

Azure Active Directory **Access Panel** Deployment Plan

**How to use this guide**

This step-by-step guide walks through the implementation of the Access Panel in a five-step process. The links below take you to each of those steps.



**1**

**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_your_Deployment)**

[Your project](#_Planning_your_Deployment)

**3**

**[Design](#_Planning_for_Overall)**

[Policies and integration](#_Planning_for_Overall)

**5**

**[Operationalize](#_Operationalize_your_Implementation)**

[Your implementation](#_Operationalize_your_Implementation)



**4**

**[Implement](#_Implementing_Your_Solution)**

[Your design](#_Implementing_Your_Solution)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

These are general recommendations, and you should only implement if they apply to your specific enterprise needs.

Table of Contents

Contents

[Introduction 4](#_Toc522786166)

[Purpose of document 4](#_Toc522786167)

[Confidentiality statement 4](#_Toc522786168)

[What is the access panel? 4](#_Toc522786169)

[Current state of end user access 4](#_Toc522786170)

[Goals for Azure Active Directory Access Panel Integration 5](#_Toc522786171)

[Stakeholders and Sign-off 8](#_Toc522786172)

[Project Scope 9](#_Toc522786173)

[Tracking Timelines 9](#_Toc522786174)

[Prerequisites 9](#_Toc522786175)

[In scope 9](#_Toc522786176)

[Out of scope 9](#_Toc522786177)

[Business Use Cases 10](#_Toc522786178)

[Planning your Deployment 11](#_Toc522786179)

[General Planning 11](#_Toc522786180)

[Environments and Project Stages 11](#_Toc522786181)

[Licensing Considerations 11](#_Toc522786182)

[Planning for Overall Access Panel deployment 13](#_Toc522786183)

[Full set of capabilities in the access panel 13](#_Toc522786184)

[Best Practices 13](#_Toc522786185)

[Deployment Considerations 13](#_Toc522786186)

[Planning for My Apps Deployment 14](#_Toc522786187)

[My Apps application launcher 14](#_Toc522786188)

[Best Practices 16](#_Toc522786189)

[Deployment Considerations 17](#_Toc522786190)

[Planning Deployment and Support 21](#_Toc522786191)

[Communications Planning 21](#_Toc522786192)

[Support Planning 22](#_Toc522786193)

[Planning Reporting and Auditing 22](#_Toc522786194)

[Implementing Your Solution 24](#_Toc522786195)

[Timelines and Environments 24](#_Toc522786196)

[Phase 1: Implementation Steps 24](#_Toc522786197)

[Solution Components 24](#_Toc522786198)

[Step 1: Application SSO access 24](#_Toc522786199)

[Step 2: Application Self-service Capabilities 26](#_Toc522786200)

[Phase 2: Verify End User Scenarios 27](#_Toc522786201)

[Step 1: Create test cases for your access panel deployment 27](#_Toc522786202)

[Step 2: Document Your Results 35](#_Toc522786203)

[Step 3: Moving into Production 35](#_Toc522786204)

[Phase 3: Rollback Steps 35](#_Toc522786205)

[Operationalize your Implementation 35](#_Toc522786206)

[Purpose of Document 35](#_Toc522786207)

[Required Roles 35](#_Toc522786208)

[Troubleshooting Guide & Steps 36](#_Toc522786209)

[Example: Single account not being able to log into the application. 36](#_Toc522786210)

## What is the access panel?

The access panel is a web-based portal offered by Azure Active Directory that offers a simple hub for users to discover and access all their company’s Azure Active Directory connected resources. In addition to this, the Access Panel provides user’s self-service capabilities such as the ability to request access to new apps and groups or manage access to these resources on behalf of others. This means IT administrators can increase productivity by delegating access management to their line managers and users who can best decide and review who needs access to an app or group.

The access panel is designed to enable enterprises to decrease support costs, reduce user frustration and lost time, and increase user productivity and security. The system includes detailed reporting that tracks when users access the system, along with notifications to alert administrators to misuse or abuse.

## Goals for Azure Active Directory Access Panel Integration

The Microsoft Azure Active Directory access panel will benefit our business in the following ways:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Increase.png | **INCREASE PRODUCTIVITY**  Enabling **single sign-on** across enterprise applications and Office 365 provides a superior log in experience for existing users, reducing or eliminating log on prompts. The user’s environment feels more cohesive and is less distracting without multiple prompts, or the need to manage multiple passwords. Access control can be managed and approved by the business group, saving IT management costs through self-service and dynamic membership, and improving the overall security of our identity system by ensuring the right people in the business manage access to this application. | |  | **INTUITIVE USER EXPERIENCE**  Enabling the access panel provides users with the ability to have a one stop place to launch all their Azure single-sign on connected applications from. Additionally, as more capabilities are enabled like group management and self-service password reset, users continue to have a unified portal to find these settings. The intuitive, easy experience will allow users to get back to work faster and be more productive, while reducing their frustration. The access panel serves as a coherent landing page for a user to quickly find what they need access to and continue their key work tasks. | | \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Within_Your_Reach.png | **MANAGE COST**  Enabling the access panel with Azure Active Directory allows divestment of on premises infrastructures. This reduces support costs by enabling users to have a consistent portal to find all the apps they have access to, request access to resources, and manage their account. Over time costs from change management is also reduced. The enterprise does not have to spend end user training costs for multiple products as users will have a unified experience all through the access panel. | | | | |  |
|  |  | |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Confidentiality.png | | **FLEXIBILITY AND SECURITY**  The access panel enables enterprises to access the security and flexibility that a cloud platform provides. Administrators can easily change settings to applications and resources and accommodate new security requirements and then roll these changes out to users without causing disruption. |
| Magnifying glass | | **ROBUST AUDITING AND USAGE TRACKING**  The auditing and usage tracking capabilities for all the end user capabilities like app access, group access, and self-service password reset makes it easy to see when users are using their resources and ensuring that business systems are stay secure. |
|  |  | |

## Stakeholders and Sign-off

The following roles will be involved in delivering this project. To see a full list of responsibilities and delivery items, see [Implementation Steps and Stakeholders](#_Implementing_Your_Solution).

* Action Required:
  + SO = Sign-off on this project
  + R = Review this project and provide input
  + I = Informed of this project

|  |  |  |
| --- | --- | --- |
| Name | Area | Action |
| Enter name and email | IT Support Manager  A representative from the IT support organization who can provide input on the supportability of this change from a helpdesk perspective. | SO |
| Enter name and email | Identity Architect or Azure Global Administrator  A representative from the identity management team in charge of defining how this change is aligned with the core identity management infrastructure in the customer’s organization. | SO |
| Enter name and email | Business Owner  A representative colleague who can provide input on the user experience and usefulness of this change from an end-user’s perspective and owns the overall business aspect of the application, which may include managing access. | SO/I |
| Enter group alias for pilot group | End Users  The group of users for which the access panel will be implemented for. They need proactive communications that the end user portal is coming, how to find it, and how to use it. [See sample communications](#_Communications_Templates). | I |

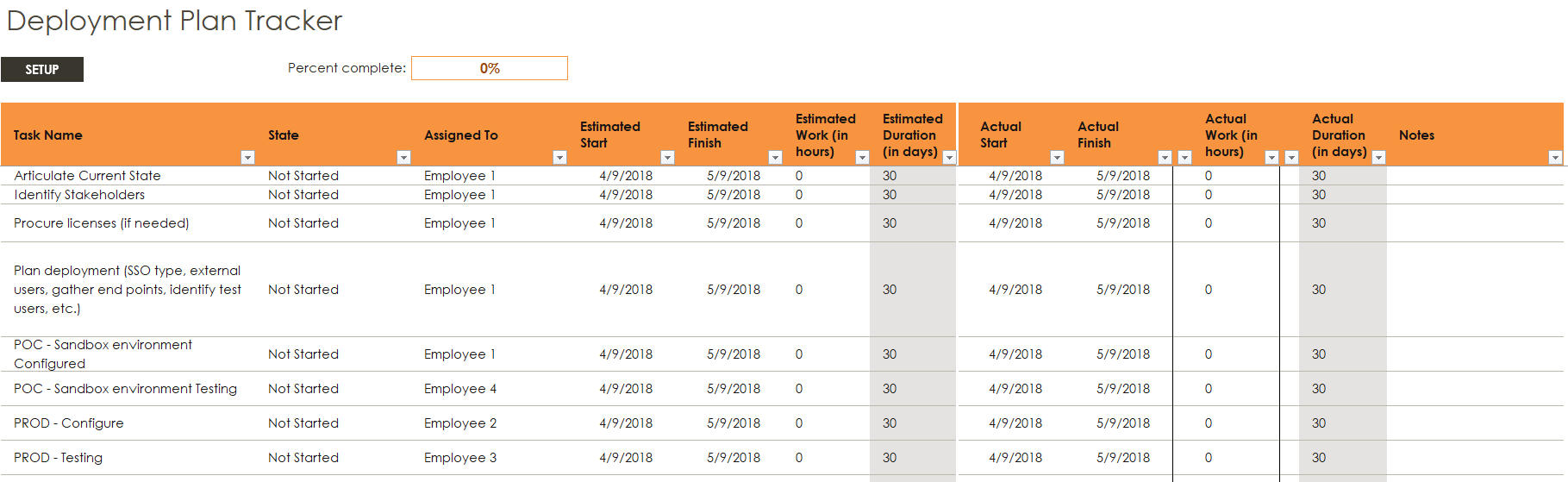
## 

# Project Scope

## Tracking Timelines

Tracking your plan is an important aspect of project success.

You may use the embedded Deployment Plan Tracker spreadsheet below to monitor and schedule your committed timelines for this project. Begin tracking additional items as you progress through the deployment plan that may require an action or prerequisite:



## Prerequisites

The following are presumed to be in place prior to the beginning of this project.

* Application SSO integration plan
* Azure AD user and group infrastructure

## In scope

The following are in scope for this project:

**Deploying the access panel My Apps launcher**

* Assigning applications to users who will be using My Apps for app access
* Enabling self-service application access
* Recommendations on access panel deployment
* Testing the deployment of My Apps (on web and mobile)

**Deployment and Support**

* Configuring end-user communications
* Working with audit logs
* Troubleshooting

## Out of scope

The following are out of scope of this project:

* Deploying additional access panel capabilities such as self-service group management, self-service password reset, multi-factor authentication, and access reviews. For implementation details to this please refer to [insert deployment guides or doc links to other resources].
* Deploying the access panel to external users

## Business Use Cases

The following table outlines the use cases to be implemented during this project.

|  |  |
| --- | --- |
| Area | Description |
| Access | Access panel portal is accessible from corporate devices within the corporate network. |
| Access panel portal is accessible from personal devices within the corporate network. |
| Access panel portal is accessible to corporate devices outside of the corporate network. |
| Auditing | Usage data is available to administrators to audit in near real time. |
| Usage data is downloaded into corporate systems at least every 29 days. |
| Governance | Lifecycle of user assignments to Azure AD connected applications and groups are defined and monitored. |
| Security | Access to resources is controlled via user and group assignments. Only authorized users can manage resource access. |
| Performance | Access assignment propagation timelines are documented and monitored. |
| User Experience | Users are aware the access panel capabilities and how to use them. |
| Users are aware of how to self-manage their access to applications and groups. |
| Users are aware of the access panel account management capabilities and how to use them. |
| Users are aware of browser compatibility. |
| Support | Users are aware of how to find support for access panel issues. |

# Planning your Deployment

## General Planning

### Environments and Project Stages

Project stages are dependent on the environments that you have available. If you have a non-production Azure tenant, you can complete a proof of concept (POC) outside of your production environment if desired.

In the table below, document the Azure AD and AD environments and stages of your project.

