Recognize

User Sync Guide

version 3.1.6

About

About this guide

The Recognize user sync guide details how company administrators can set up user synchronization with a company's corporate user directory. At this time, we support syncing:

- **Yammer**
- **Microsoft Cloud** *Azure AD, Office 365, or Exchange online*

For Admins Only

This guide is intended for system and company administrators.

Requirements

- A Recognize account that is in trial or has been purchased with full access to the Recognize company admin portal.
- A user with administrator privileges to the identity provider that is desired to be synced (Yammer or Microsoft).
    - Microsoft: User account with Application Administrator or Global Administrator Privileges
- **If you do <u>not</u> wish to sync your entire organization**, you must have one or more groups or distribution lists setup in your corporate directory that contain the users you would like to sync.

Introduction

Common Questions

What is the user sync?

The Recognize user sync is a process that provides a way for companies to keep their Recognize user directory in sync with their corporate user directory. Once setup, it no longer requires further management. The typical amount of time required for configuration depends on the identity provider but ranges from 15m to a few hours (see the section on choosing an identity provider for more information).

When is it run?

The user sync is run nightly or weekly based on subscription level. We connect to the identity provider and user directory of your choice (Yammer or Microsoft) and synchronize the users based on a few parameters. You can sync your entire organization or you can pick groups to synchronize. You can also initiate a sync at any time via the Settings page in the company admin portal. The time it takes to execute a full sync depends on the size of your directory and the size of the queue in our background tasks server. For most of our customers, it can range from 15m to 2 hours.

How secure is our data?

Recognize connects via industry standard OAuth v2 protocol to access your organizations user directory. We obtain a token that is used to access user directory data via your sync provider's api. In the case of Yammer, the token does not expire. For Office 365, we connect to the Microsoft Graph API and the token expires on a periodic basis and is refreshed on an as needed basis. No extra administrator action is required to refresh the token. Recognize only takes read-only actions via these apis. Administrators may choose to revoke access at any time.

What about syncing groups?

You can also specify if you would like to sync Recognize Teams to your directory's groups to more closely mirror your internal structure and encourage friendly competition and reporting among your business units.

Are notifications or invites sent out?

When users are synced, they are added to the Recognize directory, but **no emails or notifications are sent out**. We have a "bulk invite" feature on our Accounts page in the company admin portal where you can customize the invitation email and send it out at a time of your choosing.

What happens to users when they are removed from the corporate directory?

When a user is removed from the corporate directory, the user sync detects this and simply "disables" the user. This means they can no longer log in and access their account. However, the recognitions they may have sent will remain in the system and the points received from those recognitions remain awarded to the recipients. If you wish to fully delete users from the system, please contact us at support@recognizeapp.com.

What happens when a user changes their name, email, avatar or other attribute?

The user sync not only adds users and disables them but also updates all the attributes we sync upon creation. If a user changes their name, email, avatar, job title or any other attribute(see the Data section below), we will update that data if it is present in the identity provider's api.

How does Recognize know who to add, update, or remove?

Recognize uses an internal Microsoft Graph ID as the unique identifier to match up users. When we sync for the first time, this information is populated. On subsequent syncs, users are matched up based on the Microsoft Graph ID. If a new ID is detected, the user is created. If a user with a given ID is no longer found in the sync configuration, that user will be disabled.

Data

The data that is available to sync is as follows:

- email
- first name
- last name
- manager (optional)
- avatar
- birthday(optional, day/month only)
- hire date(optional, not available with Yammer)
- job title
- team/group affiliations
- phone number (optional)
- display name (optional)
- department (optional)
- country (optional)

Custom Fields

Recognize has the ability to sync in up to 9 custom fields. Microsoft refers to custom fields as "Schema Extensions". You can read more here: https://docs.microsoft.com/en-us/graph/extensibility-overview. If you would like to sync custom fields into Recognize, please contact support@recognizeapp.com or your customer success manager.

Custom Field Mapping

Custom Fields can be mapped into standard Recognize attributes such as: birthday, start date, job title, country, department, and locale. The main use case of this is when companies are syncing with Microsoft and are not able to populate these data points in standard fields. For instance, its very common that companies are not able to populate the birthday and hireDate in Microsoft so they populate them as custom fields and then map them to the Recognize standard fields.

Data Source Matrix

Recognize has the ability to sync different attributes depending on which sync or authentication mechanism is used.

	SAML SSO	O365/ Azure	Yammer	Workplace	spreadsheet / sFTP Import
Employee ID					X
Email	X	X	X	X	X
Name	X	X	X	X	X
Phone		X	X		X
Job Title		X	X		X
Hire Date (month/day/year)		X			X
Birthday (day/ month only)		X			X
Language preference					X
Avatar			X		
Roles					X
Teams		X			X
Manager		X		X	X
Custom Fields					X
Schema Extensions		X			

Service Accounts

It is a common practice to use service accounts to setup the consent and authentication flows. This way the connection is not tied to an individual user. Please see Appendix A for more information about setting up a Service Account for use with User Sync.

Setting Up

Choosing an Identity Provider

It is common for companies to have both Yammer and Microsoft. If you have a choice, **we recommend Microsoft**. Here is a brief description of the differences between the two providers.

