other CIAM capabilities — all managed via one console.

Solving complex identity management challenges

To address a gap in the market, Transmit Security created the only platform with a fusion of natively-built fraud prevention, identity verification and customer identity management (IDM) services, including identity orchestration, authorization and phishing-resistant authentication with passkeys, passwordless and a complete set of login capabilities.

The consolidation of three solution sets removes data silos, security gaps and complexity that hinder the ability to detect and stop today's rapidly evolving fraud with accuracy and speed. Data from each AI-driven service is correlated to provide standardized risk ratings and transparency into decisioning, resolving the problems posed by multi-vendor solutions and black box AI models.

Whether implementing the Transmit Security Platform or Transmit Security Identity Management Service, companies can solve complex IDM challenges, including but not limited to:

The inability to scale for customers: Legacy directories and LDAP were not made to store a large volume of rich user data and scale for millions of customers. In most cases, sparse identity, risk and trust data is spread across multiple databases and lines of business, resulting in data silos, blind spots and costly management overhead.

Lack of agility and speed: Overloaded, outdated systems also introduce performance delays. Cloud-migrated IAM solutions repurposed for CIAM were originally built for the workforce and cannot keep pace with today's rapidly-evolving identity threats and customer demands. As a result, security breaches and compliance violations diminish customer trust and multiply costs.

Context is lost as user profiles are splintered: Duplicate identities become a problem when one customer creates several accounts with the same business, creating a fractured view of that individual. Without the full context of each access request, the customer, their devices and behaviors across channels and applications, the power of behavioral biometrics, device fingerprinting and other capabilities are diminished.

The solution

Migrate to a cloud-native, elastic IdP that's purpose-built for customers, scale, agility and speed. The Transmit Security Platform is the only customer identity management and fraud prevention solution born in the cloud, enabling smart, adaptive protection. Transmit Security Identity Management features a consolidated user store that provides a single source of truth. It collects and utilizes context-aware intelligence to prevent account fraud and remove friction from the customer's path.

Transmit Security Identity Management Service provides the capabilities to:

- Manage identities & account access, scaling to support millions of customers in one user store
- Auto-detect returning users to avoid duplicates and unify profiles across channels & devices
- View live and historical events, providing context to improve security and CX
- Customize, collect and enrich customer data with progressive profiling
- Protect customer data to ensure compliance with strict privacy and security mandates
- Limit data exposure with role-based access control (RBAC) and contextual authorization
- Automate access decisions based on data, e.g. IP address, device or authentication method
- Adapt session length and access permissions automatically based on risk/trust signals
- Query data for contextual and scoped information that provides 360° visibility
- Utilize industry standards: SAML 2.0, OIDC, OAuth 2.0

How to migrate customer identities

Migrating customer identities and credentials is a mission-critical task that requires careful planning, expertise, and a commitment to maintaining a seamless customer experience throughout the process. At Transmit Security, we understand that a successful migration involves more than transferring data; it's about ensuring the continued trust and satisfaction of customers while providing your organization with the flexibility to address your unique business requirements.

Whether upgrading from an existing CIAM solution or implementing CIAM for the first time, this guide is designed to provide the knowledge and resources necessary to help you execute a successful migration.

Key highlights of this migration guide:

Migration strategies: This guide covers three migration strategies, including just-in-time migration, bulk data transfers and a hybrid approach, providing the context that will help you choose the method that best aligns with your organization's goals and resources.

Security best practices: Security is paramount when dealing with customer identities and credentials. This guide will provide insights into security best practices that will ensure the protection of sensitive information during the migration process.

Seamless customer experiences: Maintaining a seamless user experience throughout the migration process is essential to preserve customer trust. This paper will provide strategies and tips to ensure customers experience a smooth transition with little to no disruption.

Migration approaches

When migrating users from one IdP to another, there are three basic options:

- **Bulk migration:** Takes all required user information from the original IdP and maps it onto the Transmit Security identity store.
- **Lazy migration:** Works behind the scenes to port over user accounts in real time as they log in to the application. This method is also known as just-in-time, or JIT, migration.
- **Hybrid approach** (recommended): Combines elements of lazy and bulk migration. This approach typically initiates lazy migration for a specific duration, then subsequently applies bulk migration to users who have not migrated yet.