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

### Licensing Considerations

The Access Panel is free and requires no licenses to use at a basic all users. However, the number of objects in your directory and the features you wish to deploy may require additional licenses. Common Azure AD scenarios include the following security features:

* [Azure Multi-Factor Authentication (MFA) (P1 Required)](https://docs.microsoft.com/azure/multi-factor-authentication/multi-factor-authentication-how-it-works)
* [Group based membership](https://docs.microsoft.com/azure/active-directory/active-directory-manage-groups) (P1 required)
* [Self-service password requirement](https://docs.microsoft.com/azure/active-directory/authentication/quickstart-sspr) (P1 Required)
* [Identity Protection](https://docs.microsoft.com/azure/active-directory/active-directory-identityprotection) (P2 Required)

The following table describes some of the license requirements that may be relevant. For a full list of license requirements, click [here](https://azure.microsoft.com/pricing/details/active-directory/).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Free | BASIC | | PREMIUM P1 | PREMIUM P2 |
| Directory Objects | 500,000 Object Limit | No Object Limit | | No Object Limit | |
| Single Sign-On | 10 apps per user (pre-integrated SaaS and developer-integrated apps) | 10 apps per user (free tier + Application proxy apps) | | No Limit (free, Basic tiers + Self-Service App Integration templates) | |
| Access based on group membership | Not Available | | | Available | |
| CA based on group and location | Not available | | | Available | |
| CA based on device state (Allow access from managed devices) | Not available | | | Available | |
| MFA (cloud and on-premises) | Not available | | | Available | |
| Identity protection | Not available | | | Not available | Available |
| Self-service group management |  | | | Available | |
| Self-service password reset for cloud-only users |  | | Available | | |
| Self-Service Password Reset for hybrid users (with writeback) | Not available | | | Available | |

**Enterprise Mobility and Security (EMS) subscriptions:**

* EMS E3 includes P1
* EMS E5 includes P2

If you have an existing Enterprise Agreement or Server and Cloud Enrollment, you may already have Azure Premium. Check the details of your agreement.

## Planning for Overall Access Panel deployment

Full set of capabilities in the access panel

### Best Practices

The base level of functionality of the access panel can be enabled gradually with each new feature building upon previous ones enabled. Based on the above table, the recommended order of deployment is from feature set 1-4.

By starting with deploying the My Apps portion of the access panel users can be introduced the portal as a common place for finding access to resources they need. The experience is designed to be streamlined, abstracting away the different types of apps a user might have configured for them. The transition to discovering app launching to group management and profile management settings becomes a fluid roll out and intuitive experience for users to learn to use these new capabilities.

* **Microsoft Recommends**

### Deployment Considerations

If users are currently using an existing company portal, there may be a transition phase needed if you choose to move all users to only use the access panel, rather than support the two portals side by side.

Alternatively, if you choose to maintain the existing company portal. There are options to enable users to still leverage the access panel’s app launching capabilities by integrating this functionality into your existing solutions. This can also be done for other capabilities by leveraging their direct links as much as possible. These considerations will be noted in the Deployment Considerations section for each feature set.

**Implementation plan table**

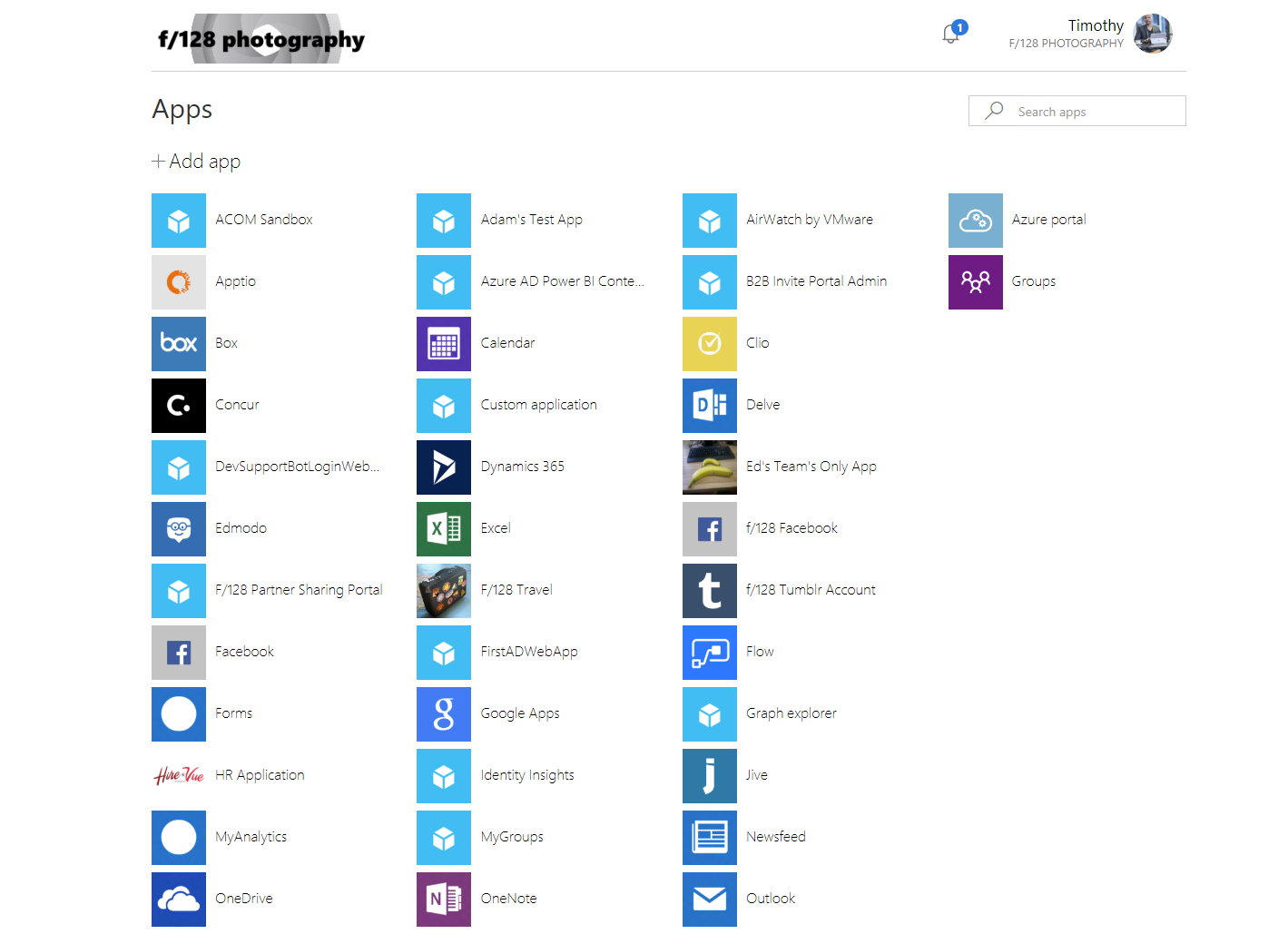
In the below table, record the values you will use when deploying the access panel.

| Configuration | Typical values | Vales to be configured |
| --- | --- | --- |
| Determine the pilot group | Identify the Azure AD security group to be used and ensure all pilot member are a part of the group. | Group: |
| Determine the group or groups to be enabled for production. | Identify the Azure AD security group9s), or AD groups synced to Azure AD, to be used and ensure all pilot member are a part of the group. | Group(s): |
| Allow users to use single-sign on to what types of applications | Federated SSO, OAuth, Password SSO, App Proxy | Value: |
| Allow users to use self-service password reset | Yes | Value: |
| Allow users to use multi-factor authentication | Yes | Value: |
| Allow users to use self-service group management for what types of groups | Security groups, O365 groups | Values: |
| Allow users to use self-service app management | Yes | Value: |
| Allow users to use access reviews | Yes | Value: |

## Planning for My Apps Deployment

### My Apps application launcher

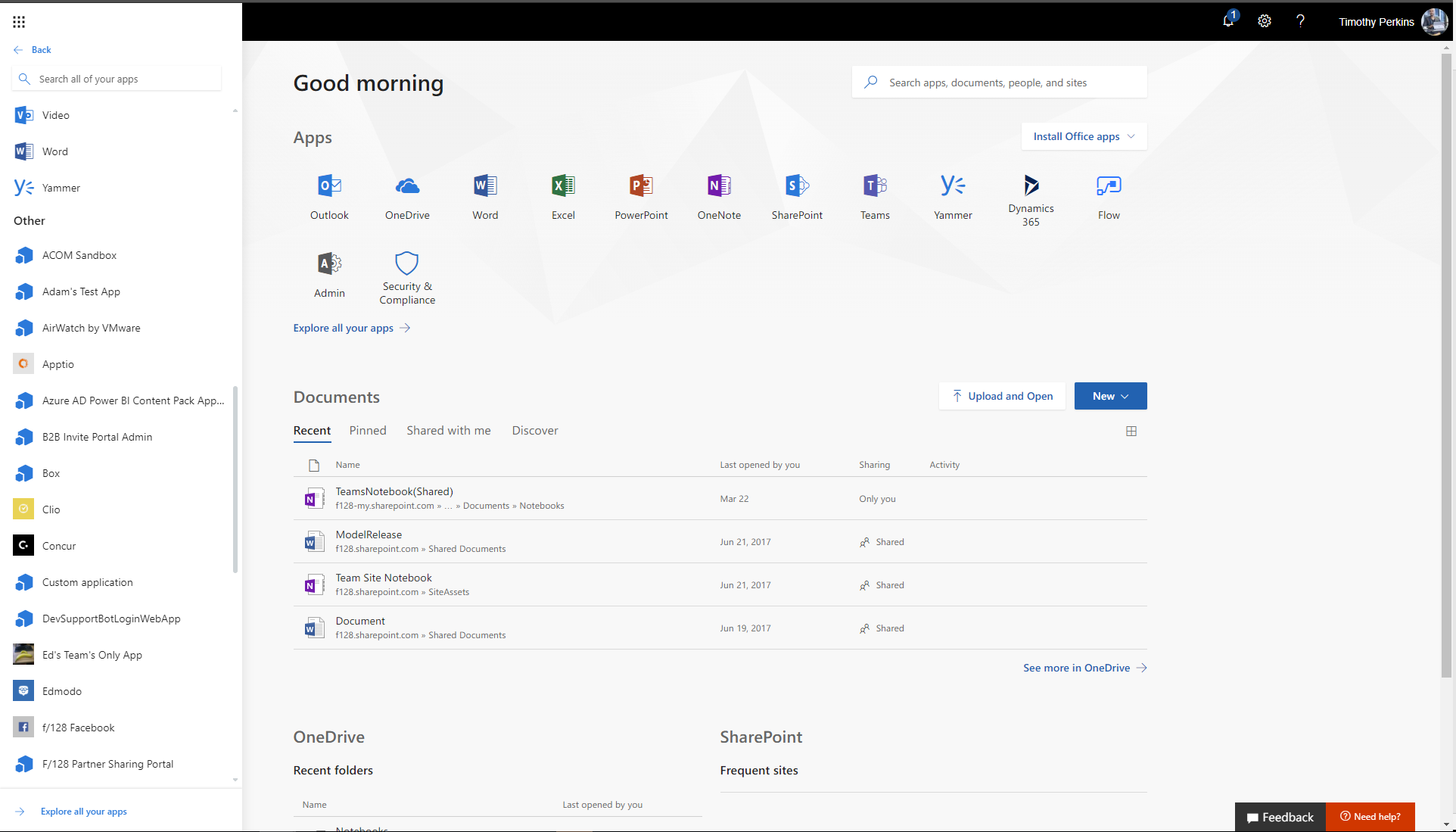
The foundation of the access panel is the app launcher, My Apps. Users can find My Apps by visiting directly [https://myapps.microsoft.com](https://myapps.microsoft.com/). Here users will find a list of all the applications they have been assigned to and have been enabled for SSO for. The My Apps pages gives users a quick place to start their work and get to their necessary applications they need to access to get their day to day tasks done.



