BEMA
INFORMATION TECHNOLOGIES

## INTRODUCTION

The BEMA Single Sign On plugin allows you to authenticate users using Office 365 or Okta accounts. This allows your users to only remember a single password, and it makes it much easier to manage users.

This plugin assumes you already have an external authenticator configured with user accounts. If you would like help configuring one, such as Azure for Office 365 authentication, please contact the BEMA Information Technologies support at 877-817-7776.

## OVERVIEW

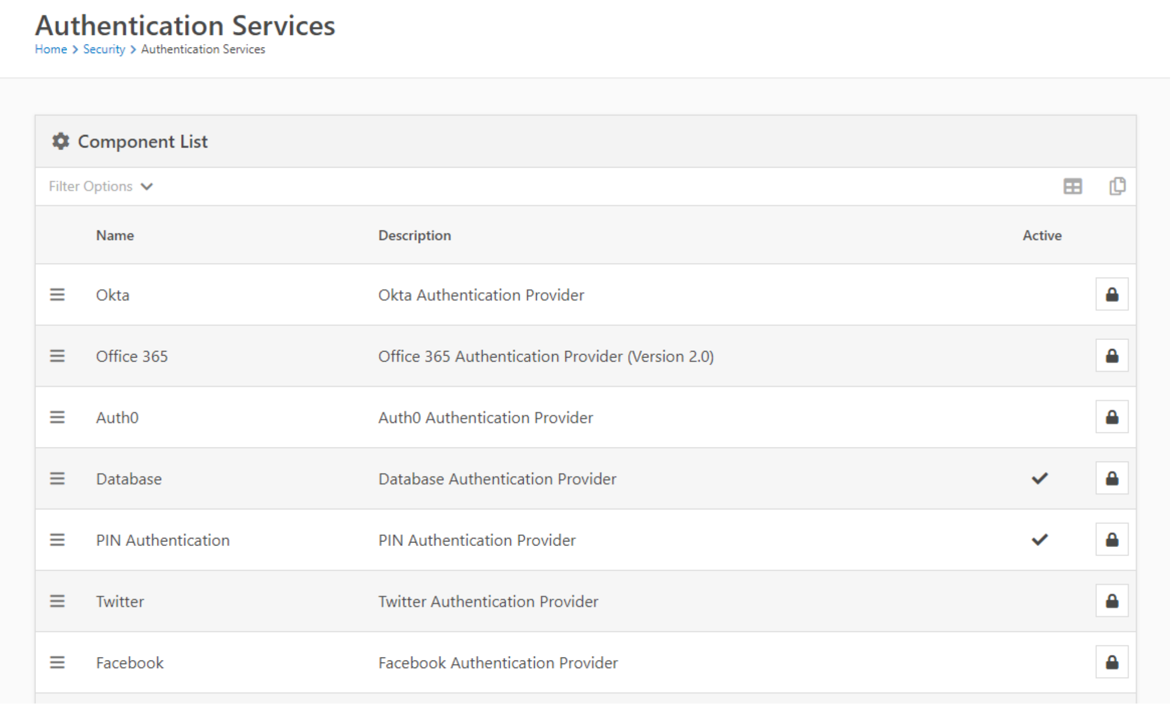
Bundled into the BEMA SSO Plugin are several authentication providers. These will not show up in *Admin Tools > Installed Plugins* but will be set up on the configured pages mentioned further on. Let’s take a look at these components.

**Office 365 Authentication Provider** – This contains all the logic and configuration required to successfully authenticate against Office 365.

**Okta Authentication Provider** – This contains all the logic and configuration required to successfully authenticate against Okta.

# SETUP

Navigate to *Admin Tools > Security > Authentication Services*. Once you arrive at this screen, you will notice there is a new Office 365 and Okta Authentication Provider. Follow the steps below for configuring your desired Authentication Provider



## Authentication Services

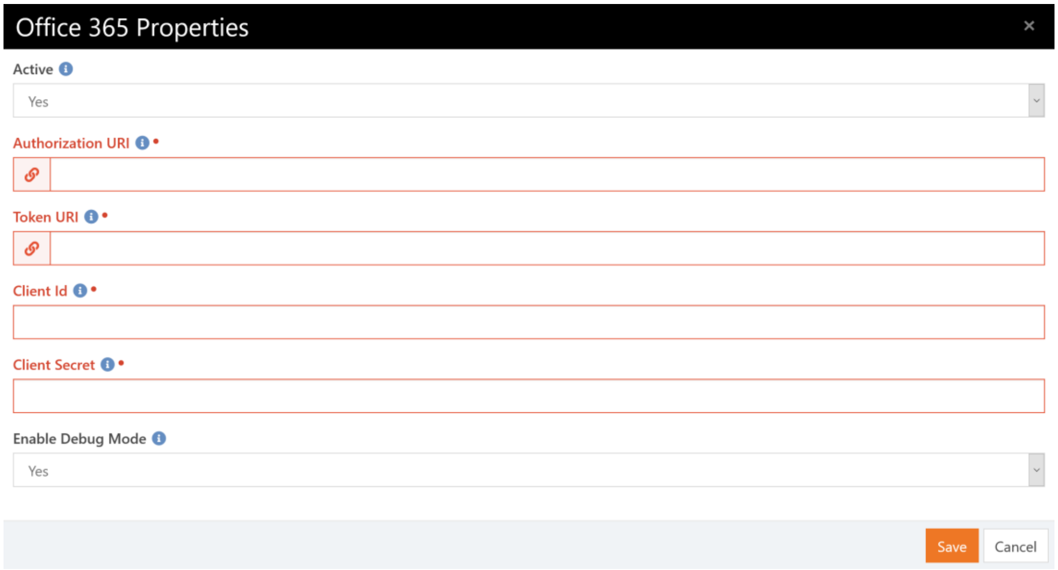
Home > Security > Authentication Services

### Component List

| Name | Description | Active |
|---|---|---|
| Okta | Okta Authentication Provider | |
| Office 365 | Office 365 Authentication Provider (Version 2.0) | |
| Auth0 | Auth0 Authentication Provider | |
| Database | Database Authentication Provider | ✓ |
| PIN Authentication | PIN Authentication Provider | ✓ |
| Twitter | Twitter Authentication Provider | |
| Facebook | Facebook Authentication Provider | |

## OFFICE 365

Clicking on the Office 365 provider, you will be brought to a screen asking for several pieces of information. These configuration items are all generated via the Microsoft Azure Portal.



### Office 365 Properties

Active: Yes

Authorization URI •

Token URI •

Client Id •

Client Secret •

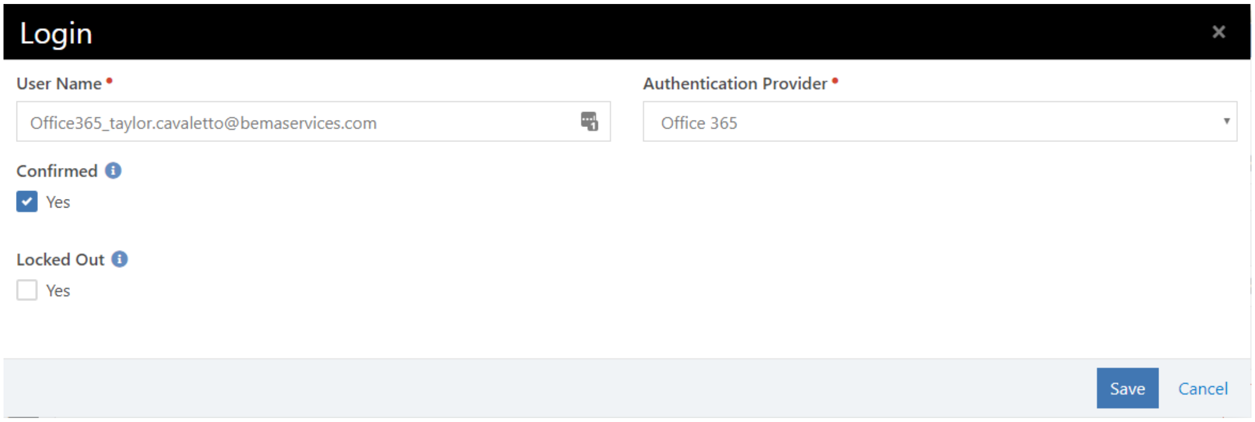
Enable Debug Mode: Yes

Creating the configuration in Azure is not a difficult task, but you want to make sure you follow the steps exactly to ensure proper configuration.

1. Log into your Azure Portal: https://portal.azure.com
2. Type Azure Active in the search bar at the top of the screen and select **Azure Active Directory**
3. Select **App Registrations** on the left side of the screen
4. Click the **New Registrations** button at the top of the screen
5. Enter a Name for your Application
    a. We generally recommend something like **Rock** as this name will be visible to authenticating users
6. Under Supported account type, ensure option **Accounts in the organizational directory only** is selected
7. The value for Redirect URI is very specific. This can be changed later, but let's do it right the first time.
    a. Type needs to stay at **Web**
    b. Value needs to be in the following format: https://<domain>:443/sso
        i. Be sure to also include https://<internal domain>:443/page/3 and https://<external domain>:443/page/3
        ii. Note: O365 will only allow HTTPS, so ensure your Rock server is configured as such.
8. Once all the information is entered, you can click the **Register** Button
9. Now that we have created our Application Config, let's configure a few things needed by Rock.
    a. Under Authentication, you will need to check the Checkbox for Access Token
    b. Under Certificates & Secrets, click the button titled **New Client Secret**
        i. Give your Client Secret a Description and select 1 Year for the Expires
        ii. Copy the Generated value as you will need this later, and you won't be able to see the full secret after you leave this screen.
10. Now that we have finished configuring our Application Config, let's get the fields we need for Rock
    a. From the **Overview** screen, we are going to click the **Endpoints** button
    b. Copy the **OAuth 2.0 authorization endpoint (v2)** link into the Rock **Authorization URI** field
    c. Copy the **OAuth 2.0 token endpoint (v2)** link into the Rock **Token URI** field
    d. From Overview, copy the **Application (client) ID** into the Rock **Client Id** field
    e. Paste the **Client Secret** obtained from **Step 9** into the Rock **Client Secret** field
    f. Lastly, we need to mark this Authentication Provider as **Active**

## USER LOGINS

The Office 365 Authentication Provider has logic built into lookup users by their First Name, Last Name, and Email. If you want to ensure their User Account are created correctly, you can "pre-create" them by creating a User Accounts with the User Name of **Office365_**<email address> IE: **Office365_bill.marble@rocksolidchurch.com .** This step is not required, but it is a great way of ensuring proper configuration.



Login

User Name * Office365_taylor.cavaletto@bemaservices.com

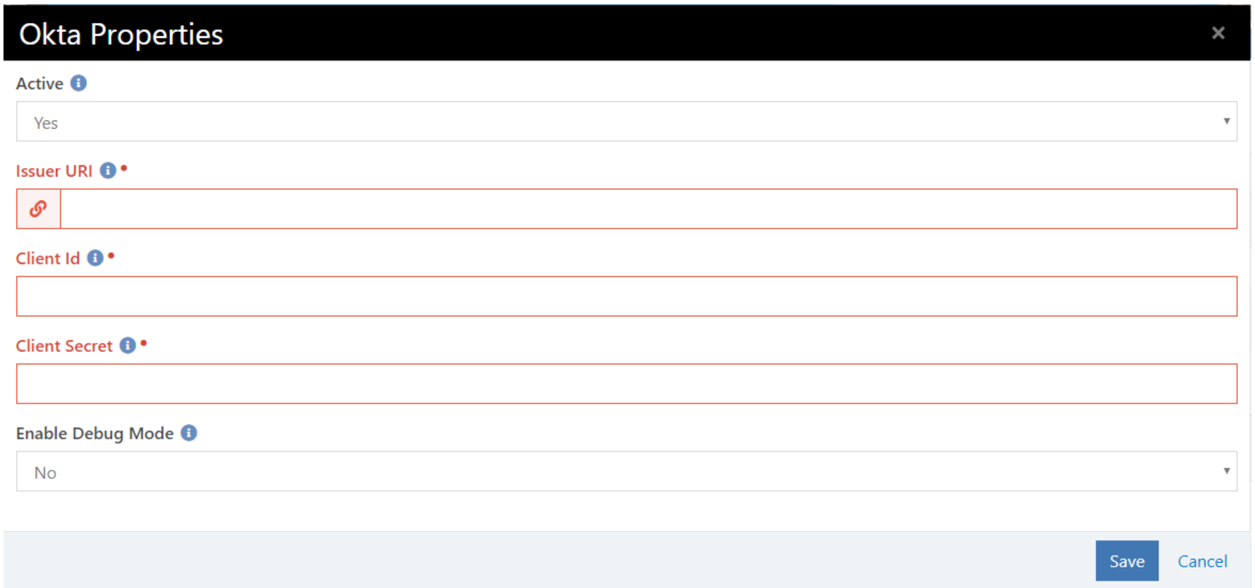
Authentication Provider * Office 365

Confirmed ☑ Yes

Locked Out □ Yes

## OKTA

Clicking on the Okta provider, you will be brought to a screen asking for several pieces of information. These configuration items are all generated via the Okta Developer Console.



Okta Properties

Active: Yes

Issuer URI *

Client Id *

Client Secret *

Enable Debug Mode: No

Creating the configuration in Okta is not a difficult task, but you want to make sure you follow the steps exactly to ensure proper configuration.

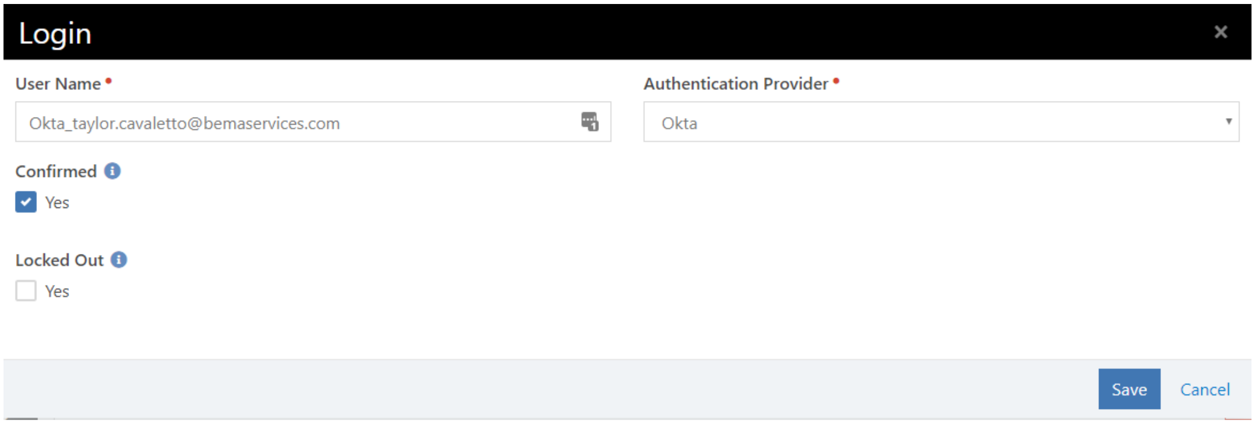
1. Log into your Okta console with your administrator account: https://login.okta.com/
2. Click on Applications.
3. Click on *Create New App* in the upper right hand corner.
4. Select *Web* as the platform and *OpenID Connect* as the sign on method. Click *Create*.
5. Fill out the general settings
    a. Name your Application *Rock* for the Application Name field.
    b. Under the *Login Redirect URIs*, add the following:

        i. https://<domain>:443/sso
        ii. https://<internal domain>:443/page/3
        iii. https://<external domain>:443/page/3
    c. Under *Logout Redirect URIs*, add https://<domain>
    d. Hit *Save*

6. On the General tab, edit *General Settings*.
    a. Under Allowed Grant Types, check *Implicit Hybrid*
    b. Under Login Initiated by, select *Either Okto or App*
    c. Under Initiate Login URI, add https://<domain>
    d. Click *Save.*
7. On the Assignments tab, assign any  people or groups that you want to be able to login to Rock to the new application.
8. On the Sign On tab, scroll down to the *OpenID Connect ID Token* section. Copy the url in the *Issuer* field into Rock's *Issuer Url* field.
9. On the General tab, scroll down to the Client Credentials section.
    a. Copy the client ID and/or client secret using the Copy to Clipboard buttons to the right of each text field.
    b. Paste the results into Rock's Client ID and Client Secret fields.
10. Lastly, we need to mark this Authentication Provider as **Active**

## USER LOGINS

The Okta Authentication Provider has logic built into lookup users by their First Name, Last Name, and Email. If you want to ensure their User Account are created correctly, you can "pre-create" them by creating a User Accounts with the User Name of **Okta_**<email address> IE: **Okta_bill.marble@rocksolidchurch.com .** This step is not required, but it is a great way of ensuring proper configuration.



Login

User Name *
Okta_taylor.cavaletto@bemaservices.com

Authentication Provider *
Okta

Confirmed
☑ Yes

Locked Out
□ Yes

## QUESTIONS

For any questions, please contact us at chris.green@bemaservices.com