okta

Office 365 Deployment Guide

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

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

Version History

Date	Document Version
September 2013	1.0
June 2014	2.0
January 2015	3.0
October 2015	4.0
December 2015	5.0
March 2016	6.0
May 2016	7.0

Table of Contents

Overview

About this Guide

This Deployment Guide contains a significant amount of information due to the complexity often involved in migrating from existing on-premises Office services (Exchange, SharePoint, Skype for Business) to the new Microsoft Office 365 cloud platform. We suggest you first scan through the document to understand the overall tasks, then read in detail the areas that apply to your deployment.

Throughout this guide we have added warning messages where we recommend that you contact Okta Professional Services for assistance before continuing. For example:

⚠ We strongly recommend that you contact Okta Professional Services before you continue with this step.

Microsoft Office 365 Overview

Office 365 (O365) is Microsoft’s cloud offering targeted at organizations using services such as Office, Skype for Business, Yammer, Exchange, and SharePoint. O365 aims to reduce the on-premises footprint previously required to run these services, as such Microsoft is recreating these services in the cloud building upon Azure services including Azure Active Directory (AAD), a cloud-based user and group directory that provides authentication, and user/group/device management services for Office 365.

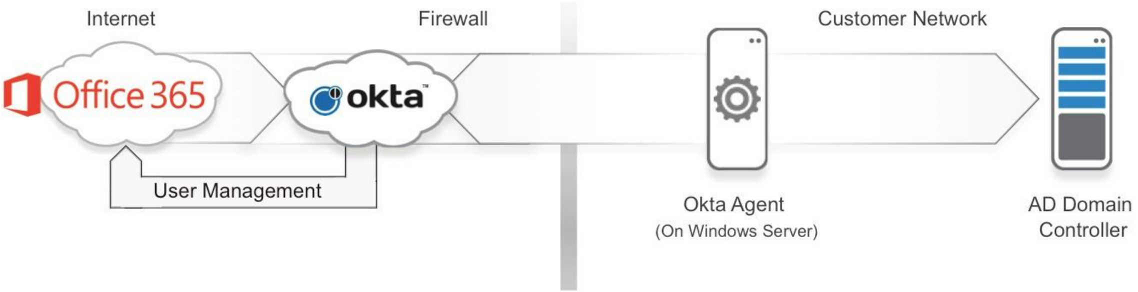
For end users, sending email, creating documents, and chatting with co-workers in Office 365 is almost identical to using the same services in your on-premises data center. The difference in Office 365 is that the need for IT to manage a large farm of servers for Exchange, Skype for Business, and SharePoint is eliminated. Traditional applications such as Word and Excel are also being rewritten to run entirely in your browser using Azure cloud.

Deploying Office 365 using Microsoft

When deploying Office 365 with the tools provided by Microsoft, you can end up deploying and managing additional servers and resources in your data center. For identity federation, Microsoft provides Active Directory Federation Services (ADFS) and for Active Directory synchronization, DirSync/Azure AD Connect (AADConnect). Both of these tools require dedicated servers, network infrastructure and skills to manage and maintain. Using these tools can also result in splitting your configuration between cloud and on-premises, with different interfaces, settings and management experiences. While Office 365 is a modern cloud productivity suite, the on-premises Microsoft components required to operate it are not.

Deploying Office 365 using Okta

Okta was designed to minimize the on-premises footprint while maximizing the advantages of cloud infrastructure. Utilizing Okta for Office 365 has allowed organizations around the world to solve complex deployments that would take months with legacy Microsoft technology. In many cases, Okta can replace ADFS and Azure AD Connect (formerly DirSync) for directory synchronization. It achieves this using a lightweight agent that can be installed on existing Windows servers in your domain. This same agent is used for synchronizing data from AD to Office 365 as well as delegating authentication back to AD as part of a federated single sign-on. Okta's directory integration agents can also read and write user and group data from AD and other LDAP servers.



For more information on AD integration with Okta, see Extend Active Directory & LDAP to the Cloud from the Okta website. Okta's Integration for Office 365 offers:

- **Certification by Microsoft** – Okta is certified by Microsoft within the Azure AD Federation Compatability List. This support applies to users both inside and outside corporate domains and is applicable to external devices.
- **Reduced infrastructure for IT administrators** – No dedicated servers are required for federation.
- **Desktop SSO** – Okta leverages Microsoft's Integrated Windows Authentication (IWA) to seamlessly authenticate users to Okta who are already authenticated within their Windows domain.

- **Active Directory integration –**The Okta AD and IWA agents eliminate the need for complicated hardware load balancers or availability solutions. Simply install multiple Okta agents for a service that is always active and integrates seamlessly with Office 365.

- **Delegated authentication to Active Directory –** Okta can delegate authentication to your AD domain controllers from Office 365 or any other cloud based application.

- **Multi-Factor Authentication (MFA) –** Okta's built-in MFA solutions boost authentication security and access to Office 365 giving you a wide range of ways to increase the security of access to Office 365.

- **Web-based password reset for AD –** Okta allows users to reset their own passwords through the web-based Okta cloud service. This reset seamlessly updates their account in AD.

- **End-to-end automation for user account management –** Add a new employee in AD and within minutes they are fully enabled to access Office 365 from both the web, desktop and mobile devices.

Before You Begin

Supported Architectures for Deployment of Updated Okta Provisioning

Before you begin the integration between Okta and Office 365, be aware of the following prerequisites:

Requirements	Description
Administrative access to an Office 365 subscription	Note that some Office 365 licenses don't allow for federation or directory synchronization. Refer to your Microsoft support contact for more clarification.
Administrative access to an Okta organization	Administrative access to an Okta subscription.
A DNS domain registered with Office 365	Your own DNS domain to register in Office 365, and federate back to Okta. By default, Office 365 offers a domain in the form yourname.onmicrosoft.com and this cannot be used for federation (this will be the O365 default domain in many cases).
Access to a domain that is joined to a Windows server*	At least one Okta AD agent installed in your environment. You need to have access to a domain-joined server with visibility to all domains in the forest being used with Office 365. While not best practice, you can install the agent on domain controllers.
Rights to create a service account for the Okta agent in your AD domain*	A service account in your Active Directory user domain for the Okta agent. Note this account can be a regular domain user with read-only rights. Admin-level privileges are required to install the agent and the account can be created during the installation. For complete details on installing the Okta agent, see Installing and Configuring the AD Agent on the Okta support website.
Outbound connectivity to Okta from a server joined to your domain*	Your Okta agent communicating with your Okta subscription. I.e., the server(s) where the agent(s) reside must connect to https://yourname.okta.com.
For Desktop SSO: A Windows server running IIS 7/7.5*	At least one IIS installed Windows server, within the authenticated domain, for Desktop SSO. For details, see Configuring Desktop SSO on the Okta support website.
The correct domain suffix and resulting UPNs for users set up in AD*	Understand how accounts are created in Office 365 and the changes required for existing AD user accounts prior to migration. For complete instructions on this topic, see Preparing user accounts prior to Office 365 & Okta integration on the Okta support website.
The most up-to-date versions of all your Microsoft systems	Ensure that all recent updates to Microsoft operating systems and other software (AADConnect, FIM\MIM, etc.) are applied.

* Note: There is no requirement to integrate Office 365 with Active Directory or an existing Windows Domain. Users for Office 365 can be sourced from Okta directly or any other supported application and service. To learn more about specific integrations, please review the Okta Help Center.

Designing the Deployment

Okta’s Office 365 integration provides several key capabilities:

- Provide Single Sign-On by means of Federation using WS-Federation and WS-Trust to web clients, rich clients and email-rich clients in a manner fully supported by Microsoft

- Provisioning user and group data from Active Directory to Office 365 and assigning licenses

- Deploy ActiveSync (EAS) profiles and Applications to end-user’s mobile devices, including ongoing management of EAS credentials

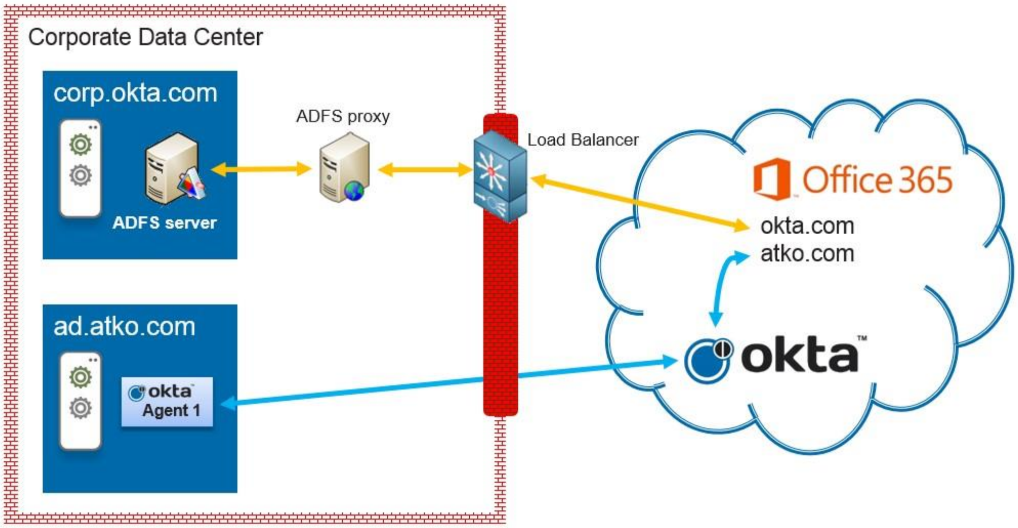
- Enable Multi-Factor Authentication for Web Clients and supporting desktop applications

Okta’s provisioning functionality has a number of key capabilities that are detailed below. In cases where you have moved completely to Exchange Online, Okta can perform full synchronization of objects and attributes between AD and Office 365, without the need for any additional deployments such as AADConnect. In circumstances where Exchange is currently, or expected to be deployed in a Hybrid Configuration with Exchange Online, it is recommended to deploy Microsoft synchronization technologies to synchronize data into Office 365 and leverage Okta to perform granular role and license management. It is important therefore to understand how Okta can work alongside Microsoft solutions.

Federation

Large-scale organizations often have complex infrastructure, with differing technology needs and perspectives. For this reason, you may find that Okta is deployed alongside various federation technologies such as Microsoft ADFS, Ping or Oracle Identity Federation (OIF).

Okta's lightweight agent architecture allows it to reside in the same environments as other federation technologies. In Office 365, it is possible to have several domains, each one can be associated with a different identity provider. In the following diagram you can see how ADFS handles federation of accounts for okta.com while Okta is managing federation of accounts for atko.com. Both domains are in the same Office 365 tenant. Note that Okta is a much more efficient solution to ADFS and requires significantly less infrastructure. Most Okta customers use Okta for authentication of all domains in Office 365.



<span>Note:</span> If you have an existing SSO solution for Office 365, and are planning to move to Okta for SSO, be sure to document any customized settings in your configuration. Examples of such configurations could be utilizing an attribute for username that is non-default (User Principal Name is the default value here, however common other settings are Email or EmployeeID). These settings will need to be reconfigured in Okta when configuring Single Sign-On.

Directory synchronization

Large organizations can have a complex mix of identity related technologies. Often you will see multiple Active Directory forests and more than one identity management solution running between them and other directories and applications. Okta's lightweight presence in the data center allows it to be deployed alongside existing identity management solutions.

It is important to note that if another technology is performing the synchronization of accounts to Office 365, and Okta is handling the federation for authentication, you need to ensure the Okta account usernames match the Office 365 usernames. This can easily be configured in Okta using Universal Directory attribute expression, this is described later in this document.

During migration to Office 365, some organizations find the need to instantiate an Exchange Hybrid configuration. in doing so, it is likely that you have one of Microsoft's technologies performing part of the directory synchronization, DirSync, AADConnect or Forefront Identity Manager (FIM). Whilst in these Hybrid deployments, Okta cannot replace the need for these tools and instead can be used directly alongside for single sign-on and role and license management.

Note: If you are currently using AADConnect or another synchronization solution and plan to move to Okta Provisioning, be sure to document any customized settings in your configuration. Examples of such configurations could be utilizing an attribute for username that is non-default (User Principal Name is the default value here, however common other settings are Email or EmployeeID). As well as the attribute for sourceAnchor (also known as ImmutableID). It is recommended to discuss with Okta Professional Services prior to making such changes.

Universal Directory and Office 365

Advantage of using Okta with Office 365, include rapidly accelerated deployment times without the need to deploy complex on-premises services and increase the overall infrastructure footprint.The ability for Okta to do this is provided by our powerful cloud directory called Universal Directory. Universal Directory can be described as a rich Metaverse in the cloud, it enables you to:

- Synchronize a wide range of attributes from Active Directory into Okta for use in Office 365
- Provision users with extensible and customizable attributes into Office 365
- Perform transformations of user attribute data from AD to Okta and also from Okta to Office 365, as well as back again

Universal Directory with Office 365 provides you full control over username transformation, email address formatting (per domain or even per-user). This document describes the areas where you can use Universal Directory, but for a full understanding of its capabilities, refer to the Universal Directory Product Documentation.

Multiple Office 365 Domains or Tenants

It is common for customers to have multiple DNS domains configured for Office 365.

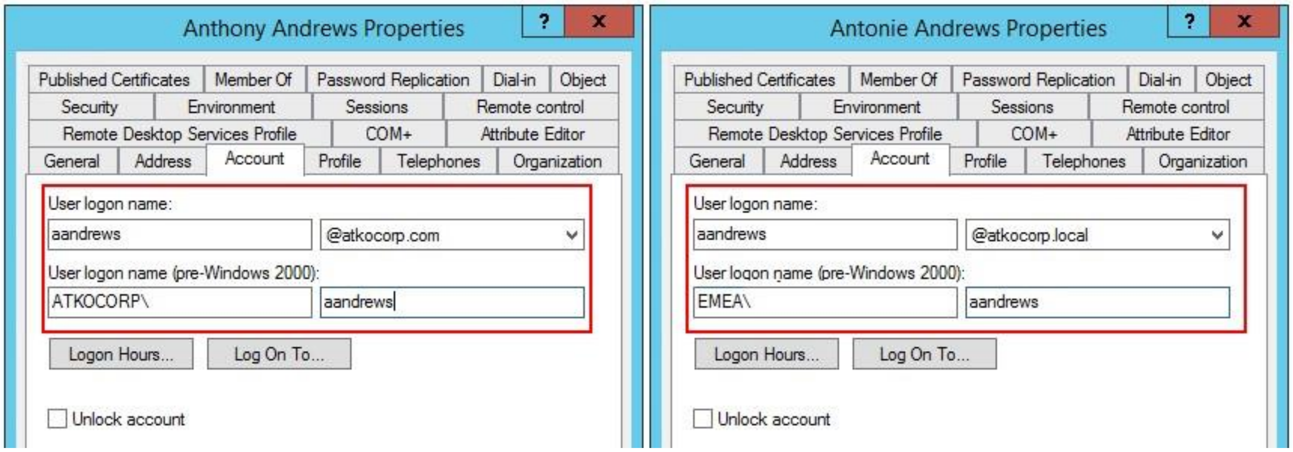
You can do this by having either:

- A single Office 365 tenant with multiple DNS domains
- Several separate Office 365 tenants, each with one or more DNS domains.

