Microsoft

2018

Migrating Your Applications to Azure Active Directory

Table of Contents

Migrating your Apps to Azure AD

Why Bother?

Today, your organization requires a whole slew of applications for your users to get their work done. Users access these applications from a vast range of devices and locations, and new apps are being added, developed, and retired every day. At the same time this is happening, we've heard from our customers that today's business goals of **managing cost**, **managing risk**, **improving user productivity**, and **addressing governance and compliance needs** are becoming more critical than ever.

In this fast-moving environment, bringing your application authentication and authorization to Azure AD provides you a host of benefits:

Managing Cost

- **Reduce dependencies on on-premises identity and access management systems**. Migrating your authentication to Azure Active Directory enables you to retire your on-premises AD FS system if desired, reducing licensing and infrastructure costs.
    - Setting up Azure AD as the trust decouples the application from the on-prem credential approach in your tenant, which gives you flexibility to move from federation to Azure AD password hash sync or to pass-through authentication and reduce on-premises infrastructure in the future. To learn more about choosing the right sign-in method for your organization, see this article on the topic.
    - Using the Azure AD Application proxy technology can also enable you to reduce infrastructure requirements further by reducing or eliminating the need for a DMZ and expensive network proxy solutions. To learn more about the Azure AD Application Proxy, see How to provide secure remote access to on-premises applications.

Managing Risk

- **Improve access security** – Secure user access to applications and associated corporate data using conditional access policies, Multi-Factor Authentication, and real-time risk-based Identity Protection technologies.
- **Protect high-privilege accounts** – Protect privileged access to the environment through just-in-time admin access.
- **Stop worrying about availability and reliability** – The multi-tenant, geo-distributed, high availability design of Azure AD means that you can rely on it for your most critical business needs. Azure AD runs out of 28 data centers around the world with automated failover. Consequently, Azure AD is highly reliable and even if a data center goes down, copies of your directory data are live in at least two more regionally dispersed data centers and are available for instant access.

Increasing Productivity

- **Improve your end user's experience** – Improve end-user Single Sign-On experience through seamless and secure access to any application, from any device and any location, including deep integration to Windows, Office, Intune, and Information Protection technologies.

- **Enable delegation and self-service** – Leverage self-service identity and access management capabilities, such as password reset, group management, and application access requests to empower end-users and reduce administrative overhead.
- **Increase administrative efficiency** – Reduce administrative overhead by managing only a single identity for each user across cloud and on-premises environments. Azure AD, as an identity provider for SaaS apps, supports additional capabilities such as:
    - Automated provisioning of user accounts (in key Azure Marketplace apps) based on Azure AD identities.
    - Independent token signing certificates per app, reducing the rollover impact
    - Configurable certificate expiration dates.
- **Empower your developers** – Enable developers to secure access to their applications and improve end-user experience by using a common identity with modern authentication and authorization protocols and APIs.
- **Empower partners** -- After sign-on to SaaS apps is based on Azure AD, you can give partners access to cloud resources with Azure AD B2B collaboration. This removes the overhead of setting point to point federation with your partners.

Addressing Compliance and Governance

- **Meet your compliance requirements** – Ensure compliance to regulatory requirements by enforcing corporate access policies and monitoring user access to applications and associated data using integrated audit tools and APIs.

With that said, we've heard from the same customers, who see these benefits and are interested in all that Azure AD has to offer, that understanding and breaking down their entire app ecosystem and understanding which apps to move first and the steps involved can be challenging. Fortunately, through these discussions, we've learned that breaking this into four phases will help you to understand which apps to start with and start your migration journey quickly. You'll learn about what Microsoft recommends you do to discover, classify, migrate, and manage your apps, and all of the great tools we provide to get all your apps up and running quickly and efficiently.