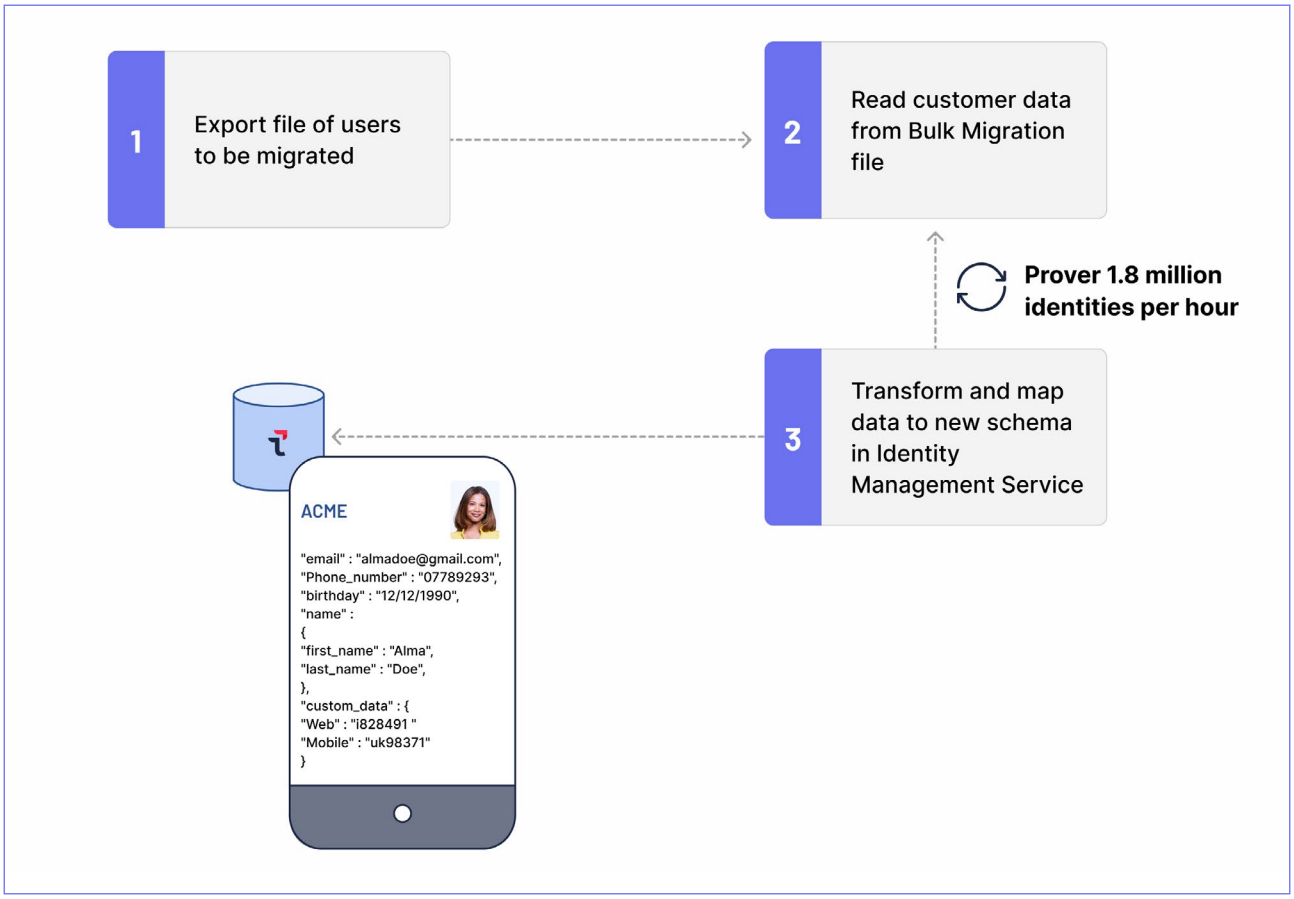
Although Transmit Security recommends a hybrid approach to migration, all three approaches are viable options for migrating to Transmit Security. When choosing a migration strategy, it's essential to choose the approach that aligns most effectively with your organization's goals and resources. Below, we delve into the three primary migration approaches, each tailored to meet distinct needs and priorities.

Bulk migration

Bulk migration ensures a quick and efficient migration process by transferring all end user identities from your existing system to IDM within the Transmit Security Platform using a Migration Utility. The Migration Utility takes a user file as its input, iterates through it and creates the users one by one in Transmit Security's identity store based on your schema mapping. Once the desired schema mapping is received, Transmit Security will adjust the Migration Utility with no additional work from your development team and then provide it to your organization.