Both of these scenarios are supported by Okta and are easy to configure. If you are going to have multiple DNS domains within a single Office 365 tenant, see Using multiple federated domains in Office 365 with Okta from the Okta Community.

Active Directory Domains and Forests

Okta works well with multiple Active Directory domains and forests. However, it is important to note that Active Directory is a hierarchical system with forests, domains and organizational units. It is possible to have identical usernames, but using separate domains avoids a conflict. However, when you synchronize this data into both Okta and Office 365, the name spaces of these systems is flattened. The diagram below shows how a user with the same logon name can exist in Active Directory due to the scope of the domain and the UPN. In Okta you can use custom expressions to create Okta users from AD users, but ensure that you use enough data from the user objects to maintain uniqueness. So if you are going to use a custom mapping for the creation of the Okta username, be aware of the possibility of clashes in usernames of the same name.



Anthony Andrews Properties

User logon name: aandrews @atkocorp.com

User logon name (pre-Windows 2000): ATKOCORP\ aandrews

□ Unlock account

Antonie Andrews Properties

User logon name: aandrews @atkocorp.local

User logon name (pre-Windows 2000): EMEA\ aandrews

□ Unlock account

Multiple Okta AD agents

An important design feature of the Okta architecture are the lightweight agents that communicate with Active Directory. These Windows services maintain an active connection back to the Okta cloud service and all Okta agents are continuously active. This means that you don't need to implement any extra high availability or redundancy solution with Okta. However, we do recommend that you install at least 2 agents. The more agents you install, the more resilient and performant your deployment will be. When you work with Okta we guide you through your deployment, ensuring your connectivity to AD is as scalable and available as possible.

Deploying Okta with Office 365

To configure Okta with Office 365

- Import users from your existing Active Directory into Okta [**Optional**]
- Configure Okta for single sign on (SSO) with Office 365
- Configure Okta to automatically provision users and groups to Office 365 [**Optional**]
- Configure increased security for accessing Office 365 [**Optional**]
- Configure Okta to manage Licenses in O365. [**Optional**]

Note that importing users from your AD environment is optional, but common. You can create users directly in Okta, and then provision them to Office 365. In rare instances, you could create users in Okta, manually create users in Office 365 and use our Secure

Web Authentication (SWA) for SSO. The most common use case is to import users into Okta using the Okta AD agent and then use Okta's federation to Office 365. More information on SWA can be found here,

https://support.okta.com/articles/Knowledge_Article/28328856-Overview-of-ManagingApps-and-SSO

Importing Users to Okta

The most common use case to get user information into Okta is to leverage a directory that contains existing user and group information. Okta supports two main technologies for on-premises user directories:

- Microsoft Active Directory
- LDAP (Sun ONE, Sun DSEE [Now Oracle Directory Server], OID, Upend, OpenLDAP, and AD LDS)

While it is possible to use accounts from an LDAP server for migration to Office 365, Active Directory is by far the most common method of integration. Okta can also perform delegated authentication for LDAP as well as Active Directory (described later in this document).

Due to the pervasiveness of Active Directory, this guide focuses on installing the Okta agents for Active Directory. For information on deploying the LDAP agents (Windows and Linux versions) see the LDAP Agent Deployment Guide:

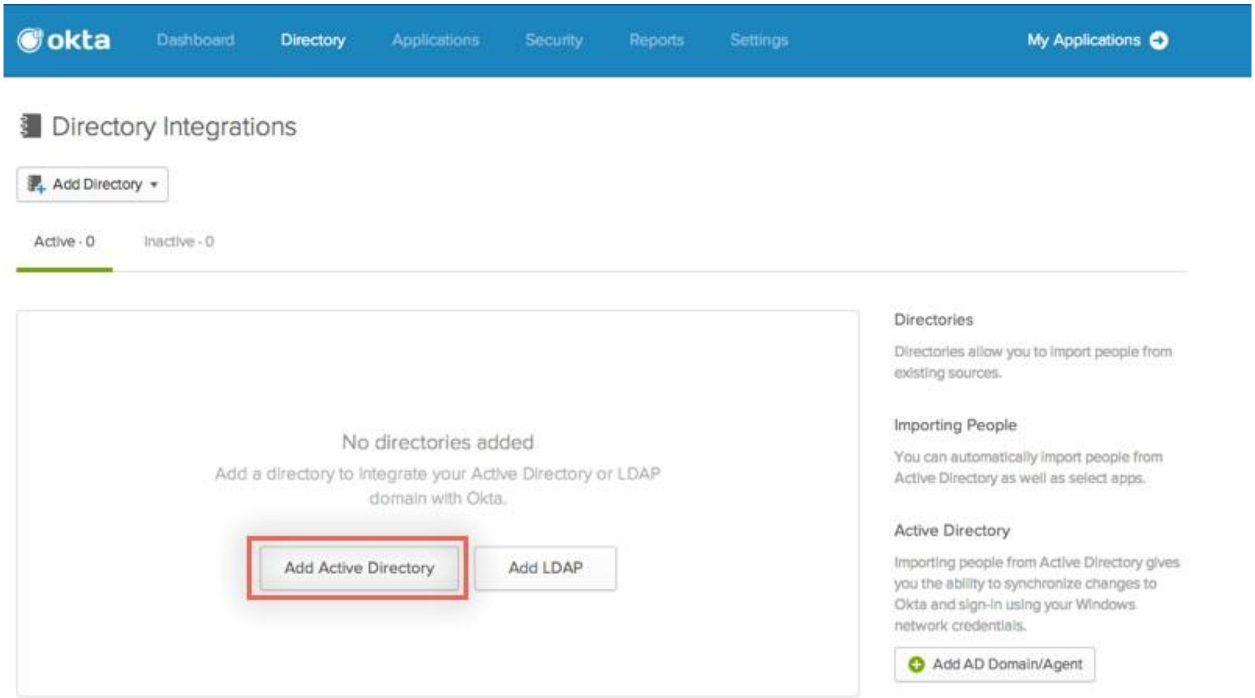
Okta also has a technology called *Okta On-premises Provisioning* that allows for Okta to be connected to ANY data source. This can also be used to bring user information into Okta, but the topic is beyond the scope of this document. For more information on On Premises Provisioning see the OPP Deployment Guide:

Configuring the First Okta AD Agent

1. Login to the Windows Server on which you wish to run the agent. Ensure that you login with domain administrative permissions. Note this server needs to be a member server of the

domain from where you are going to synchronize users. It can be a domain controller if you wish, but this is not a requirement.

2. Open a browser and login to your Okta org. Navigate to **Directories > Directory Integrations**. Click the **Add Directory** button:



Directory Integrations

No directories added

Add a directory to integrate your Active Directory or LDAP domain with Okta.

Directories

Directories allow you to import people from existing sources.

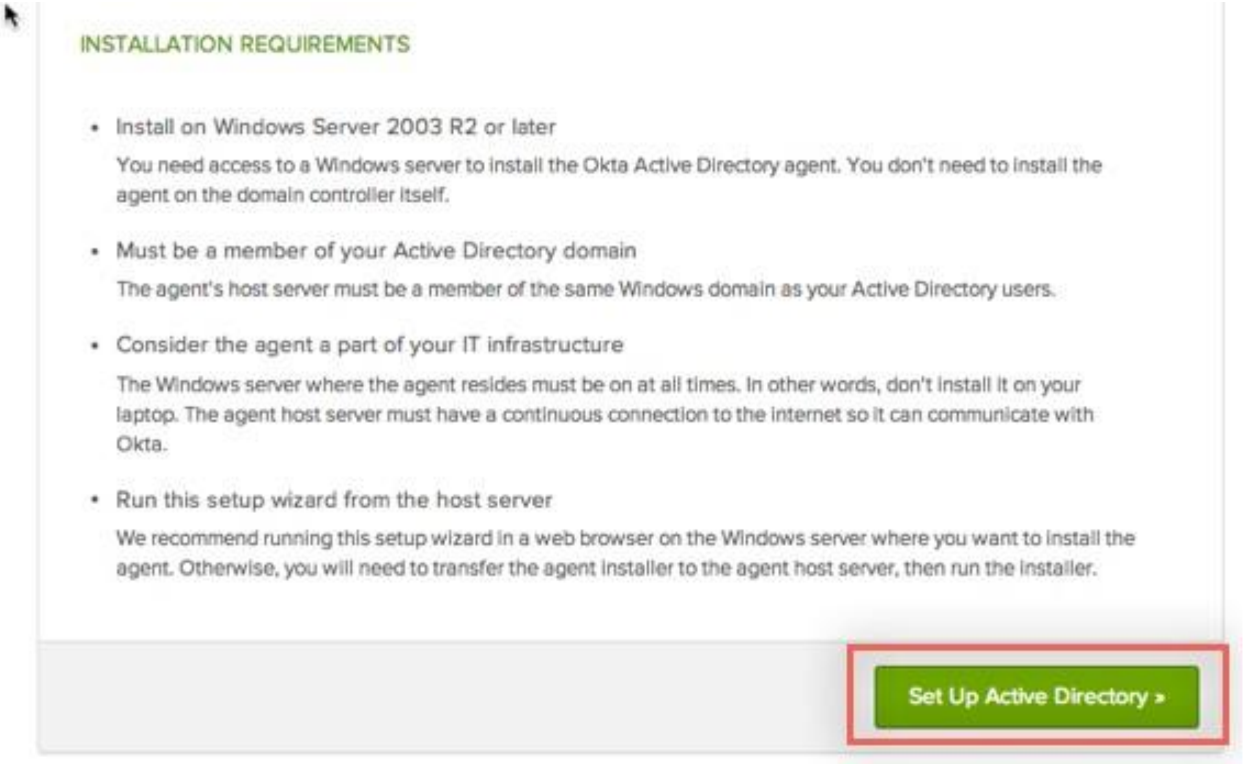
Importing People

You can automatically import people from Active Directory as well as select apps.

Active Directory

Importing people from Active Directory gives you the ability to synchronize changes to Okta and sign-in using your Windows network credentials.

3. On the next page, scroll down to the bottom of the page and click the **Setup Up Active Directory** button.



INSTALLATION REQUIREMENTS

- Install on Windows Server 2003 R2 or later

  You need access to a Windows server to install the Okta Active Directory agent. You don't need to install the agent on the domain controller itself.

- Must be a member of your Active Directory domain

  The agent's host server must be a member of the same Windows domain as your Active Directory users.

- Consider the agent a part of your IT infrastructure

  The Windows server where the agent resides must be on at all times. In other words, don't install it on your laptop. The agent host server must have a continuous connection to the internet so it can communicate with Okta.

- Run this setup wizard from the host server

  We recommend running this setup wizard in a web browser on the Windows server where you want to install the agent. Otherwise, you will need to transfer the agent installer to the agent host server, then run the installer.

4. Select the **Download Agent** button, save the AD agent installer to the local machine then run the installer as an administrator.

Note that the Okta page in the background change and has the notice “waiting for the agent installer to update this page…”. Don’t worry if this window is closed accidentally, the Okta instance will still be waiting for the agent to connect.

5. Click **Next** on the Okta AD Agent install dialog until you get to the **Select AD Domain** dialog, confirm that it has detected the right domain to import users from. Click **Next** to continue. If you are installing in a forest with more than one domain, you can add more after the install process has completed.

6. On the service account page, you can either allow the installer to create the account or you can choose an existing one. If you allow the installer to create the account, the password is set on the following dialog box.

7. If you require a proxy server to connect the agent back to the Okta cloud service, enter the details on the proxy dialog, otherwise continue.

8. The final screen, **Register Okta AD Agent**, needs the information that is displayed on the Okta page from which you downloaded the agent. Cut and paste the Organization URL and Okta administrator details and provide the password for the admin account. Note that it is good practice to create a separate administrative user account for the agent to connect back to Okta. Clicking **Next** connects the agent to Okta and completes the installation.

9. If the browser window is still open, you will see a **Next** button, which takes you to a settings screen. Note that you may experience a timeout if it took a long time to install the agent. If so, continue by clicking the retry at the bottom of the screen.

   Notes:

   It is good practice to set **Automatically import from AD** to **Never** when you first set up the agent. This allows you to verify the import of users and setup of the agent. You can change this setting later on when you are confident everything works correctly.

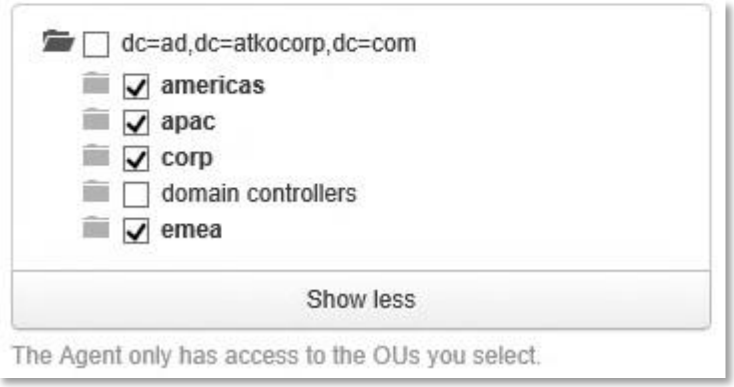
   You can specify which attribute on the Active Directory user will be used for creating the account in Okta (Okta username preference) but the most common practice is to leave the default set to User Principal Name (UPN).

   Next **Build User Profile**. Here Okta selects a set of default attributes that are updated during import of users from AD. During this step you can add more attributes to Okta that you wish to use in Office 365. Note that by default Okta does not select “facsimileTelephoneNumber” or “co” attributes and often you will want this data in Office 365. So enter these into the search box and to add them to your profile for the AD user. But if you are using Okta provisioning for O365, Okta will automatically update the attributes when you select the Okta DirSync provisjoning in O365 App.

10. After clicking **Next**, you may be asked if you want to import users from All OUs. This imports every user in the domain for which the agent was configured. If you have a large number of users and want to finish the configuration first, answer **No**. Note that you can filter by OU (described next) to fine tune the users you want to import.

The agent is now configured. If you selected **No** in step 10 above, no user data has actually been read into Okta. Group information however is automatically imported at the time of configuring the agent. If you navigate to the **Groups** tab in the **People** section, you can see all the groups imported by the agent. It's not important if you have imported groups you don't wish to reside in Okta. If you limit the scope of the OUs to be imported, the groups will be automatically updated to reflect this.

Now you need to review what organization units you want to import. Return to the directory configuration page by navigating to **Directories > Directory Integrations**.



☐ dc=ad,dc=atkocorp,dc=com
☑ americas
☑ apac
☑ corp
☐ domain controllers
☑ emea

The Agent only has access to the OUs you select.

There should be just one Active Directory listed, select this and switch to the settings page. If you wish to limit the scope of the agent to a range of OUs, deselect the root and choose which OUs.

***Note**: There are some built-in nodes that are not OUs, they are not listed when you attempt to filter the list. These containers are imported if you select the root, but because they are not OUs, they are not visible for filtering.*

Delegated Authentication

A useful feature of Okta and its lightweight on-premises architecture is delegated authentication (DelAuth). This means that when you login to Okta, either directly into the Okta portal or from the Office 365 website, the authentication can be taken right to the directory where the user account was imported from.