Azure AD supports in three different ways to sign in to applications:

* **Federated single sign-on** enables applications to redirect to Azure AD for user authentication instead of prompting for its own password. This is supported for applications that support protocols such as SAML 2.0, WS-Federation, or OpenID Connect, and is the richest mode of single sign-on.
* **Password-based single sign-on** enables secure application password storage and replay using a web browser extension or mobile app. This leverages the existing sign-in process provided by the application but enables an administrator to manage the passwords and does not require the user to know the password.
* **Existing single sign-on** enables Azure AD to leverage any existing single sign-on that has been set up for the application but enables these applications to be linked to the Office 365 or Azure AD access panel portals and enables additional reporting in Azure AD when the applications are launched there. This includes using Azure Application Proxy and the Linked single sign-on mode.

More information about application single-sign on modes can be found here: <https://docs.microsoft.com/azure/active-directory/active-directory-appssoaccess-whatis>

Aside from the My Apps portal, the same applications will also be shown in the Office365 app launcher for convenience when users are using the Office 365 portal.

### Best Practices

#### App launching

For users to have the best experience with the My Apps page, we recommend prioritizing integrating cloud applications available for federated SSO since unlike password-based SSO users will need to take on a dependency on installing the accompanying extension (see My Apps Secure Sign-in Extension requirements). Federated SSO allows users to have a consistent one click experience across their app launching surfaces and tends to be more robust in configuration control.

* **Microsoft recommends** using Federated SSO with Azure AD (OpenID Connect / SAML) when an application supports it, instead of password-based SSO and ADFS.

For more information on how to deploy and configure you SaaS applications please refer to the SaaS SSO Project Plan: [SaaS SSO Deployment Plan.docx](https://microsoft.sharepoint.com/:w:/t/InterviewMode/EUWZ1Ctci7pHkVsdBKMeecMBFAs7V6mgLh6U-OhmtIIh_g?e=Gamagr)

However, if password-based SSO applications are selected a way you should define a mechanism to deploy the extension at scale with [supported browsers](https://docs.microsoft.com/azure/active-directory/active-directory-saas-access-panel-introduction). Options include:

1. [Group Policy for Internet Explorer](https://azure.microsoft.com/documentation/articles/active-directory-saas-ie-group-policy/)

* [System Center Configuration Manager (SCCM) for Internet Explorer](https://docs.microsoft.com/sccm/core/clients/deploy/deploy-clients-to-windows-computers)
* [User driven download and configuration for Chrome, Firefox, Edge, or IE](https://docs.microsoft.com/azure/active-directory/active-directory-saas-access-panel-introduction#my-apps-secure-sign-in-extension)

Learn more: [How to configure password single sign on](https://docs.microsoft.com/azure/active-directory/application-config-sso-how-to-configure-password-sso-non-gallery)

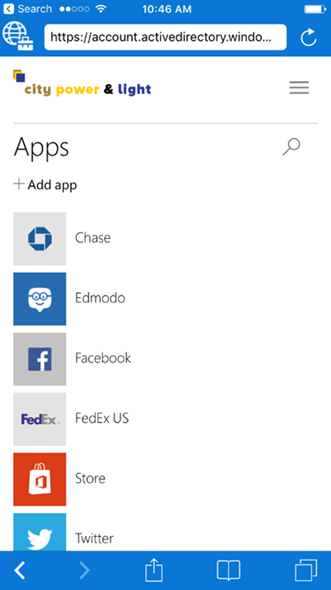
#### Self-service Application Access

Once a core set of applications have been deployed to user’s My Apps page. The recommended progression for the full set of features in My Apps is next enabling the self-service app management features. This allows user to find new apps they may add to their My Apps, this serves to offer optional apps when you may not know who the full set of users at setup time need access to the application. Additionally, if an approval workflow is required such that another user need to approve a request to access the app before the user can use it, this can also be enabled for the application. Users who are approvers will receive notifications within the My Apps portal when there are pending request for access to the application.

* **Microsoft recommends** enabling self-service app access to enable users to easily discover and request access to applications.

#### Mobile My Apps Access- Managed Browser

For the best experience on mobile, we recommend user download the Intune Managed Browser to access their My Apps page. Users do not have to be enrolled with Intune to use the Managed Browser. With the Managed Browser users will automatically find a bookmark to My Apps on the start page. Once signed in they will have the same responsive experience on mobile. Intune Managed Browser is available at the [Apple App Store](https://itunes.apple.com/us/app/microsoft-intune-managed-browser/id943264951?mt=8) and [Google Play Store](https://play.google.com/store/apps/details?id=com.microsoft.intune.mam.managedbrowser&hl=en). Learn more: [Mobile app support](https://docs.microsoft.com/azure/active-directory/active-directory-saas-access-panel-introduction#mobile-app-support)



* **Microsoft recommends** using Intune Managed browser for access to My Apps on mobile.

### Deployment Considerations

#### App Integration in Existing Portals

If an existing portal is already being used as a starting point for users, an alternative option to operationalizing the access panel to end user is the use of “user access URLs”. User access URLs function as direct links to the applications available in the My Apps portal. These can be embedded within any existing website and when a user accesses the link it will take the same effect as launching the application from the My Apps portal.

Example of where to find the **User access URL** property in the **Properties** blade of the application.

A screenshot of a cell phone

Description generated with very high confidence

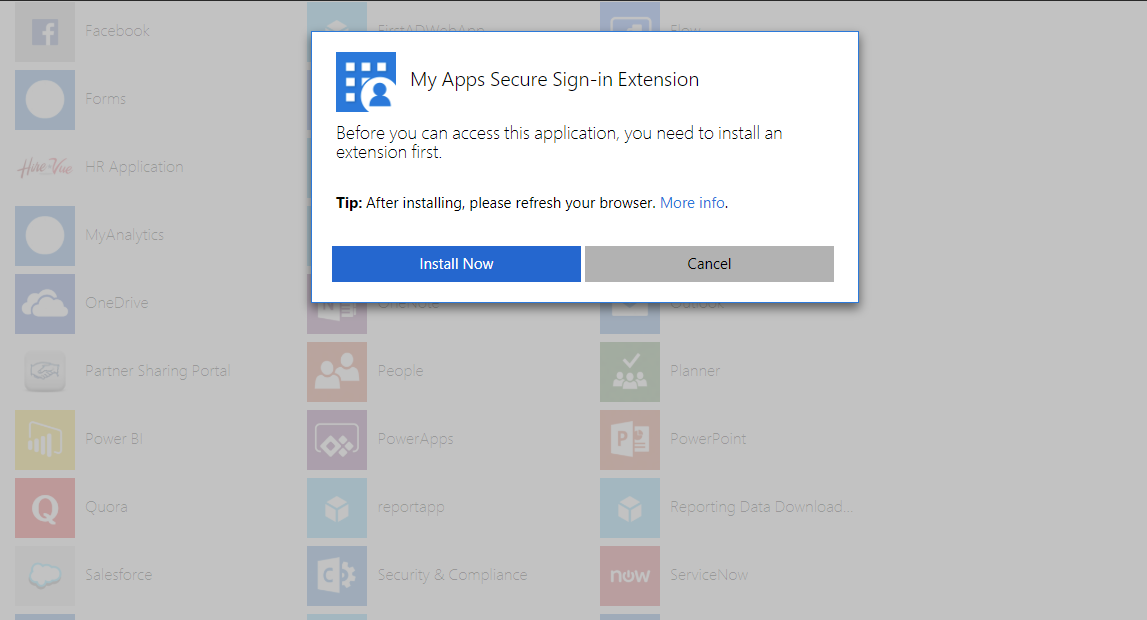
#### Migration from Existing Single Sign-on Solutions

A quick way to start migration of applications for users is leveraging the Linked SSO option. This allows you to configure an application tile on user’s application launches that links to the URL of your existing application. This in effect will allow you to start directing users to the My Apps portal without having to migrate all the applications to Azure Active Directory for single-sign on (SSO). Gradually, the applications can be swapped out for Azure AD single-sign on configured applications and users will not find an interruption in their experience as the applications remain the same on their app launchers.

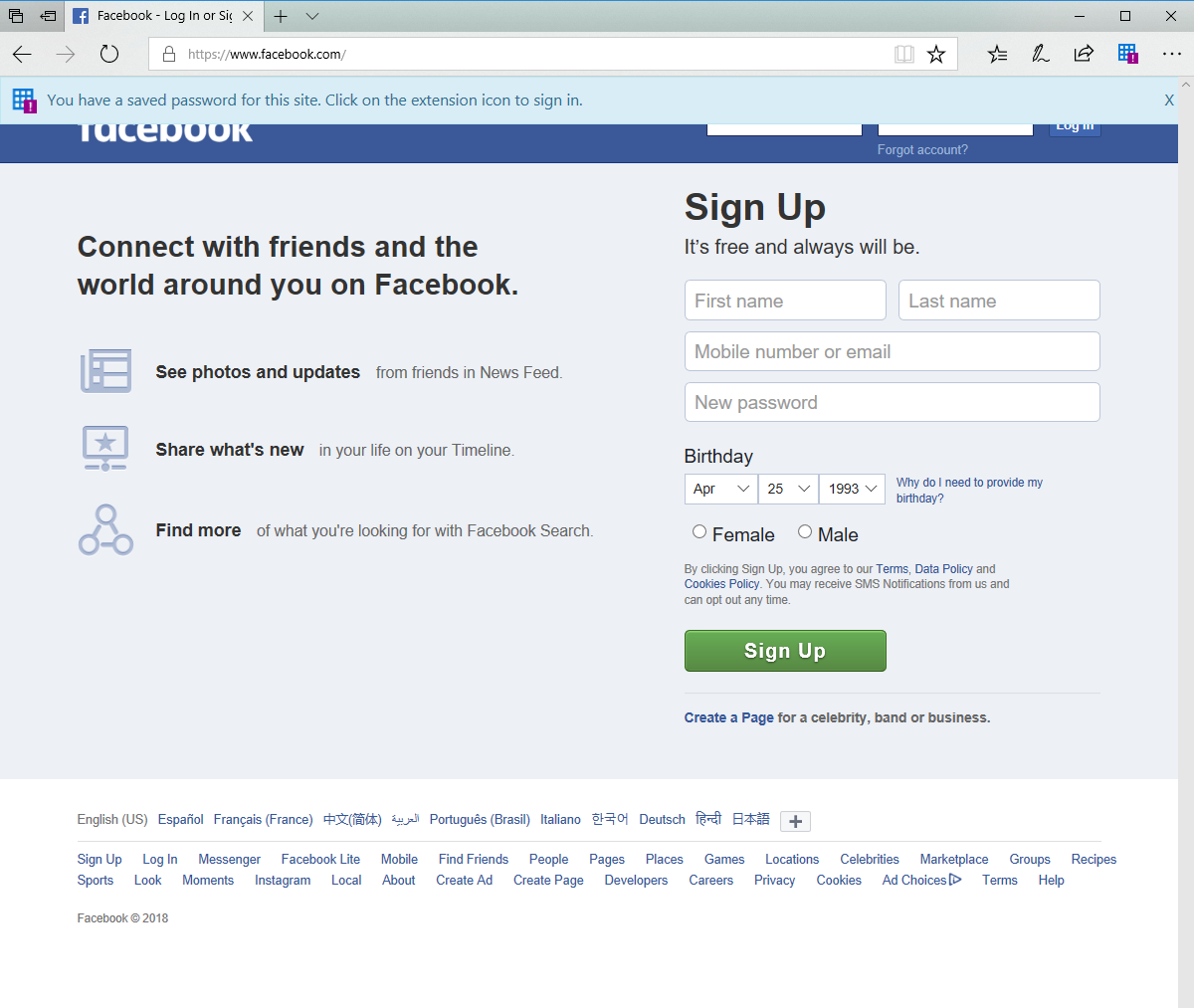
#### My Apps Secure Sign-in Extension Requirements