To provide flexibility, the Migration Utility can run on either Transmit Security's service or your organization's own service. Bulk migration can also scale to handle a high volume of identities, migrating up to 500 identities per second, making it suitable even for the largest-scale migrations.

Although bulk migration does not require orchestration capabilities in order to execute, orchestration can ease this process by enabling you to migrate specific user groups in batches, testing the migration on live loads in order to observe and troubleshoot any potential issues.



Benefits:

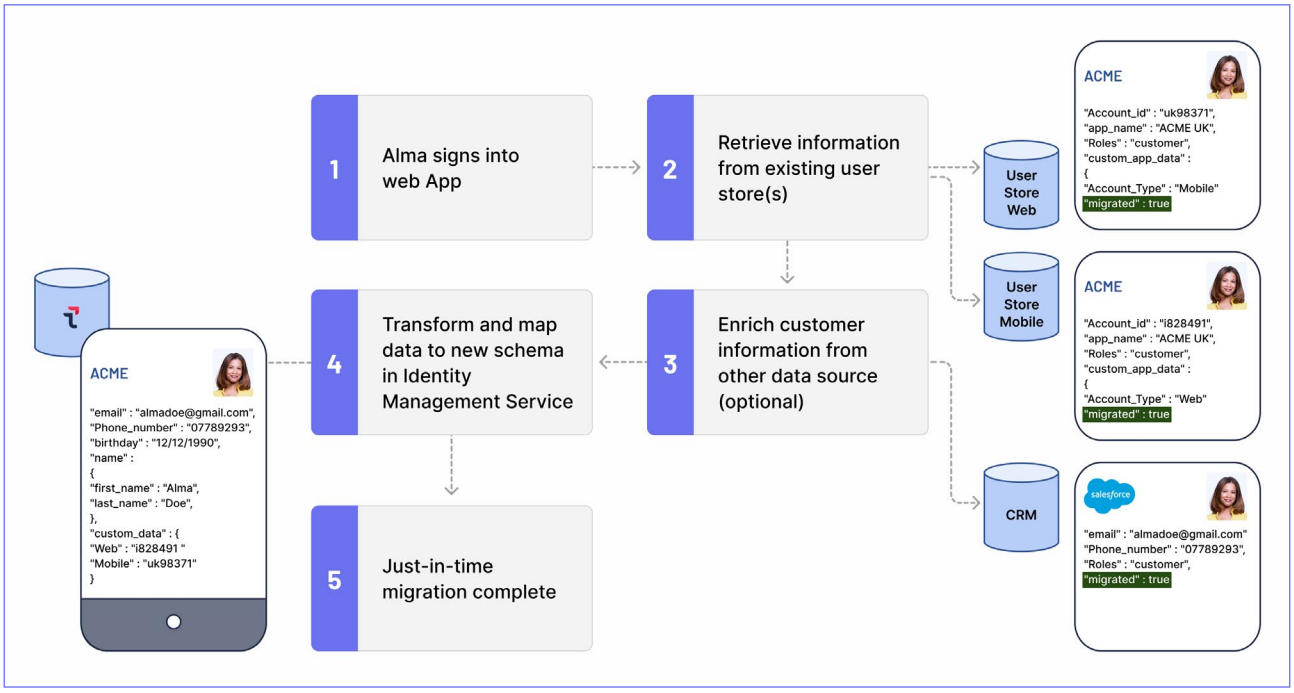
- **Speed and efficiency:** The Migration Utility can rapidly migrate a large number of identities, ensuring a swift migration process and a clear cutoff date for migration.
- **Comprehensive transfer:** All customer identities and their associated credentials are migrated simultaneously.
- **Minimal user involvement:** End users do not need to take any action for their accounts to be migrated (if hashed passwords are available using a supported algorithm).
- **Simplicity:** Bulk migration is the easiest method to implement, requiring less technical expertise from teams, and orchestration is typically not needed to assist with the migration.

Considerations:

- Potential downtime and data inconsistencies can occur during the bulk migration process.
- Identities should be exportable from the current system in a JSON format.

Just-in-time migration (lazy migration)

Just-in-time migration, often referred to as lazy migration, involves gradually transitioning customer identities and credentials to IDM within the Transmit Security Platform during the login process. This approach ensures a smooth migration experience for active users while leaving dormant and infrequently used accounts untouched until the customer's next authentication.