Yammer

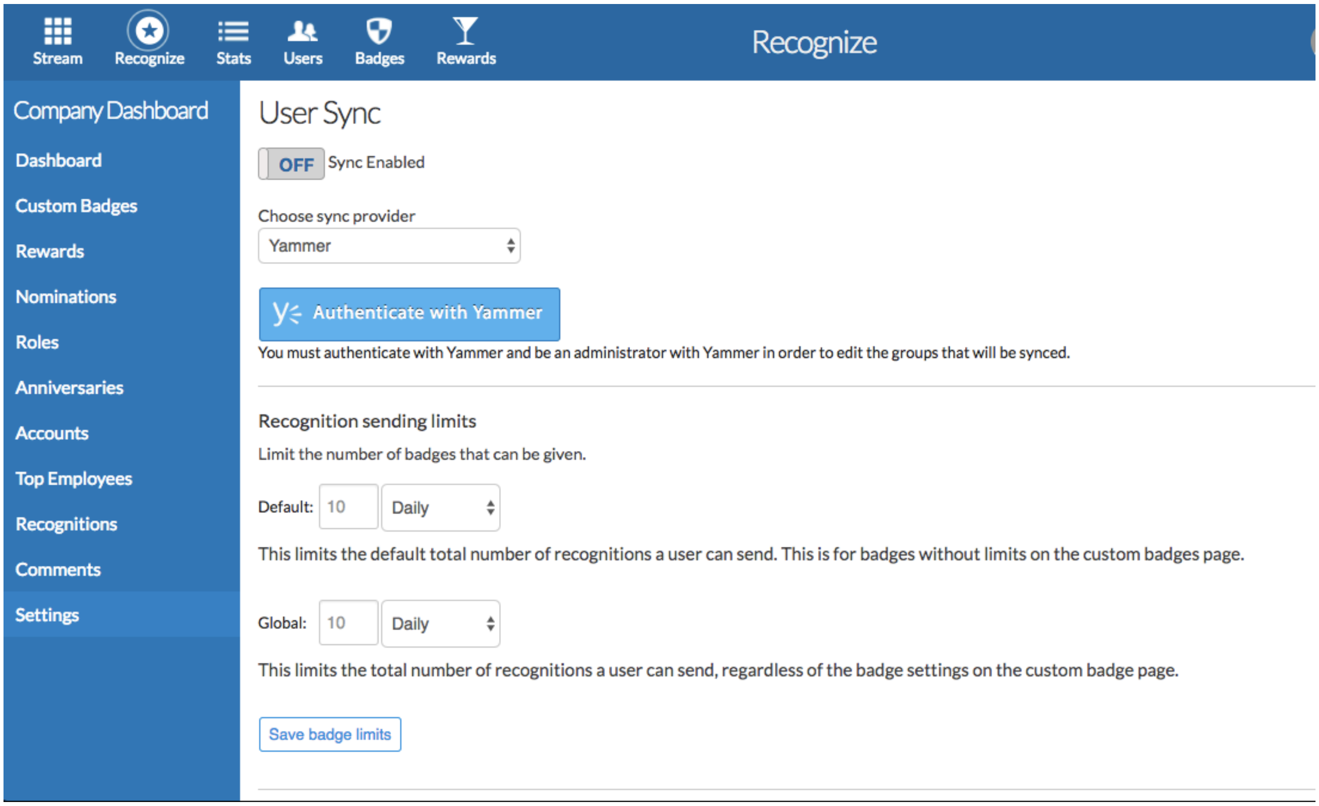
Syncing with Yammer is often easier and requires less IT involvement. In most cases, any standard user can authenticate and initiate a sync. In some cases, an admin on your Yammer network is required. Also, Yammer is much more limited in terms of the data that can be synced. For instance, Yammer does not have a data field for hire date and thus you will not be able to sync hire dates for use with Recognize's Anniversary feature.