In most cases, this is Active Directory, but could also be an LDAP service. DelAuth allows Okta to log users into Office 365 using their current Active Directory credentials and means Okta doesn’t need to sync and maintain any passwords in the cloud. After installing the Okta AD Agent, delegated authentication is enabled by default.

Universal Directory – Mapping and Transforming Data from AD to Okta

We strongly recommend that you contact Okta Professional Services before you continue with this step.

Before you import users from AD to Okta, review what information you want to transform and map. First it is worth understanding how information for users gets from AD to Okta to Office 365. There are two ways:

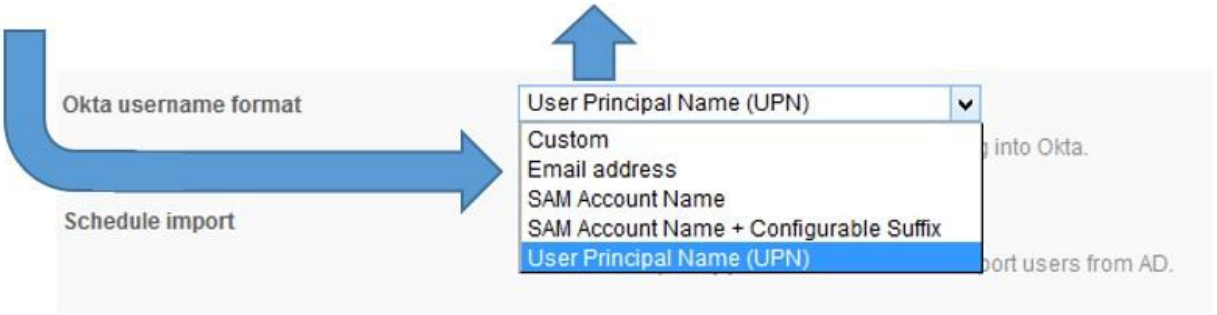
- **AD -> Okta -> O365**. Attributes such as username, email address, first name, last name and display name are usually pieces of information you want in Okta for use in other applications you connect to, not just Office 365. In this instance, you want to map these attributes from AD to Okta. Then when you provision a user in Office 365, you use the value from the Okta user's profile.

- **AD -> O365**. Okta can import over 100 attributes from AD into Okta. But that doesn't mean all of those attributes need to be associated and the data copied to the Okta user. Some attributes are very specific to Office 365 migrations from Exchange on premises, like "proxyAddresses". In another example, you might want to copy the "Department" attribute from AD to Office 365, but have no need for it in Okta.

Before moving onto the next section about importing users, verify you have selected the attributes from AD that you are interested in. Note that Okta automates most of the popular mappings for the basic profile. So you only need to review if you have something specific you need. Also, you can easily add new attributes at a later date and map those. Okta will automatically update all the users and get the new data.

There is one use case for Office 365 that requires special attention. That is the username you are going to use for the Okta user and also the Office 365 user. In a simple environment, you have an Active Directory with a username format of user@company.com, where company.com is a public routable DNS domain, meaning it is possible to send email to that address. If you are also going to use Office 365 with the same domain, then configuration with Okta is simple. Use the Active Directory username format (UPN) for the Okta user and then create Office 365 users using the same format, as shown here:

Active Directory Username	Okta Username	Office 365 Username
bill.jones@redskycorp.com	bill.jones@redskycorp.com	bill.jones@redskycorp.com


Okta username format: User Principal Name (UPN)

However things are not always this simple. Many Active Directory environments use a username suffix (that is the domain piece after the @ symbol) that isn't a valid publically resolvable domain. This can be due to many reasons; one being that the Small

Business Server (SBS) installation from Microsoft used the domain format

"*yourcompany.*local" during installation. Your users may be familiar with their username and you may not wish to change their behavior or force them to start using a new format. There are other reasons why you might want to continue with using this format in your Active Directory, other applications may be configured to use it. However you cannot use a non-public DNS domain in Office 365. All users in Office 365 that are to be federated to Okta, must be created in a DNS domain that is publically resolvable.

As many Office 365 deployments are about using email you need consider what the email address for the Office 365 user needs to be. In most cases email uses public DNS. Your local AD may or may not have this information already or the information may not reflect the email domains you wish to use in Office 365.

Due to these conflicting and complex requirements, you need flexibility in creating users in Office 365. Universal Directory in Okta provides you with many options. You can manipulate and change the username format or email address either:

- When users are imported into AD (*Preferred*)
- When they are provisioned to Office 365

In most cases it makes sense to create the user in Okta to match the domains in Office 365. But there may be reasons why you want the Okta user to have the same username as that in AD or that the email address can't be created at the time of import from AD. The most common scenario is that the username in AD doesn't match the domain in Office 365 and that the email address in AD is either wrong, incorrectly formatted, or missing. Therefore, what you want to achieve is the following:

Active Directory User	Okta User	Office 365 User
Username: bill@company.local Firstname: Bill Lastname: Jones Email: *<blank>*	Username: bill@company.com Firstname: Bill Lastname: Jones Email: bill.jones@product.com	Username: bill@company.com Firstname: Bill Lastname: Jones Email: bill.jones@product.com

The above table shows how the data has been correct at the time of import into Okta. To do this, you need to modify the UD attribute mappings for the AD import into Okta.

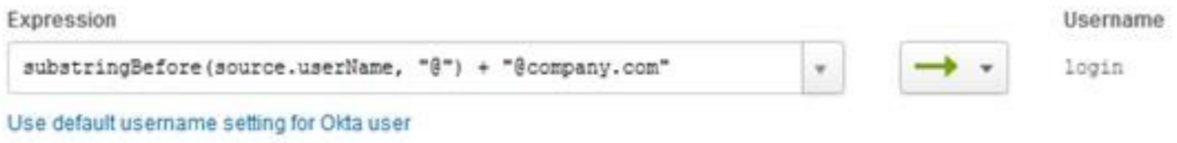
1. Login to your Okta org as an administrator and navigate to **Directories** > **Directory Integrations**, then select the Active Directory domain you've added.

2. Select the **Settings** and scroll to the bottom and click on the **Edit Mappings** button and then the **Map Attributes** button.

3. From here you can modify the mapping of AD attributes to Okta. In the table above we need to change the username from @company.local to

   @company.com but keep the same username prefix. Also we want to create an email address using the first name combined with the last name separated by a "." and on a specific domain. Below is an example of how this is done in UD.

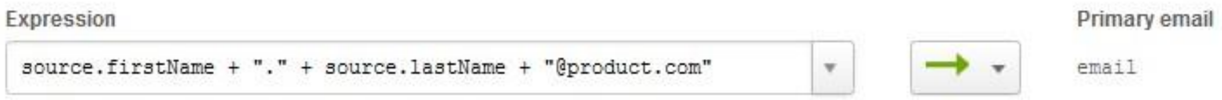
   (Note you need to click on the "**Override with mapping**" button on the **Username** field.)



Expression

```
substringBefore(source.userName, "@") + "@company.com"
```

Username: login



Expression

```
source.firstName + "." + source.lastName + "@product.com"
```

Primary email: email

What the above shows first is the hard coding of the domain "company.com" into the username that is created when users are imported from this AD domain into Okta. The second then shows the email being built from the AD firstname and lastname (separated by a period, ".") and then the email domain, different from the username domain, "product.com".

There is a lot more that can be done with Universal Directory and mapping / transformations. But the above is a common example for Office 365. For more details about the various possibilities, see the Okta Expression Language reference here, http://developer.okta.com/docs/getting_started/okta_expression_lang.html

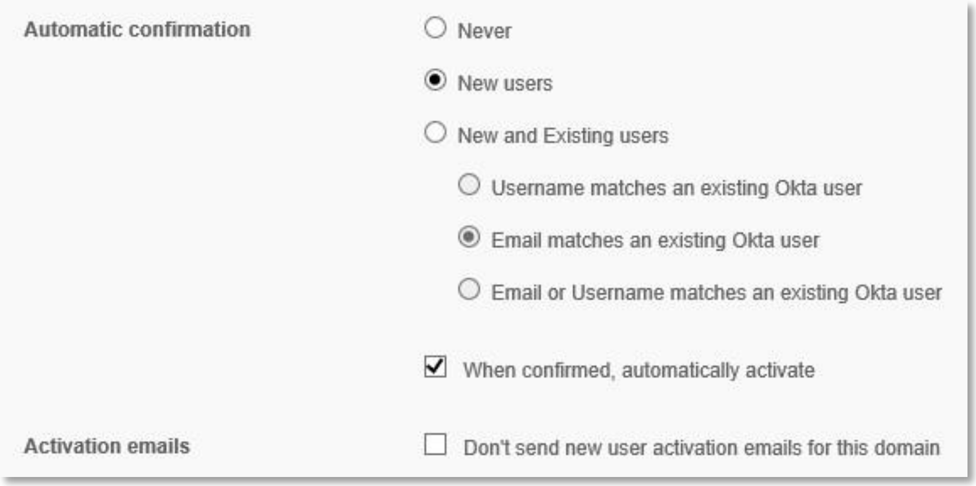
Importing users

Before importing users, it is worth reviewing the process of creating and importing users in Okta. The following table provides an overview of how users are created in Okta and the stages within their lifecycle.

Stage	Description
Create	The first step in the user life cycle is the creation of the user account. This can either be a directory (Active Directory), or a cloud service like Workday or Salesforce. Okta can also be the service where the user account is first created, in which case we skip the need to import.
Import	Once a user has been created in an external system, Okta needs to run an import. The import can either be manual or it can be setup to run on a scheduled basis. Some systems (such as Active Directory) can be configured to notify Okta of new users in real time. Depending on system, the imported user results in an Okta owned user (for example importing from Office 365) or it may result in the user being permanently tied to the source system, such as users from Active Directory.
Confirm	Once imported, a user needs to be confirmed before an Okta user is created / associated. Some systems such as Active Directory can automatically confirm users. If a user already exists, no Okta user profile is created, instead the source system user is mapped with the existing Okta profile. Once new user accounts are confirmed, they can be viewed in Okta by admins and assigned to accounts. But end users are unable to login until they are activated.
Activate	Users can only login to Okta with an active account. Some systems like Active Directory can automatically activate accounts on import, and therefore a new user account creation in AD can automatically result in an active user account in Okta. The process of activation also sends out an email to both the primary and secondary email addresses.
Assign	While an active user account can authenticate to Okta. They can’t access any applications until the user has been assigned. The assignment of users to applications can be done either directly or via group membership. Group membership is by far the preferred and most common method. Once a user has been assigned to an application, they are able to sign in.
Provision	Some application integrations in Okta support automated provisioning. This means at the time of assignment, Okta will create their user accounts for you. Some applications, like Office 365, Okta also automatically assigns the user license, therefore enabling a true end-to-end enabling of the user in the application.
Sign In	Once all the steps above have been completed, the end user can access the application. This could be done via the Okta end user homepage, or by attempting to sign in directly with the service or by using one of Okta’s mobile applications.
De-provision	If the application integration in Okta supports, it is possible to automatically deprovision user accounts. This happens when the user is un-assigned from the application in Okta. If you are using groups for the assignment, then a user being removed from a group will prevent them from accessing the application.

Now that the AD agent is installed, you can import users. By default, when users are imported from AD they are not automatically made active users in Okta. Users go through two phases before they can login to Okta. First they need to be confirmed. After which you can view them in Okta and assign them to applications. But before a user can actually login, they need to be activated, a process that also triggers an email to the email address specified in the imported account.

If you have a large number of users, a manual approach is not feasible. For this reason, once testing of the Office 365 implementation is complete, you can switch to automatic confirmation and creation of Okta users. Make this change from the **Settings** tab of the Active Directory domain in question. If you want Okta to automatically create and activate users, set the radio buttons and checkboxes as shown below. Note that if you already have a process in place to communicate the use of Okta to your users, you can also disable the sending of new user emails.



Automatic confirmation

○ Never

● New users

○ New and Existing users

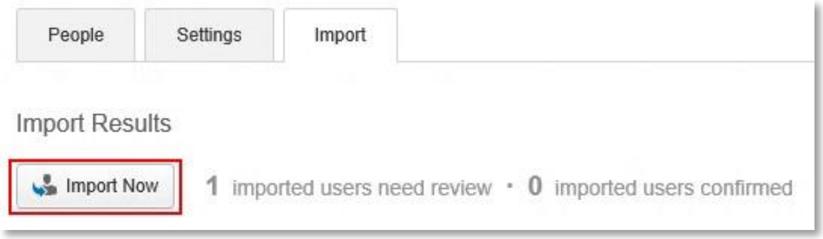
- ○ Username matches an existing Okta user
- ● Email matches an existing Okta user
- ○ Email or Username matches an existing Okta user

☑ When confirmed, automatically activate

Activation emails

□ Don't send new user activation emails for this domain

Once you've confirmed the settings, switch to the **Import** tab and press the **Import** button. You choose to perform a full or incremental import. Select **Incremental Import** and wait for it to complete.



1 imported users need review · 0 imported users confirmed

After the import a list of users appears in the results pane. If you are going to perform a manual Okta user creation, you can see users that have been imported displayed in the left hand column, on the right you can decide if an Okta user should be created. If you have elected for this to happen automatically, you will only see accounts in this list that require some sort of manual decision. Once you have users in Okta, you are now ready to configure SSO and Provisioning.

Understanding App Assignment

Before we go into the configuration of SSO and provisioning, it is worth understanding how Okta controls access to these applications. To be able to provision an account in Office 365 and provide SSO, you need both a user account in Okta (described in “Importing Users into Okta” earlier) and the user needs the Okta Office 365 app assigned to them (described in “Assigning users to Office 365” later).

Assigning an app in Okta to a user:

- Allows that user to login to the application via Okta.

- If the target application has been setup to provision new users, then assigning the app to the user causes Okta to provision an account in the target system. The inverse is also true, when you remove the app assignment, Okta will deprovision the user. In Office 365 this means the user account is set as Blocked.

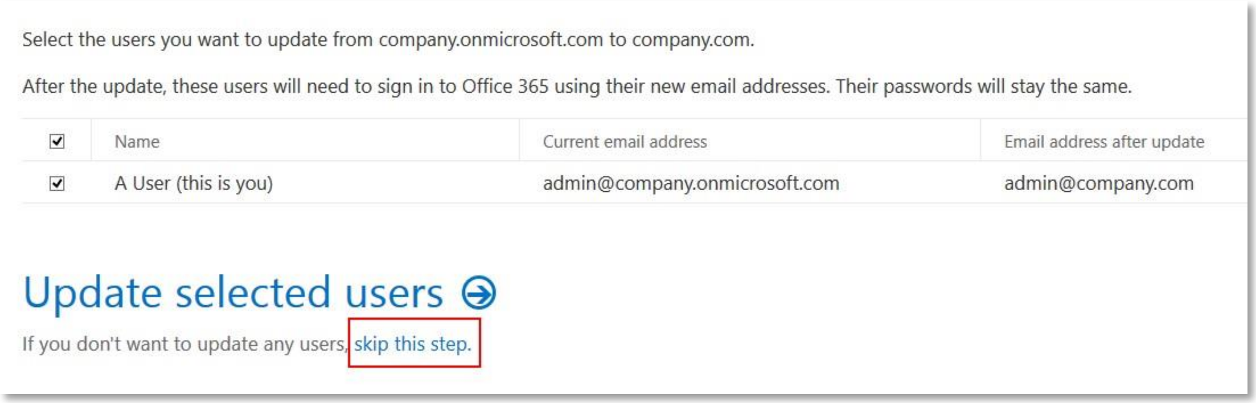
Configuring SSO

Registering Domains in Office 365

Before you can configure users for federated authentication with Office 365, you need to add a domain. By default, when you create your Office 365 subscription, Microsoft gives you a default domain in the format *yourcompany*.onmicrosoft.com. Users with a UPN that resolves to this domain (i.e. bill.smith@yourcompany.onmicrosoft.com) cannot be federated, therefore you need to add another domain.