If password-based SSO applications are made available to end users, they will need to install the extension to sign in to these applications. The extension handles the execution of a script that transmits the password into the applications sign in form. Users will be prompted to install the extension when they first launch the password-based SSO application. More information about the extension can found: [Install the access panel browser extension](https://docs.microsoft.com/azure/active-directory/application-access-panel-extension-problem-installing?/?WT.mc_id=DMC_AAD_Manage_Apps_Troubleshooting_Nav)

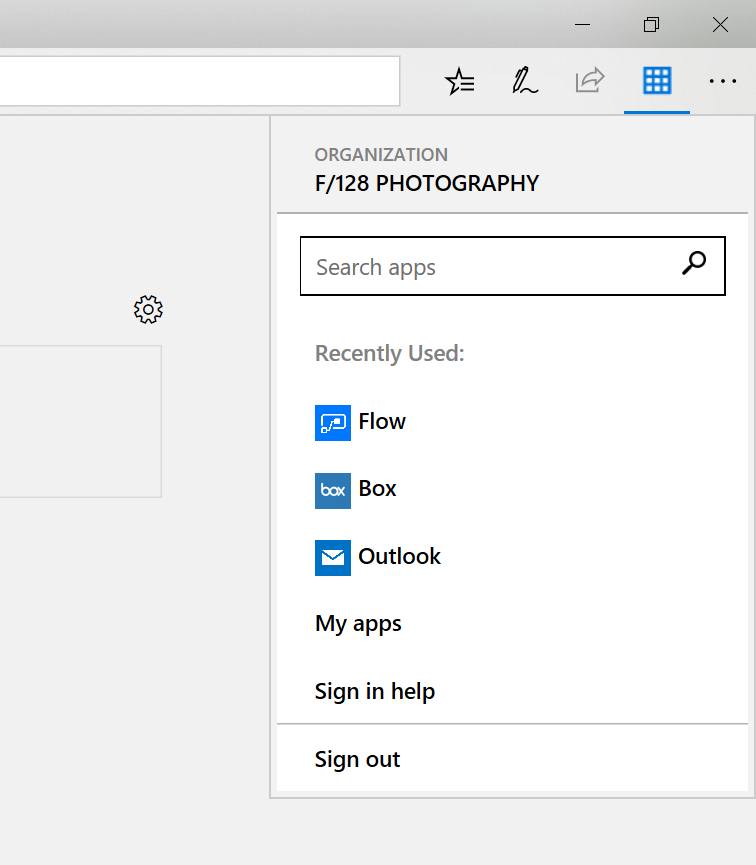
What the user will see when launching a password-based SSO application for the first time:



An additional convenience the extension offers is that if a user goes directly to the sign in page of the application and a password is available for the app the extension will offer to sign in the user in.



Even if users are not using password-based SSO applications, they will still benefit from having the extension. These benefits include the ability to quick launch any app from its search bar, finding access to recently used applications and having a quick link to the My Apps page.



* **Microsoft recommends** installing the My Apps Extension for users to take advantage of quick app launch features from anywhere on the web from the browser bar directly.

**Implementation plan table**

In the below table, record the values you will use when implementing area one

| Configuration | Typical values | Vales to be configured |
| --- | --- | --- |
| Determine the pilot group to test application SSO | Identify the Azure AD security group to be used and ensure all pilot member are a part of the group. | Group: |
| Determine the group or groups to be enabled for production. | Identify the Azure AD security group9s), or AD groups synced to Azure AD, to be used and ensure all pilot member are a part of the group. | Group(s): |
| Determine applications that will be connected to Azure Active Directory for SSO | 0365 applications, Box, Salesforce | Values: |
| Determine what licenses may be required for applications you want to enable | O365 license, EMS license | Values: |
| Determine what type of application SSO mode will be used for the applications selected | SAML, OAuth, Password-based SSO | Values: |
| Determine what self-service app management capabilities you will enable | Add new apps, approval workflow requirements | Values: |

## Planning Deployment and Support

An important part of planning deployment and support is ensuring that your end users are proactively informed about the service, can easily use the service and are adequately supported if they run into problems.

### Communications Planning

The end user experience for the access panel and using the different capabilities available will be different from any existing toolset. There are multiple elements to planning your communication strategy. These include:

* Notifying users of upcoming and released functionality via
  + Email and other internal communication channels
  + Visuals such as posters
  + Executive live or other communications
* Determining who will customize and who will send the communications, and when.

Use the following table to plan your communications strategies. In the channels column, record the channels you will use for communications, including email, Yammer, Slack, intranet sites, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Channels | Person customizing content | Person communicating | Date of communication |
| Initial communication to pilot users |  |  |  |  |
| Posters for pilot |  |  |  |  |
| Exec comms for pilot |  |  |  |  |
| Initial communication to all users for launch |  |  |  |  |
| Posters up for Launch |  |  |  |  |
| Exec. comms for launch |  |  |  |  |
| Post-launch follow-up communications |  |  |  |  |

### Support Planning

While the access panel does typically not create user issues, it is important to have support staff prepared to deal with issues that may arise.

Although an administrator can troubleshoot an issue an end user runs into through the Azure AD portal, it is generally better to help resolve the issue via a support process.

In the operational guide section of this document, create a list of support cases and their likely causes, and create a guide for resolution.

#### Communications Templates

Below you will find customizable templates for emails. You can adapt the emails for use in other communications channels as appropriate for your corporate culture.



#### Communication Tutorial Videos

Below are a few videos that walkthrough the My Apps experience and provide users a quick way to get started using the My Apps portal.

[Welcome to my apps](https://microsoft.sharepoint.com/:v:/t/iam-cass-pm/EVfwu-Uc3DxMk6bql_iMY78BSotic2fWiinq8Arbwt5Mbw?e=BbH162) – Intro to the My Apps portal

[My apps on the go](https://microsoft.sharepoint.com/:v:/t/iam-cass-pm/EZ6zO2_MrqtIicibYi91PEwBzjpusZQ3eX3rR2_geAI6IA?e=0l02aq) – How to use the My Apps extension and managed browser

## Planning Reporting and Auditing

Azure AD provides reports that provide technical and business insights. It is recommended that you work with your business and technical application owners to assume ownership of and consume these reports on a regular basis based on your organization’s requirements. The table below provides some examples of typical reporting scenarios.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Manage Risk |  | Increase Productivity |  | Governance & Compliance |
|  |  |  |  |  |  |  |
| Report types |  | Application permissions and usage. |  | Account provisioning activity |  | Review who is accessing the applications |
| Potential actions |  | Audit access; revoke permissions |  | Remediate any provisioning errors |  | Revoke access |

Azure AD retains most auditing data for 30 days and makes the data available via Azure Admin Portal or API for you to download into your analysis systems.

Learn more: [View your access and usage reports](https://azure.microsoft.com/documentation/articles/active-directory-view-access-usage-reports/)

### Auditing

Audit logs for application access are available for 30 days. Therefore, if security auditing within a corporation requires longer retention, the logs need to be exported and consumed into a SIEM tool such as Splunk or ArcSight.

In the table below, document the backup schedule, the system, and the responsible parties. You may not need separate auditing and reporting backups, but you should have a separate backup from which you can recover from an issue.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Frequency of download | Target system | Responsible party |
| Auditing backup |  |  |  |
| Reporting backup |  |  |  |
| Disaster recovery backup |  |  |  |

# Implementing Your Solution

The foundation of proper planning is the basis upon which you can deploy an application successfully with Azure Active Directory. It provides intelligent security and integration that simplifies onboarding while reducing the time for successful deployments. This combination ensure that your application is integrated with ease while mitigating down time for your end users.

Use the following phases to plan for and deploy your solution in your organization:

[Phase 1: Implementation Steps](#_Phase_1:_Implementation)

[Phase 2: Change Communications](#_Phase_2:_Change)

[Phase 3: Verify End User Scenarios](#_Phase_3:_User)

[Phase 4: Rollback Steps](#_Phase_4:_Rollback)

## Timelines and Environments

In the table below, copy in the information from planning environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

## Phase 1: Implementation Steps

### Solution Components

Implementation includes the following primary components:

**Step 1:** Application SSO access

**Step 2:** Application self-service capabilities

### Step 1: Application SSO access

#### How to configure application single-sign on

When a user “signs in” to an application, they go through an authentication process where they are required to prove that they are who they say they are. Without single sign-on, this is typically done by entering a password that is stored at the application, and the user is required to know this password.

More info about configuring the application’s SSO mode can be found here: <https://docs.microsoft.com/azure/active-directory/active-directory-appssoaccess-whatis>

#### How to deploy applications to user’s My Apps launchers

After an application has been configured for single-sign on, the next step is assigning the applications to users designated to have access to the application. Once a user is assigned to an application this will result in the application appearing on their My Apps page and O365 app launcher.

A screenshot of a cell phone

Description generated with very high confidence

Additionally, you may choose to hide the app by selecting if you are not ready to expose the application to all users during the testing phase. Learn more: [Hide an application from user’s experience in Azure Active Directory](https://docs.microsoft.com/azure/active-directory/active-directory-coreapps-hide-third-party-app)

#### How to deploy Microsoft Office 365 applications to My Apps

For Office 365 applications, users receive a set of Office based on licenses assigned to them. A prerequisite for access to Office applications is assigning users to the correct licenses tied to the Office applications. Once a user is assigned the license they will automatically see the applications associated with the license in their My App’s page and O365 app launcher.

Additionally, if you would like to hide this set of Office applications for users, there is also an option to hide the set of apps from the My Apps portal, but still allow users to access the Office applications from the O365 portal. Learn more: [Hide an application from user’s experience in Azure Active Directory](https://docs.microsoft.com/azure/active-directory/active-directory-coreapps-hide-third-party-app)

A screenshot of a cell phone

Description generated with very high confidence

#### How to deploy My Apps on mobile using the Managed Browser

The Managed Browser will be necessary for mobile if users are launching password-based SSO applications because the Managed Browser will facilitate the transfer of the password saved for the application. If deployed with Intune, the Managed Browser provides a set of other web data protection features. Learn more: [Manage Internet access using Managed Browser policies with Microsoft Intune](https://docs.microsoft.com/intune/app-configuration-managed-browser)

The Managed Browser can be downloaded directly from the [iOS](https://itunes.apple.com/us/app/intune-managed-browser/id943264951?mt=8) and [Android](https://play.google.com/store/apps/details?id=com.microsoft.intune.mam.managedbrowser) stores.

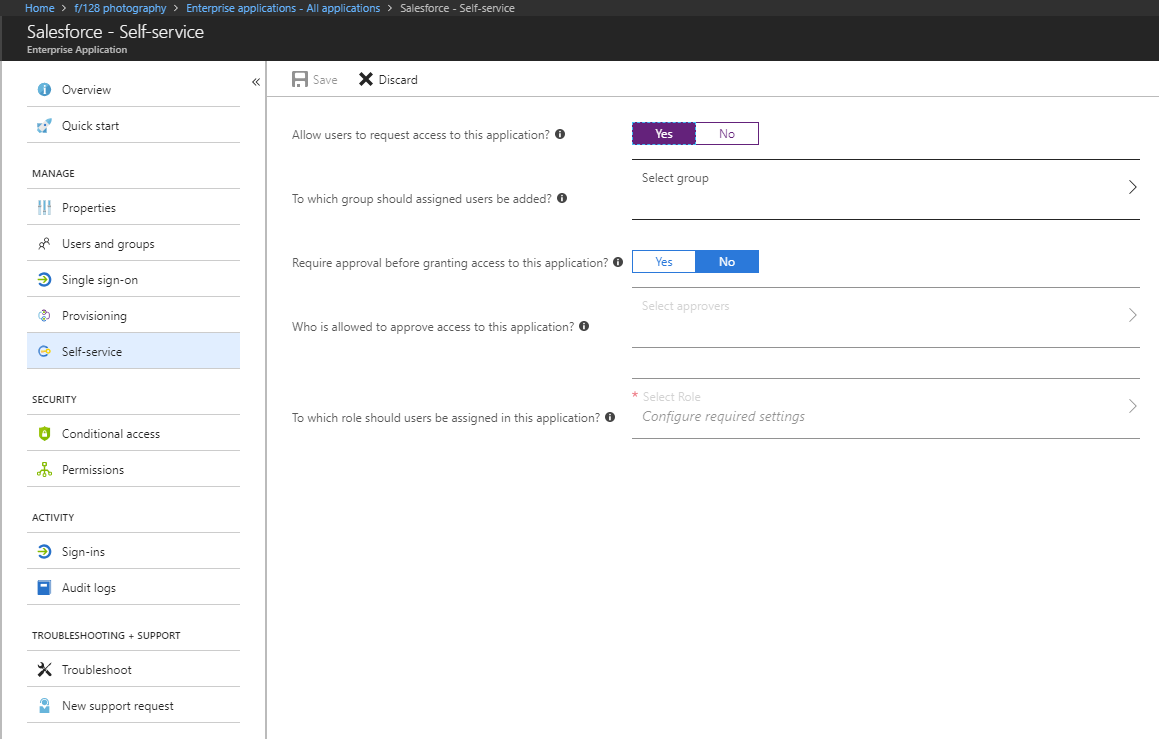
### Step 2: Application Self-service Capabilities

#### How to configure self-service application access

Self-service application access allows users to self-discover and request access to any applications. Users are given the freedom to get access to the apps they need without going through an IT group each time to request access. You can add users to a pre-configured group to manage their access and this will provide reporting on who has request access, removed access, and continued control over managing the roles assigned to them.

