**Life Cycle Management**

**Introduction:**

**What is Life Cycle management in Okta?**

It’s Okta’s solution to bridge the gap between HR and IT for automation of the onboarding and separation process for the full life cycle of an employee.

**Processes to get this accomplished**

Before you begin, select a source of all your user provisioning and deprovisioning. It could be anywhere, HR’s app, Active Directory, O365 - Azure Active Directory, Okta, etc. Most people use Active Directory but it doesn’t really matter just pick one.

**Provisioning provides the following primary features:**

* **Account management –** Use Okta to create and assign user names, profiles, and permissions and binding your users' accounts to a single corporate user ID and password.
* **Importing users –** You can import users from Active Directory (AD), LDAP, or certain apps. You can configure Okta to continuously push user profiles to ensure that your system has the latest updates.
* **Configuring rules and workflows –** You can require specific passwords, synchronize and import groups from applications, and automatically deprovision users in Okta, AD, or LDAP.
* **Reports –** You can generate reports and audit trails to help you ensure efficient account usage.

**For integrations, Okta supports OAuth 2.0-based authentication and the SCIM standard.**

If an application supports lesser known standards such as SCIM or SPML, Okta can leverage those as well. Similar to its SSO access features, Okta connects to these APIs for you. You can configure Okta with credentials for your API user and select the features you want. Everything else is handled by Okta, including continuous automated testing and updates.

On-premises applications can also be integrated into Okta to enable provisioning. This can be done in one of two ways: leveraging Active Directory (AD) or using web services to manage user accounts in applications:

* For enterprises that on-board users using a Human Resource Management System (HRMS) like Workday, Okta provisions and deprovisions users into on-premises applications by using AD as a meeting point. You can configure Okta to manage accounts in your AD instance, and Okta will create and update users in AD based on user accounts in Workday. This information can then be used by any on-premises web app that uses AD as its user store.
* Okta supports provisioning and deprovisioning for any on-premises web app that has a web services API that is available to Okta using a publicly addressable connection. Okta makes calls to that app's web service to create new user accounts, update attributes, and deactivate users as needed based on the user assignment rules configured in Okta.

**Provisioning Methods**

**Okta provides several provisioning methods:**

1. **AD integration –** Use Okta's lightweight, on-premises Active Directory agent to synchronize with your AD configuration. You can set up real-time synchronization and just-in-time (JIT) provisioning to ensure that you always have the latest user profiles and do not have to wait for scheduled imports.
2. **LDAP integration –** Okta provides integration with several popular LDAP vendors using a lightweight agent. Okta's LDAP agent provides real-time synchronization and JIT provisioning, similar to its AD agent.
3. **HR-driven IT –** Okta provides automated provisioning from HR (for example, Workday). This type of provisioning is useful for companies that want to use their HR systems as their main user store. AD becomes a downstream provisioning target. This feature provides ongoing profile synchronization and ensures efficient on-boarding.

**Step 1 Getting your HR App integrated with Okta**

* You’ll have to open a support ticket to have them help you integrate the HR App into their SSO. After opening a ticket they’ll provide instructions and walk you through to getting it integrated.

After your HR App is integrated we are ready begin setting up the provisioning.. This Doc assumes you already have your on-premise AD already syncing with Okta as well as Office 365 (Azure AD). So, for instance, if you want your provisioning to start at the on-prem AD like most companies you’ll create a user in AD, Sync with Okta, and okta will provision all the other other apps.

**Step 2. Provisioning and Deprovisioning**

Okta’s provisioning features enable you to manage user accounts automatically within applications. This saves time and ensures that your users' access privileges are up to date. Provisioning and deprovisioning is bi-directional. Centralization into Okta provides users with a single access point so they don't have to remember multiple usernames and passwords. All provisioning options are located on the Provisioning tab for apps and the Settings tab for directories.