You can add a domain through the Office 365 portal interface or by using PowerShell. The Microsoft guide, Add your domain to Office 365 provides instructions on how to add a domain. If you plan to use Okta’s Office 365 integration for provisioning new accounts, and your users in Active Directory do not have a username that reflects the domains you wish to use in Office 365, then refer to the sections in this document on Universal Directory.

Important: When using the web interface to add DNS domains, after initial verification, Office 365 asks if you want to update your users that use the default vanity domain to usernames on the new domain you are adding, it will look something like the screen below. If you are setting up the domain for the first time in in Office 365 and the only user is the admin user for that tenant. Do NOT change their username to one that is in the new domain. This will cause problems later when you attempt to setup federation to Okta. Therefore always leave your admin account on the *.onmicrosoft.com domain.



Select the users you want to update from company.onmicrosoft.com to company.com.

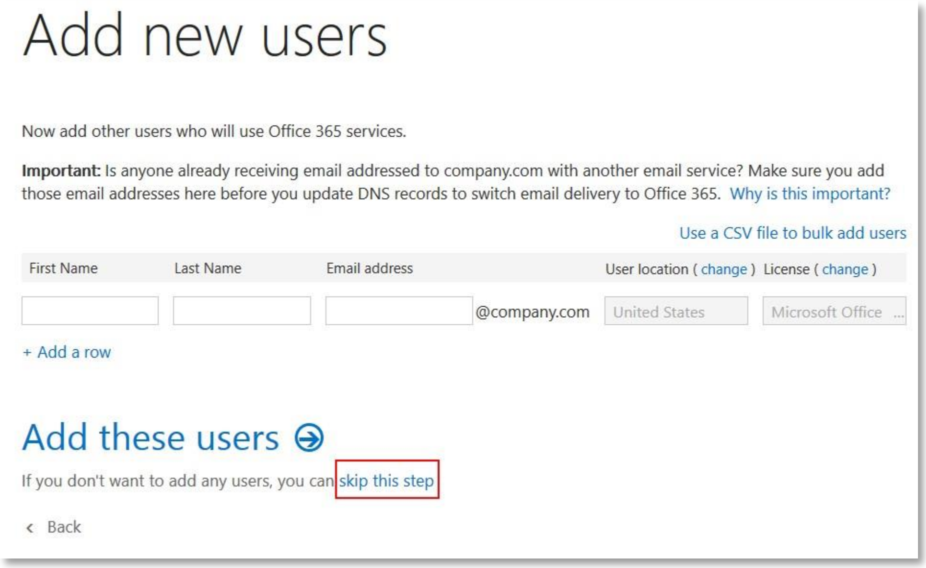
After the update, these users will need to sign in to Office 365 using their new email addresses. Their passwords will stay the same.

☑	Name	Current email address	Email address after update
☑	A User (this is you)	admin@company.onmicrosoft.com	admin@company.com

Update selected users ➔

If you don't want to update any users, skip this step.

After this step, Office 365 will ask if you want to add new user accounts. Continue and select the option to skip the step again.



Add new users

Now add other users who will use Office 365 services.

Important: Is anyone already receiving email addressed to company.com with another email service? Make sure you add those email addresses here before you update DNS records to switch email delivery to Office 365. Why is this important?

Use a CSV file to bulk add users

First Name	Last Name	Email address	User location (change)	License (change)
		@company.com	United States	Microsoft Office ...

+ Add a row

Add these users ➔

If you don't want to add any users, you can skip this step

‹ Back

On the next screen, set the domain purpose and let Office 365 configure your domain if you intend to use Exchange or Skype for Business services.

Using Secure Web Authentication

Before going into the detail of using federation, it is worth noting that Okta can authenticate users into Office 365 using our Secure Web Authentication (SWA) mechanism. If the user is on a desktop, they must install a browser plugin to use SWA and if they are using a mobile device, they should install our free Okta Mobile app that can be downloaded from the Apple App Store or Google Play. SWA can be useful with Office 365 if you want to share an Office 365 mailbox between federated AD accounts, or if you have a complex AD infrastructure that is limiting your ability to 100% enabled federated delegated authentication. For more information on how SWA works, see Overview of Managing Apps and SSO and About the Browser Plugin, both on the Okta support website.

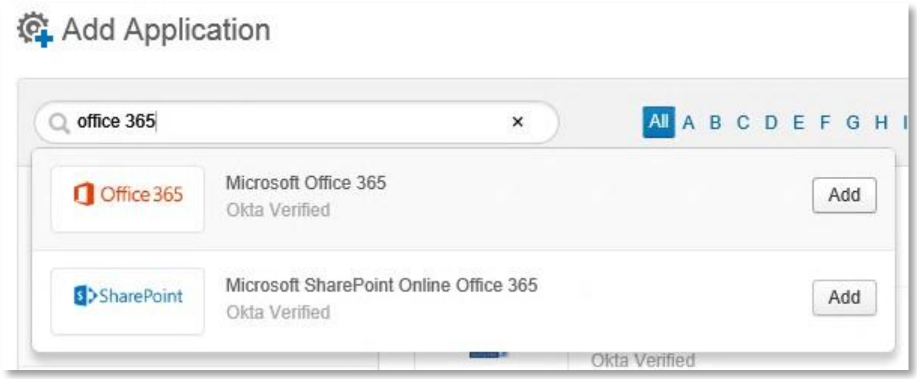
Note : This is web authentication only. Does not do anything with thick client.

Federating Domains to Okta

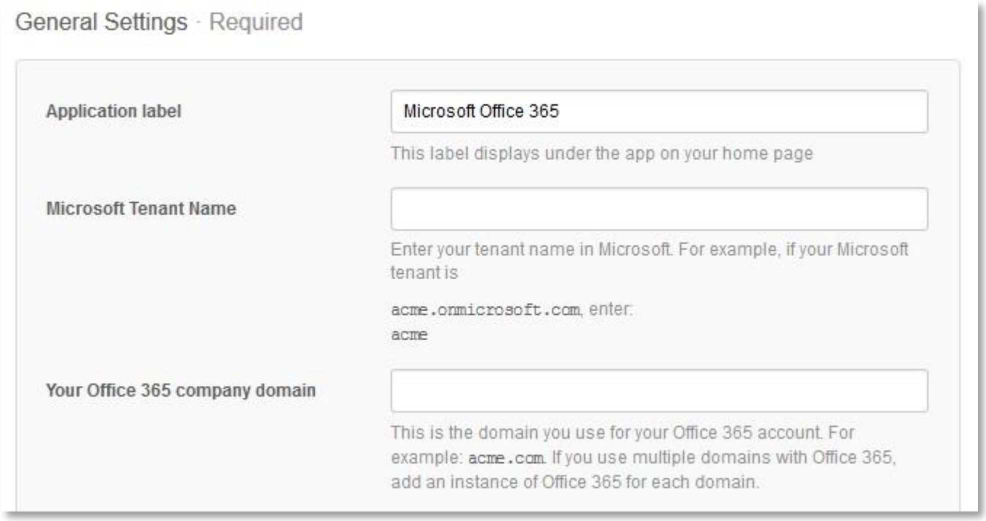
Now that you have a domain ready in Office 365, you need to setup the domain to use Okta as the federated identity provider. You do this by adding the Office 365 application to your Okta org.

1. Login to your Okta organization and select **Applications** > **Add Application**.

2. In the search dialog, type in *Office 365* and then click the **Add** button.



3. On the **General Settings** tab, provide the Office 365 tenant name and the domain you just added to your Office 365 subscription. If you are planning to federate multiple domains in either one or more Office 365 subscriptions you will need to add more than one Office 365 app in Okta. (Read more about this at https://community.okta.com/docs/DOC-1266) It is worth changing the application label to indicate which domain this configuration is for. Then select **Next**.



General Settings · Required

Application label: Microsoft Office 365

This label displays under the app on your home page

Microsoft Tenant Name:

Enter your tenant name in Microsoft. For example, if your Microsoft tenant is

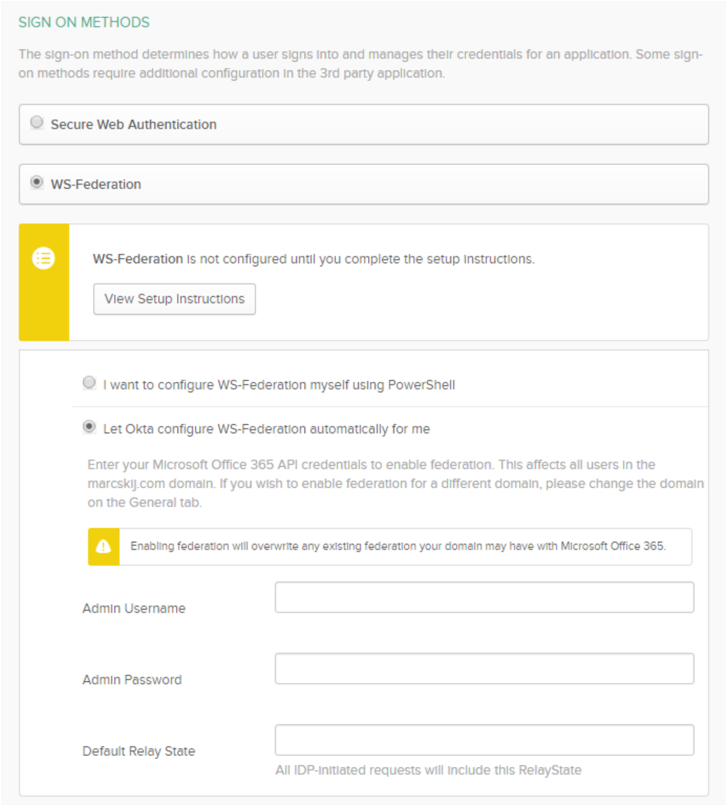
acme.onmicrosoft.com, enter:
acme

Your Office 365 company domain:

This is the domain you use for your Office 365 account. For example: acme.com. If you use multiple domains with Office 365, add an instance of Office 365 for each domain.

4. Most organizations require use of federation, therefore on the **Sign-On Options** tab and change the sign on method to WS-Federation. Then enter the user name and password of a global admin account for your Office 365 tenant. You will need to make sure to use an account that is for your tenant.onmicrosoft.com domain and not the domain you are configuring for federation.

Note : Make sure you have atleast one admin user setup with domain.onmicrosoft.com username. So that you don't loose access after you federate the domain



SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

○ Secure Web Authentication

● WS-Federation

WS-Federation is not configured until you complete the setup instructions.

○ I want to configure WS-Federation myself using PowerShell

● Let Okta configure WS-Federation automatically for me

Enter your Microsoft Office 365 API credentials to enable federation. This affects all users in the marcskij.com domain. If you wish to enable federation for a different domain, please change the domain on the General tab.

Enabling federation will overwrite any existing federation your domain may have with Microsoft Office 365.

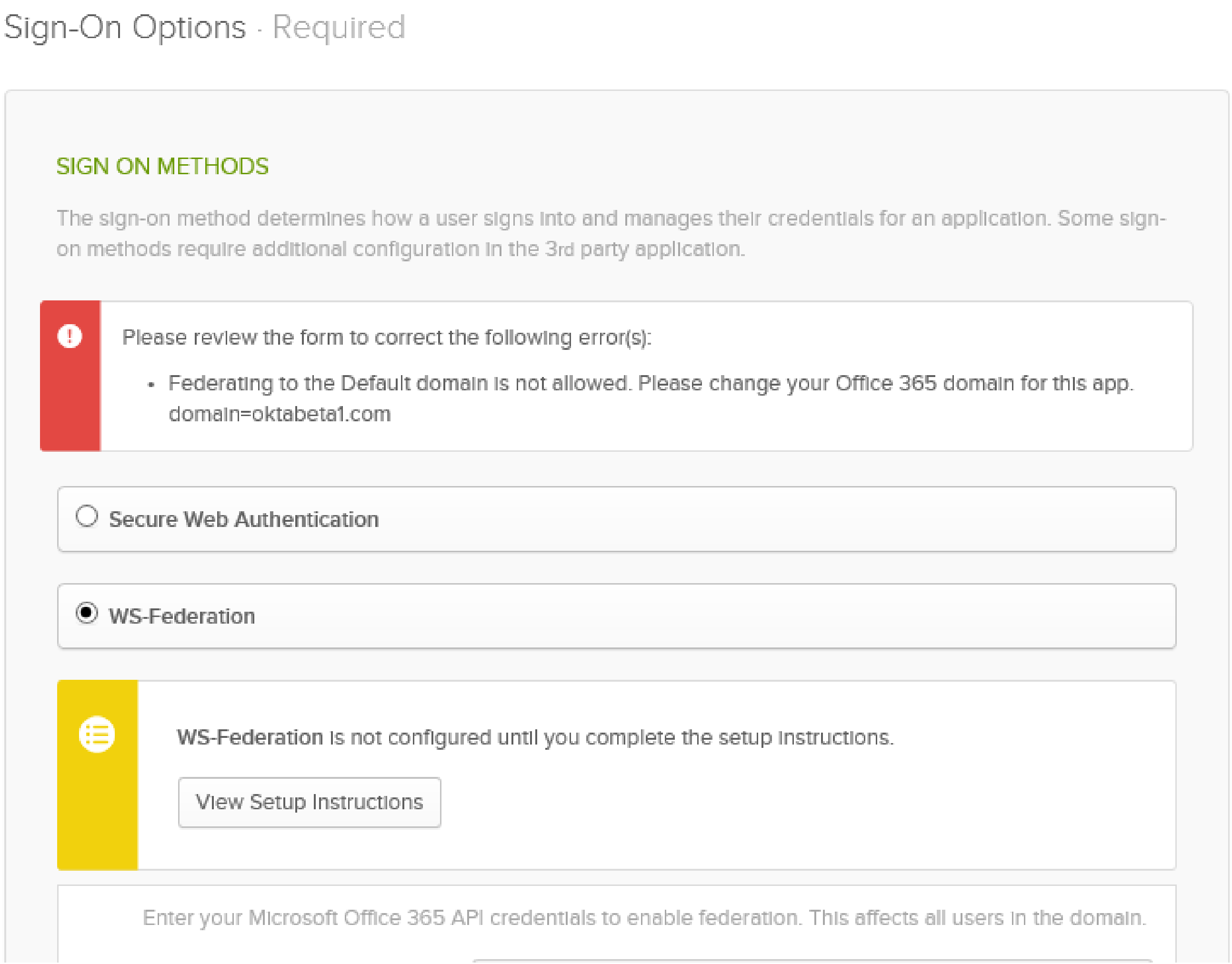
Admin Username:

Admin Password:

Default Relay State:

All IDP-initiated requests will include this RelayState

You might find that when attempting to federate the domain, you get an error, as follows:



Sign-On Options · Required

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Please review the form to correct the following error(s):

- Federating to the Default domain is not allowed. Please change your Office 365 domain for this app. domain=oktabeta1.com

○ Secure Web Authentication

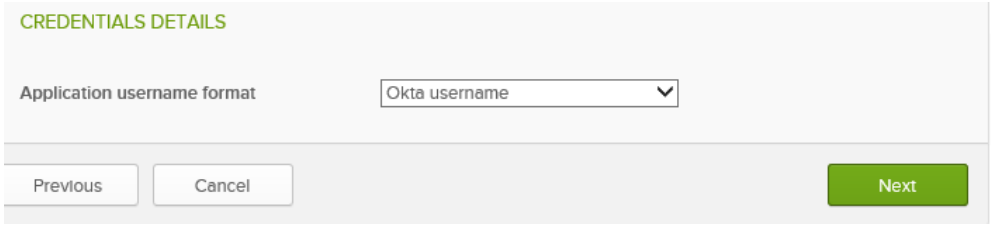
● WS-Federation

WS-Federation is not configured until you complete the setup instructions.

Enter your Microsoft Office 365 API credentials to enable federation. This affects all users in the domain.

This is because the new domain has been set as the default, this can happen automatically after you've added a new domain. If this happens, switch the default domain back to the *yourcompany*.onmicrosoft.com from the vanity domain. Instructions on how to do this are here. Note that the change can sometimes take a few seconds, so after changing the default domain wait for a moment before re-running the Okta federation PowerShell command.

a. Return to the browser where you are configuring SSO for Okta. Below the **View Setup Instructions** button is a dropdown that allows you to specify what attribute in Okta is used for the identifier for federation with Office 365. Generally this should be UPN



CREDENTIALS DETAILS

Application username format: Okta username

b. It is important to note what attribute is set here, because later on when accounts are created in Office 365, their username must match this setting.

5. After setting up SSO, select **Next**, leaving **Provisioning** disabled (this step is covered separately in the next section). Select **Next** again, but do not assign the application to anyone, just select **Next**, then **Done**.

Note : If you are not doing Okta provisioning. Then please go ahead and assign the users to respective AD group.

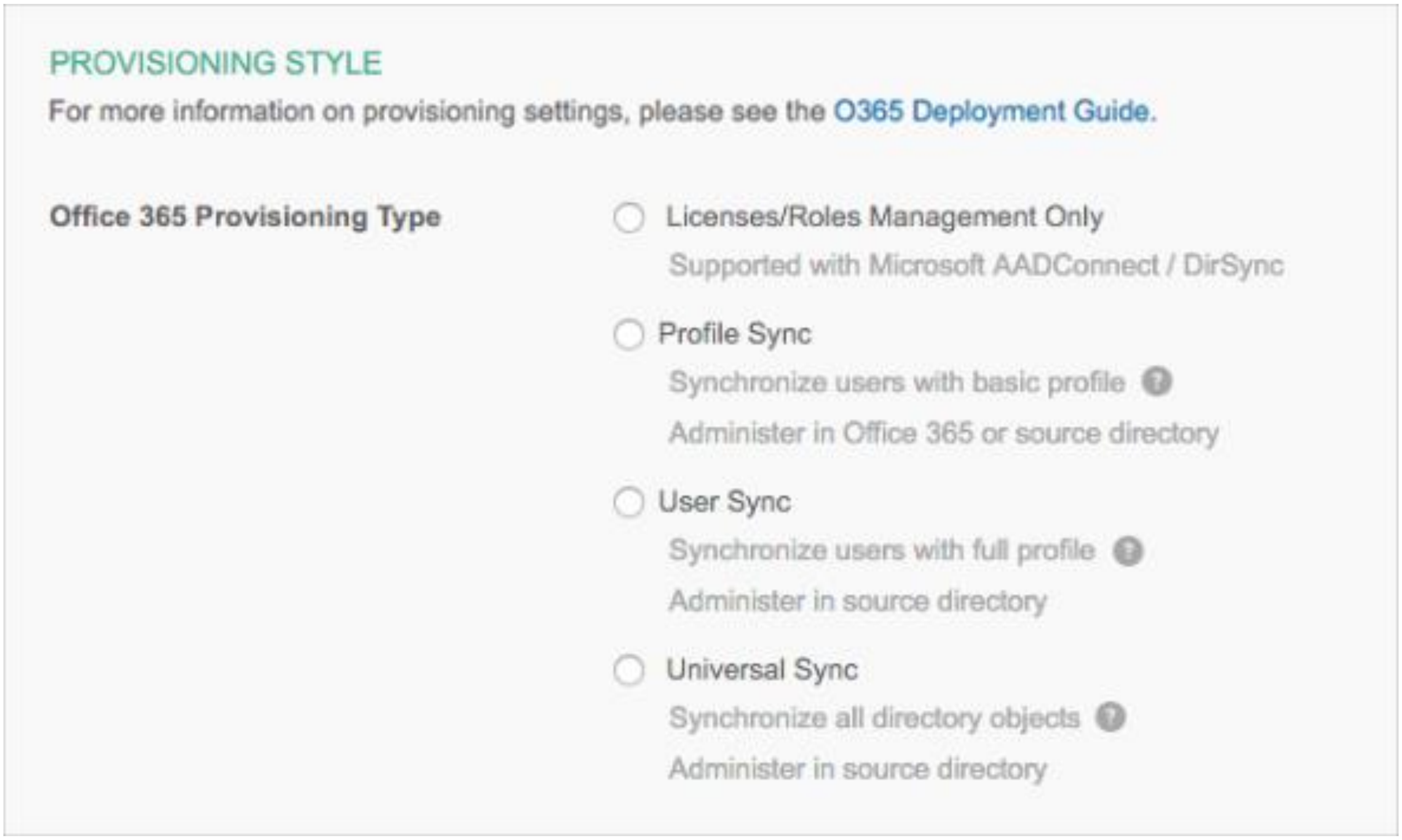
Provisioning to Office 365

⚠ We strongly recommend that you contact Okta Professional Services before you continue with this step.

Now that a) Users exist in Okta and b) Office 365 is prepared to federate user authentication to Okta, you are now ready to create users in Office 365.

Using Okta

There are four methods by which Okta can provision users in Office 365:



PROVISIONING STYLE

For more information on provisioning settings, please see the O365 Deployment Guide.

Office 365 Provisioning Type

○ Licenses/Roles Management Only
Supported with Microsoft AADConnect / DirSync

○ Profile Sync
Synchronize users with basic profile
Administer in Office 365 or source directory

○ User Sync
Synchronize users with full profile
Administer in source directory

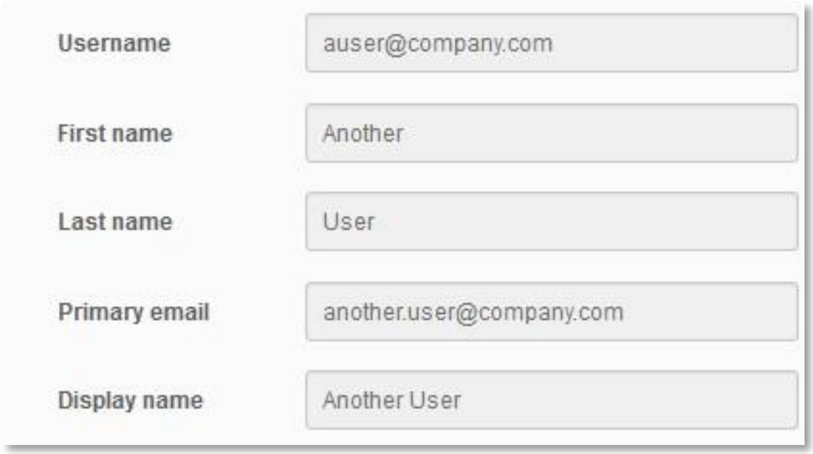
○ Universal Sync
Synchronize all directory objects
Administer in source directory

- **Licenses/Roles Management Only**

  Licenses/Roles Management Only has been built to work alongside Microsoft's Azure AD Connect infrastructure, and is the only provisioning type that can be used in conjunction with AADConnect Sync. This functionality allows you to leverage Okta's advanced Roles and License functionality in order to assign specific licenses to users automatically, depending on attributes or group membership within Okta. The only attributes available with this type of provisioning are licenses and roles. If you select this provisioning type, the only provisioning features that are available are **Update User Attributes** and **Deactivate Users**.

- **Profile Sync**: Okta creates “in cloud” users and synchronizes only Username, First Name, Last Name, Email, and Display Name.

The advantage of this provisioning method is that these types of users can be edited directly in the Office 365 portal, whereas all other provisioning types will appear as ‘Synced with Active Directory’ in the Office 365 portal and will require changes to happen at the location the account was mastered (Okta, AD or another Directory\Service)



Username	auser@company.com
First name	Another
Last name	User
Primary email	another.user@company.com
Display name	Another User

- **User Sync**: This provisioning type leverages Universal Directory. When you select this, Okta automatically sets up “Active Directory synchronization” for you in Office 365. This allows you to create users with 16 more attributes. For attribute details refer to the following information: https://support.okta.com/help/articles/Knowledge_Article/Okta-Enhancements-with-Microsoft-Office-365-Integration When these users are created, they are marked as “Synced with Active Directory”. This means they cannot be edited in the Office 365 portal, instead Office 365 will advise you to edit them in Active Directory. However, in this instance, Okta is taking on the role of Active Directory. This means that:

    - If your users did originate in Active Directory, then Office 365 is accurate. For changes to the users attributes, you need to edit in the relevant user account in Active Directory. Okta will import that change and update Office 365.

    - If the user was created directly in Okta, then you can edit the user directly in Okta and the user in Office 365 will be updated. Note that with Universal Directory, you can make some of these attributes editable by the end user via the Okta end user portal. The section below goes into detail of using Universal Directory.

    - You can actually have users from Active Directory and those that are only in Okta being provisioned to the same Office 365 user domain. This is a very powerful feature and allows you a wide range of ways to manage Office 365 users.

If you choose the **User Sync** option, see the later section about using Universal Directory for attribute mapping and transformations. But first, we need to finish describing how to enable provisioning with Okta.

- **Universal Sync (Enhanced Provisioning)**: Similar to the User Sync provisioning features detailed above, this provisioning mode sets up Active Directory Synchronization and synchronizes additional objects including:

    - Security Groups
    - Distribution Lists
    - Contacts
    - Resource Mailboxes

  In addition to the additional object types, the number of attributes synchronized has now been extended to 142 total attributes, allowing for rich user profiles and a higher fidelity synchronization. This method of synchronization enables proprietary attributes such as those used by Exchange and Skype for Business to be synchronized from on-premises to Office 365 without the need for additional synchronization technologies such as Azure AD Connect.

  Note: The object types above will be synchronized directly from Active Directory to Office 365 and will not be represented in Okta's universal directory. Changes to these objects should be made in AD directly.

Switching on Office 365 provisioning in Okta

We strongly recommend that you contact Okta Professional Services before you continue with this step.

If you have followed this deployment guide, you will have an Office 365 app configured for SSO. This next section will walk you through editing that app to include managing the provisioning.

1. Login to your Okta org and navigate to **Applications**. Click on the Office 365 app you previously created.

2. Switch to the **Provisioning** tab and select **Edit** and then **Enable provisioning features**.

3. You need to provide a username and password for a user in your Office 365 subscription that has Global Administrative rights in Office 365. We recommend that you create a separate account that is not the admin account first created when you signed up to Office 365. Press the **Test API Credentials** to verify the connectivity from Okta to Office 365.

4. Select the **Office 365 Provisioning Type**. Refer to the previous selection on which to choose.

   Note that switching from **Profile Sync** to **User Sync** or **Universal Sync** means that user accounts mastered in Okta or AD will only be modified in the system of record (and not in Office 365). These accounts will be represented in the Office 365 portal as users that are **Synced from Active Directory**.

5. Make a decision on which provisioning feature to enable.

   User Import – It is possible to have users imported from Office 365 into Okta. These users can be linked to existing Okta accounts through either their email address or a custom expression. Only users with an Office 365 license are imported.

   Note that once users are imported from Office 365, they become Okta users where you can modify their attributes, unless of course they have been associated with an existing Active Directory account. While it is possible to schedule imports, an administrator must still manually activate user accounts.

   The ability to import users is mostly used when you have an existing Office 365 tenant and you need to do a one-time import of users into Okta. Typically, after this import, Okta owns the provisioning of new users into your Office 365 tenant.

   Okta automatically assigns any imported users to the Office 365 application itself so they are able to SSO back into Office 365 through Okta. Be aware that if the imported user is from a domain that is not federated or the *.onmicrosoft.com domain, it is not possible to federate sign on BUT you can enable the Okta app for SWA authentication. If you deactivate the user in Office 365 and do another import, Okta will un-assign the application from the user.

   a. **Create Users** – Using Okta to provision accounts to Office 365 is as simple as enabling the checkbox. When the application is assigned to a user, Okta will create a new account for them in Office 365. The new account will use the username that is specified in the **SSO** settings page, or if you are using the **User Sync** provisioning type, you can specify the username via Universal Directory. An in-depth guide is later in this document.

      New users can also be assigned an Office 365 license when Okta provisions the account and you can specify if the user has an Office 365 administrative role. More information about what happens is discussed later in the section about application assignment.

   b. **Update User Attributes –** When you enable this feature, any changes to the user profile are automatically updated in Office 365. Changes in Office 365 will be over written. This is useful when another external source to Okta (Workday HR or Active Directory on-premises) makes a change, it can be propagated to Office 365.

   c. **Deactivate Users** – Okta automatically creates Office 365 accounts when a user is assigned to the Okta Office 365 app. If you un-assign the user from the app, Okta will switch the Office 365 account's sign in status from Allowed to Blocked.

   Note: Unlicensing a user in Office 365 will result in all associated data being deleted after 30 days. This will include (but is not limited to) all contents of the users mailbox and OneDrive folders as well as settings and customizations. As part of deactivation, Okta will maintain the license on the user so administrative tasks such as archiving or data sharing can be completed.

   d. **Sync Okta Password –** If you are not federating accounts to Office 365, you can have Okta manage the password. If the user changes their password in Okta, this password is then updated in Office 365 automatically.

6. At the point of saving your configuration, Okta communicates to Office 365 and will synchronize any groups in Office 365 into your Okta org. Those groups will also have membership of Office 365 users that exist and are active in Okta.

Now that Provisioning is enabled, you will need to go through the process of assigning users.

The below sections detail Universal Directory transformations that are commonly associated with assigning the Office 365 application, skip the sections below and go right to Assigning Users to Office 365 if there is no need to transform values (such as username) from on-premises to O365.

Universal Directory: Mapping and Transforming Data to Office 365

If you have selected the **User Sync or Universal Sync** option on the provisioning page, you enable the Office 365 integration to use Universal Directory (UD) to manage the mapping of attributes from AD/Okta to Office 365. This allows you to:

- Have total control over the username being created in Office 365, even if the data from AD/Okta isn't correct, UD allows you to standardize how Office 365 users are created.

- Pass attributes from AD direct to Office 365 without that information living on the Okta user profile.

- Make decisions on what an attribute should be, based on other attributes or states of the user.

- Okta here most importantly can act as an idfix tool to transform your data

The following section details common use cases where UD is used with Office 365, however this isn't an in-depth guide into Universal Directory.

UD is all about giving you the power to control the mapping of attributes to Office 365 from either the source directory, or the user in Okta. It also lets you, using expressions, manipulate the data in those attributes. For Office 365, these are the most common situations where you want to make changes to the default configuration of UD.

- Username of the AD user (UPN) that was copied into Okta is not what you want to use in Office 365. (Idfix transformation)

- Primary email address for the AD user that was copied into Okta is not what you want in Office 365.

- You have a mix of AD and Okta users that both need to conform to a common username/email format in Office 365

- Different domains in Office 365 and want to handle the mapping of users differently between them.

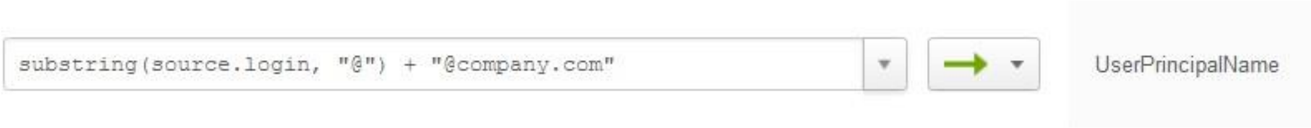
Example Scenario 1 – *Customizing a users User Principal Name for Office 365*:

1. Login to your Okta org as an administrator and navigate to the **Applications \ Office 365** app instance you wish to control the username formats of provisioned users. Select the **Provisioning** tab.

2. Make sure that **Provisioning** has been enabled and that the type is **User Sync**. Scroll to the bottom and click on "**Edit Mappings**".

3. You are then presented with buttons at the top. The first is for mapping attributes when you import from Office 365 into Okta, but we are interested in mapping attribute when we create the Office 365 user from Okta. So click on the button for **Okta to Microsoft Office 365**.

4. You will now see the list of 20 attributes and by default, they will map to either existing Okta attributes or there will be an expression to get the attribute from the AD user, if there is one. The use case we want to address here is that the username from AD that is used in Okta, might not be the username you want in Office 365. Therefore change the value in the UserPrincipalName field (which will be *login* by default) to the expression shown below.



```
substring(source.login, "@") + "@company.com"
```

The expression takes the same username prefix (sam.smith) from the current Okta username but forces the domain you have configured in Office 365.

5. Click on the **Save Mappings** button and this will update the configuration. Note if you have any users that are currently assigned and provisioned, the new changes will automatically update.

Example Scenario 2 – *Customizing user attributes*:

- By default the FacsimileTelephoneNumber is the following expression:

```
hasDirectoryUser()?findDirectoryUser().facsimileTelephoneNumber:null
```

Which will use whatever is set in AD but default to blank if there is no value. You could extend this to evaluate if the AD user's fax is blank and always set to the main company fax number. i.e.

```
hasDirectoryUser()?((findDirectoryUser().facsimileTelephoneNumber==null

OR findDirectoryUser().facsimileTelephoneNumber=="")?"555 123

4567":findDirectoryUser().facsimileTelephoneNumber):"555 123 4567"
```

- Create a displayName with more data in it than default and force a standard displayname over whatever came in from AD.

```
source.firstName + " " + source.lastName + "(" + source.department + ")"
```

- You could use a custom attribute in AD for setting titles. For example, if you added a customer attribute (or used one of the exchange customer attributes) in AD, and stored in it a true or false depending on if the user was a contractor. You can use the following expression for the Office 365 title.

```
source.title + (source.customAttribute01 == "true"?" (Contractor)":"")
```

Resulting in a title of “Sam Smith” for employees and “Alex Andrews (Contractor)” for contractors.

Another important aspect about Universal Directory and Office 365 is that you have complete control over different domains of users. For example, you might have two Active Directory domains with different email address formats.

	Domain A	**Domain B**
Email Format	Firstname(1)LastName@company.com	firstName.lastName@company.com
Example	ssmith@company.com	sam.smith@company.com

Then in Office 365 you might have two domains, @company.com and @product.com and users in Domain B need accounts in @product.com but Domain A in @company.com. But you might want to have firstName.lastName for the first part of the email on both domains. UD from Okta makes this easy. In Okta you add a separate Office 365 app for each domain in Office 365 for which you are provisioning users.

You can set all the usernames in Okta to be a common format when you import users from the two Active Directory domains, because you have separate UD mappings and expressions for each domain. (See earlier in this document for mappings when bringing users in from AD). Then because you have two Office 365 apps in Okta for each domain, you can simply use different mappings to ensure the right emails and usernames are created in Office 365.

Using PowerShell

It is possible to build scripts around PowerShell to manage users in Office 365 using the New-MsolUser cmdlet. Note that when a user domain is federated, you must also provide an immutableId. When Okta provisions users using the **Default** provisioning type, it uses a unique value on the Okta user. The following is a simple script that will convert the AD ObjectGuid to the immutableId.

```
Get-ADUser username | ForEach-Object {

        $immutableId = [Convert]::ToBase64String($_.ObjectGuid.ToByteArray());
        Write-Host $_.UserPrincipalName, $_.Name, $immutableId;

        New-MsolUser -DisplayName $_.Name –UserPrincipalName
        $_.UserPrincipalName -ImmutableId $immutableId; }
```

It is important that if you intend to have these users federated back to Okta that the users are setup correctly. The scope of this is beyond this document, please contact your Okta account team for help.

Using DirSync / AADConnect

AADConnect (formerly known as DirSync) is the common name for a free piece of software from Microsoft that copies data from your Active Directory into Office 365. For more information, on AADConnect, refer Integrating your On-Premises Directory with Azure Active Directory on the MSDN website.

To synchronize data into Office 365, AADConnect may already be in use or is a requirement. If you are migrating to Office 365 and run Exchange on-premises and will be migrating in phases, this is usually called a Hybrid migration. In this scenario AADConnect is needed to synchronize hybrid specific data between Office 365 and your on-premises Active Directory.

When you install AADConnect you still need to install the Okta AD Agent for each domain.

AADConnect is creating users in Office 365, but the AD Agent from Okta creates users in Okta and also handles part of the SSO process (delegation of authentication to AD) and password management (being able to reset your AD password from Okta).

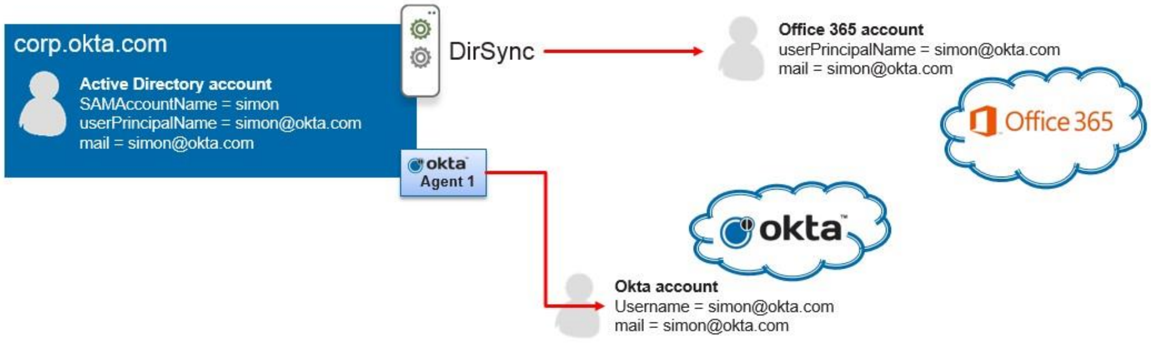
AADConnect, has brought multi forest sync capabilities to this tool. However many customers still struggle with the need to maintain network connectivity between the single and only AADConnect server to all forests. The solution is to use AADConnect for the primary forest and then Okta for users in other forests/domains. FIM is also an option, but the consulting costs for deploying FIM can be significant. Most people avoid using FIM where possible due to high costs in purchasing, deploying and maintaining it.

Note: **Do not run DirSync/AADConnect and Okta for the provisioning of user accounts in the SAME domain in Office 365. This is unsupported and Okta has not tested the side effects of doing so. With AADConnect running, the only supported Provisioning configurations is Roles/License Management Only.**

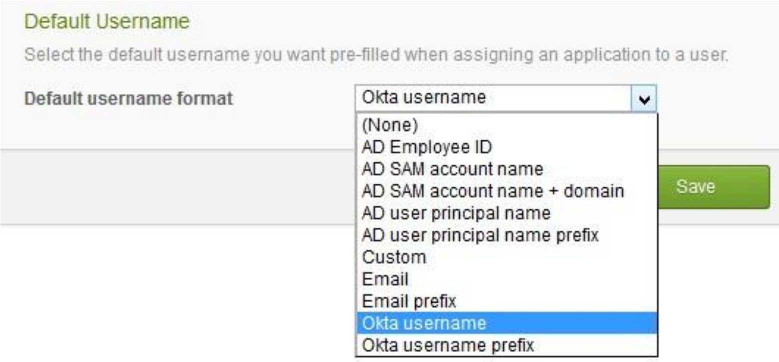
Note: When deploying AADConnect, you may be prompted to select the attribute for a users sourceAnchor (https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-get-started-custom/). The default for both AADConnect and Okta is objectGUID. If you have a need to modify this setting in AADConnect, it is recommended to engage Okta Professional Services to assist with this transformation in Okta Universal Directory.

AADConnect is unable to automatically assign user roles and licenses, this must be manually done through the Office 365 web portal or PowerShell scripts. When using Okta to provision the user to Office 365, you can assign licenses at the time of user creation.

When AADConnect is being used for provisioning (with Okta in use for SSO), it is important to ensure that the UPN of a user that is created in Office 365 matches the UPN Okta is using for federation. The diagram below shows how DirSync creates a user directly in Office 365.



Okta also creates a copy of the same user in its own directory. When the SSO step takes place, Okta is going to pass to Office 365 a username and it needs to match the value for the corresponding user in Office 365. The value for the username is set on the **Single Sign On** tab of the Okta Office 365 application as shown below. Whatever format you select, this is the value that must match the one in Office 365.



Default Username

Select the default username you want pre-filled when assigning an application to a user.

Default username format: Okta username

See the community article, Preparing user accounts prior to Office 365 & Okta integration in the Okta Community for an explanation of the required considerations.

Assigning Users to Office 365

At this point you have users in Okta and one or more DNS domains in Office 365 that are configured for Okta for federation. If you are not using Okta for the provisioning of users, you may also have users in Office 365. Now we need to tie all of this together. This is done by assigning the Office 365 application in Okta to users. This achieves two goals.

- Okta users with the Office 365 app assigned are able to login to Office 365 through Okta.

  If Provisioning is enabled in Okta:

  - A user account will be created at the time of assigning the app. If a user already exists in Office 365, Okta will match the users up and maintain the relationship.
  - A role and/or license will be assigned to the user in Office 365. This fully automates the ability to provision fully working accounts for end users to log right into.

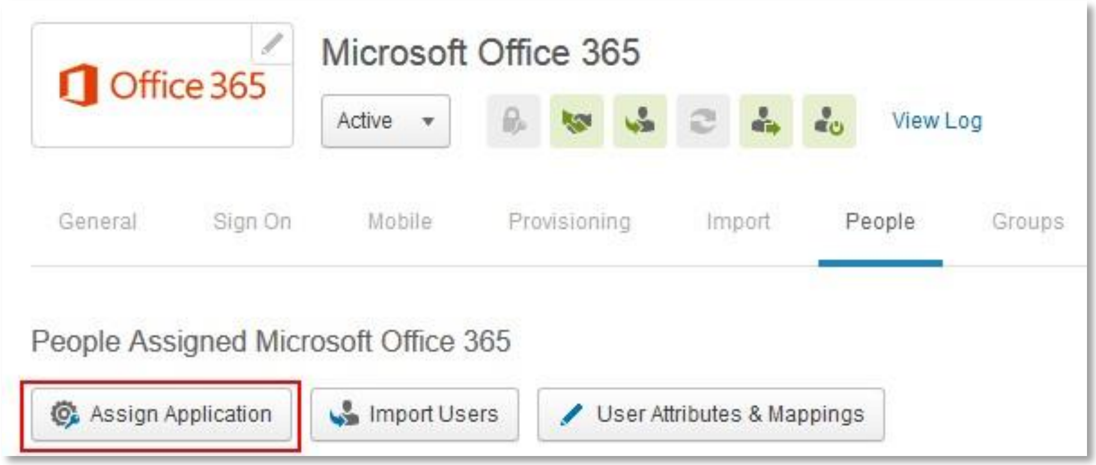
Assignment can happen in two ways, directly to a user account (individual assignment) or indirectly by using groups (group assignment). The automation of role and license assignment is described at the end of this section.

User assignment

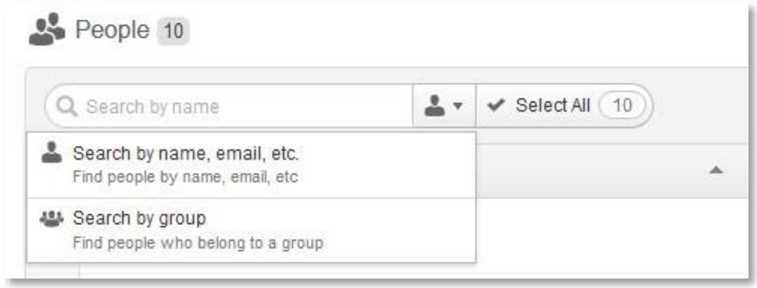
There are two methods by which you can assign the Office 365 application to a user. First through the application:

1. Select **Applications**, then from the list below select the Office 365 application you wish to assign to a user. Note that if you have multiple DNS domains in Office 365, you will have multiple Office 365 applications listed. Make sure you chose the right one.

2. By default the application will display the **People** tab. Click on the **Assign Application** button.



3. A list of all users in Okta will be displayed. You can either chose by scrolling down the list, or you can search for users either by their attribute or you can search for a group and list the users in that group from which to assign the app. Select the user/s you wish to assign to Office 365.


People 10
Search by name
Select All 10
Search by name, email, etc.
Find people by name, email, etc
Search by group
Find people who belong to a group

4. If you have provisioning enabled, you will be asked to provide some information.

    a. What license in Office 365 to assign to the user/s. Most commonly you will see just one license type here, but if you have multiple different license subscriptions in Office 365, you can chose them from here. More about licensing below.

    b. You can decide to assign any Office 365 administrative roles to the user/s.

    c. For each user you are assigning to the application you can specify the **Username**. The **Username** defaults to whatever has been set on the **single sign on** page. However it is possible to override if you need.

5. When you confirm assignments, Okta will enable those users to login to Office 365. If you have provisioning enabled, Okta will create the accounts in Office 365.

The other method for assigning users to applications is by starting with a user account.

Note that in the above method you can choose many users in one action, the method below limits you to a single user at a time:

1. Click on the **People** tab and by using the search field and applying filters, locate the user you want to assign.

2. Click on the user and it defaults to the **Applications** tab. From here you can click on the **Assign Applications** button. You will then be required to enter in the same information as the process above.

