

Okta User Migration Guide

Secure, seamless
customer migrations

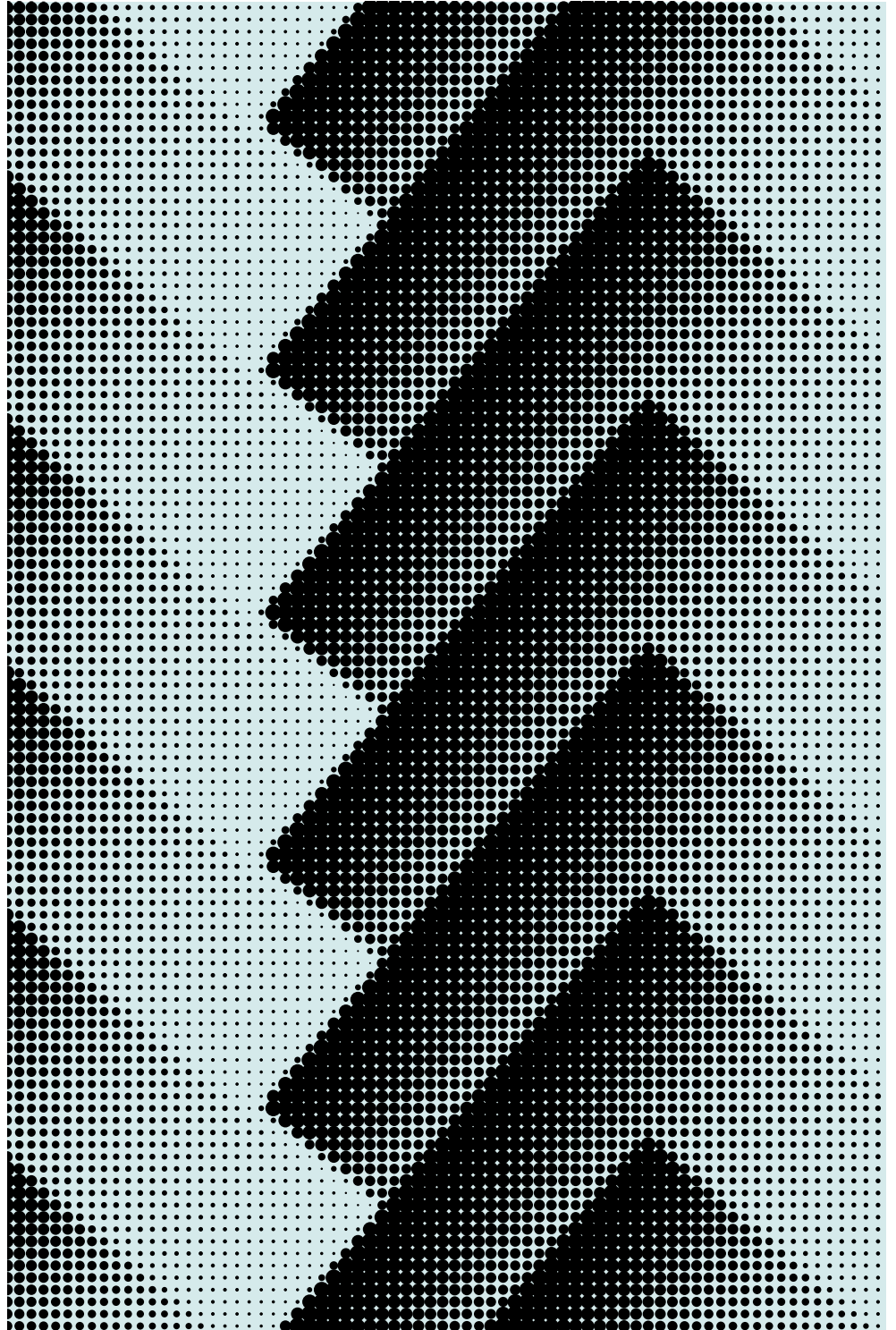
Okta Inc.