Optionally allow a business approver to approve application access requests so the IT group doesn’t have to. The business approver can also set the passwords users can use to sign in to the application, right from the business approver’s My Apps page.

Learn more: [How to use self-service application access](https://docs.microsoft.com/azure/active-directory/application-access-panel-self-service-applications-how-to)



## Phase 2: Verify End User Scenarios

### Step 1: Create test cases for your access panel deployment

The following tests will be conducted with both Corporate Own devices and personal devices. These test cases should reflect your Business Use Cases. These will be used to verify whether this solution meets your requirements.

### Testing implementation

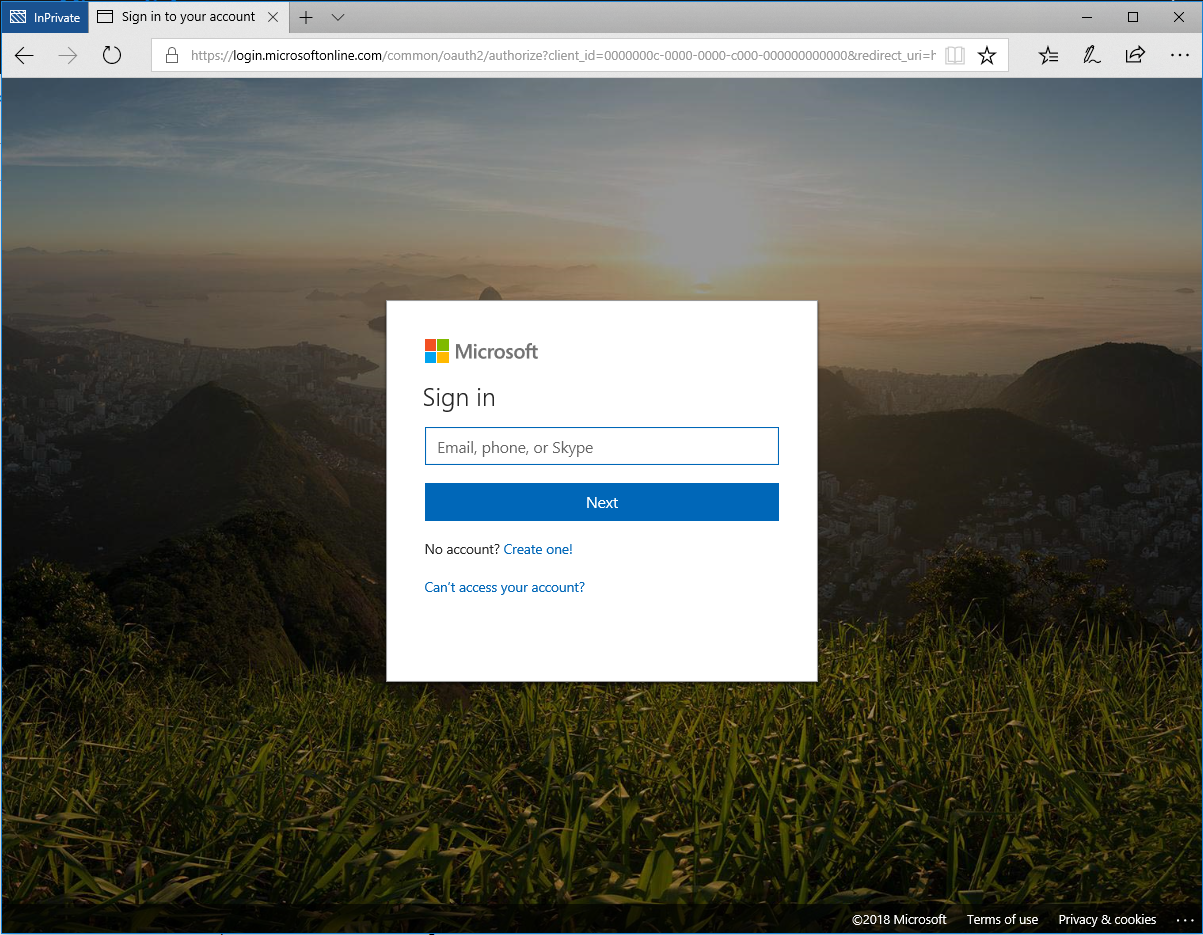
In this section, document how you will test during the pilot or other pre-production phases of your roll-out, as well as post-launch. Testing should ensure that your business use cases are covered. You can then use this table to record results. We have added a few cases based on the sample business requirements in this document, and on typical technical scenarios. You should add others specific to your needs.

### Application SSO access test case examples:

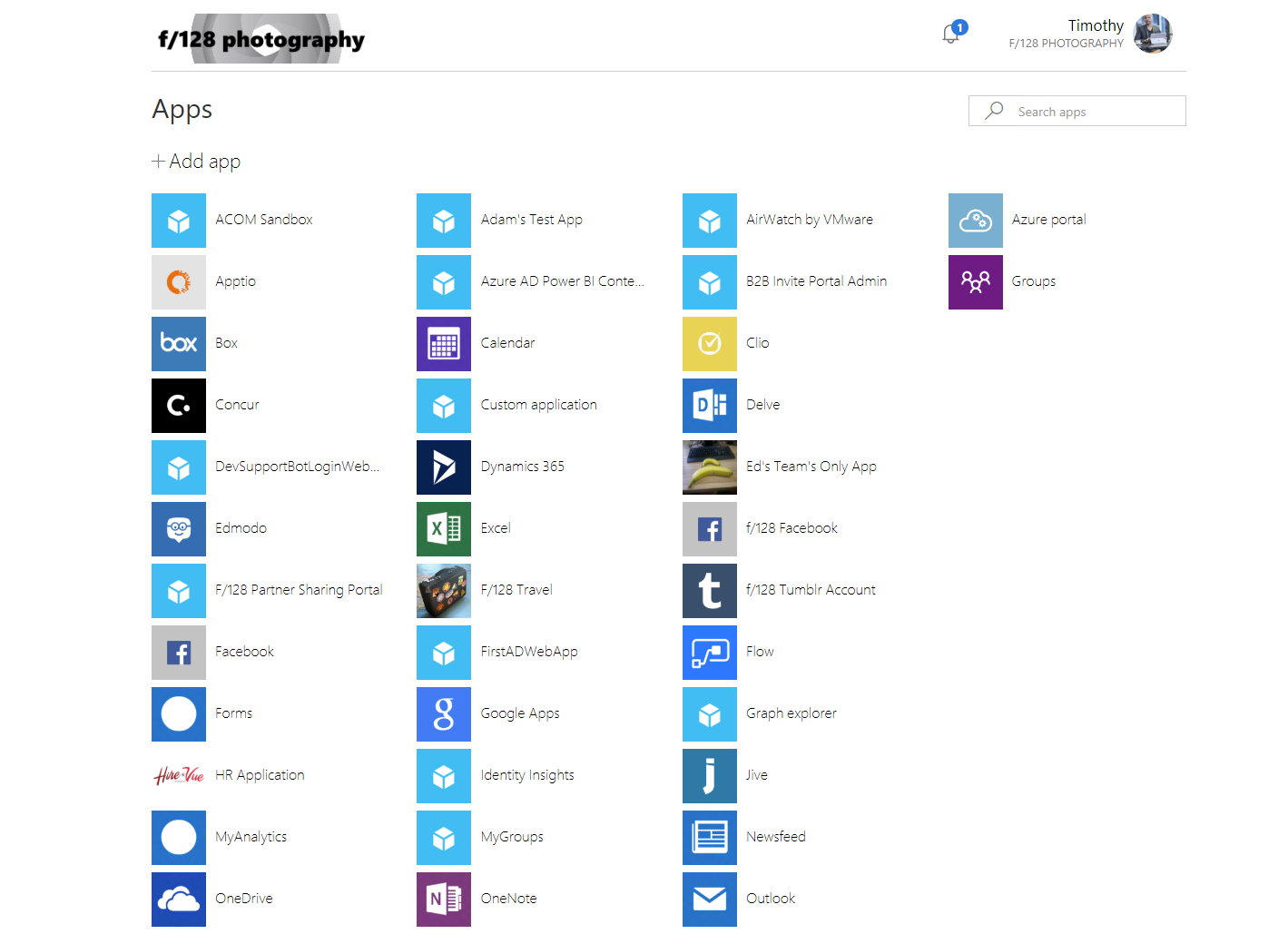
|  |  |  |  |
| --- | --- | --- | --- |
| Business case | Device type | Expected result | Actual result |
| 1) User signs in into the My Apps portal | Any allowed device | User can sign in and see their applications |  |
| 2) User launches a federated SSO application | Any allowed device | User is automatically signed into the application |  |
| 3) User launches a password SSO application for the first time | Any allowed device | User needs to install the My Apps extension |  |
| 4) User launches a password SSO application a subsequent time | Any allowed device | User is automatically signed into the application |  |
| 5) User launches an app from O365 Portal | Any allowed device | Same behavior of app launching from above |  |
| 6) User launches an app from the Managed Browser | Any allowed device | Same behavior of app launching from above |  |