3. Clicking **Save** will assign the app to the user.

Group assignment

Assigning users, one by one, isn't a scalable approach. Therefore, Okta allows you to assign groups to applications instead. This dramatically improves your ability to manage who can access Office 365 and what accounts are created. Note that assigning the group to the Office 365 app in Okta does not actually create a group in Office 365. It's just a mechanism by which to define what users in Okta can login to Office 365.

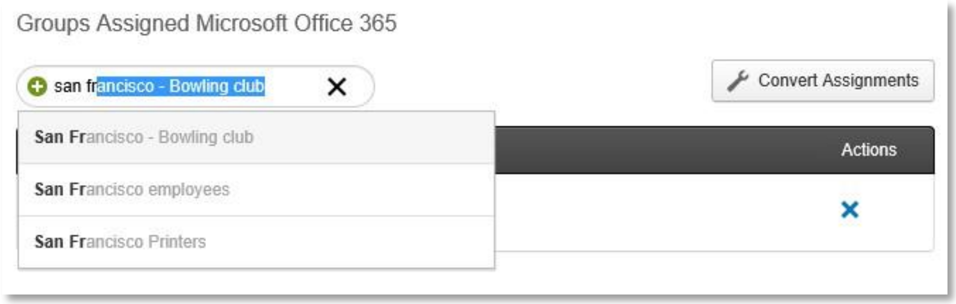
The most common type of group to use is from Active Directory. If you want all users in all AD domains to have access to Office 365, simply assign each "Domain Users" group from all connected AD domains. Note you can use any group in Okta. So if you are using Okta to manage contractor accounts, and they also require access to Office 365, you can assign a native Okta group to provision contractor accounts to Office 365.

When assigning groups to apps with provisioning enabled, you don't have the ability to override the **Username**. The **Username** defaults to whatever is set on the **single sign on** page or if you are using Universal Directory, the mapping/expression will define the username.

There are two ways to assign groups to apps, first through the application:

1. Click on the **Applications** tab and click on the Office 365 application. Switch to the **Groups** tab.

2. Start typing into the search box and a list of groups will start to appear.


Groups Assigned Microsoft Office 365
san francisco - Bowling club
Convert Assignments
San Francisco - Bowling club
San Francisco employees
San Francisco Printers
Actions

3. If you have provisioning of new users to Office 365 enabled, selecting one of the groups will display the option to choose what license and what role/s you want

   users in this group to have. Otherwise Okta will just assign the group to the application.

The other method of assigning groups is through the group:

1. Navigate to **Directories > Group** from the Admin dashboard. Scroll or search for the group you want to assign to Office 365 and choose it.

2. Click on the **Manage Apps** button and you will see two lists, one that shows all applications not assigned to the group and the ones that are. Simply scroll to the Office 365 application (you can also search using the box between the lists) and add it.

3. Once again, if provisioning of users to Office 365 is enabled on the app, you will be asked to specify what licenses and roles users should get.

Assigning Office 365 licenses and roles

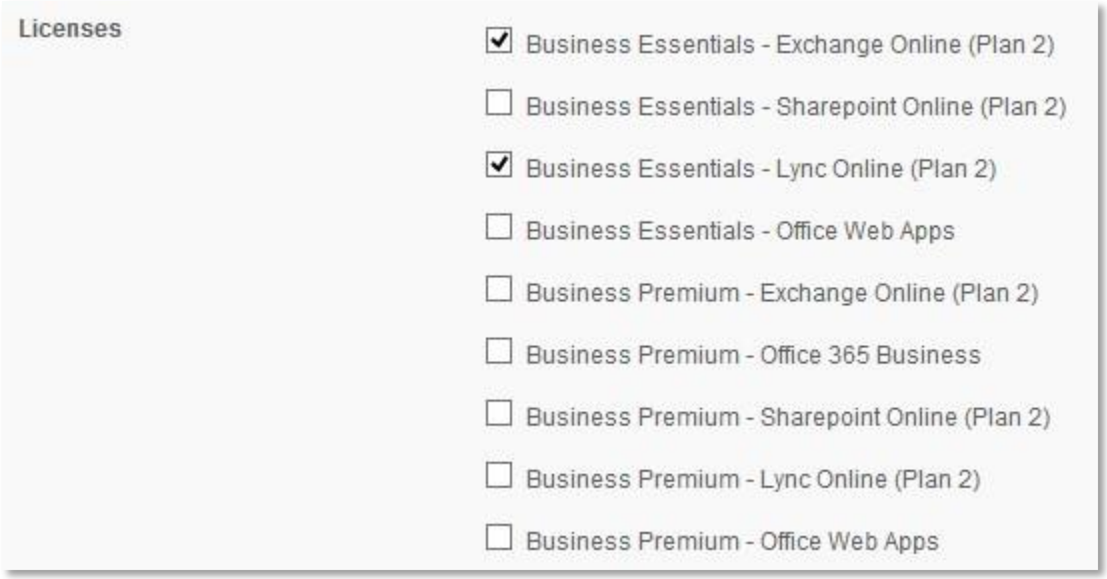
We strongly recommend that you contact Okta Professional Services before you continue with this step.

Okta is always focused on making the process of getting users ready for work in Office 365 as easy and quick as possible. One aspect of this relates to assigning a license or a role and Okta can assign these automatically for you.

- Licenses in Office 365 enable a user to access the different services in Office 365. You might have several different subscriptions in Office 365. i.e. Enterprise licenses (E3 for example) for your employees and Kiosk (K1) licenses for contractors or seasonal workers.

  Okta allows you to choose which of these licenses you want to assign to users. When assigning users via groups (highly advised and described in the previous section) you can assign a whole range of users to one license type. For example, you might take the groups Sales, HR and Finance from your AD domain and assign to Office 365 with the E3 license. You may then choose the Contractors group, that is native to Okta, and assign that the K1 license.

  When selecting the license, you also get to choose which service to enable. In the image below you can see the "Business Essentials" license type as well as "Business Premium" and that only Exchange and Lync (Skype for Business) have been enabled for this assignment.

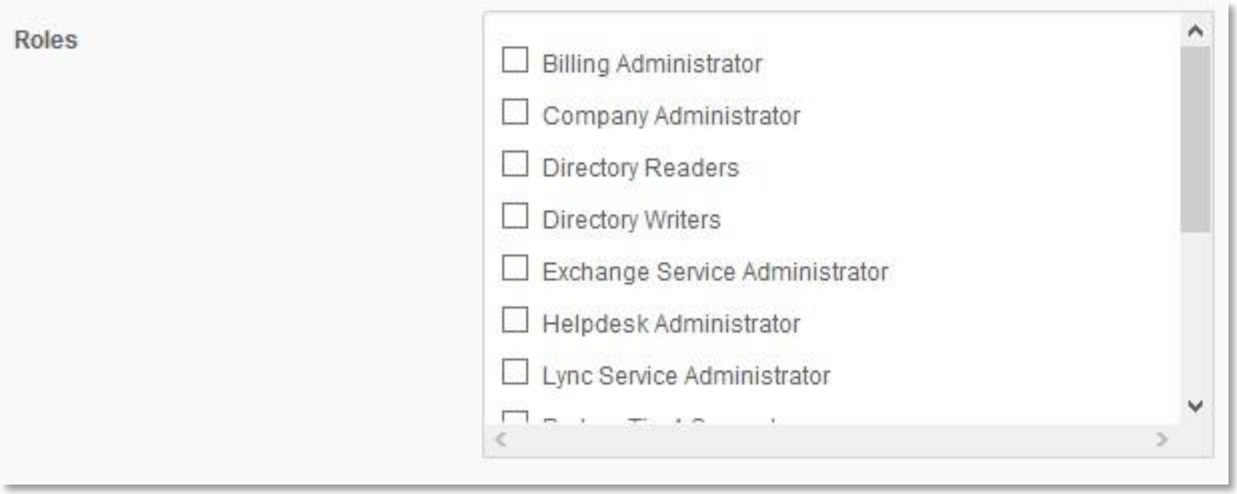


Licenses

☑ Business Essentials - Exchange Online (Plan 2)
□ Business Essentials - Sharepoint Online (Plan 2)
☑ Business Essentials - Lync Online (Plan 2)
□ Business Essentials - Office Web Apps
□ Business Premium - Exchange Online (Plan 2)
□ Business Premium - Office 365 Business
□ Business Premium - Sharepoint Online (Plan 2)
□ Business Premium - Lync Online (Plan 2)
□ Business Premium - Office Web Apps

- Roles in Office 365 are about allowing users the ability to administrate certain services and aspects of Office 365. For a full list of roles and what permissions they relate to, refer to: https://support.office.microsoft.com/enus/article/Permissions-in-Office-365-da585eea-f576-4f55-a1e0-87090b6aaa9d

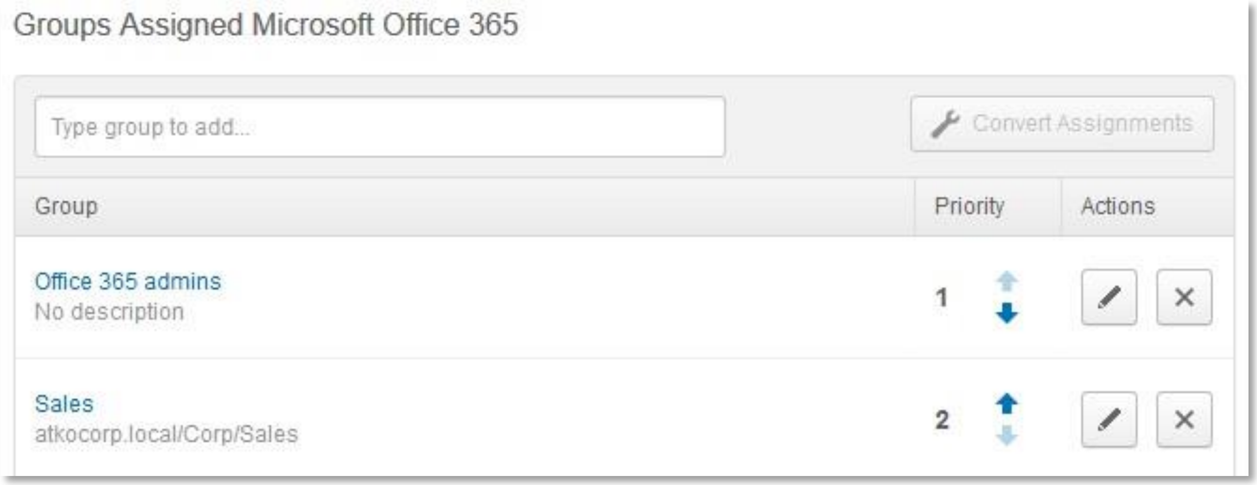
  In Okta you can choose what roles to assign to users at the time of assignment:



Roles

- □ Billing Administrator
- □ Company Administrator
- □ Directory Readers
- □ Directory Writers
- □ Exchange Service Administrator
- □ Helpdesk Administrator
- □ Lync Service Administrator

When assigning multiple groups to Office 365 for both license and role assignment, it is important to note the order of the groups. The image below shows that the *Office 365 admins* group is higher than the *Sales* group. Just in case someone in the Office 365 admin groups is also in Sales, you want to ensure they get the role assignment first.



Groups Assigned Microsoft Office 365

Group	Priority	Actions
Office 365 admins No description	1	
Sales atkocorp.local/Corp/Sales	2	

Groups: From AD to Okta to Office 365

We strongly recommend that you contact Okta Professional Services before you continue with this step.

Another feature of the Office 365 integration in Okta is that, just like users, you can also provision groups to Office 365 from Okta. This functionality is called **Push Groups**. It means that from the range of groups you can have in Okta, you can have some of them automatically created and their memberships updated in Office 365.

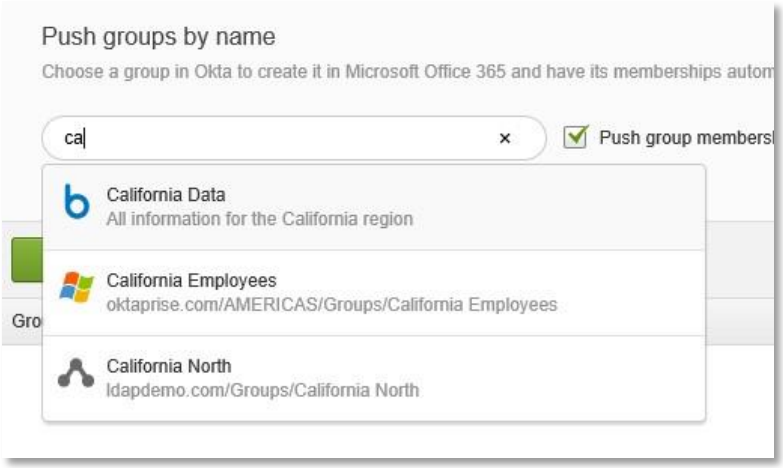
In Okta there are a variety of groups that can be imported. You can get groups from

Active Directory and LDAP servers as well as online services like BOX.net and Workday. Okta also has its own native groups that are created and managed directly in the Okta portal. All of these groups can be provisioned into Office 365.

There are two ways you can create groups in Office 365 from Okta. The first is by referencing the group directly:

1. Select **Applications**, then select your Office 365 application. Switch to the **Push Groups** tab.

2. Click on the green **Push Groups** button and select **Find groups by name**. You can then start typing into the search box and select a group from Okta. In the example below you can see groups from BOX.net, an Active Directory domain and an LDAP server.



Push groups by name

Choose a group in Okta to create it in Microsoft Office 365 and have its memberships autom

ca ×

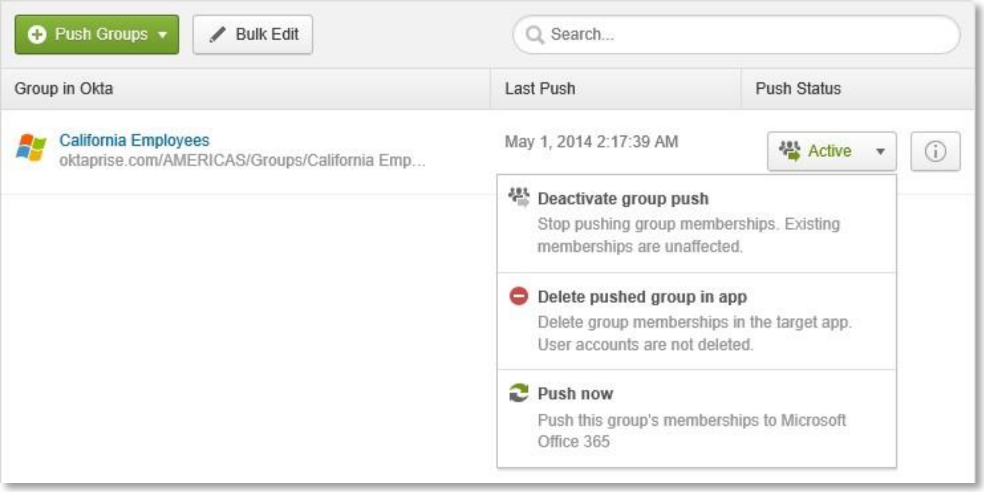
☑ Push group membersl

California Data
All information for the California region

California Employees
oktaprise.com/AMERICAS/Groups/California Employees

California North
ldapdemo.com/Groups/California North

3. If you leave the **Push group memberships immediately** checked, when you select and add the group it will be created in Office 365. After clicking on the **Active** button, you can deactivate, delete, or push the group membership from the interface shown below.



