okta

Three Approaches for Storing and Managing Accounts for External End Users

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Introduction 3

Scenarios 3

If You Already Have a User Store 3

If You Don't Already Have a User Store 4

Here's How to Manage Customer Users in Okta UD 7

Conclusion 10

Related External Identities Whitepapers 10

Introduction

If you've rolled out an identity platform for your employees to make them more productive and secure, it won't be long before you've got partners and customers with the same requirements. Luckily, any identity platform worth its salt is built to manage access for users of any type—internal or external—with the same level of ease. If you've got a requirement to share some of your internal files, folders, or resources to external users or to build a digital customer experience, such as a portal, you're faced with a design decision about how to manage the users outside of your organization.

This whitepaper describes your options for where and how to store external identities and how Okta Universal Directory can be used to manage them.

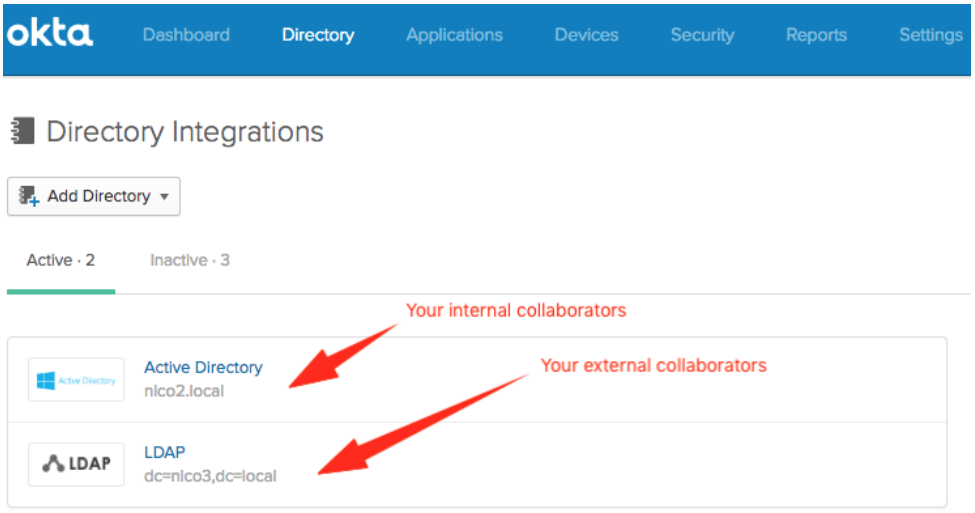
Scenarios

The main question to ask beforehand is: do you already have a place where you currently maintain those external identities?

If You Already Have an External User Store

If you already use an AD or LDAP to store your external users, then you just have to configure another AD/LDAP integration on your Okta tenant.

Ex:



You can import the users, their attributes, their groups like you've already done it for your existing AD.

If You Don't Already Have a User Store

You have 3 options here:

- Adding external users in your existing AD
- Creating a new AD/LDAP domain/instance/forest dedicated to those external users
- Create and manage external users directly in Okta Universal Directory aka Okta UD

1. Adding external users in your existing AD

Before considering that option, you may want to verify your current provisioning process and rules in place:

- Is there any "everyone in AD" group that may be used across access control rules or app assignation? If yes, you don't want to risk allowing external users to access internal-only resources.
- Does the creation of a user in AD requires having a real email address/an inbox on exchange with your corporate domain? Those are external identities, you may not necessarily want to create an inbox for them, especially under your corporate domain.

If you still want to add those external identities in AD (assuming you answered "No" to the 2 questions above), you will have to find a way to easily differentiate internal users vs external users: a different domain, different OUs, different groups, etc.... This could increase the complexity of your current AD environment, on top of requiring your IT team/helpdesk team to be an AD admin to manage external identities.

Advantages:

- Minimal changes – Use systems and software that you already have
- Data control – Keep your customer data stored on hardware you own
- Single Control Pane – Active Directory becomes the one place to get a consolidated view of all users of all types, and manage them

Tradeoffs:

- Requires infrastructure upgrade – You may need to upgrade the infrastructure on which your domain controllers run, since the number of users may increase significantly
- Extra point-of-failure – Authentication depends on a persistent connection between Okta and AD
- Increased authentication latency – Authentication is delegated to AD in real-time, rather than executing directly on the Okta platform

- No REST API accessibility – While Okta UD provides REST APIs to manage users, Active Directory provides no such interface
- Potentially vulnerable to lateral movement – Customer accounts can be given privileged rights in your domain due to admin error or lateral movement

2. Adding external users in a new AD/LDAP

Creating a brand new AD/LDAP could require a certain effort: new server, new domain, new Firewall rules, new backup/failover server, handling load balancing, hardware + professional services costs, and implicates maintenance of those different components.