Microsoft

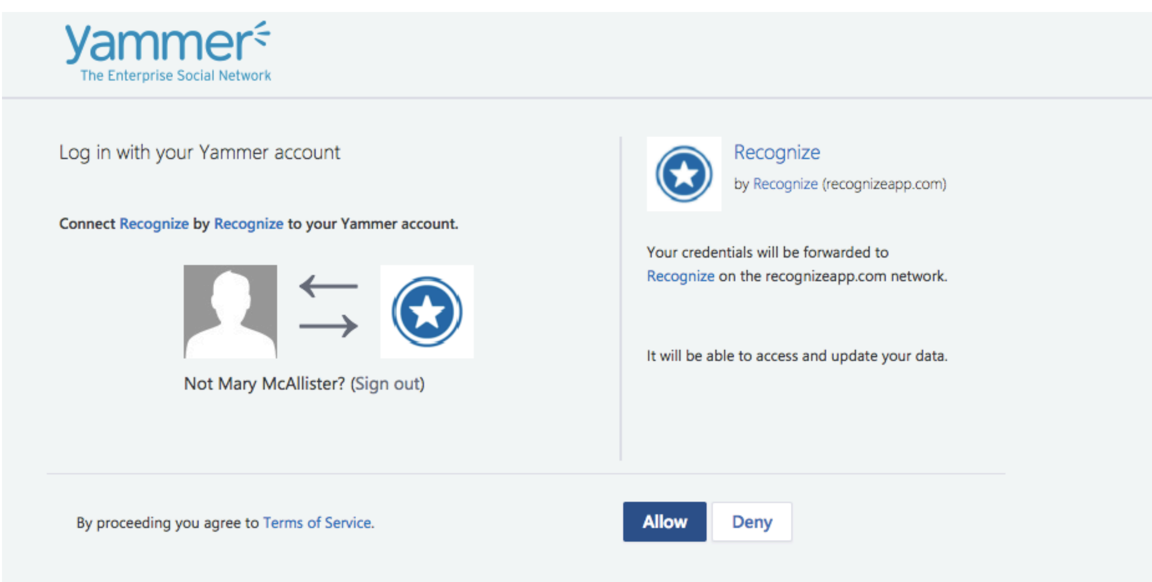
Syncing with Microsoft can be a bit more involved but is also more robust. Microsoft's api allows us to sync manager, hire date, and birthday for full use of the Recognize platform. A common problem with syncing with Microsoft is that companies do not often have groups that directly match the users they would like in their Recognition platform. Companies often sync their on-premise Active Directory with Azure AD, and the hierarchy present in 'on-prem' AD is not present in Azure AD. Therefore, this typically requires more IT involvement in order to get the groups in the right shape for syncing.

Syncing with Yammer

Visit the Company Admin > Settings > User Sync section to get started. Begin by clicking "**Authenticate with Yammer**". Remember, it is recommended you are an administrator on your Yammer account.

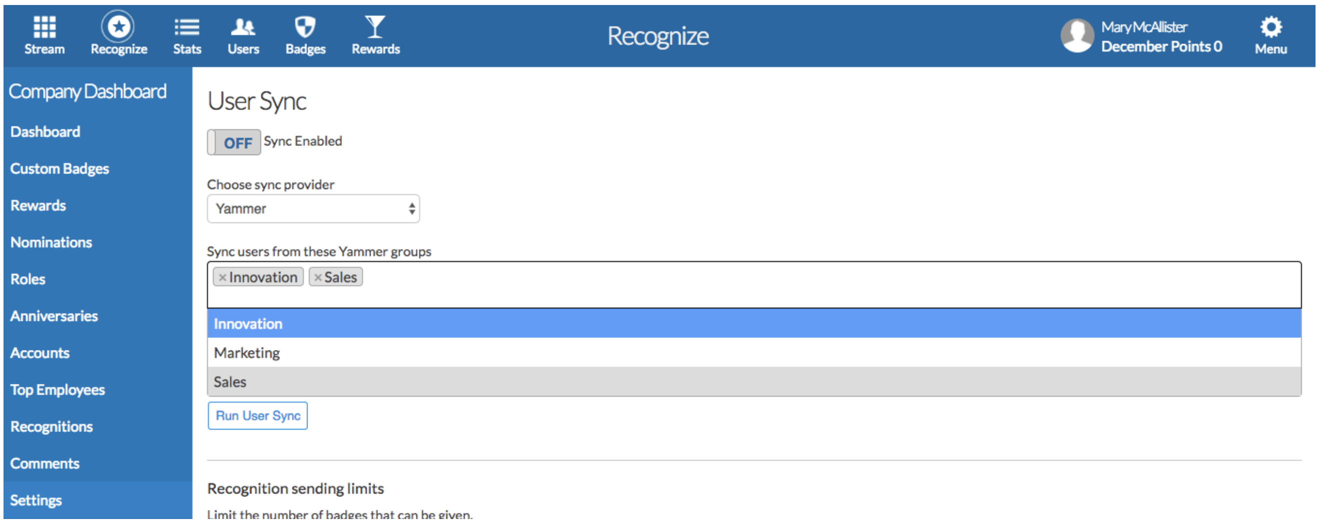


Allow permission for Recognize to access your Yammer account



After authenticating, return to the Company Admin > Settings > User Sync section.

If you would like to sync your entire network, leave the **groups** section blank. Otherwise, specify a group or groups that you would like to sync.