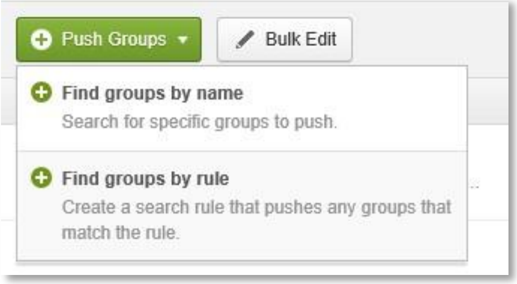
Group in Okta	Last Push	Push Status
California Employees oktaprise.com/AMERICAS/Groups/California Emp...	May 1, 2014 2:17:39 AM	Active

Deactivate group push
Stop pushing group memberships. Existing memberships are unaffected.

Delete pushed group in app
Delete group memberships in the target app. User accounts are not deleted.

Push now
Push this group's memberships to Microsoft Office 365

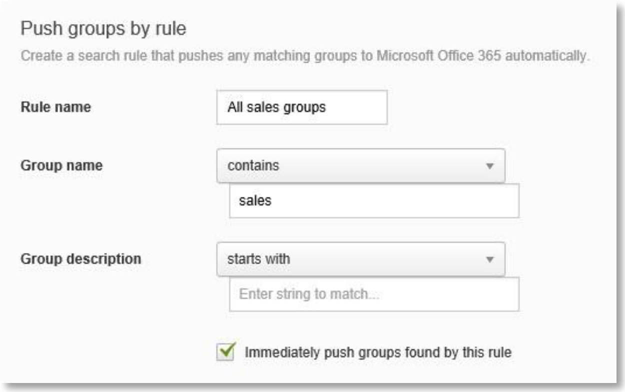
The second method to defining what groups you can push from Okta into Office 365 is by rule. In this method, click on the green **Push Groups** icon and select **Find groups by rule**.



Find groups by name
Search for specific groups to push.

Find groups by rule
Create a search rule that pushes any groups that match the rule.

From here you are presented with a simple interface that allows you to name the rule and define the parameters by which groups are selected to be pushed to Office 365. You can search based on the group name or description. There are a variety of filters by which to define the search. Again there is a checkbox to immediately initiate the group push once the rule is defined.



Push groups by rule
Create a search rule that pushes any matching groups to Microsoft Office 365 automatically.

Rule name	All sales groups
Group name	contains sales
Group description	starts with Enter string to match...

☑ Immediately push groups found by this rule

Summary

You now have a fully functional integration of Okta with Office 365. If you have any issues. The following sections detail Okta features that can increase the security and ease of use for your Office 365 deployment.

Improving the Office 365 Experience with Okta

Okta balances two important issues in IT

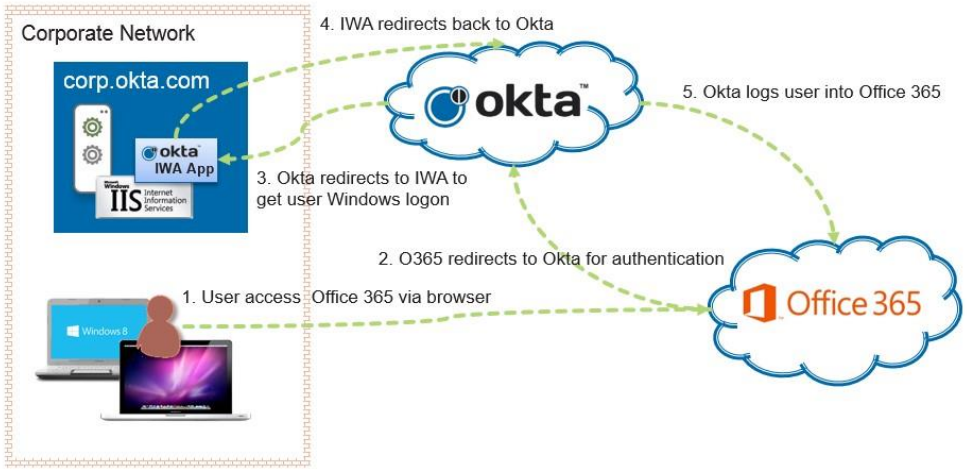
- Improving a user's computing experience.
- Securing the applications they use.

The following sections guide you through using features in Okta to maintain this balance and elevate your use of Office 365.

The Integrated Windows Authentication Desktop SSO Experience

Office 365 is the evolution of a lot of on-premises services for email, document collaboration and file servers. Traditionally those on-premises services leveraged the tight integration of Windows desktops with Active Directory and their user accounts. Therefore, it is common for a customer to have users on Microsoft Windows operating systems that are part of a Microsoft Active Directory domain. By logging into a Windows desktop, the Active Directory services provide a desktop SSO experience. Cloud services were unable to communicate back to Active Directory to verify the Windows credentials of the logged in user.

Okta has a solution for this by implementing a simple web service inside your Active Directory environment. The SSO IWA Web App runs in Microsoft's IIS server and is used to pick up the existing credentials of a user logged into either a Windows desktop or a domain joined OSX computer.


Corporate Network
corp.okta.com
okta
IWA App
IIS Internet Information Services
4. IWA redirects back to Okta
okta
5. Okta logs user into Office 365
3. Okta redirects to IWA to get user Windows logon
2. O365 redirects to Okta for authentication
1. User access Office 365 via browser
Windows 8
Office 365

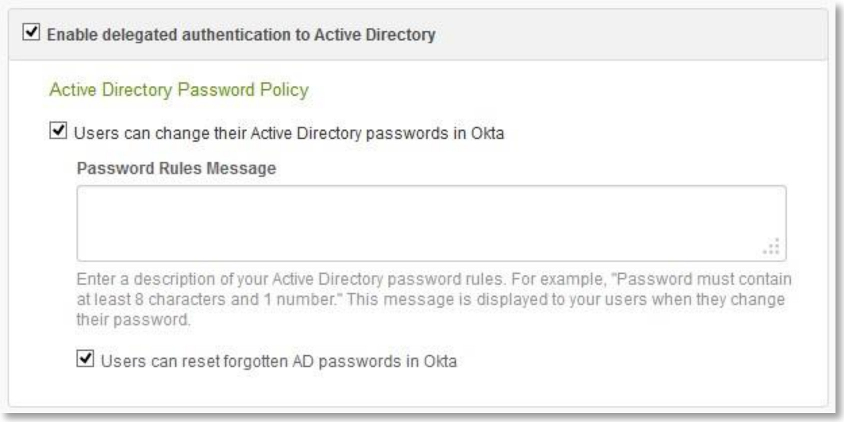
Okta decides to redirect the user to the IWA app based on the IP address of the incoming request. If the user is coming from a known corporate network point, then they are redirected to the local

Okta IWA App running in IIS. This picks up the users Windows credentials and maps them to the Okta user account. If the user has been assigned the Office 365 app, Okta signs the user into the service.

For details about setting up IWA for your organization, see Configuring Desktop SSO on the Okta support website.

Password Reset from Okta to AD

Another useful Okta feature is having a web-based point of access for resetting your password. When Okta is the identity provider for applications, users can change an existing or reset a forgotten password, saving time and reducing help desk requests.



☑ Enable delegated authentication to Active Directory

Active Directory Password Policy

☑ Users can change their Active Directory passwords in Okta

Password Rules Message

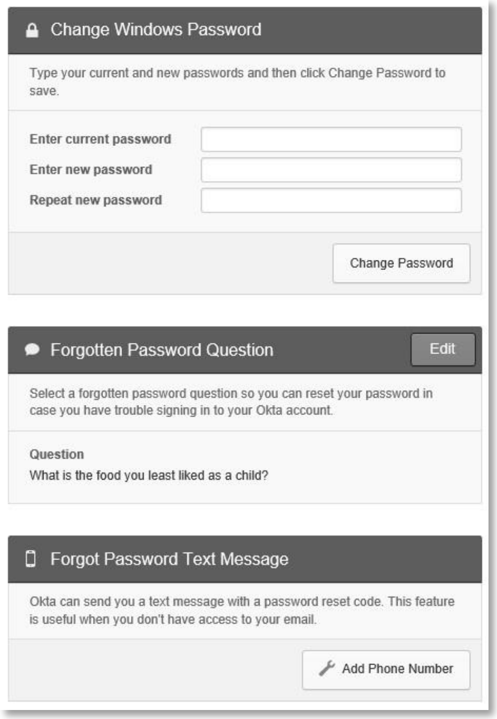
Enter a description of your Active Directory password rules. For example, "Password must contain at least 8 characters and 1 number." This message is displayed to your users when they change their password.

☑ Users can reset forgotten AD passwords in Okta

To enable the ability to both change and reset the password, navigate to **Security >**

Authentication. Edit the **Delegated Authentication** section and check the boxes as shown above. Use the **Password Rules Message** field to inform users of your organization's AD password policy.

Once this is enabled, a user can then navigate to their account and change their password. From the Okta portal, a user selects **Settings** in the top right menu. From here they can edit several related password items, as shown below.



Change Windows Password

Type your current and new passwords and then click Change Password to save.

Enter current password

Enter new password

Repeat new password

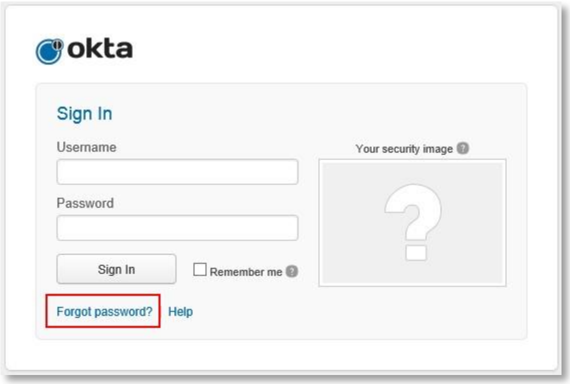
Forgotten Password Question

Select a forgotten password question so you can reset your password in case you have trouble signing in to your Okta account.

Question
What is the food you least liked as a child?

Forgot Password Text Message

Okta can send you a text message with a password reset code. This feature is useful when you don't have access to your email.



Changing the Windows password causes Okta to communicate with one of the Okta AD agents and to pass the password reset to the local Active Directory infrastructure. This feature doesn’t require that the Okta agent service account have write access to Active Directory.

The forgotten password question and text message are used for the password reset process. Password reset is accessed through the Okta login page or by navigating directly to the URL below:
https://yourcompany.okta.com/reset-password

Increasing the Security of Office 365 Access

The previous features are designed to simplifying user access to applications. Okta also has a range of features that work in conjunction with those features to provide increased app security.

Multifactor Authentication

By default, Okta provides one-factor authentication—your username and password. But many companies want to increase the methods by which they identify valid users. In the security realm, factors of authentication are often grouped into three categories:

- What you *know* (your own username and password)
- What you *have* (a token, phone or security device)
- Who you *are* (a physical characteristic such as a fingerprint)

But using more than just a username and password to authenticate a user, you are using multiple factors of authentication (MFA). Okta has pre-integrated a range of services to provide increased security through the use of multiple factors. You can see the list of currently supported MFAs options by accessing the **Security** tab, selecting **Authentication** and the clicking on the **Multifactor** tab. Here you can see a list of all currently supported MFA options. For some, there are extra tabs to the right for further configuration.

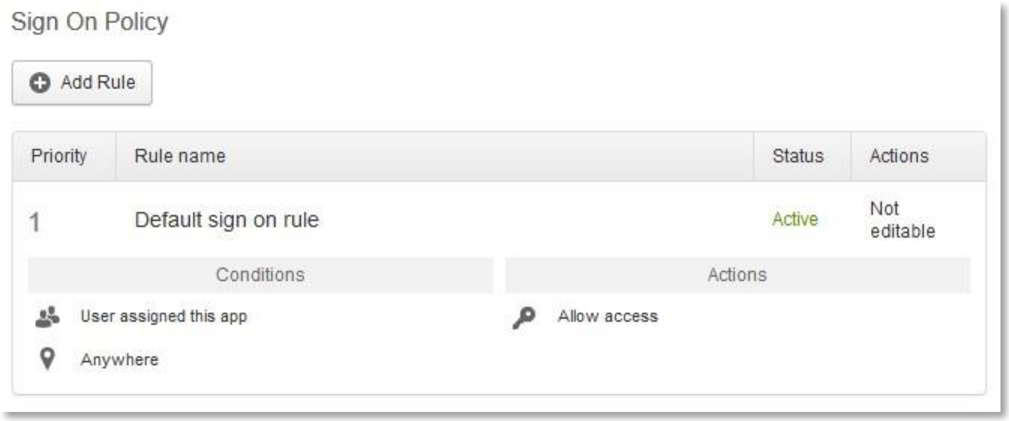
Out of the box Okta offers mobile app based MFA with Okta Verify and Google Authenticator as well as a SMS solution. When you enable any MFA option, you also have the ability to fine-tune when this feature is required for the user. This is an important part of configuring your Okta deployment; you always want to balance the needs for security with the impact to the user.

Okta Sign On Policy allows you to determine if you enabled MFA for signing into Okta, as opposed to requiring MFA on a per application basis, see the next section for more detail on that. If you enable MFA for all users signing into the Okta service, you can determine how often the request for the additional factor happens. You can also apply this to only a specific group of people, for example non-employees who might be a higher risk to handling your corporate information.

Another way to balance the use of MFA is by using the IP address the user is coming from. Okta can switch off MFA if the user is not on the corporate network. This is basically adding another authentication factor, What you are, by saying that if you are physically in a company office, then you must have passed the security measures to get into the building. For more details about configuring multifactor authentication, see the Configuring Multifactor Authentication on the Okta support website.

App Sign On Policy

You don’t have to apply MFA across all users logging into Okta. If you want, you can apply a sign on policy at the application level. This is useful if you don’t want to impact all of your users, only those accessing critical applications.



Sign On Policy

Priority	Rule name	Status	Actions
1	Default sign on rule	Active	Not editable

Conditions	Actions
User assigned this app	Allow access
Anywhere	

Navigate to the **Sign On** tab of your Office 365 application, (**Applications** > **Office 365**) and scroll down to the **Sign On Policy** section, a picture of which is show above. By default there is one rule. If a user is assigned the app in Okta, they are allowed to access the target service from anywhere. Clicking on **Add Rule** allows you add multiple rules to define how access to the application is controlled. The rules are broken down into two main sections:

- Conditions for whom the rule applies. You can specify users who have already been assigned the app, filter by group and also use their location.
- Conditions for what access action is allowed. They are either allowed or denied access, or allowed only with the use of another factor.

The rules allow you to setup scenarios where you can deny access to Office 365 if the user is not on the corporate network and enforce MFA for all those in the contractors group. The ability to deny access to Office 365 is usually only used in combination with network location. If you setup a deny rule and base it on group membership, there will be users who see the Office 365 icon on their Okta portal but will never be able to access it. This might result in a confusing and frustrating experience for users, so be careful and always try to achieve a balance between security and the impact to users.

For details on setting up per app sign-on policies, see Configuring Application-Level Multifactor Authentication on the Okta support website.