100 First Street

San Francisco, CA 94105

info@okta.com

1-888-722-7871



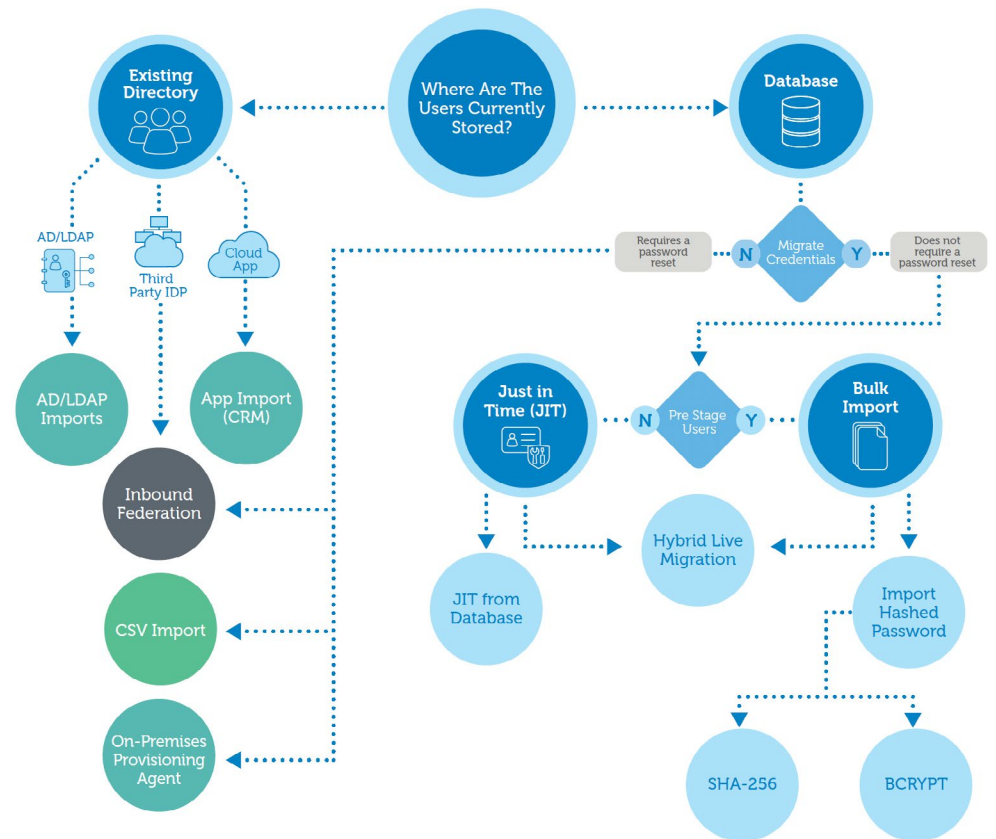
Contents

- 2 Migrating User Identity Profiles
- 3 Examine Key User Migration Design Considerations
- 5 Choose the Appropriate Migration Method
- 6 Bulk Import Migrations
- 9 Just-in-time Migrations
- 11 Existing Directory Migrations
- 12 Prepare Your User Migration
- 13 Plan for a Successful Migration

Migrating User Identity Profiles

Okta provides customers multiple ways to seamlessly migrate their user profiles from an existing user repository into Okta. This guide outlines various design considerations and available options that can help you achieve a smooth user migration process. Before initiating any move to a new identity platform, it's important to understand that such migrations present risks. This includes potential disruptions to end user experiences, such as requiring users to reset their passwords.

Decision process for migrating users flowchart



Examine Key User Migration Design Considerations

Proper planning is critical to a successful migration. To plan properly you need a thorough understanding of your existing user repositories. You need to be able to design for scale. Will you use delegated authentication? What can you do to ensure a seamless credential store migration? The sections below discuss some of the key points you need to consider in your design regarding these common user migration issues.

Assess your existing user repository

The first step to a successful migration is to understand the current state of your user profiles, including where they're stored, how they're accessed, and how their passwords are handled. For example, profiles stored in an existing on-premises directory, such as Active Directory or LDAP, can be easy to export and import, but gaining external access to those profiles requires more attention.