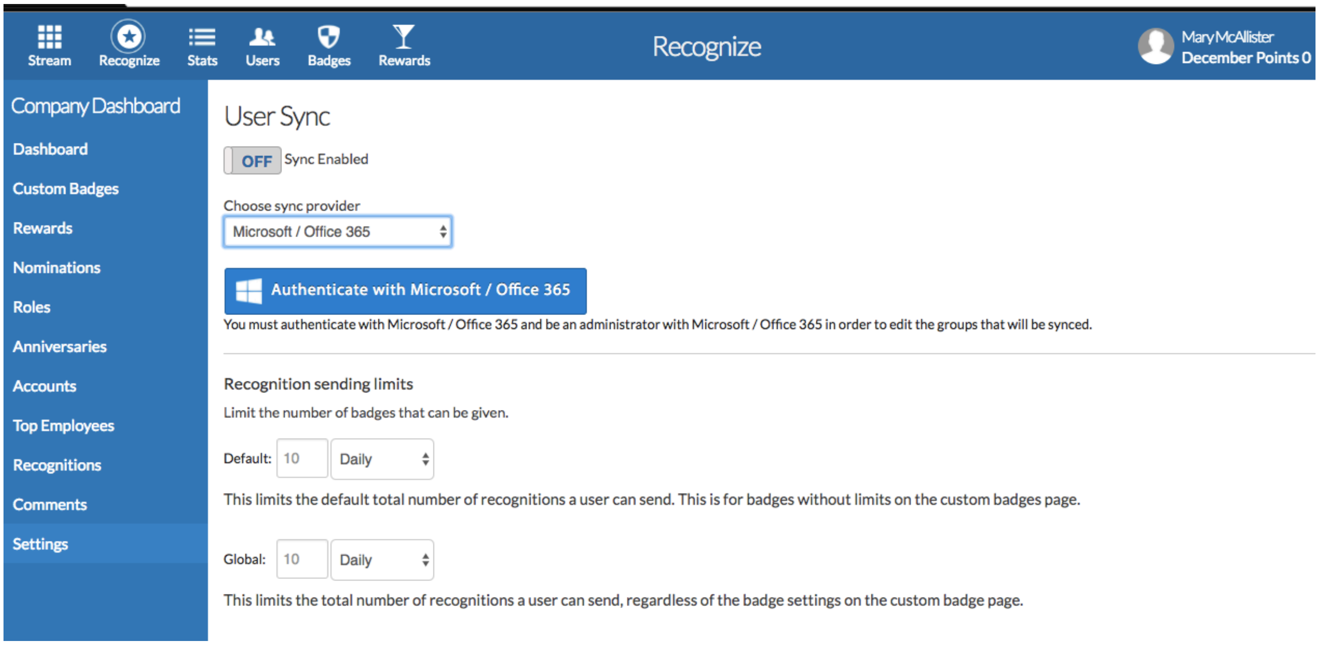
Configure whether you would like to mirror Yammer groups to Recognize teams. When ready, switch the toggle for "Sync enabled" to turn on the sync. The sync will proceed that night or if you want to expedite things, click "Run user sync" and the sync will be added to our background task server.

NOTE: *Currently, there is no notification when the sync has completed, you will just need to check back.*

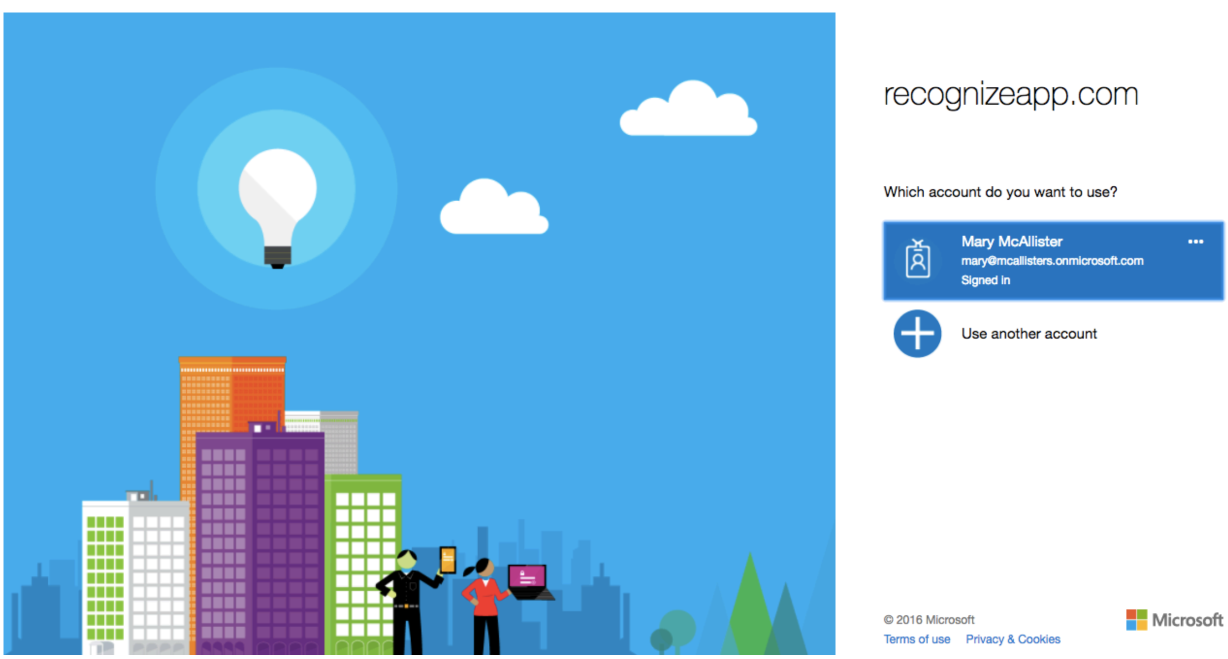
Syncing with Microsoft

Begin by clicking "**Authenticate with Microsoft / Office 365**" to authenticate your admin account with Microsoft. Visit the Company Admin > Settings > User Sync section to get started.