Getting Started is Easy

What we've heard from customers

When it comes to thinking about all the apps in use in your organization today, we understand there are a lot of variables to consider, and tons of questions that come up along the way. We know this because, we've had a bunch of great opportunities to connect directly with customers of all sizes and talk with them about how their organizations use apps today. Here are some of the challenges we've heard from them:

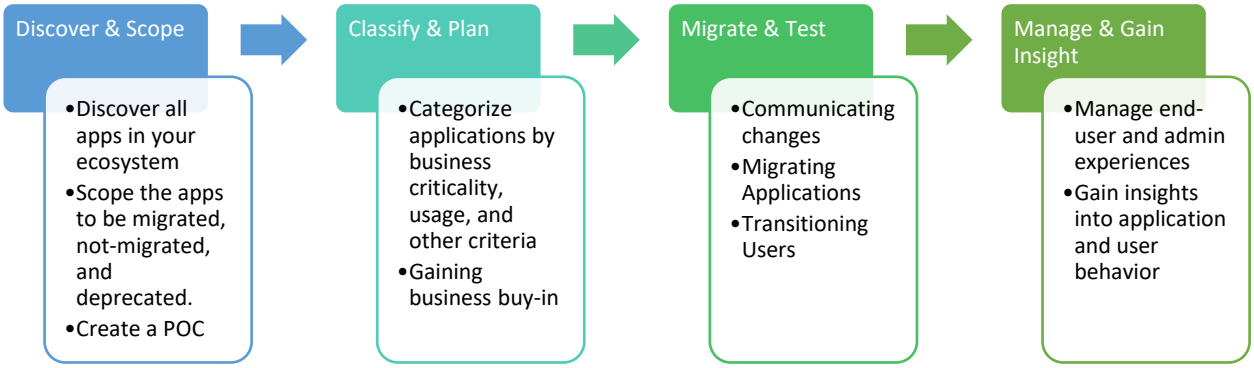
- There are tons of apps in scope for my migration! So many that I don't even know how many there really are 😊.
- I've got a good sense of how many apps I have, but they are each so complex and different from one another that it's tough to get them into an ordered list for my organization to come up with a plan to make progress.
- I've got a bunch of apps in Azure AD today. So, I have a good handle on certain classes of apps, but I've got this one really complicated one for which I'm not quite sure what to do.

- I'm afraid of breaking my user's experience as part of the transition process, what should I do?
- I'm totally in on Azure AD! Now how do I show my business the progress we've made, that users have what they crave, and all the money we've saved?

Fortunately, Azure AD provides a complete set of application discovery, migration, audit, and analytics tools and guidance that will get you migrating in no time at all.

The Phases of Migration

Before we get into the tools you should understand how to think through the migration process. Through several direct-to-customer workshops we've held on-site here in Redmond and abroad, we've found that almost all app migration projects can be broken into the four distinct phases listed below.



Next, we'll walk through these phases, describing what Azure AD tooling and guidance will help – and what success looks like – In each stage.

Phase 1: Discover the apps you have

In the **Discover & Scope** step, you take inventory of all the apps currently in use in your organization. These apps may range from that 15-year-old web app doing HTTP-based authentication to SiteMinder, a modern SaaS app connected through a federation solution, native Windows or Kerberos authenticated apps, or more modern web apps using open authentication standards like SAML or oAuth 2.0. Your users may be accessing these apps from company portals, direct browser bookmarks, links that are pushed down to their mobile devices, or from a native desktop client authenticating to your domain.

It may seem like a tangled and confusing web, but we've found customers are very successful by breaking the problem down into three parts. You can do this, too! First, by understanding what places you need to look, then by finding the apps connected to those systems, and finally by narrowing the list of found apps down to those the business agrees are in scope for your migration project.

Understanding Systems in Scope

There are two effective ways to understand how to find what systems to look for your apps: based off **system architecture** and based off **user access patterns**. Taking a system architecture-based approach will result in finding 70-90% of your apps and is a fantastic way to get started quickly. For the remaining 10-30%, the process may take a bit longer, but we've seen customers reach 95%+ coverage simply by adding to the list of apps discovered in the first stage by inspecting common user entry points to their apps ecosystem.

Types of Systems to Consider

Here are some of the most familiar places apps live that you can start with:

- Apps connected to an on-premises federation solution (ADFS, Ping, etc.)
- Apps connected directly to Active Directory (Kerberos Auth, Windows Integrated Auth, etc.)
- Apps running in on-premises web infrastructure (IIS, Apache, etc.)
- Apps running in cloud-hosted infrastructure (Azure, AWS, etc.)

Types of User Access Patterns to Consider

Once you do an analysis of your systems, you should also consider the types of apps your users use today and where they are coming to use them:

- Apps linked from a company homepage or portal
- Apps users bookmark on their browsers
- Apps your executive team uses
- Apps that may be used by a small number of users, but are considered business-critical
- Apps for which you've pushed links directly to user's desktops or mobile devices via an MDM/MAM solution

  ✓ **Microsoft recommends** that since finding the apps which fall into this category can be a bit of a slower process, so we'd recommend you start with the systems architecture-based approach, and then add to that list later by considering the areas above.

Find your Apps

Now that you have a good understanding of the systems and access patterns in scope, the next step is to find the apps your users use today. There are two approaches here: through out-of-box Azure AD tooling, and through other, more manual means.

Finding Apps Using Automatic Tooling

For apps connected to your **on-premises IDP**, consider using the following approaches to discover the apps being used in your tenant:

- Review **Sign In Logs** for your on prem IDP. Organizations using Active Directory Federation Services (ADFS) can deploy Azure AD connect health to start analyzing on premises traffic. Learn More about Azure AD Connect Health

  ✓ **Microsoft recommends** deploying Azure AD connect health to analyze the app usage in your On Prem environment (if using ADFS). After completing your migration, deploying Cloud Discovery will allow you to continuously monitor Shadow IT in your organization once you're in the cloud.

- Deploy **Cloud Discovery** to identify applications in use in your organization. Cloud Discovery analyzes your traffic logs and matches it to its continuously growing catalog of applications. Learn More about Cloud Discovery

For apps connected to **cloud infrastructure** you can use the APIs and tools on those systems to begin to take an inventory of hosted apps:

- Enumerate your Azure Websites through the Azure Service Management PowerShell interface. Learn more about Get-AzureWebsite
- Find all your Azure Web Apps through the Azure Service Management PowerShell interface. Learn more about Get-AzureRMWebApp
- Find all the apps running on Microsoft IIS from the Windows command line. Learn more about AppCmd.exe
- Use your favorite hosted solution's provider API to enumerate apps connected through those systems. Learn more about how to enumerate Applications and Service Principals on Azure AD

Finding Apps Using Manual Processes

Once you've taken some of the automated approaches described above, you'll probably find you have a good handle on most of your apps. However, you might consider also doing the following to ensure you have good coverage across the various user app access patterns described earlier.

- Contact the various business owners in your organization to identify the applications in use in your organization.
- Run an HTTP inspection tool on your proxy server, or analyze proxy logs, to see where traffic is commonly routed.
- Review web logs from popular company portal sites to see what links users access the most.
- Reach out to executives or other key business members to ensure business-critical apps are covered.

Classify in-scope applications

Scheduling the migration of your apps is an important exercise in and of itself. Not every app needs to be migrated and transitioned at the same time. Understand what apps are present in the environment and assess the challenges and impact each one has. With the information that has been collected about each of the apps, you can rationalize which apps should be migrated first and which may take additional time.

One way to think about this is along the axes of business criticality, usage, and lifespan, each of which may all be made up of multiple factors. Within your organization, you should determine these factors, and assign a points value to the individual factors, and to the areas at large. Following are some guidelines you may want to consider.

Business Criticality

Business criticality will take on different dimensions for each business, but two measures you should consider are features and functionality and user profiles. Apps with unique functionality should be assigned a higher point value than those with redundant or obsolete functionality.

Features and functionality

User profiles

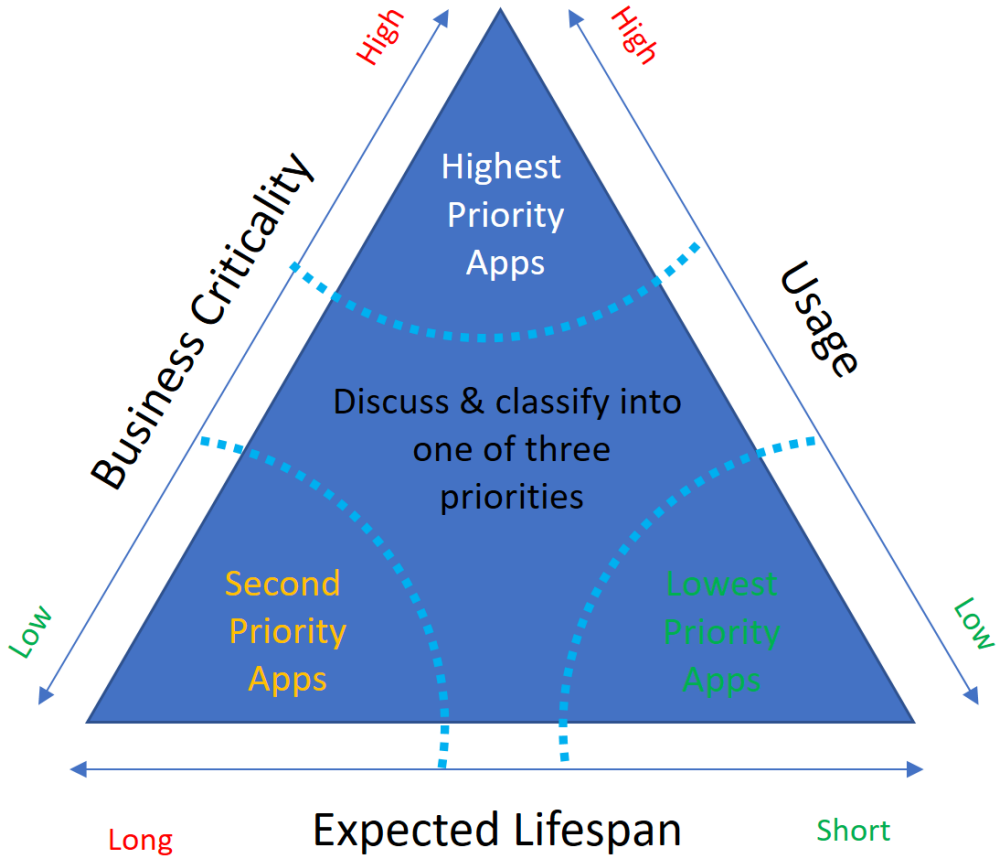
Usage

Applications with high usage numbers should receive a higher value than apps with low usage. Apps with external, executive, or security team users should be assigned a higher value than other apps. For each app in your migration portfolio, complete these assessments.

User Volume

User Breadth

Once you have determined values for business criticality and usage, you can then determine application lifespan, and create a matrix of priority. One such matrix follows.



Begin by selecting those apps in the **high priority** bucket, and the proceeding to those **second priority** apps next. Depending on what you find in the **discuss** category in the middle, and the outcomes of the deliberations you have within your IT and business organizations, you may choose to pull in apps from the center into the **high** or **second** priority buckets. But, you'll probably find that most of your apps are squarely in one or the other.

For apps in the **lowest priority** category, you can safely scope these out for now. Although, we'd recommend you keep them in your list for consideration, because later we'll get into how you can understand the relative effort required for each type of app in your organization. It could be that some of these apps in the **low priority** category are trivial to move and should be brought under consideration for that reason.