Benefits:

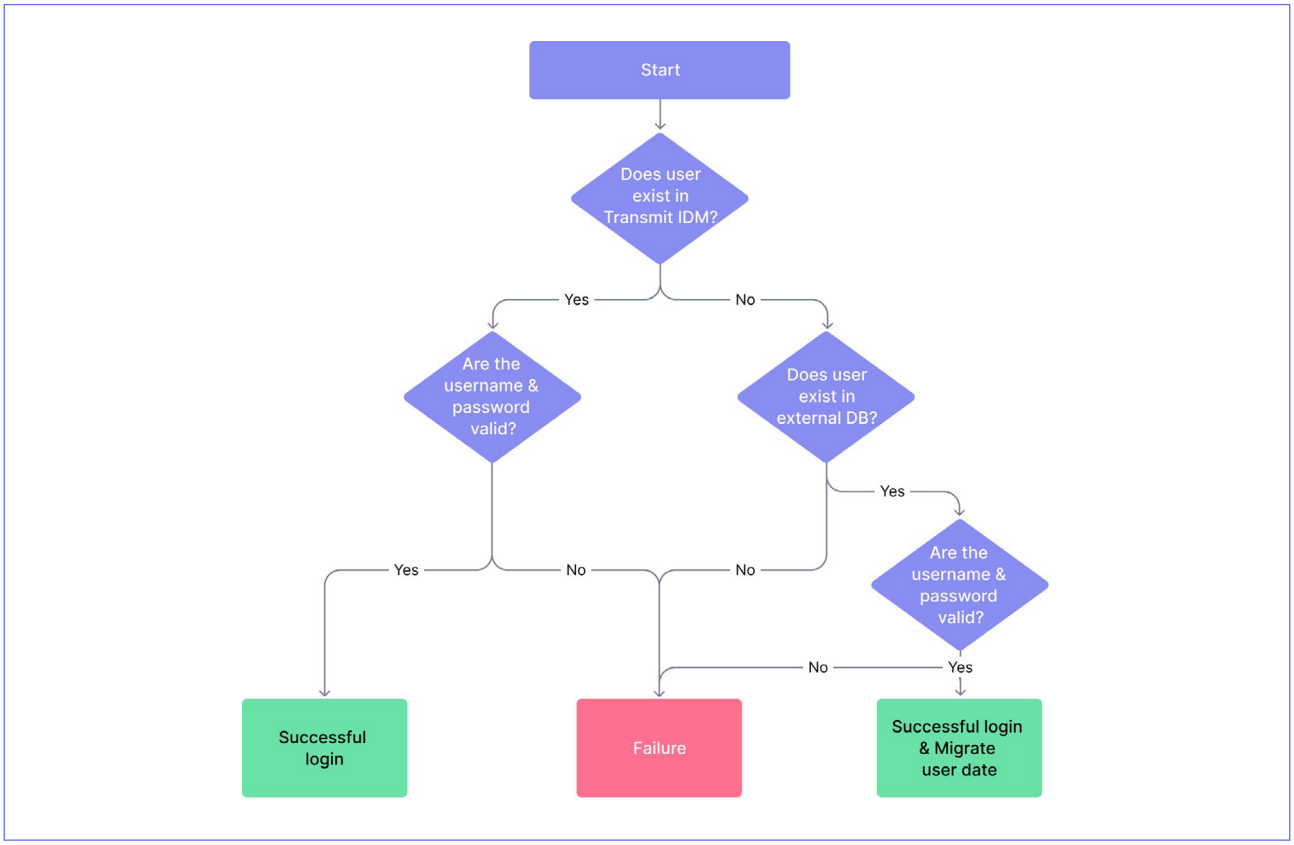
- **Minimal disruption:** Active users are migrated seamlessly during their next login, minimizing any inconvenience.
- **User experience:** Offers the opportunity to introduce new authentication mechanisms at the time of migration, enhancing the user experience.
- **Immediate time to value:** Immediately leverage features such as risk-aware role-based access control, contextual authorization, passwordless authentication options (e.g., passkeys, email magic links, TOTP) provided by Transmit Security.
- **Testing:** The transition can be tested under a live load.
- **Risk Mitigation:** Monitoring and fixes can be done on an as-needed basis, allowing teams to mitigate any issues as they go.
- **Availability:** Lazy migration does not run the risk of downtime, ensuring customer-facing services remain available throughout the migration process.

Considerations:

- **Development efforts:** Creating a seamless migration for end users requires additional development efforts and additional logic to implement. Your teams can build this on their own or with the use of orchestration tools.
- **Migration timeline and potential costs:** Infrequently used / dormant accounts will remain on the old system until the next login event, requiring the old system to be maintained in parallel with Transmit Security until all users are migrated.