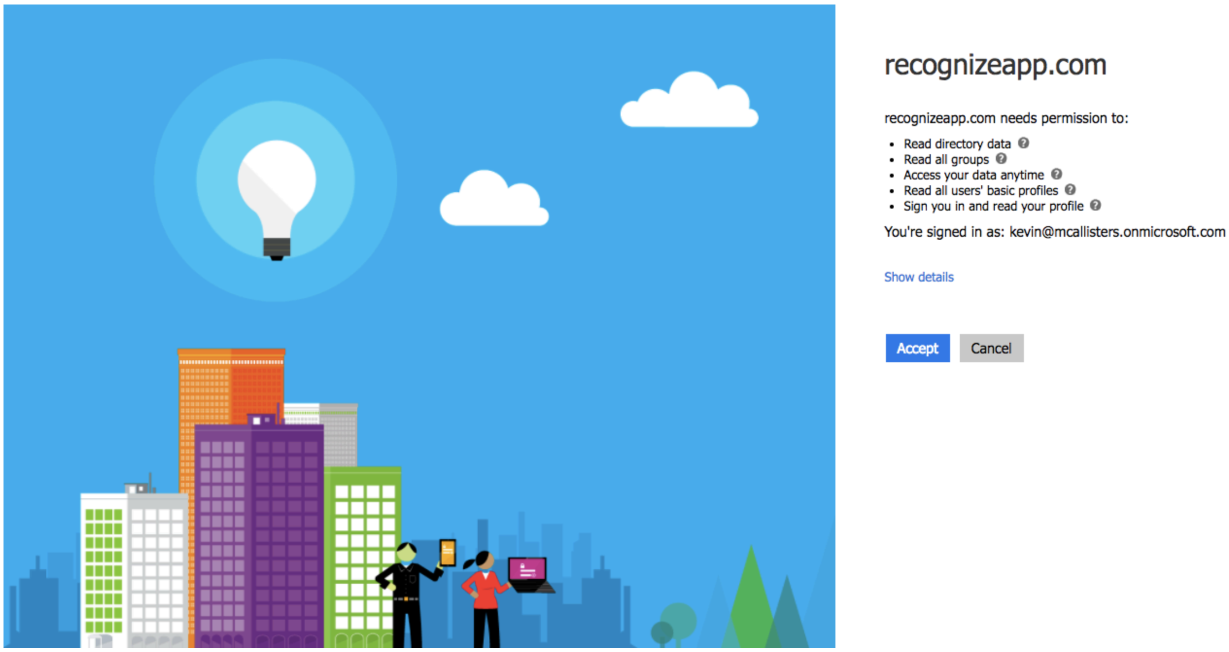
NOTE: It is a common practice to set up a Service Account to perform this step.



Select which account you would like to authenticate as.

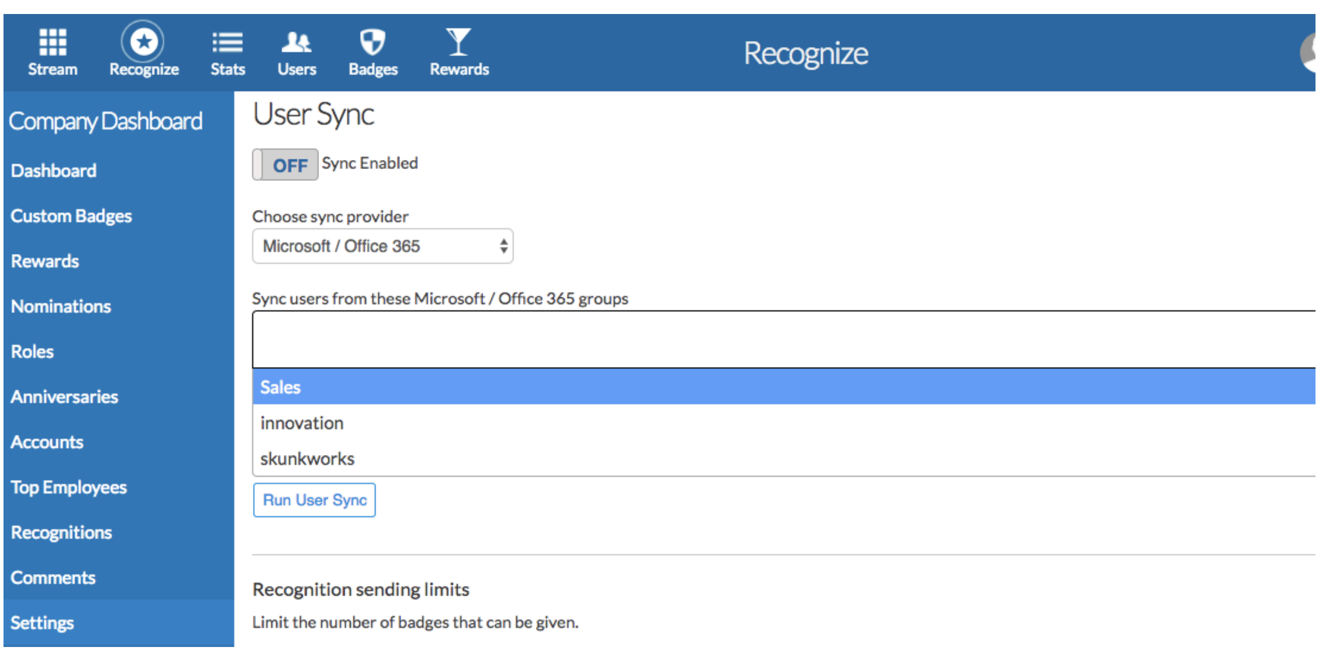


Allow permission for Recognize to access your Microsoft cloud account.