Exit Criteria

Success in this stage is defined as:

- A good understanding of the systems in scope for your migration (that you can retire once you've moved to Azure AD!)
- A list of apps that includes:
    - What systems those apps are connected to
    - Where users access them from

    - Usage volume to the app
    - Business criticality of the app
    - Lifespan / future of the app
- The beginnings of a prioritized list based off the relative priority buckets defined above

In the next stage, we'll begin to **classify** these apps further by how easy they are to move, and what you can get started with quickly.

Phase 2: Classify the apps you found & plan your migration

One of the toughest challenges we've seen our customers face is understanding how to **classify** the apps in their system in a way that allows them to move forward with large migration projects. It's a common (and very human) condition to suffer from a bit of analysis paralysis when faced with a list of hundreds of disparate and potentially complicated apps.

It's also a commonly held belief that you must understand everything there is to know about an application's configuration before it can be migrated. However, it turns out that you only need to know some quite basic information about how the app authenticates to get going with migrating your apps to Azure AD quickly.

Types of Apps

Working with customers, we've found that almost all applications in organizations today fall into just two categories:

- Existing apps you want to migrate to native cloud authentication, which may need to be modernized.
- On-premises apps you want to keep on-premises and extend to the cloud

Apps you want to migrate to cloud authentication

These apps fall into two categories:

New line of business (LOB) apps under active development during your migration project

These are perhaps the most exciting app types for our customers, as by moving to Azure AD for core authentication and authorization unlocks all the power and data-richness that the Microsoft Graph and Intelligent Security Graph have to offer.

> ✓ **Microsoft recommends** for apps in this category, consider updating those applications using legacy authentication or other standards to native Azure AD Authentication and Authorization using the OAuth 2.0 / OpenIDConnect framework. Get started with the Microsoft Graph

Existing (LOB) apps you're migrating to Azure AD

These apps fall into two categories:

- Any line of business or third-party SaaS application connected to on an existing on-premises federation solution or IDP
- Your custom line of business applications running in cloud infrastructure.

These apps will probably make up most of the apps in your organization today, and will be the bulk of the apps you end up migrating the Azure AD. In the **plan** section, we'll get in to how you can start to break down the apps in these categories to help you get migrating quickly. Learn more about application types and single sign-on modes

- ✓ **Microsoft recommends** for apps in this category:
  - If the app is a 3rd-party SaaS app, use the **Azure AD Application Gallery** to search our catalog of thousands of apps, and connect them quickly to Azure AD using our application integration tutorials using password vaulting or SAML standards.
  - If the app is an existing line of business app that you don't plan to modernize, use the custom application feature to enable SSO using those same password vaulting or SAML standards.
  - Finally, consider modernizing any long-lived line of business apps to native Azure AD Authentication so you can extend them with all the power of the Microsoft Graph set of APIs.

On-premises apps you're extending to the cloud

These apps fall into a few categories:

- Apps you want to keep on-premises for compliance or control reasons
- Classic (or legacy) apps connected to an on-premises identity or federation provider that you want to secure with Azure AD conditional access technologies
- Applications your business has developed using on-premises authentication standards that you have no plans to modernize (Windows Integrated Authentication, Kerberos Constrained Delegation, HTTP Headers-based authentication)

What distinguishes these apps from the previous group is that either you need to keep these apps running on-premises for business reasons, or otherwise do not have plans to migrate them to cloud infrastructure any time soon. These apps are prime candidates for extending to Azure AD securely using the Azure AD Application Proxy. This can bring great benefits to older apps, as you can enable modern Azure AD security and governance features like Multi-Factor Authentication, Conditional Access, Identity Protection, Delegated Application Access, and Access Reviews against these apps without touching the app at all! Get started with the Application Proxy

- ✓ **Microsoft recommends** for apps in this category, get going quickly!
  - Start by extending these apps into the cloud with the Application Proxy using simple means of authentication (like Password Vaulting) to get your users migrated quickly.
  - Next, work on configuring more native forms of authentication (like Windows Integrated Authentication, Kerberos, or HTTP-headers) for those that support it.
  - Finally, after you have your initial set completed, modernize those that make sense with native Azure AD Authentication and get them running on cloud infrastructure.

Classifying and Prioritizing Apps

Now that you have a good understanding of the broad categories of applications in your environment, it's time to get specific. Fortunately, understanding your apps deeply enough to get a sense of which ones will be easy to start with and which can come later is straightforward.

Details to Gather about your Apps

First, start by gathering key details about your applications. Doing so will help you to make your migration decisions quickly and get a recommendation out to your business group in no time at all.

Information that is important to making your migration decision includes:

- **App Name** – what is this app known as to the business?
- **App Type** – is it a 3rd party SaaS app? A custom line of business web app? An API?
- **Business Criticality** – is it high criticality? Low? Or somewhere in between?
- **User Access Volume** – does everyone access this app, or just a few people?
- **Planned Lifespan** – how long will this app be around? Less than 6 months? More than 2 years?
- **Current Identity Provider** – what is the primary IDP for this app? Or does it rely on local storage?
- **Method of Authentication** – does the app authenticate using open standards?
- **Whether you plan to update the app code** – is the app under planned or active development?
- **Whether you plan to keep the app on-premises** – do you want to keep the app in your datacenter long-term?
- **Whether the app depends on other apps or APIs** – does the app currently call into other apps or APIs?
- **Whether the app is in the Azure AD gallery** – is the application currently already integrated in the Azure AD Application Gallery?

Additional data that will help you later, but that you don't need to make an immediate migration decision includes:

- **App URL** – where do users go to access the app?
- **App Description** – what is a brief description of what the app does?
- **App Owner** – who in the business is the main POC for the app?
- **General Comments or Notes** – any other general information about the app or business ownership

Deciding How to Migrate

You have three main options for migration in Azure AD that map to the three types of apps described above:

- **Register or consent** to a new app, which can be used for:
  - Single-Tenant apps you plan to modernize or create.
  - Multi-Tenant apps you want to share with business partners.
  - Multi-Tenant apps built on Azure AD that you want use in your organization.
  - Multi-Tenant apps you want to get into the Azure AD Application Gallery so the whole world can use them.
- Integrate an app from the **Azure AD Application Gallery**, or a custom app, which can be used for:
  - Thousands of 3rd Party SaaS applications (**Gallery App + Password or SAML Single Sign-on**)

    - Simple URLs you wish to publish to a user's access panel (**Custom Non-Gallery App + Linked Single Sign-on**)
    - Single-Tenant apps that sign in using local application storage / a web form username and password prompt (**Custom Non-Gallery App + Password Single Sign-on**)
    - Single-Tenant apps that sign in using open standards like SAML (**Custom Non-Gallery App + SAML Single Sign-on**)
- **Extend an existing app** from on-premises using the Application Proxy, which can be used for:
    - Simple URLs you wish to publish to a user's access panel (**App Proxy + Linked Single Sign-on**)
    - On-premises web apps that sign in using local application storage / a web form username and password prompt (**App Proxy + Password Single Sign-on**)
    - On-premises web apps that sign in using HTTP headers-based authentication (**App Proxy + HTTP Headers Single Sign-On**)
    - On-premises web apps that sign in using Integrated Windows Authentication or Kerberos Auth (**App Proxy + Windows Integrate Auth Single Sign-On**)
    - Common on-premises native client workloads (**App Proxy + Remote Desktop, SharePoint, Microsoft Teams, Tableau, Qlik**)

Exit Criteria

Success in this stage is defined as:

- A list of the top 10 or more apps you'll start considering migrating based off business priority, usage volume, and lifespan, along with an understanding of the steps Microsoft recommends for you to get going quickly.

In the **migrate** stage, we'll give you resources you can use to migrate each class of apps you describe above.

Phase 3: Migrate and test your apps

Tools to Migrate Apps to Azure AD

Use the tools and guidance below to help you move your apps to Azure AD.

- **General migration guidance** – use the whitepaper, tools, email templates, and applications questionnaire in the Azure AD Apps Migration Toolkit to discover, classify, and migrate your apps.
- **SaaS applications** – see our list of hundreds of SaaS App tutorials and the complete Azure AD SSO Deployment Plan to walk through the process end-to-end
- **Applications running on-premises** – learn all about the Azure AD Application Proxy and use the complete Azure AD Application Proxy Deployment Plan to get going quickly
- **Apps you're developing** – read our step by step integration and registration guidance

Next, let's test your apps to make sure everything is working correctly.

How to Test

Once you migrate, ensure you've done the following to enable you to test:

- Find the application in the list of **All Applications** under **Enterprise Applications** in the **Active Directory** extension from within the Azure Portal.
- Ensure you have at least one user or group assigned to the app by navigating to **Users and Groups** and assigning them there.
- Ensure you are not blocking access to the application with a Conditional Access policy by reviewing your list of policies from the **Conditional Access** navigation path under the application.

Next, depending on how the application is configured, ensure you've done the following to verify that single sign-on works properly.

- If the application uses **OAuth / OpenIDConnect**, navigate to the application URL and ensure you have consented to the application to be used in your organization. Ensure you are not blocking by reviewing the **Users can consent to apps** setting under the **User Settings** node of **Enterprise Applications**.
- If application uses **SAML-based** single sign-on, use the **Test SAML Settings** button found under **Single Sign-On.**
- If the application uses **Password-Based** single sign-on, ensure you have the My Apps Secure Sign-In Extension installed and navigate to myapps.microsoft.com as an assigned user to test the app.
- If the application is extended using the **Application Proxy**, ensure your connector is running and assigned to your application, and review the Application Proxy troubleshooting guide for further assistance.

If you run into problems, check out our apps troubleshooting guide to get help.

Exit Criteria

Success in this stage is defined as:

- Your highest priority apps migrated and piloted within your organization
- Single sign-on tested and verified for your top apps
- A scale out plan to get more users accessing your apps over time

Finally, in the **excite** stage, you can learn about all of the cool things you can do with your apps to get users excited and show off insights to your organization.

Phase 4: Excite your users and get insights

Now, you should have a few apps for your users to try out. Here are some of the cool things you can do:

Things you can do for your users

- **Link to your users to any app** – got an app you aren't ready to migrate yet? Use the Existing Single Sign-on feature to get a link to any arbitrary URL right on a user's myapps experience.
- **Let users add apps you curate** – enable Self-Service Application Access to an application and tell your users to click the "add" button on myapps.microsoft.com to see the apps you curate for them.
- **Launch apps from Office** – have your users go to **Office.com**, search for their apps, and have their most recently-used apps appear for them right from where they do work.
- **Launch apps from the Intune Managed Browser** – have your users go to myapps.microsoft.com from their mobile devices to get all of the same single sign on experiences
- **Launch apps from a browser extension** – download the MyApps Secure Sign-in Extension on Chrome, Firefox, or Edge and let your users launch apps right from their browser bar.
- **Auto-redirect to internal URLs using the browser extension** – use the MyApps Secure Sign-in Extension to also automatically convert internal URLs you have configured in the Application Proxy to the appropriate external URLs so your users can work with the links they are familiar with no matter where they are.
- **Link to apps with deeplinks in your company portals** – view the **Properties** of any **Enterprise Application** in the Azure Portal to get persistent deeplinks to apps that you can publish wherever your users go to get access to their apps today.

Things you can do for your business

- **Test apps using a browser extension** – browse to the Single Sign-on section in the Azure Portal with the MyApps Secure Sign-in Extension installed and get automated testing experiences for common errors encountered when setting up Federated Single Sign-on technologies like SAML.
- **Delegate user access** – enable Self-Service Application Access in the Azure Portal to an application and assign a business approver to approve access to those applications. Use self-service groups management for groups assigned to collections of apps.
- **Secure user access** – manage how users can access apps from the Azure Portal under **User Settings** from **Enterprise Apps**. Enable Conditional Access Policies or Identity Protection to secure user access to applications based off device state, location, and more.
- **Delegate admin access** – assign admins the **Application Administrator, Cloud Application Administrator,** or **Application Developer** roles from the **Directory Role** navigation item under a specific **User** in the Azure Portal.
- **Audit your apps** – view all your application changes in a single place from the **Audit** navigation path under **Enterprise Applications** in the Azure Portal. Access the same information from the Azure AD Reporting API to slurp into your favorite tools.
- **Get sign-in insights** – view all your sign-ins in a single place from the **Sign-Ins** navigation path under **Enterprise Applications** in the Azure Portal. This same information can be accessed from the Azure AD Reporting API.

- **Visualize your apps usage** – if you use PowerBI, check out the Azure AD PowerBI Content Pack for cool visualizations of all that is going in your organization.
- **View permissions an app has** – for apps using OAuth / OpenIDConnect, see all of the permissions assigned to them from the **Permissions** navigation path under **Enterprise Applications** in the Azure Portal.
- **See all apps assigned to a user or a group** – check out the **Applications** navigation item under a **User** or a Group from the Azure Portal to see all the apps assigned and drill into permissions and application info for each of those apps.

Do Even more with Deployment Plans

Deployment plans walk you through the business value, planning, implementation steps, and management of Azure AD solutions, including app migration scenarios. They bring together everything that you need to get started deploying and getting value out of Azure AD capabilities. The deployment guides include content such as Microsoft recommended best practices, end user communications, planning guides, implementation steps, test cases, and more.

Many deployment plans are available for your use, and we're always making more! Access all of them at http://aka.ms/deploymentplans, and take our survey to request other plans and let us know if they are useful to you!

- Enable Single Sign-on to a SaaS application
- Enable Single Sign-on to an on-premises application with the Application Proxy
- Automate account management in SaaS applications with outbound user provisioning
- Migrate your authentication from ADFS to the cloud
- Manage risk by implementing Conditional Access
- Manage help desk costs with Self-Service Password Reset
- Take our survey to request other plans…more are coming every day!

Take our survey to shape the future; we'd love your feedback!

If you want to shape the future of apps in Azure AD directly, take our survey!

http://aka.ms/apps-survey

We're always listening, and if you want to get in touch with us directly, send an email to aadappfeedback@microsoft.com.

Getting support from Microsoft

There are several different avenues from which you can get support during your AD FS – Azure AD migration:

Azure Support: Depending on your Enterprise Agreement with Microsoft, you can call Microsoft Support and open a ticket for any issue related to your Azure Identity deployment. For more information on how to get in touch with Microsoft Support, please visit our Azure support portal: https://azure.microsoft.com/support

FastTrack: If you have purchased Enterprise Mobility and Security (EMS) licenses or Azure AD Premium licenses, you may be eligible to receive deployment assistance from the FastTrack program. For more information on how to engage with FastTrack, please refer to our documentation on the FastTrack Center Eligibility Benefit for Enterprise Mobility and Security

Engage the Product Engineering Team: If you are working on a major customer deployment with millions of users, you can work with your Microsoft account team or your Cloud Solutions Architect to decide if the project's deployment complexity warrants working directly with the Azure Identity Product Engineering team.

EMS Blog: Subscribe to the EMS Blog to stay up to date with all the latest product announcements, deep dives, and roadmap information provided directly by the Identity engineering team. Further, you can also post comments and get feedback from the engineering group.

Azure Active Directory Public Forums: Azure AD also has several closely monitored channels available to the public. Here are some useful links:

- StackOverflow using the tags 'adfs'
- UserVoice to submit or vote on new feature requests in Azure AD
- Microsoft Azure on Reddit: https://www.reddit.com/r/AZURE/
- MSDN Forum for Azure AD