Just-in-time migration technical sequence flow

Lazy or JIT migration requires additional logic to migrate users in real time, as they log into the application. To help with the lazy migration flow, orchestration is highly recommended, using either Transmit Security Orchestration or your organization's existing orchestration tool to graphically design user journeys rather than coding complex logic. In either case, the basic user flow can be seen on the following page as an example that can be customized to suit your organization's needs.



Recommended strategy: The hybrid approach

Our recommended approach is to combine both just-in-time and bulk migration strategies to strike a balance between minimal disruption and optimal performance. This allows testing, monitoring and fixes to be implemented as the first users are migrated, ensuring a smooth rollout.

At the same time, this approach provides a clear cutoff date for completing migration, as remaining users will be migrated in bulk at a predetermined time — limiting its impact to a small number of users, most of whom are likely to be inactive. As a result, the risk of any potential downtime or data inconsistencies during this final step is minimal.

Benefits:

- Allows businesses to test the transition under a live load
- Monitoring and fixes can be done on an as-needed basis
- Provides a more seamless transition for customers
- Clear cutoff date for completing migration to the new IdP
- Minimal risk of downtime or data inconsistencies

Considerations:

- Not as easy to implement as bulk migration alone
- Requires organizations to maintain legacy systems longer compared to bulk migration only
- Orchestration capabilities are recommended to assist during the lazy migration phase

The hybrid approach: How it works

Just-in-time migration: This first phase will initiate the migration by moving frequently used identities to the new platform during their next login. This allows users to enroll in new, innovative authentication mechanisms and immediately benefit from a range of passwordless authentication options.

Bulk migration: After the initial just-in-time migration phase, the remaining users will be migrated to IDM within the Transmit Security Platform by executing the bulk Migration Utility, based on the schema you provide. This ensures all identities are eventually moved, allowing your organization to decommission your old customer identity store and authentication platform.

Migrating passwords

During the migration process, passwords can be migrated, but only if hashed passwords are available for export and provided using one of the following hashing algorithms:

- Bcrypt
- Firebase (a modified Firebase version of SCrypt)
- Argon2

In addition, the following hashing algorithms will soon be available:

- SHA-256
- SHA-512
- MD5

If hashed passwords are available for export (typically from homegrown databases) using a supported algorithm, end users will experience a seamless transition without any added friction.

However, if hashed passwords can't be exported from existing systems (typically when migrating from third-party IdPs) or use an incompatible hashing algorithm for one or more user groups, end users may need to reset their passwords upon successfully authenticating against the old IdP, adding friction to the user experience. Alternatively, lazy migration can be applied, coupled with orchestration tools (or your organization's own custom logic) to ensure a smooth migration.

When migrating passwords, the schema should include all the necessary fields that you would like to migrate. The user data for these fields will be mapped to the Transmit Security Identity Management Service. Common user attributes (email, phone, username, etc.) will be directly mapped to the core user attributes provided by Transmit Security. The rest of the attributes can be placed in the custom user data. An example of the user schema is shown here:

```
[
  {
    "accessRoles":"web",
    "uuid":"1efg1111-410f-8ea6-5f4a4f82c2c6",
    "mobileNumber":"+112345678",
    "created":"2015-06-22 19:26:25.687608 +0000",
    "lastUpdated":"2020-05-25 16:31:55.097392 +0000",
    "lastLogin":"2015-06-22 19:26:25 +0000",
    "password":{

"value":"$2a$10$zbanJDReg4nbEEsgtEaJBOmNiROAeLVYSAVVH6Z7HxBP40npFFUcS",
      "type":"password-bcrypt"
    },
    "hygieneDate":"2020-05-25 12:31:55 +0000",
    "hygieneStatus":"Password Change"
  }
]
```

Once a sample schema has been provided, Transmit Security will map the attributes from the old system to Transmit Security's system and provide an updated Migration Utility.

Rollback options

In the event you wish to reverse migration to Transmit Security, data sync from the Transmit Security identity store to your old IdP, can be done through:

- API: This option will provide automated data transfer in a JSON format.
- Admin portal: In this option, data will be manually exported to a CSV file.

Due to security practices, these rollback options don't include user password export by default. However, if you need password export, Transmit Security can provide a secure file containing user IDs and passwords.

To learn more about Transmit Security Identity Management, visit our Developer Hub.