After authenticating, return to the company admin > settings > user sync section.

If you would like to **sync your entire organization, leave the groups section blank**. Otherwise, specify a group or groups that you would like to sync.

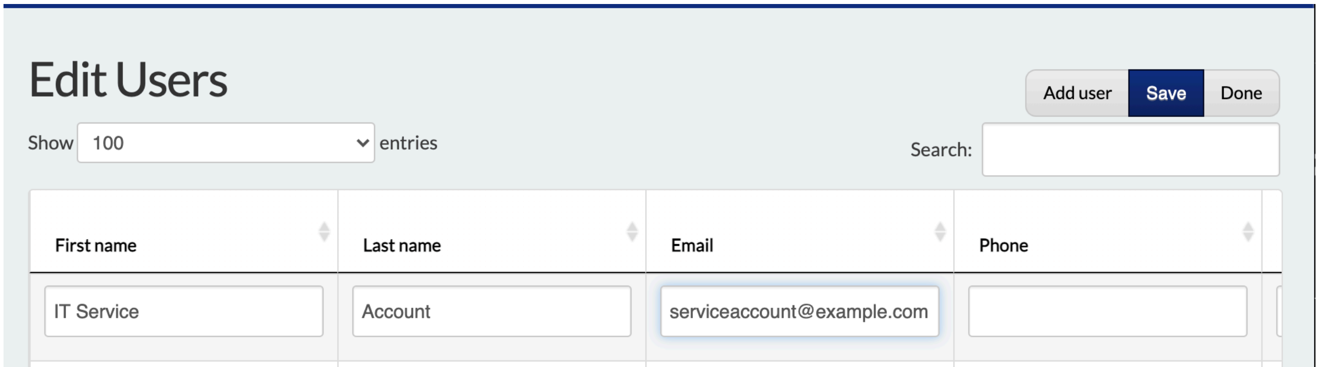


Configure whether you would like to mirror Microsoft groups to Recognize teams. The sync will proceed that night or if you want to expedite things, click "Run user sync" and the sync will be added to our background task server.

NOTE: *Currently there is no notification when the sync has completed, you will just need to check back. If you need help or confirmation the sync has completed, please email support@recognizeapp.com*

Additional Information

- At this time, selective choosing of which data to sync is not possible. We sync all the data specified in the Data section depending on availability from the identity provider.
- If you do not want to or cannot sync your user directory, we support "just-in-time" user provisioning. This is where we create accounts and permit access to Recognize when a user logs in via OAuth or SAML. Please see our SAML documentation available at https://recognizeapp.com/resources

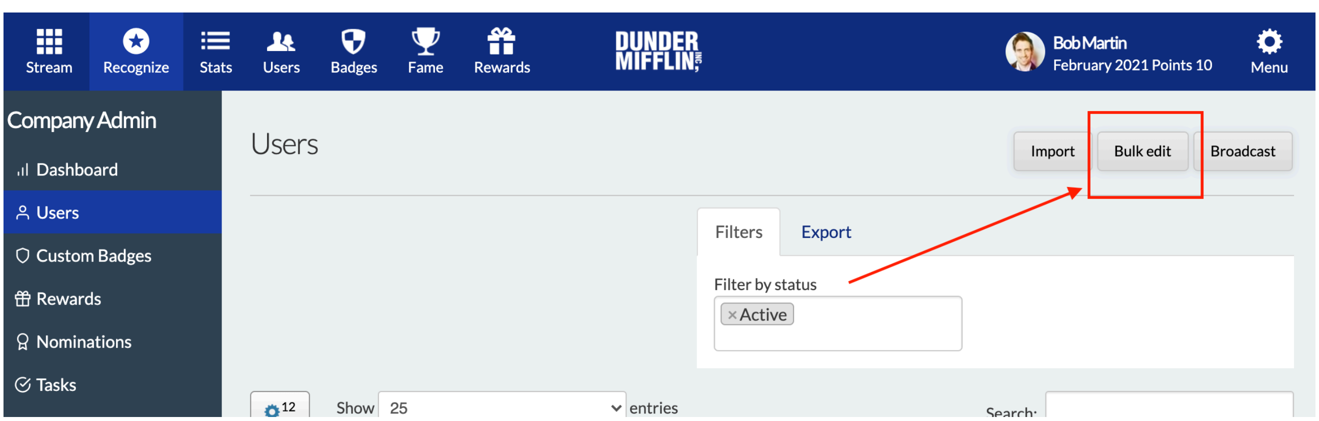


Appendix A - Service Accounts

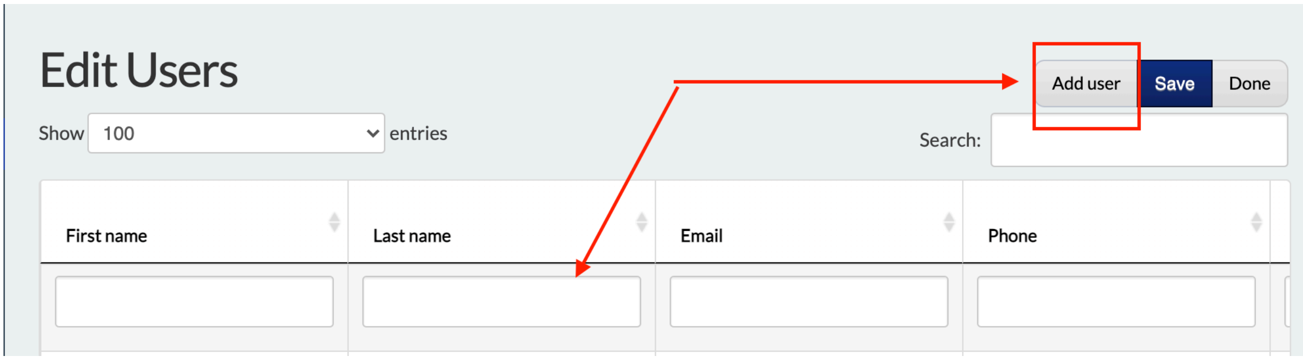
It is a common practice to use service accounts to create the authentication connection. This allows the connection to not be dependent on an individual user. Creating a service account on the sync provider side is out of scope of this document. However, here are some tips to set up a service account in Recognize.