Understand delegated authentication

Delegated authentication allows you to “delegate” a third-party system to perform the validation for your user credentials. Delegated authentication is often used with third-party systems such as an existing user database like Oracle, MS SQL, MySQL, and others. It can also be used with identity providers. The “Migration methods” section later in this guide discusses a few delegated authentication options.

Ensure a seamless credential store migration

The current state of your user credentials can impact the migration method you use. For example, you can choose to do a directory import if the profiles exist in your Active Directory or LDAP directory. If the credentials are hashed, you might choose to do a bulk import for hashed passwords using the Okta Users API. If your passwords are in plain text or decryptable, you might simply write a script to set the password.

Secure customer PII

One of your highest priorities needs to be to ensure that your customers' personally identifiable information (PII) remains secure before, during, and after the migration. It's always best to be extra cautious when dealing with data that contains customer PII. For a user profile migration you need to make sure you safeguard your customer passwords to prevent any exposure of customer PII. Passwords must be encrypted and you need to make sure no user profile directories or databases have any direct exposure to the public internet. Failure to do so puts your customer PII at risk.


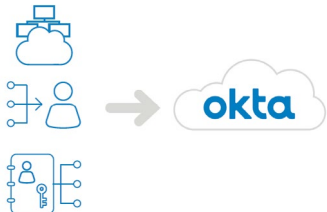
When considering your credential migration method, it's best to choose an option that minimizes the impact on your customer user experience. For example, while it might be easy to migrate passwords as plain text and then re-hash them after the migration, that can create a major security vulnerability. Since the person performing the migration will have access to every password, the best practice would be to require a password reset for all users on their first login after the migration completes. However, forcing password resets or requiring account reactivations for all your customers significantly disrupts the customers' experience and should be avoided. Where possible, choose a migration option that allows for a more seamless migration and a better customer experience.

As a side note, it's helpful to understand that migrations to some non-Okta solutions require you to open firewall ports or grant database access to external or cloud systems, which can create complexity and security vulnerabilities that put PII at risk of exposure. Okta migrations don't require you to expose your data in this manner.

Choose the Appropriate Migration Method

Migrating users can be separated into the following three main categories:

- Bulk import
- Just-in-time
- Existing directories

Main Migration Categories	Migration Variations	
Bulk Import Migrations	CSV Import Okta Users API <ul style="list-style-type: none"> • Importing Hashed Password • Hybrid Live 	
Just-In-Time (JIT) Migrations	Inbound Federation Existing Database <ul style="list-style-type: none"> • JIT from database • JIT from database with delegated authentication 	
Existing Directory Migrations	Directory Import (Active Directory/LDAP) App Import (CRM) On-Premises Provisioning	

Bulk Import Migrations

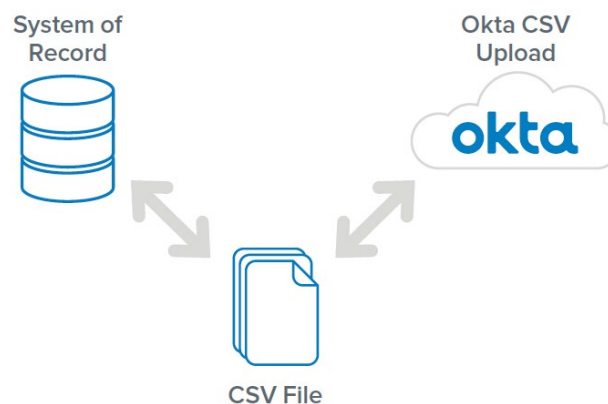
With a bulk import you pre-load (also known as pre-staging) all the user profiles into Okta before the go-live date of your migration. This method is a back-end process that creates all the users at once before they start using the Okta system rather than one at a time as is done with the just-in-time method. Since the entire import occurs ahead of time, the bulk method can help reduce many issues that users might typically encounter with other types of migrations. It also gives the import time to process the various tasks involved in properly setting up each user profile. You can perform a bulk import by doing either a CSV import or by using one of the two Okta Users API methods.

CSV import migration

A CSV import gives you the flexibility to import a user base from any system that has the ability to export the user base into a CSV format. In spite of that flexibility, CSV imports are not designed for large scale migrations. Additionally, passwords cannot be imported using this method and will require users to set their passwords when they first log in to the system.

To perform a CSV import you use an Okta provided CSV file to serve as a base template for your users. From the People page of the Okta administration user interface you can import the template file directly into the Okta Universal Directory once you've added all the users to the template.

More information on CSV imports.



Okta Users API import migration methods

Of all the user migration methods, the Okta Users API import method is the least disruptive. It allows you to create and set passwords for new users. There are two different ways to use the Okta Users API to migrate users—the importing hashed passwords migration and the hybrid live user migration.

Importing hashed passwords (Okta Users API migration)

To use the Okta Users API to create a user with a hashed password value you specify a supported algorithm, encrypted password value and the salt used to encrypt that password. These must all be included in the password credential object when creating a user with the Okta Users API. In this method, Okta hashes the hashed password using an Okta algorithm and then finalizes the creation of the new user by setting the user's password.

[More information on creating users with an imported hashed password.](#)



Hybrid live migration (Okta Users API migration)

A hybrid live migration combines aspects of bulk import and a live migration. A live migration is typically referred to as a just-in-time migration, which is the process of creating users when they log in for the first time.

By first bulk importing the identity attributes of the users and then setting their password during their first login you create a hybrid migration.

For a hybrid live migration, users are bulk imported with two temporary custom attributes—their hashed password and the salt used in that hash—that are created in their profile in the Okta Universal Directory. When logging in, you redirect users to a custom login page that compares the password entered by the user against the hashed password. If it matches, the custom login page sets the entered password in the user's Okta profile. This is the just-in-time aspect of the migration that makes it a hybrid live migration.

Once the password is verified and set, the profile's hashed password and salt temporary attributes can be deleted since they are no longer needed. If the entered password and hashed password don't match, you can deny the login, redirect the user to a password reset process, or trigger some other desired action. When the migration completes, you can remove the migration code from your custom login page or simply start using the regular Okta login page instead.



Just-in-Time Migrations

Just-in-time is a method of creating users on demand as they log in to Okta for the first time. You can perform a just-in-time migration using the inbound federation method or one of two existing database methods.

Just-in-time methods can simplify your migration since they automate the process and only create new users if they don't already exist in Okta. While in some ways just-in-time methods are easier than importing users in bulk, they can cause users to experience delayed login times if there's a large influx of new user logins once Okta goes live. However, there are ways you can prevent this through rate limit adjustments and performance testing.

Just-in-time inbound federation

For an inbound federation just-in-time migration you can use an existing trusted authentication provider to sign into Okta. This is also known as a federated login. You can do this using any SAML 2.0 supported application or social authentication provider, such as Facebook, Google, LinkedIn, and Microsoft. That also includes any OIDC/Oauth 2.0 compliant provider.

When using inbound federation, you can enable just-in-time to automatically create a new user account in Okta if the federated account logging in does not already exist in Okta. This automates and speeds up user creation since it can pull the user identity information directly from the identity provider. The user password will not be set in Okta at this point, but their identity attributes will be imported.

[More information on identity providers.](#)

Just-in-time existing database methods

You can choose from either of the the following just-in-time existing database migration methods:

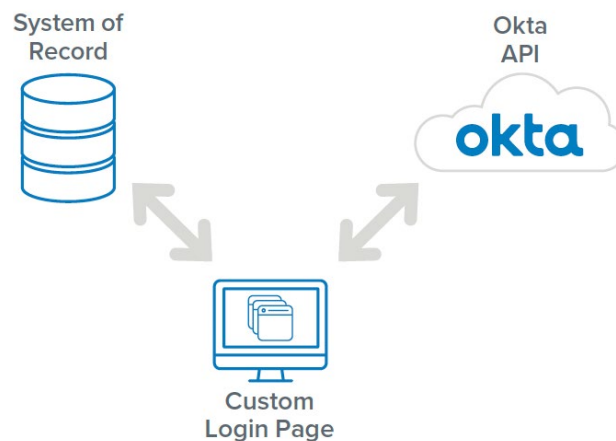
- Just-in-time from database
- Just-in-time from database with delegated authentication

JIT from existing database

If you store your user profiles in an existing database or if you're migrating to Okta from a different identity provider, you can do a just-in-time from database migration. Using the Okta Users API and a custom login page, you can route user authentications to authenticate against your existing database or identity provider. When a user successfully authenticates, the provided credentials are used to create a user profile in Okta that includes the provided password.

JIT from existing database with delegated authentication

The existing database with delegated authentication migration allows you to maintain your own local user system of record, while using Okta cloud authentication. While this is typically only done during the migration phase, if you want to keep your user credentials stored locally, that local repository can remain active even after the migration.



Existing Directory Migrations

You can also migrate user profiles using an existing directory, such as Active Directory, LDAP, a CRM cloud app, or other on-premises user repositories. Typically, these migrations leverage a small agent running on the directory or use one of the 130+ pre-existing provisioning integrations provided in the Okta Integration Network to automatically import the users from your existing directory system.

You can choose from the following methods for existing directories:

- Directory imports (Active Directory/LDAP)
- App import (CRM)
- On-premises provisioning

Directory import migration (Active Directory/LDAP)

A directory import is a common user migration method for organizations that store user profiles in Active Directory or LDAP directories. To use this method, you install and configure a small Okta agent on an internal network server that can use user information stored in your directory to automatically create user profiles in Okta. You can limit user creation to users in a particular organization unit (OU). You can also use standard LDAP queries to filter user creation/import based on specific criteria and confirmation matching rules.

[More information on Active Directory agents.](#)

[More information on LDAP agents.](#)

On-premises provisioning (agent based)

The Okta On-Premises Provisioning (OPP) agent extends provisioning capabilities to a wide variety of on-premises systems. The OPP agent allows you to import users into Okta directly from existing user repositories.

[More information OPP agents.](#)

App import migration (CRM)

You can also migrate users into Okta who exist in existing downstream applications, such as customer relationship management (CRM) systems or other customer data platforms that act as your master source of truth. An app import works similar to a directory import, but rather than using a local agent to perform the migration, this method uses pre-existing app-specific integrations and APIs to import your users. As with directory imports, you can also configure user matching rules and confirmations when doing app imports.

[More information on App imports.](#)

[More information on Okta integrations.](#)



Prepare Your User Migration

After taking into account the necessary design considerations and deciding what migration method will best address your needs, you can prepare for your migration. In most cases, these preparations should include making any needed rate limit adjustments and conducting performance testing before you begin your migration.

Avoid rate limit impacts

Okta employs built-in rate limit controls designed to protect the Okta service from the negative impacts that high traffic levels can create. This enables Okta to maintain service uptime and stability. As a result, during heavy usage periods an Okta tenant might experience traffic spikes that cause rate limits to go into effect. To avoid having rate limits impact your migration it's suggested that you work with Okta support to plan your user migration during a time when rate limits can be temporarily adjusted and identify what the available options are for doing so.

[More information on rate limits.](#)

Plan for a Successful Migration

User profile migrations that force a password reset on a considerable number of your users can have detrimental impacts on your customer experiences and your customer relationships. In today's modern authentication age, unexpected password resets not only spike helpdesk calls and support issues, but they can cast doubt in your customers' mind regarding your competence to serve their needs and ability to keep their customer data secure. The same thing can occur if you fail to actually migrate their profiles to the new platform.

To provide a seamless transition that enhances your customer experiences and relationships, it's critical to plan ahead. This includes taking into account all the essential design considerations, making sure you know how to move your users to the new platform, designing an efficient architecture, choosing the most appropriate migration method, planning in a way that results in minimal customer action, planning resources accurately, and ensuring you do all that you can to successfully and securely migrate your customers' current passwords to the new platform.

Want to learn more? We'd love to hear from you.

Please email us at: info@okta.com

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit okta.com.