If you haven't already invested that time + money in it, and if you don't absolutely need it to be a AD/LDAP user store, then that may not be the best course of action.

Advantages:

- Data control – Keep your customer data stored on hardware you own
- Delegated administration – The operator of the customer application can manage the app directory without permissions to manage internal employee accounts

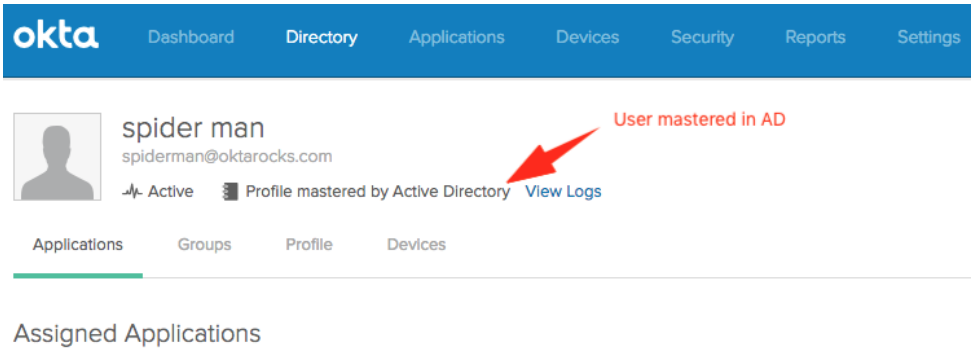
Tradeoffs:

- Multiple administration interfaces – There are multiple points of control for your end users. While Okta can consolidate a view of the users, management is delegated to the directory interfaces themselves.
- Requires infrastructure – You will need to procure, deploy, and manage the hardware and software for the directory. Depending on the criticality and scale of the application, this could be significant.
- Extra point-of-failure – Authentication depends on a persistent connection between Okta and AD, and the availability of the AD or LDAP infrastructure itself
- Increased authentication latency – Authentication is delegated to AD in real-time, rather than executing directly on the Okta platform
- No REST API accessibility – While Okta UD provides REST APIs to manage users, Active Directory provides no such interface

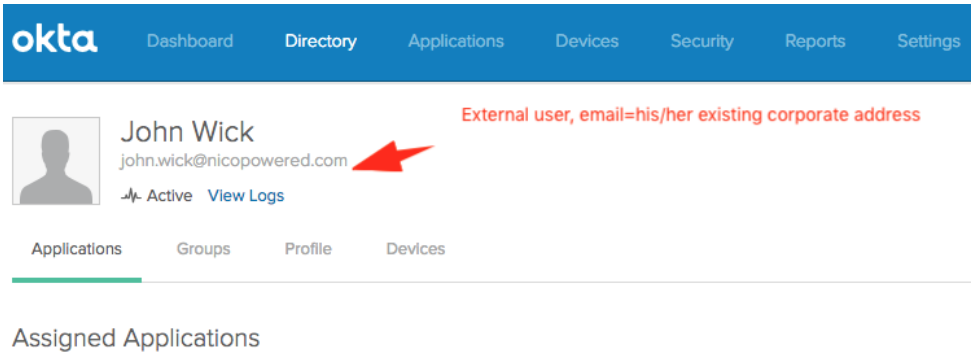
3. Adding external users in Okta Universal Directory

As highlighted in the resources section at the bottom of this whitepaper, Okta Universal Directory is your "One place to manage all your users, groups and devices, mastered in Okta or from any number of sources."

You can have on one hand your internal identities stored in AD, mirrored in your Okta Universal Directory:



and on the other hand your external identities directly managed in Okta Universal Directory:



Advantages:

- Single view of users – View all users in a single interface, purpose-built to streamline user management at scale
- Scale – The Okta platform scales flexibly to accommodate any number of users, including 'spikes' of activity which are common for external applications
- No infrastructure to manage – Okta UD is 100% cloud-native. Users are securely stored in the cloud and managed through a modern web interface.
- Delegated administration – Okta provides administrative roles on a per-group basis, to give the application owner control of customer accounts, and the IT admin control of employee accounts

- Convenient and extensible REST APIs – Okta UD provides REST APIs to manage users, which allows application owners to extend Okta to meet their requirements, or write automation scripts
- Speed and performance – Authentication is executed locally in the cloud; no latency incurred by delegating authentication to an external directory
- Secure user storage – Okta invests in security so that you don't have to. We have all the leading industry security certifications due to our commitment to protect customer data.

Tradeoffs:

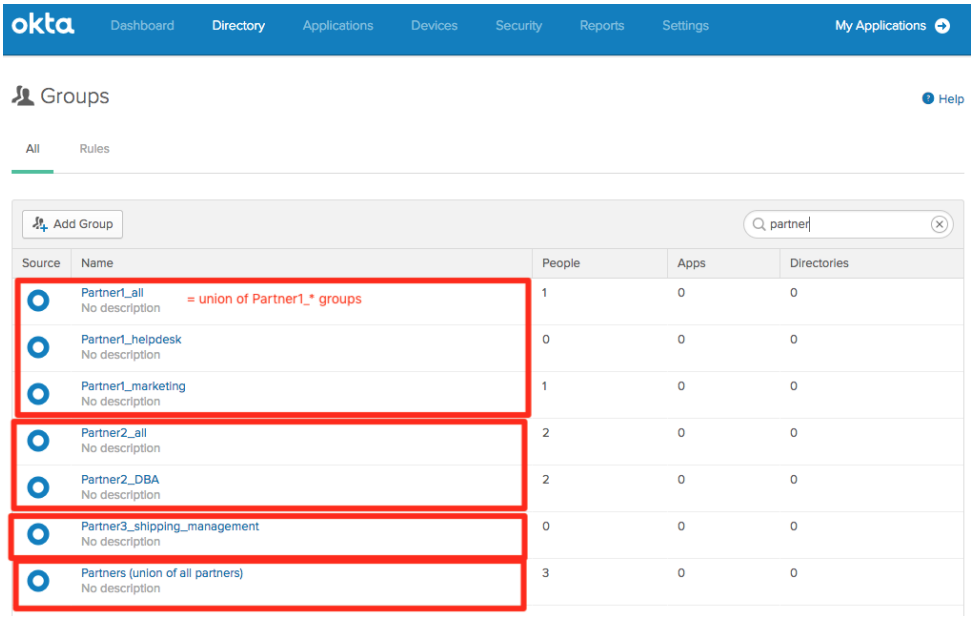
- Multiple administration interfaces – Commonly done using native AD or LDAP tools, while Okta consolidates a view of users, user management for employees is commonly still done in the directory, while management of customers occurs in the Okta Admin UI
- Migration costs – Okta provides several ways to migrate users from an existing repository, but migration inevitably takes time and resources

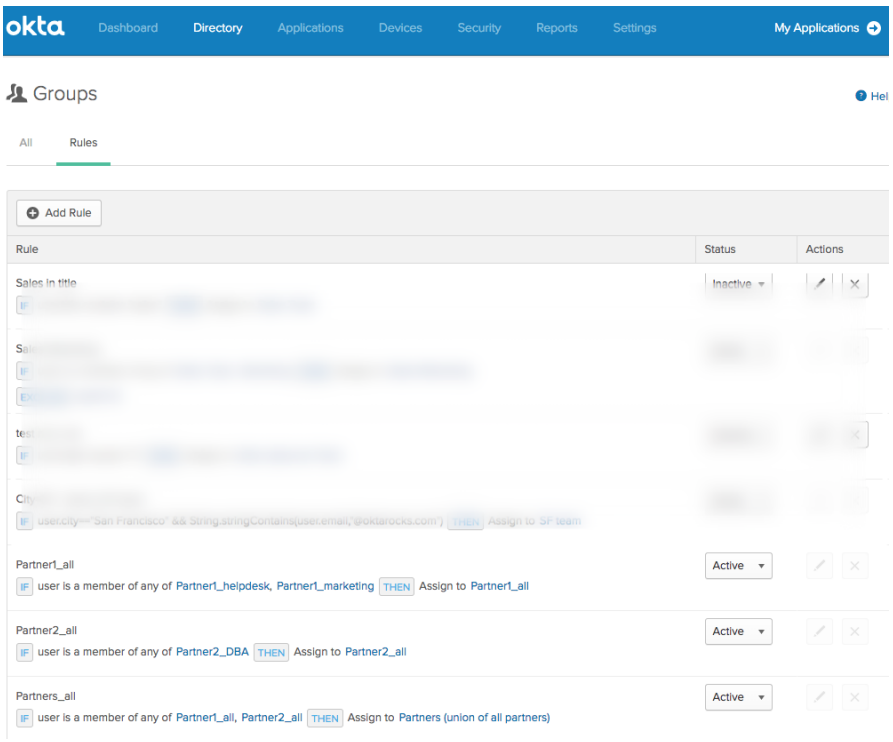
Here's How to Manage Customer Users in Okta UD

Okta's Admin UI is purpose-built to make managing customer identities a breeze. Here's a quick tour of some of the common management tasks, and how to complete them with Okta.

You can define your own guidelines to create/name groups. A recommended approach would be to have:

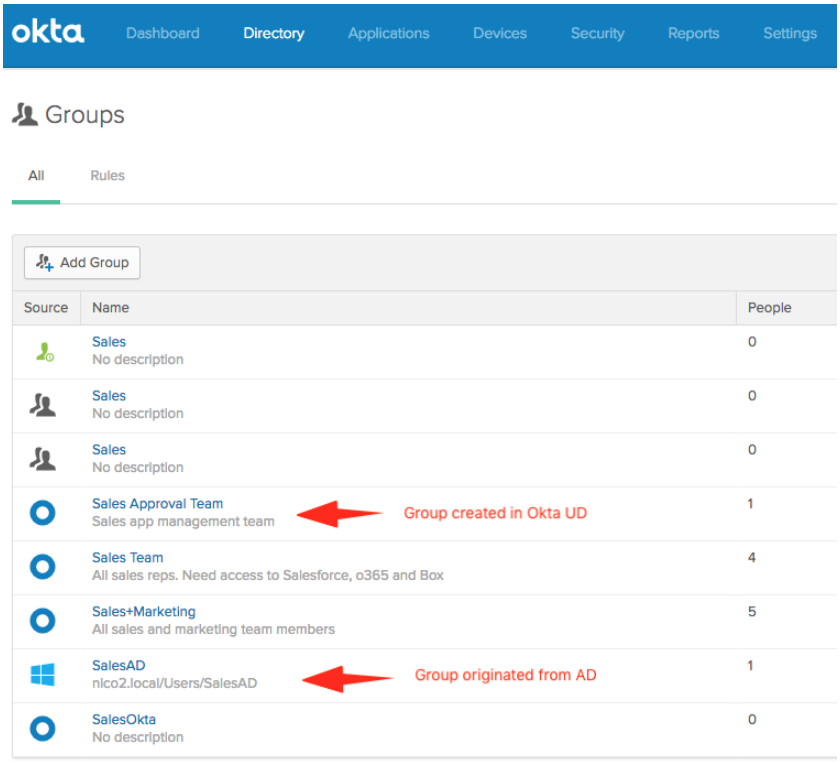
- If you're working with a team of external users belonging to the same company, you could create a dedicated group in Okta UD. That fits the B2B scenario. If you have different teams as part of the same external company, you could use the same prefix as part of your group's naming convention, and you can leverage Okta group rules to create union of groups. Ex:

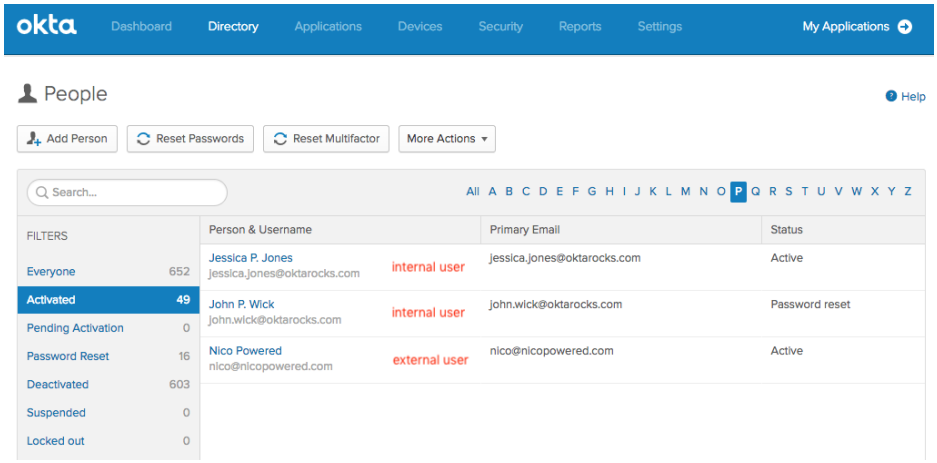




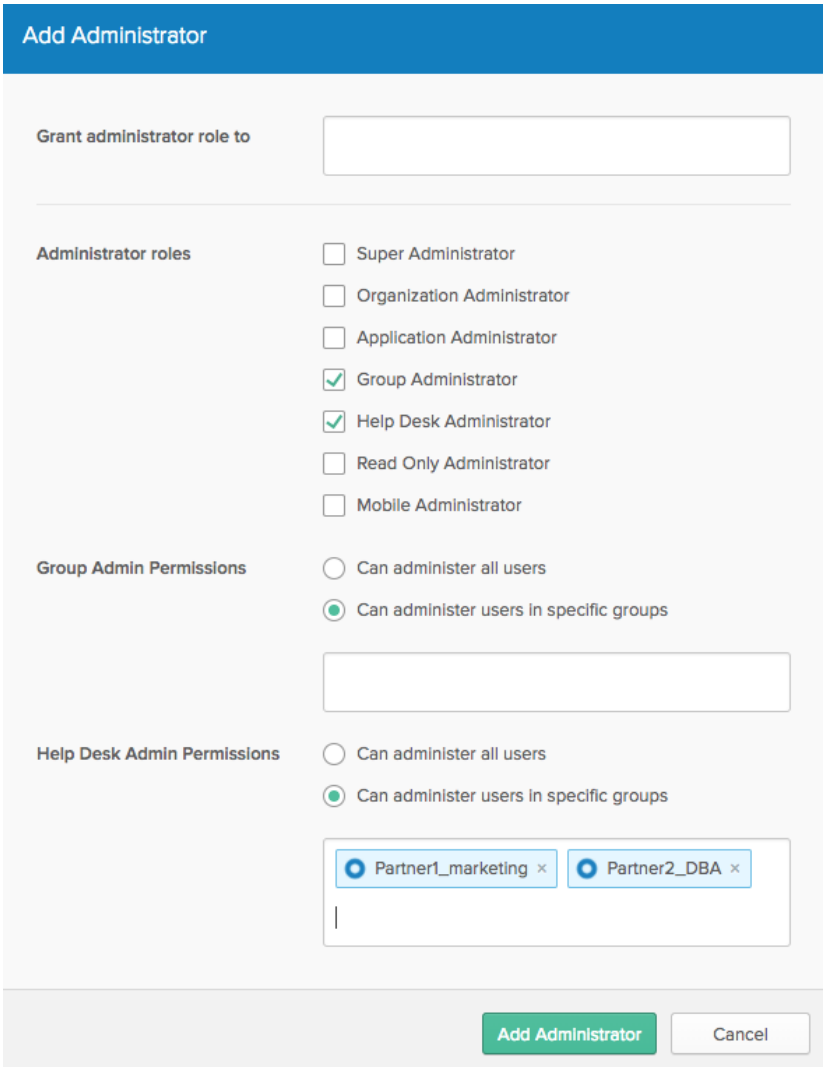
Note: Okta group rules can leverage group membership + user attributes

Regardless of where your users are originated from (AD or Okta UD), you'll be able to manage the corresponding groups and users from Okta UD:





Also, you can easily configure who is authorized to maintain those external user groups:



As a conclusion, our recommendation if you don't already have an existing user store for your external identities, is to leverage Okta UD which results in a quick deployment.

Conclusion

When you're looking to store and manage users in your extended enterprise, you've got options. You can store them in your existing AD or LDAP directory, you can deploy a new on-premises LDAP directory specifically for these users, or you can use Okta Universal Directory to manage users of all types at scale. We built Universal Directory specifically for this purpose, and by using it you can take advantage of numerous usability benefits, better scaling and availability, better security, and more. To get started with Universal Directory for free, go to okta.com/free-trial and get your own Okta instance today.

Related External Identities Whitepapers

To read more about how to manage external identities, check out the following resources:

- Cloud Identity for Customer and Partner Portals: **https://www.okta.com/resources/whitepaper-managing-customer-partner-identities-with-okta/**
- Okta for Your Customer and Partner IAM Architecture: **https://www.okta.com/resources/whitepaper-iam-architecture/**


okta