Step 1 - Add user to Recognize

- Visit Company Admin > Users > Bulk Edit

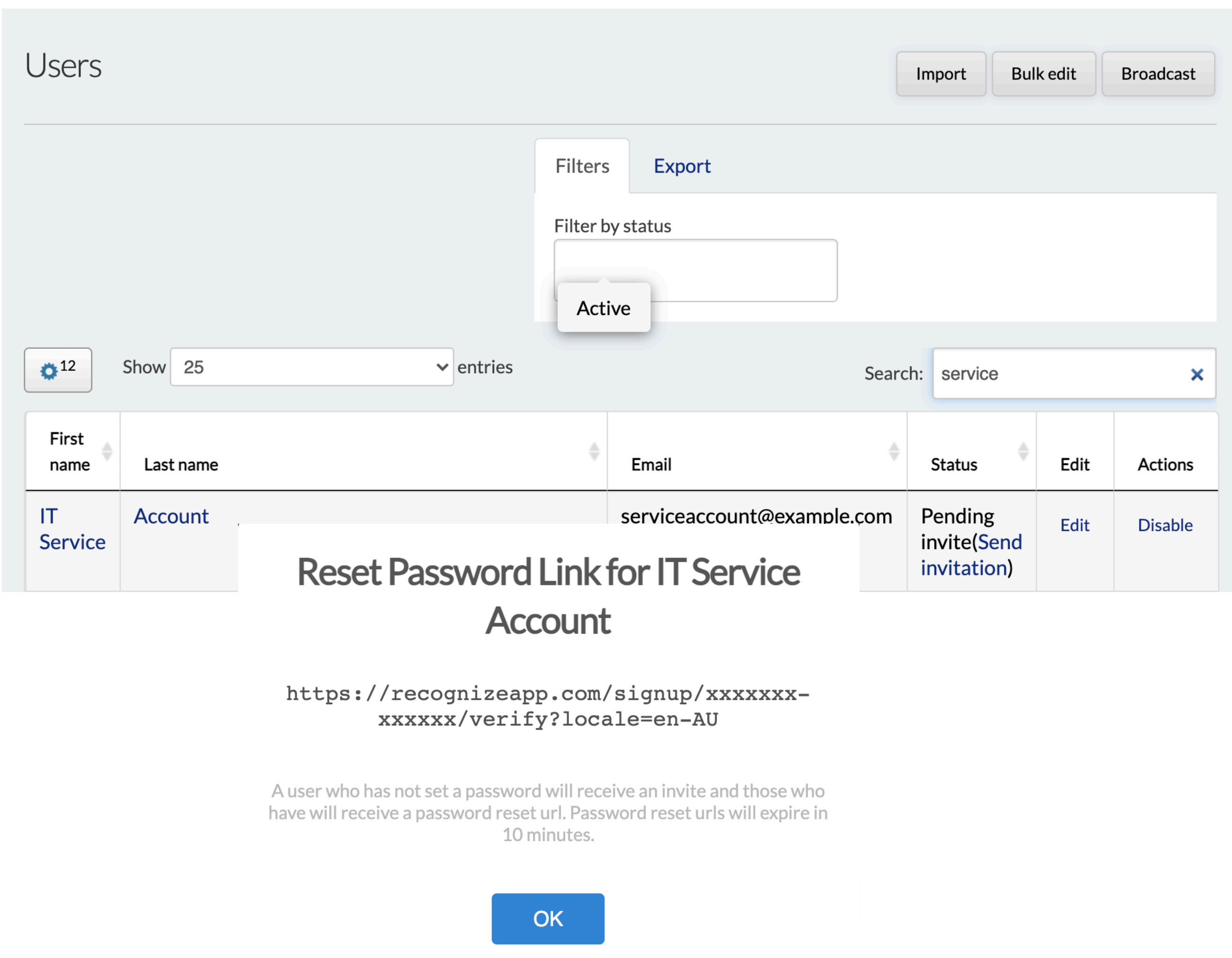


- Click Add User to add a row

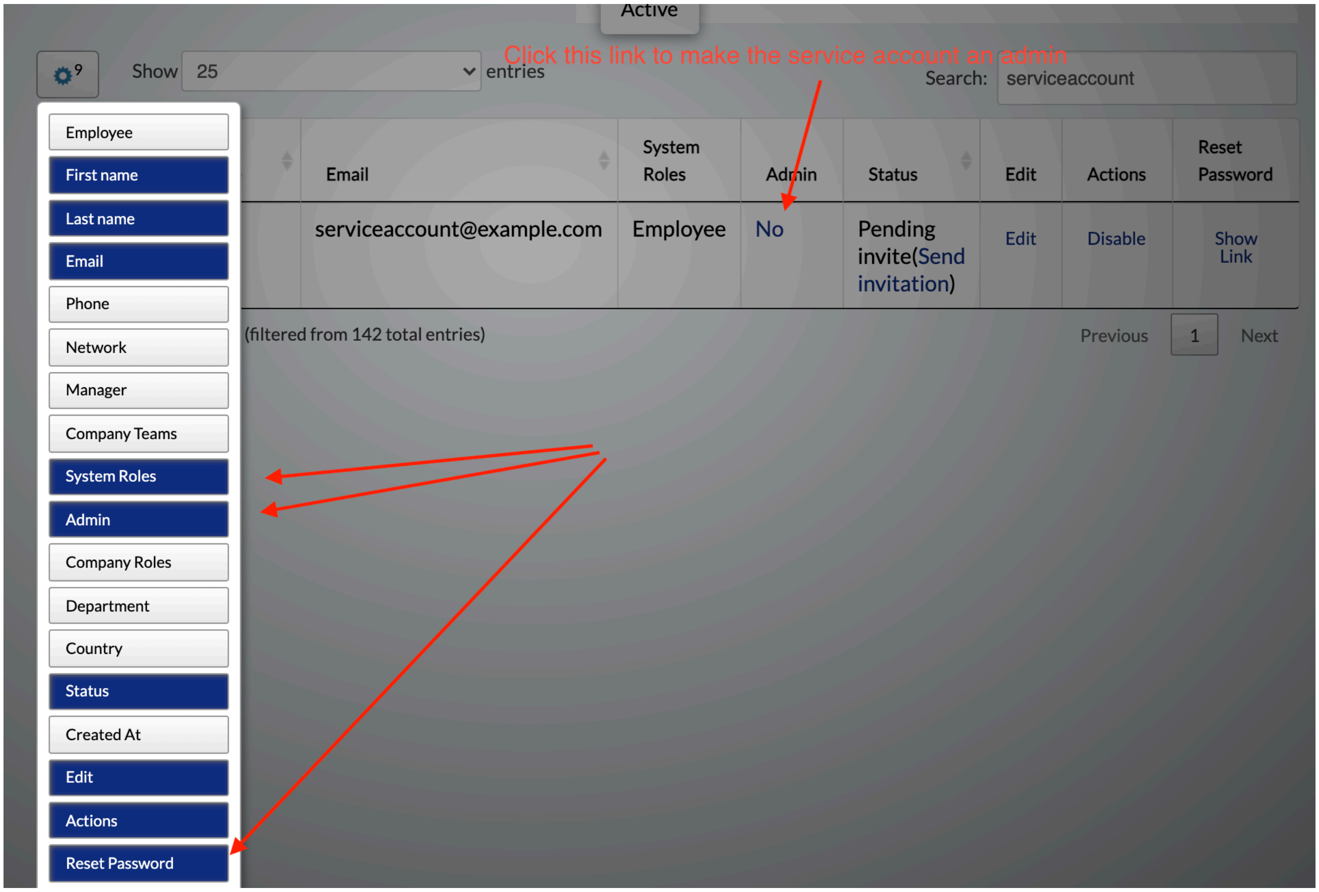


- Enter service account information and click Save and then Done

- Back on the Users page, remove the "Active" filter and search for your service account



- Click on the gear icon at the top left of the table (not the top right of the page) to show more columns, and select the Reset Password column.



- Click "Show Link" next in the row for the corresponding service account user. This will give you a link to set a password and log in as the Recognize service user account.

- Do not visit this link in your current browser session! Either log out or visit this url in a private / incognito browser session. Once you set a password, you can log in and go through the consent flow described in this document.
- Once you have completed the authentication, you can safely disable the service account from future logins. Even though the service account is disabled (from login), the sync will still use it to keep users up to date. You can always re-enable it from another admin account if you need to re-establish the connection.

First name	Last name	Email	System Roles	Admin	Status	Edit	Actions	Reset Password
IT Service	Account	serviceaccount@example.com	Employee	No	Active	Edit	Disable	Show Link Reset Password

Showing 1 to 1 of 1 entries (filtered from 142 total entries) Previous 1 Next

Contact support@recognizeapp.com if you have any questions.