1. From the Okta Dashboard, --> Applications menu → scroll down to Applications.
2. From the Applications page → select your app.
3. Click on the Provisioning tab on the Applications page.
4. From the Settings column on the left, choose you desired configuration from the three possible configurations of Okta provisioning: Okta To App, App To Okta, and API Integration.

**Enhanced Provisioning for Specific Apps**

App-specific provisioning guides are accessible from the Okta Provisioning tab in the product.

**Profile Master and User Life Cycle Management**

After provisioning has been enabled, the flow of a user's identity throughout its different stages is known as a user’s life cycle. A profile master is the "source" from which users are imported or the target to which attributes are sent. Again there are three possible configurations of Okta provisioning: Okta To App, App To Okta, and API Integration, each of which are accessed under Settings on the left of the screen.

**Okta To App**

This screen contains settings for all information that flows from Okta into the app. Not every feature in the following list is available for every app.

Create Users

* Assigns a new app account to each user managed by Okta. Okta does not create a new account if it detects that the username specified in Okta already exists in the app. The user's Okta username is assigned by default.

Update User Attributes

* Updates the profiles of users assigned to that app and syncs those changes to downstream apps. Profile changes made in the app are overwritten with their respective Okta profile values.

Deactivate Users

* Okta automatically deactivates user accounts when they are unassigned in Okta or their Oktaaccounts are deactivated. Okta also reactivates the app account if it is reassigned to a user in Okta.

Exclude Username Updates

* Disallows the downstream application profile from overwriting the Okta user profile when using the profile push feature.

Sync Password

* Ensures users' app passwords are always the same as their Okta passwords or allows Okta to generate a unique password for the user. For more details, see Using Sync Password. - See doc Okta - Using Sync Password

Profile Attribute Mappings

**App To Okta**

This tab contains settings for all information that flows from the App to Okta.

Click the Edit buttons to make changes in the following sections.

**General**

* Use this section to schedule imports and dictate a username format that Okta will use for imported users. You can also define a percentage of acceptable app assignments before the Import safeguard feature is automatically triggered. If the Okta username is overridden due to mapping from a provisioning-enabled app, the custom mapping appears here.

**User Creation & Matching**

* Matching rules are used in the import of users from all apps and directories that allow importing. Establishing matching criteria allows you to specify how an imported user should be defined as a new user or mapped to an existing Okta user.
* **Imported user is an exact match to Okta user if:** Exact matching occurs when the Okta username format, email, attribute (base or custom), or attribute combination matches that of an Okta user.
* **Allow partial matches:** Partial matching occurs when the first and last name of an imported user match those of an existing Okta user, but the user’s username and/or email address do not.
* **Confirm matched users:** Select to automate the confirmation or activation of existing users. Unchecked, matches are confirmed manually.
* **Confirm new users:** Select to automate the confirmation or activation of a newly imported user. If this option is selected, you can uncheck it during import confirmation. Note that this feature does not apply for users who already exist in Okta.

**Profile & Lifestyle Mastering**

Use this section to allow the current app to profile master Okta users. Once enabled, the app appears in the list of profile masters on the Profile Masters page.

* **Allow <app> to master Okta users:** Determine what happens when a user is deactivated or reactivated in an app.

Remember that only the highest priority profile master for that Okta user can deactivate or suspend an Okta user. To verify the highest priority profile master, review the Profile Masters page.

* **When a user is deactivated in the app:** Choose to deactivate, suspend, or do nothing. Do nothingprevents activity in the app from controlling the user cycle, but still allows profile master control of attributes and mappings.
* **When a user is reactivated in the app:** Choose whether reactivation in the app applies to suspended or deactivated Okta users. When a user is reactivated in the app, the user profile must be an exact match to the Okta profile for the reactivation to also occur in Okta. Otherwise, after importing the reactivated users, they appear in Pending Activation state.

**Inline Hooks**

* Use this section to add custom logic to the process of importing new users into Okta from an app. You can resolve conflicts in profile attributes and control whether imported users are treated as matches for existing users.

**Inline Hooks is an Early Access feature.** To enable it, please contact Okta Support.

Inline hooks are outbound calls from Okta to your own custom code, triggered at specific points in Oktaprocess flows. They allow you to integrate custom functionality into those flows.

You implement your custom code as a web service with an Internet-accessible endpoint. It's your responsibility to arrange hosting of your code on a system external to Okta. Okta defines the REST API contract for the requests it sends to your custom code, as well as for the responses your custom code can send back.

The outbound call from Okta is called a hook. Your code, which receives the call, is referred to as your external service.

Inline hooks use synchronous calls, which means that the Okta process that triggered the hook is paused until a response from your service is received.

**Inline Hook Setup**

After creating your external service, you need to tell Okta that it exists and enable it for a particular process flow.

1. Select Workflow > Inline Hooks in the Okta Admin console.
2. Click Add Inline Hook, and then select the type of hook.
3. Define the following attributes:

* Name: a descriptive name for the inline hook
* URL: the external service's endpoint URL, to which the inline hook sends the request
* Authentication field: the name of the authorization header
* Authentication secret: the value string that corresponds to the field name
* Custom header fields: optional field name / value pairs to send with the request

1. Click Save. The inline hook is now Active.
2. Associate the endpoint with an Okta process flow. How to do this varies by inline hook type.
3. To delete an inline hook, first deactivate it.

**Okta Attribute Mappings**

* Use this portion of the page to edit attributes and mappings in the Profile Editor.

**API Integration**

* Some apps require a token to authenticate against their API. Click the Authenticate with App Name button to generate a token. You are redirected to the app where you must authenticate to obtain your token.

**Deprovisioning**

* Okta's deprovisioning features ensure that people who are no longer with your company do not have access to sensitive applications and documentation. Deprovisioning is also important for compliance reasons and to help you maintain an accurate usage count for your applications.
* You can deprovision users in Okta or AD. Users are automatically deprovisioned from supported apps. Admins receive an email describing any apps that require them to manually deprovision users.

**Profile mastering**

A profile master is an application (a directory service like Active Directory or LDAP, or an HR-management app such as Workday) that can act as the "source of truth" for user identities. Once enabled from the app or directory's Provisioning tab, it appears in the list of profile masters on the Profile Masters page. Without the inclusion of any external profile “master”, all profiles are mastered by Okta.

Currently, if more than one profile master exists on the Profile Masters page, they can be prioritized so that end users can be mastered by different systems, based on their assignments. At any given time, there can only be one profile master that masters a user's entire profile.

Profile masters are powerful tools that can potentially manage the entire life cycle (creation, updates, and deactivation) of an Okta user. Admins leveraging Workday, for example, can allow Okta to receive user creation, updates, and termination events from Workday.

Okta is periodically adding profile master capabilities to an expanding number of apps and directories. The following apps and directories are among those available for profile mastering: Active Directory, BambooHR, G Suite, LDAP, NetSuite, Namely (build by ISV), Salesforce, SuccessFactors, UltiPro, Workday

**Prioritize Profile Masters**

When an app or directory is designated as a profile master, it is listed on the Profile Masters page. This page is also used to sort the priority order of apps that support profile mastering. If more than one profile master exists, they must be prioritized so that end users can be mastered by different systems, based on their assignments. Without Attribute-level mastering, there can only be one profile master that masters a user's entire profile.

Note: When a new profile master is added, it is immediately placed as the lowest priority. This insures that any existing priority master(s) are not altered.

1. From the Dashboard, click to the Directory drop-down menu.
2. Scroll down to Profile Masters.

All profile masters are listed, and their status is indicated under the Priority column.

1. Click the arrows to change the profile status of the corresponding app or directory.

**Attribute-Level Mastering**

Attribute Level Mastering (ALM) delivers finer-grain control over how profiles are mastered by letting you specify different profile masters for individual attributes. This Early Access feature is a powerful element of Okta Provisioning. For details, see Setting up Attribute Level Mastering.

**Rules for Incoming Imports**

Using a profile master necessitates a clear distinction between new imported users verses updates to current Okta users. Okta uses matching rules to maintain a link between the profile master source and Okta to prevent conflicts. These rules can be set from the Provisioning/Settings tab of the mastered app or directory (see User Creation & Matching under Provisioning and Deprovisioning for details).

**Profile Mastering and Life Cycle**

The flow of a user's identity throughout the different cycles of access (creation, update, and removal of access to resources) is known as a user’s life cycle. A profile master can determine the beginning of this cycle, and is enabled within the provisioning and import space. For details on how profile mastering factors into provisioning, and a general overview of all provisioning options, see Provisioning and Deprovisioning.

**Attribute-level mastering**

Attribute-level Mastering (ALM) is a powerful feature of Okta Provisioning. For general information about provisioning, see Provisioning and Deprovisioning Overview. For details about profile mastering, see Profile Masters.

A profile master is an application (a directory service like Active Directory or an HR management software such as Workday) that can act as the "source of truth” for user identities. Currently, if more than one profile master exists on the Profile Masters page, they can be prioritized so that end users can be mastered by different systems, based on their assignments. At any given time, there can only be one profile master that masters a user's entire profile. However, ALM delivers finer grain control over how profiles are mastered by letting you specify different profile masters for individual attributes.

For example, an Okta user may have most of their profile attributes like first name, last name anddepartment, mastered by an HR system like Workday. With attribute-level mastery, their phone number andemail address attributes could be mastered by Active Directory. Furthermore, their personal email address or preferred display name could be mastered inside Okta, and managed by an Okta admin or the end user themselves.

Note: Profile mastering only applies to Okta user profiles, not app user profiles.

**Setting up ALM**

Using the ALM feature requires that (1) profile mastering is enabled, (2) you have chosen a profile master from the list under Profile master priority on the Profile Editor page, and (3) any desired mappings are specified through UD mapping.

The first step in setting up ALM is to enable profile mastering. Use of ALM assumes that more than one profile master is set on the Profile Masters page. In order for these profile-mastered apps to appear on the Profile Editor under Profile master priority, as shown below, profile mastering must be enabled for those apps.



**Enable Profile Mastering for Active Directory**

1. From the Administrative Dashboard, go to the Directory drop-down menu.
2. From the drop-down menu, choose Directory integrations.
3. Click the Active Directory instance.
4. Choose the Settings tab.
5. Scroll down to Provisioning Features > Profile Master.
6. Check the Enable button.

**Enable Profile Mastering for Other Profile Mastering Apps**

1. From the Administrative Dashboard, go to the Applications drop-down menu.
2. From the drop-down menu, choose Applications.
3. Choose the app from the list of applications.
4. From the <app> page, choose the Provisioning tab.
5. From the left-side Settings panel, chose To Okta.
6. Scroll down to Profile & Lifecycle Mastering and click the Allow <app> to master Okta users check box.

**Establish Profile Masters by attribute**

The second step of setting up ALM is to establish mastery by attribute. if your profile master(s) has been successfully enabled, they appear as a list under User > Profile master priority. When you scroll down to Attributes > Master priority (in the right-side column), the default state is Inherit from profile master, which retains the profile master set for the entire profile. To change the priority, you have the following options:

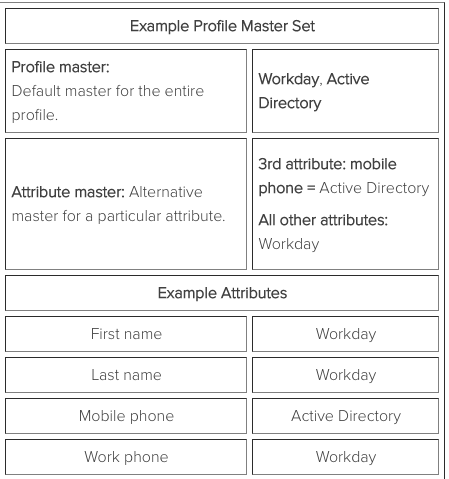
* Inherit from profile master: Picks up the default profile master for the entire profile, as shown in the Profile master priority field.
* Inherit from Okta: Picks up this particular attribute value from Okta. This attribute value can be edited in three ways: via the user's Profile tab, the Okta API or, if appropriate for end-user modification, by the end user.
* Override profile master: Overrides the default profile master. Click the Add Master drop-down menu to choose another available profile master.

**To change the priority:**

1. From the Directory drop-down menu, choose Profile Editor.
2. From the Profile Editor page, select the source you wish to edit, then click Profile in the Actions column.
3. From the left-side column (Base or Custom), choose an attribute. An example might be Last name. Click the Information icon in the right-hand column.
4. From the Master priority drop-down list, you can choose to either Inherit from profile master, Inherit from Okta, or Override profile master.

Note: The Override profile master option allows you to delete a master here if you don't want it available to a particular attribute –this does not generally disable the app as a master. Do this by clicking the Xbeside the app name.

See below for an example scenario of how this might work with Workday and Active



Mapping the Attribute on the Profile Mappings Page

The third, optional step of setting up ALM is to map the attribute through UD. If no mapping are set up, the attribute has a null value.

After you have chosen an attribute to change and set the Master priority to Override profile master, for example, the attribute must be mapped. To map the attribute, do the following:

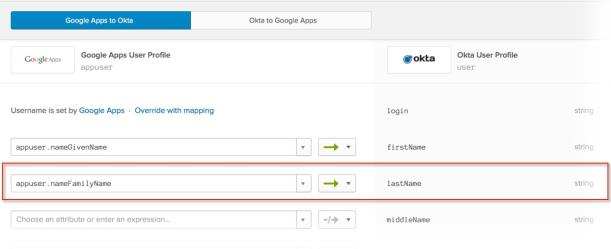
1. From the Profile Editor page, click the Profile Mappings tab.

2. Choose the app instance of the profile master you wish to map.

3. Click the Edit Mappings button.

4. From the list of attributes on the left, find the attribute (such as Last name) you have chosen to change. Note: ALM only maps from a profile mastered app to Okta –it is not bidirectional.

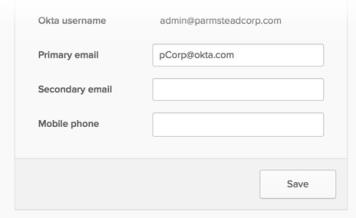
5. Click the Save Mappings button to save your choices.



If you have selected an attribute that has no mapping from the primary profile master, the attribute has a null value. A value is not pulled from any other master apps in the priority list.

Allowing End-User Edit Permissions

There are some attributes that can be mastered inside Okta, then managed by an Okta admin or their end users. Although end-users cannot change their most primary attributes (such as first name, last name, or primary email), you may want to allow them to add or change attributes like personal email address orpreferred display name. These attributes would appear as editable fields on their Settings > Account page.



To allow end-user editing of certain attributes, do the following:

1. From the Directory drop-down menu, choose Profile Editor.
2. From the Profile Editor page, on the left-side panel under Filters, select a profile type to narrow the list of apps.
3. Find the app source you wish to edit, then click the Profile button under the Actions column on the right-side column.
4. Under Attributes, from the left-side column (Base or Custom), choose an attribute, then click the Information icon in the right-hand column.
5. From the User permission drop-down menu you can choose one of the following options:

* Hide: Hides the attribute field from the end-user list.
* Read Only: Does not allow the field to be edited.
* Read-Write: Allows the end-user to change or add information to the attribute field.

1. From the Master priority drop-down list, choose Inherit from Okta.
2. Once completed, click the Save Attribute button.