### Expected result examples:

**Case 1**: User signs in into the My Apps portal

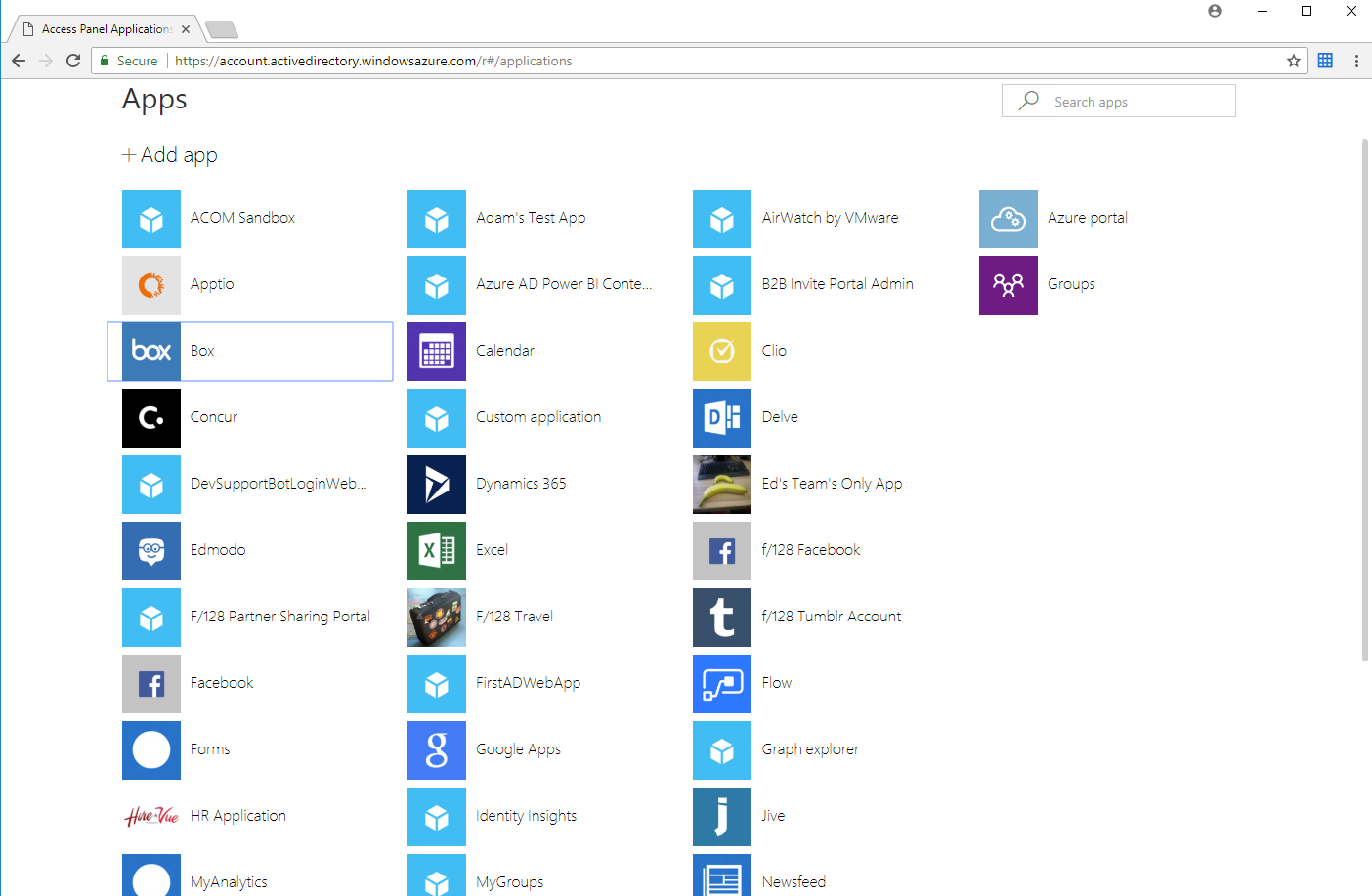
User sees sign in prompt:

User logs in successfully and sees their My Apps page:

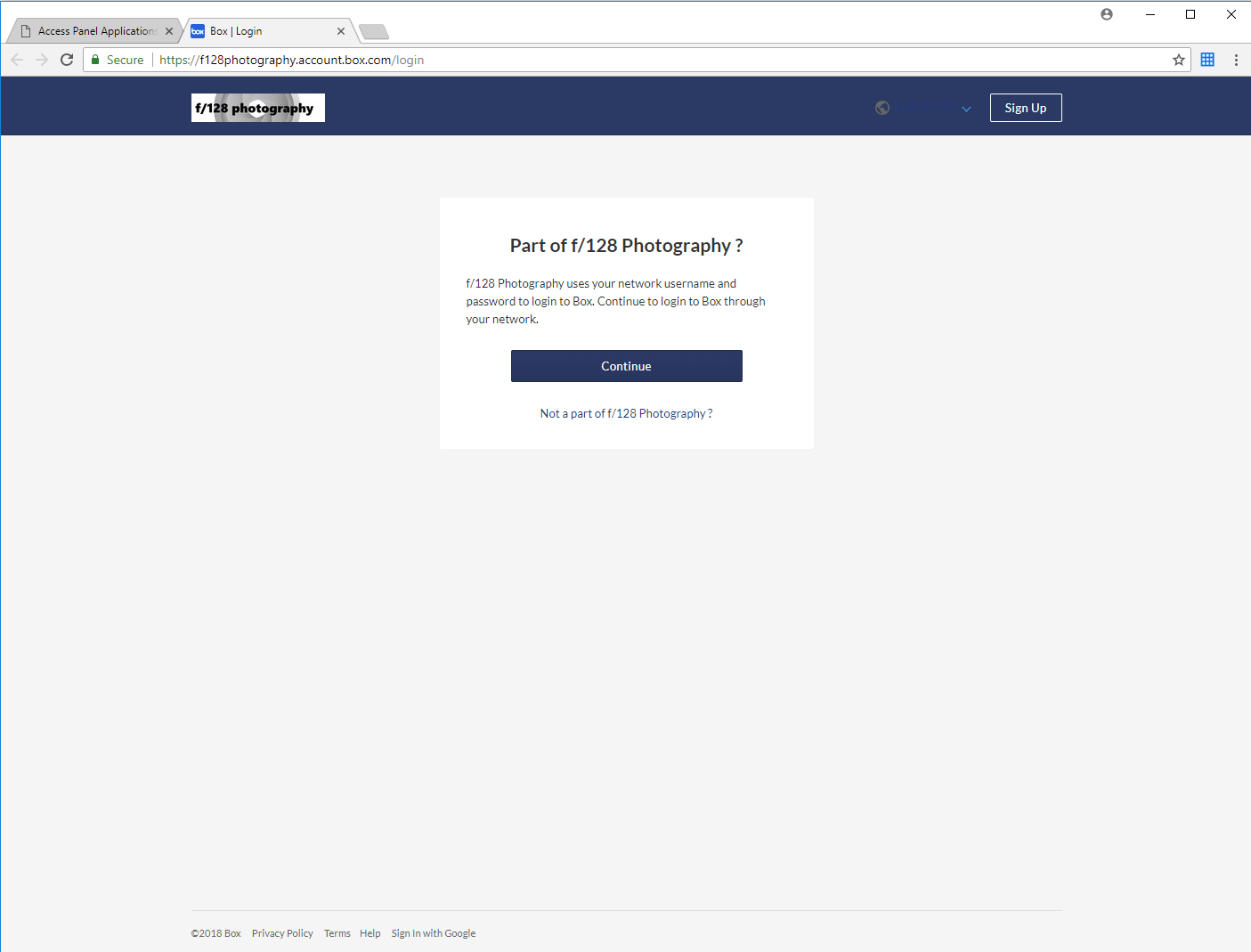


**Case 2:** User launches a federated SSO application

User launches Box from My Apps:

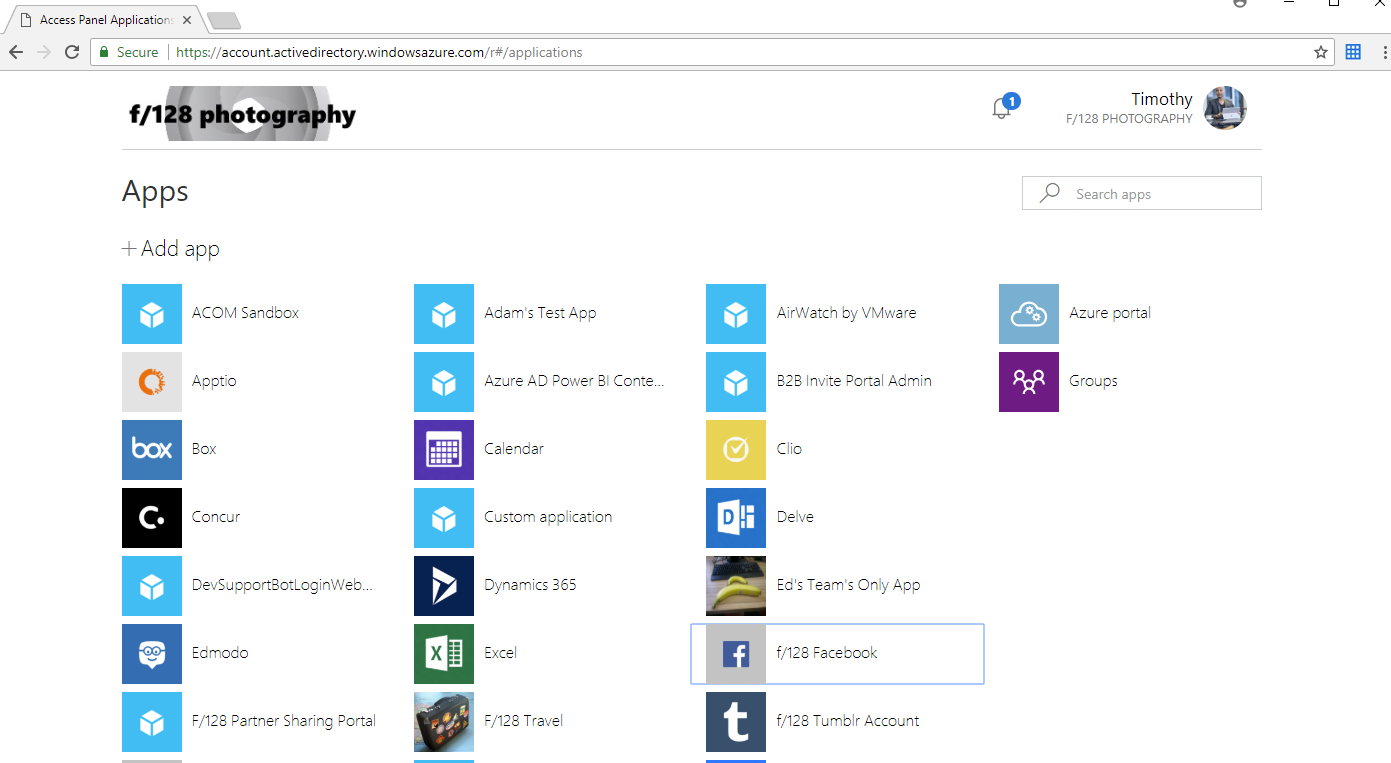


User is redirected and signed into Box:

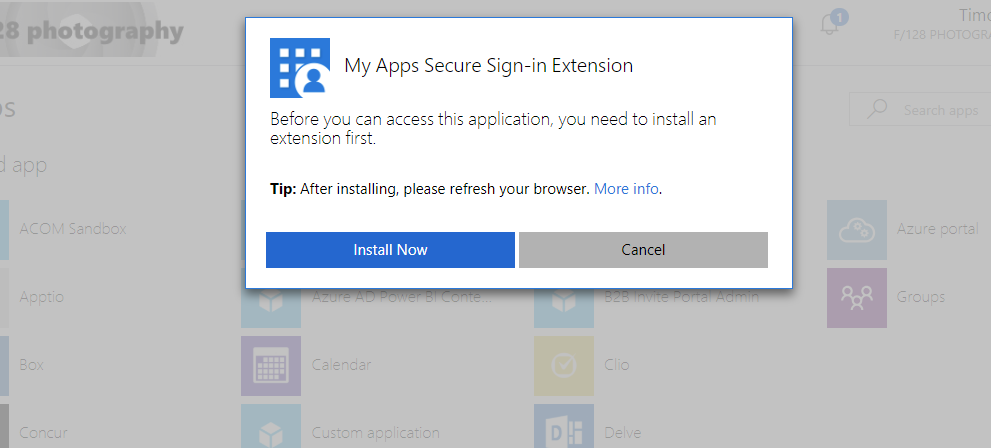


**Case 3:** User launches a password SSO application for the first time

User launches Facebook

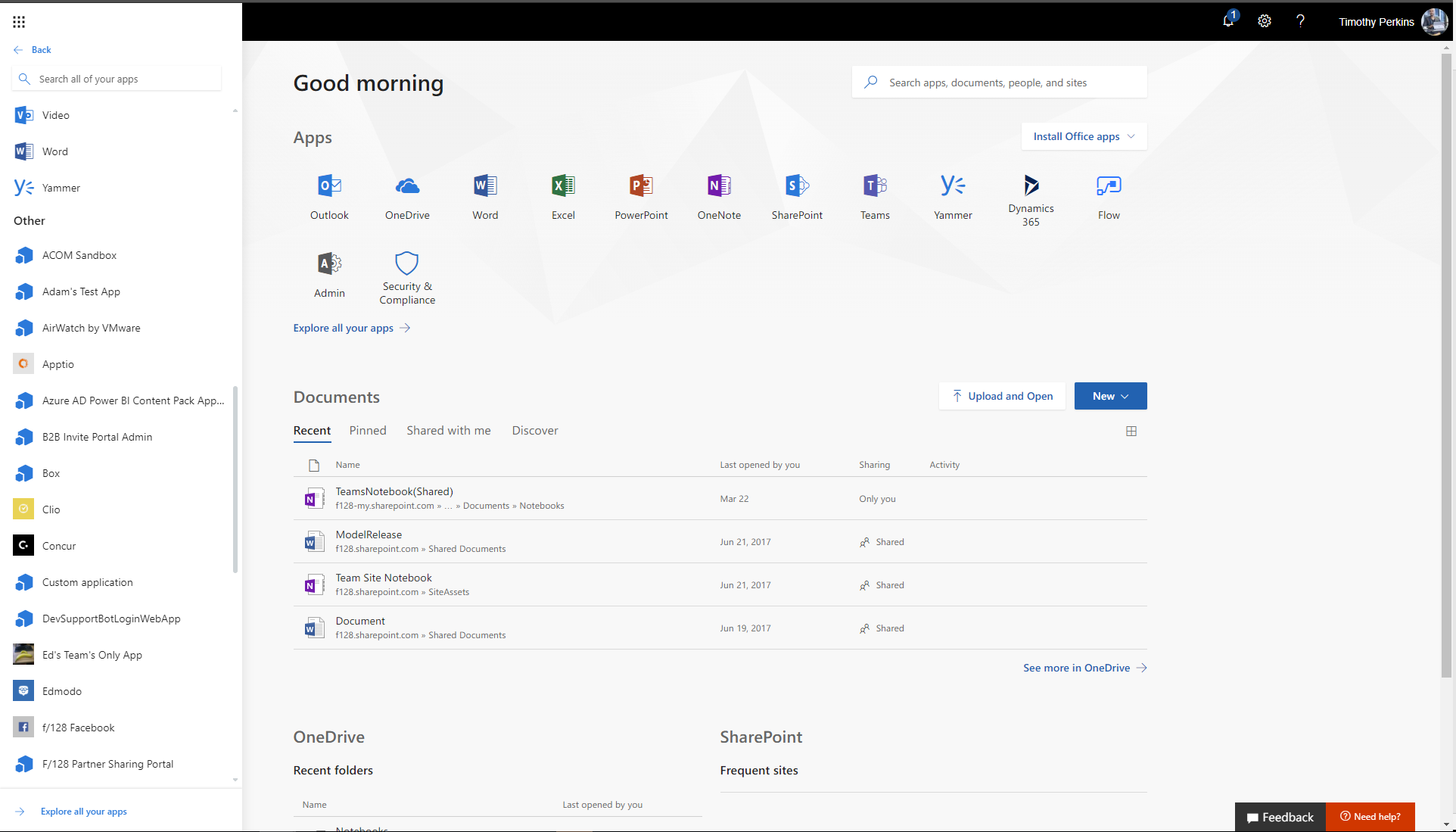


User sees install extension prompt



**Case 5**: User launches an app from O365 Portal

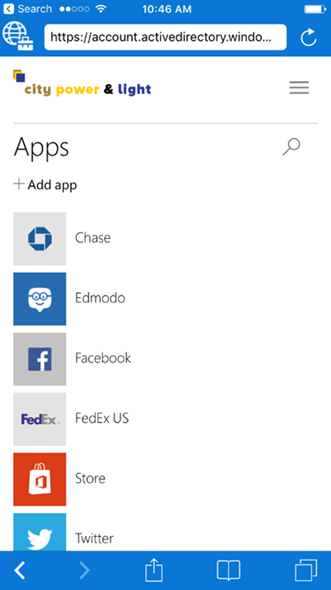
User launches an app from O365 portal



User is automatically signed in as **Case 2**

**Case 6:** User launches an app from the Managed Browser

User launches an app from the Managed Browser



User is automatically sign in as **Case 2**

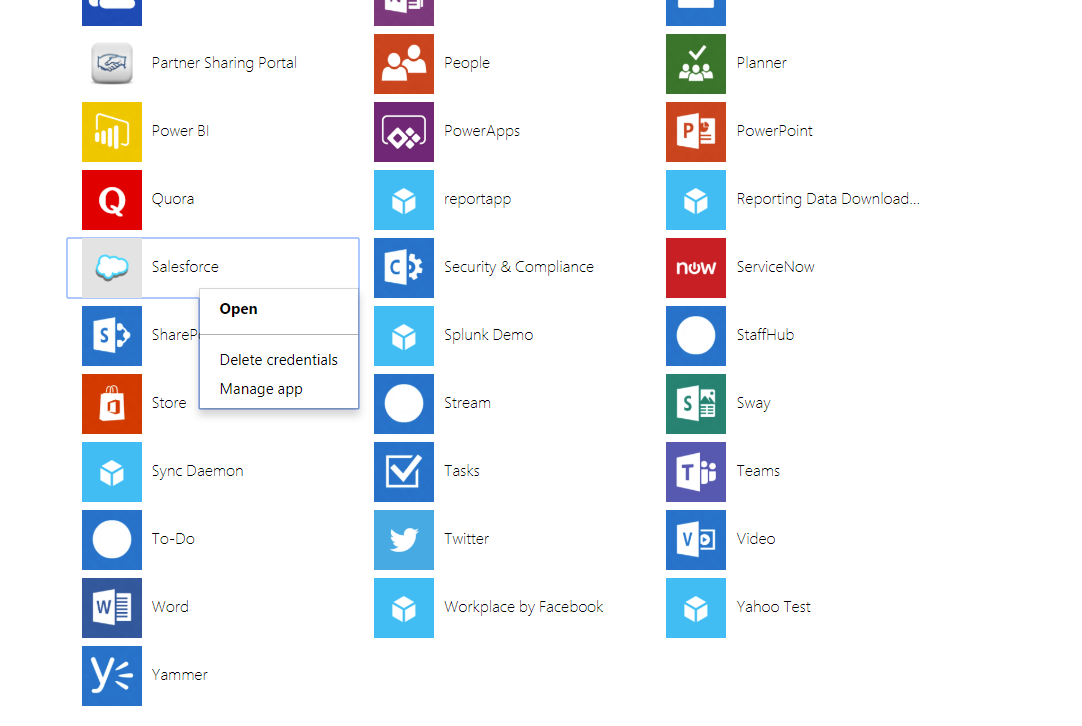
###### Application self-service capabilities test case examples

|  |  |  |  |
| --- | --- | --- | --- |
| Business case | Device type | Expected result | Actual result |
| 1) User can manage selected apps they are owners of | Any allowed device | User can find the option to manage an application |  |
| 2) User can manage membership to the application | Any allowed device | User can add/remove members who have access to the app |  |
| 3) User can edit the application | Any allowed device | User can edit the application’s description and credentials for password SSO applications |  |

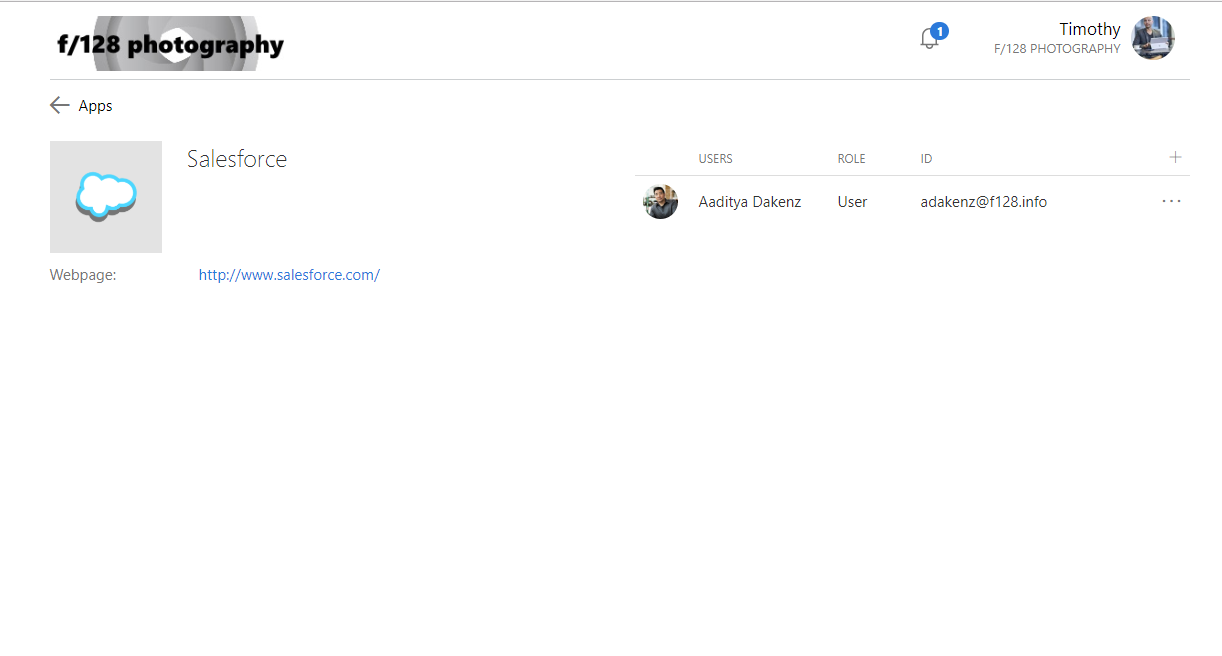
###### Expected result examples:

**Case 1:** User can manage selected apps they are owners of

User can find the “manage app” option on the application

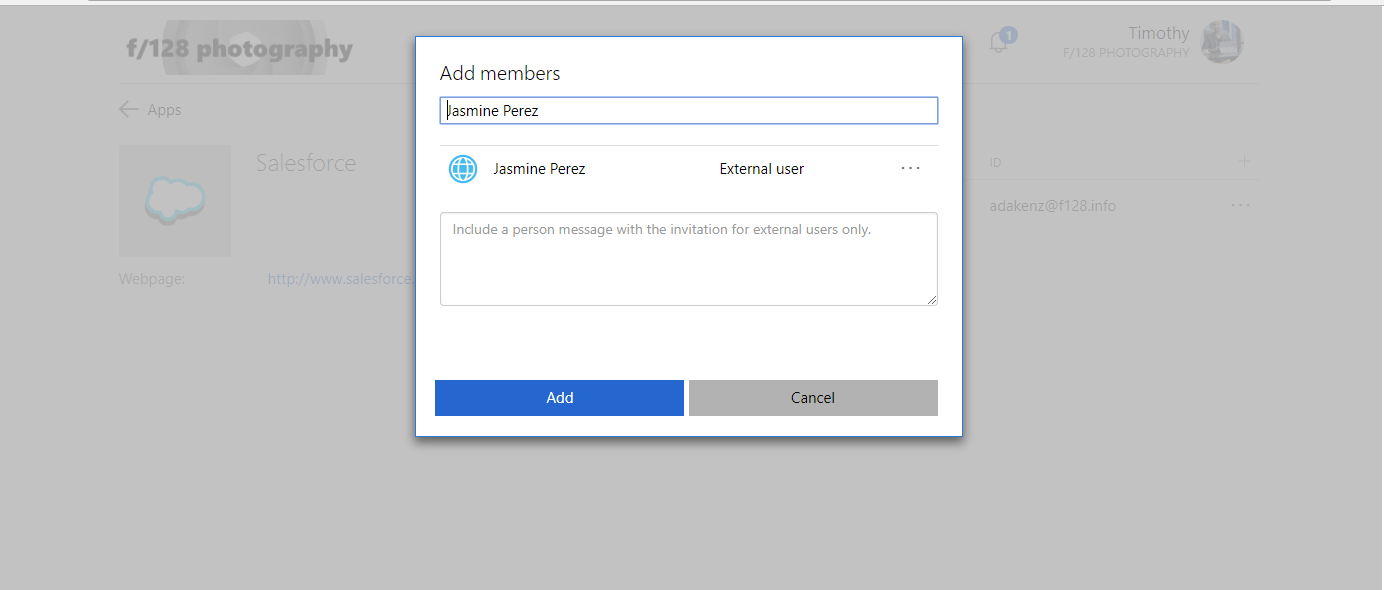


User clicks manage app to find the application management view

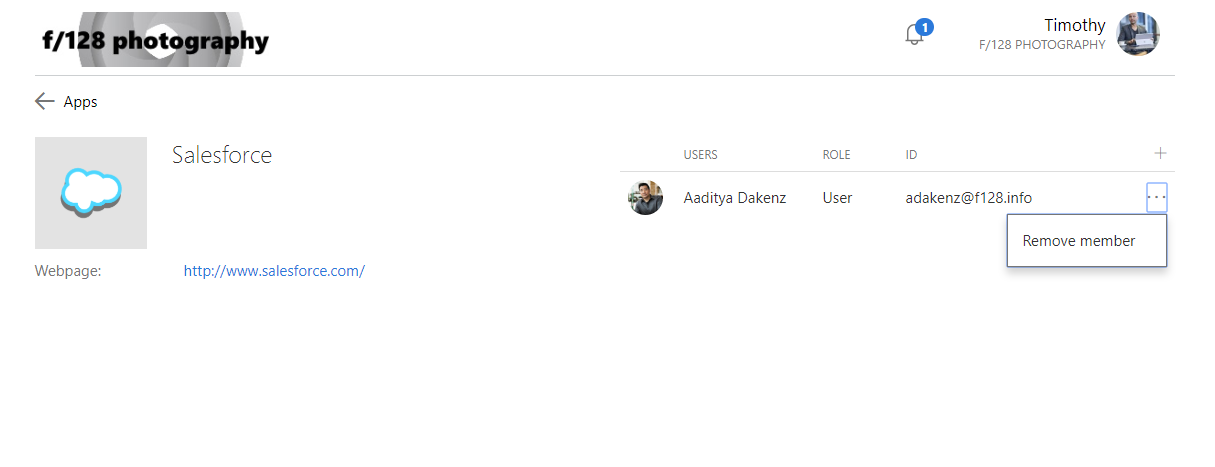


**Case 2:** User can manage membership to the application

User can add users from the app management view

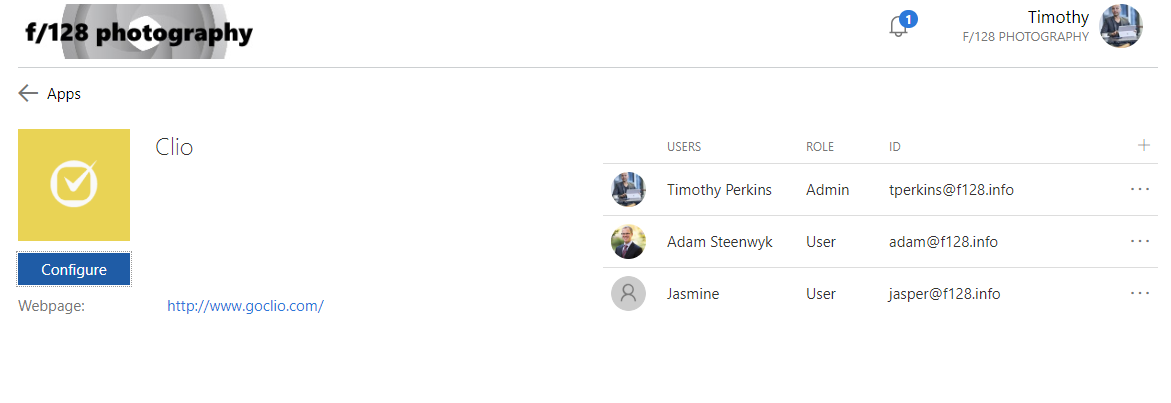


User can remove from the management view

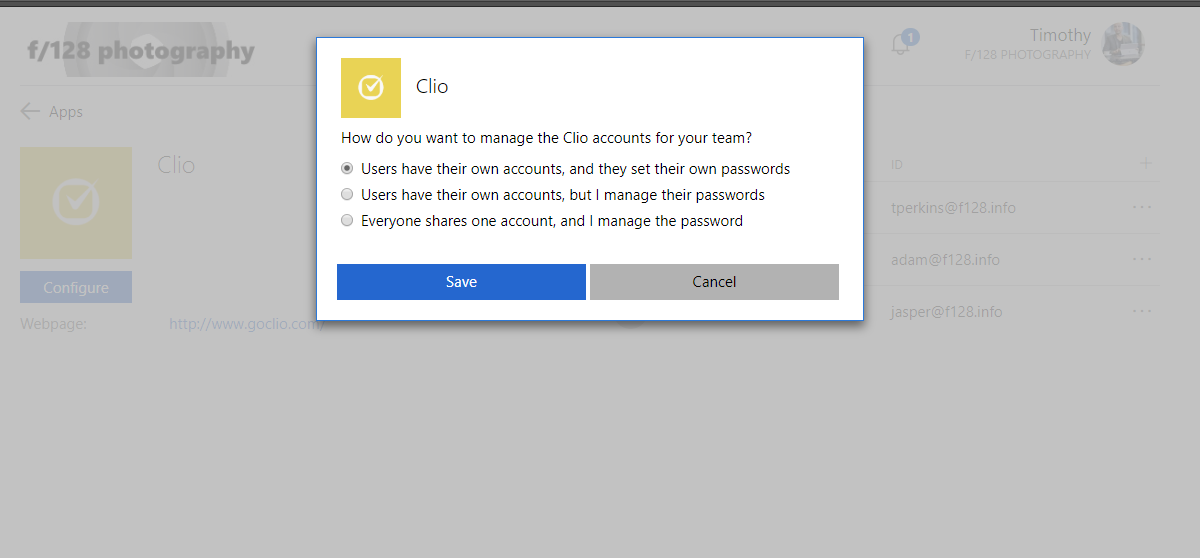


**Case 3:** User can edit the application

User clicks on configure



User sets the way to set the password for the app



### Step 2: Document Your Results

Document the outcomes for both **Expected Results** and **Actual Results** in [Step 1](#_Step_1:_Create). Use this to determine to move forward into production based on your established timelines.

### Step 3: Moving into Production

After you complete all of testing based on your test cases, it’s time to move into production with your My Apps deployment.

## Phase 3: Rollback Steps

It’s important to plan what to do in the case during your deployment doesn’t go as planned. If the SSO configuration fails during the deployment, you must understand how to mitigate any outage and reduce impact to your users.

# Operationalize your Implementation

## Purpose of Document

The intent for the *Operationalize your Implementation* is to address the day-to-day operations for maintaining the application that has been deployed over the life of the application. This includes the roles, certificate lifecycle, troubleshooting steps, access management and attestation of user access and roles.

## Required Roles

Microsoft recommends using the less role to accomplish the required task within Azure Active Directory. Microsoft recommend [review the different roles that are available](https://docs.microsoft.com/azure/active-directory/active-directory-assign-admin-roles-azure-portal) and choose the right one to solve your needs for each persona for this application. Some roles may need to be applied temporarily and removed after the deployment has been completed.

|  |  |  |  |
| --- | --- | --- | --- |
| Personas | Roles | Azure AD role (if required) | Assign to |
| Help Desk Admin | Tier 1 Support | None |  |
| Identity Admin | Configure and Debug when issues impact Azure AD | Global Admin |  |
| <<APPLICATION NAME>> Admin | User attestation in <<APPLICATION NAME>>, configuration on users with permissions | None |  |
| Infrastructure Admins | Cert Rollover Owner | Global Admin |  |
| Business Owner/Stakeholder | User attestation in <<APPLICATION NAME>>, configuration on users with permissions | None |  |

* **Microsoft recommends** using [Privileged Identity Management](https://docs.microsoft.com/azure/active-directory/active-directory-privileged-identity-management-configure) to manage your roles to provide additional auditing, control, and access review for users with directory permissions.

## Troubleshooting Guide & Steps

You should create troubleshooting guides for your support organization. In this section you will find examples of Tier 1, 2, and 3 guides for common scenarios. You should modify these to fit your organization.

### Example: Single account not being able to log into the application.

|  |  |  |  |
| --- | --- | --- | --- |
| Tier | Condition: If… | Verification | Details / actions |
| 1 | ***Tier 1*** *– you will need to verify the user’s access status, state of the account (enable/disable) from Azure AD & application attempting to access, and whether there is conflict between multiple accounts.* | | |
| User owns multiple accounts | Verify that user is using the correct account / URL pair. | Provide [instructions to log](https://support.microsoft.com/help/4026200/windows-browse-inprivate-in-microsoft-edge) into a private session to reduce conflict of existing sessions |
| User can login to network but not application. | Step 1: Verify that user is assigned to the application. | In the [Azure Portal](https://aad.portal.azure.com), select **Enterprise applications**, find the application, and see if the user has been directly assigned or has been assigned as a member of a group. |
| Step 2: Verify that user has an account in the application. | Step 1: Log in to the application’s administrative portal (the ISV) and verify the user has an account.  Step 2: Verify that the account is not disabled or otherwise inactive. |
| Step 3: Verify that user can login to MyApps and see the application in the Access Panel | Have user log into [Access Panel](https://myapps.microsoft.com) at myapps.microsoft.com. |
| User can log in to application directly, but not through SSO. | Verify that the user has an account provisioned in AAD, and has the account is at the Premium level. | This is only applicable if you allow the users to perform forms-based authentication directly to the application |
| *2* | ***Tier 2*** *– you will need to collect logs of the traffic between the client and application using your preferred method of decrypting authentication traffic.* [*Fiddler*](https://docs.microsoft.com/azure/active-directory/develop/active-directory-saml-debugging) *or* [*SAML Tracer browser extensions*](https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/) *are generally the most common tools.* | | |
| User can login to network but not application. | Step 1: Review the logs on the application that the user is attempting to access | Logs here will generally reveal bad requests. If there is no logs, then either application does not offer these logs or it has not received a Response from Azure AD. |
| Step 2: Validate the certificate has not expired | Step 1: Verify the certificate thumbprint matches between Azure AD and the application that is attempting to be accessed  Step 2: Verify the certificate is still valid and has not been expired |
| Step 3: Validate endpoints are correct | [Compare the endpoints configured on the application object in Azure AD to what has been configured in the ISV (e.g. the application that the user is attempting to access)](#_Endpoint_Information) |
| Step 4: Validate claims (NameID) mapping between AAD and application or the attribute name you have chosen to map to for the application you user is attempting to access | If the attribute that is being sent does not match to what is being expected, you will either receive an error or mismatching may occur and authenticate the wrong user   *(e.g. Azure AD sends “john@contoso.com” and the application is expecting employeeID “john1445”)* |
| *3* | ***Tier 3*** *– at this point all endpoints has been verified, certs are valid, claims are correct. Contact the application owner and begin steps to escalate to Microsoft support to assist resolving the issue* | | |
| Not resolved by Tier 2 | Notify business owner for <<APPLICATION NAME>> |  |
| Not resolved by Tier 2 | Create a support ticket with Microsoft | Include Repro Steps, UPN, CorrelationID, Timestamp, and Fiddler Trace(s).  **Note:** *Make multiple attempts to authenticate and provide timeframe.* |
|  |  |  |

© 2018 Microsoft Corporation.  All rights reserved.  This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.   
Some examples are for illustration only and are fictitious. No real association is intended or inferred.   
   
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes