KAKAPO
SYSTEMS

UNITY PARTNER PORTAL

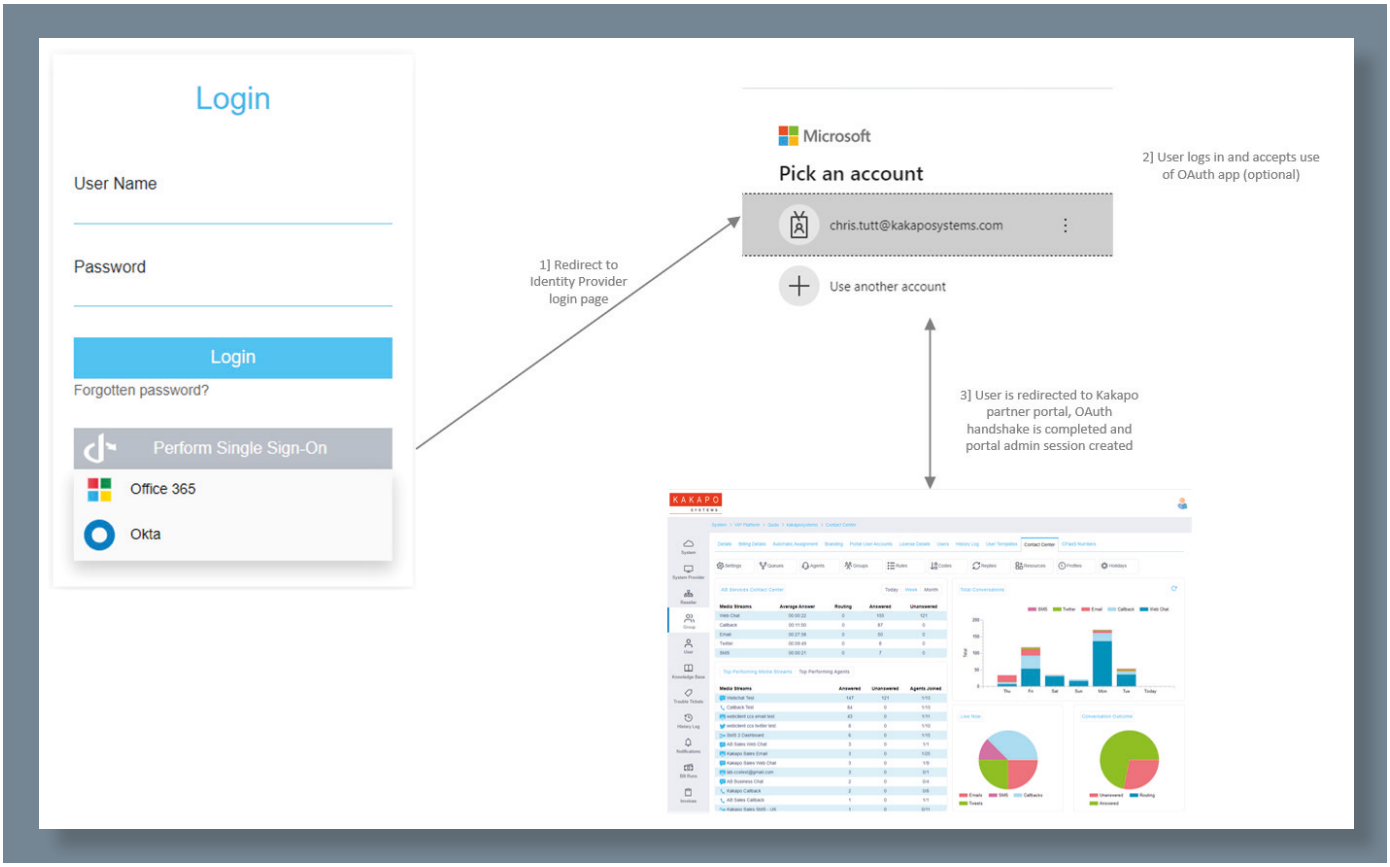
Single-Sign On (SSO)

CONTENTS

1 OVERVIEW

This document outlines how to incorporate Single-Sign On (SSO) into the Kakapo partner portal in order to streamline login and facilitate effective password management.

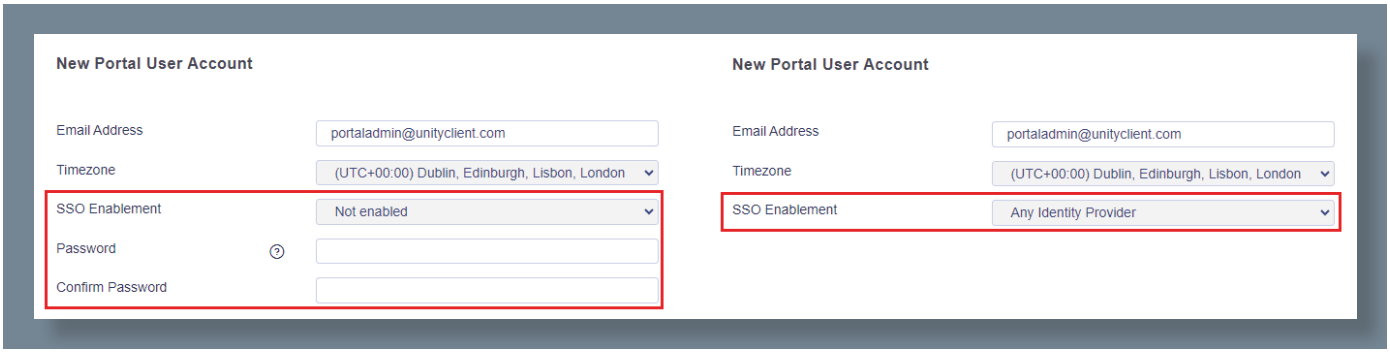
Single-Sign On is achieved through OAuth (https://en.wikipedia.org/wiki/OAuth), in that an OAuth application is created on the Identity Provider (IdP) platform, which the Kakapo partner portal uses to authorise a user. Once the OAuth handshake has completed between the Identity Provider and Kakapo portal, the OAuth token is used to find the portal admin account in the portal and create a web session using that identity. This process is illustrated below:



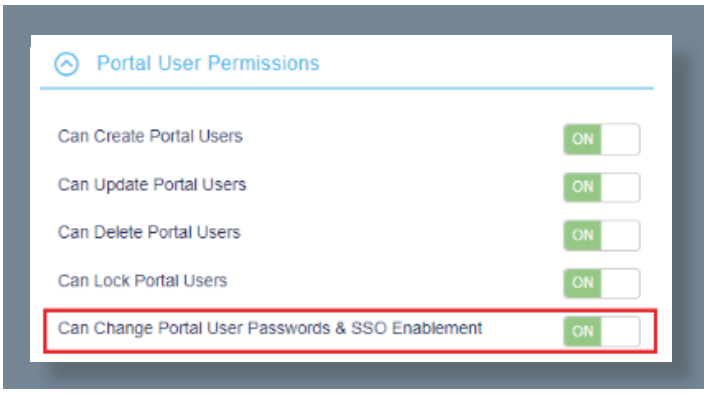
2 PORTAL ADMIN CONFIGURATION

All portal admin accounts must exist in the Kakapo portal, even those using SSO. This is because SSO is used to authenticate the user, rather than using a login ID and password. However internal permissions that have been assigned to the portal user provide authorization parameters.

The SSO Enablement setting dictates if SSO is available to the portal admin, and can be set when creating or updating an account. If SSO enablement is not enabled then only a password can be used to log into the partner portal. Otherwise if any other option is selected then a password cannot be used. It is not possible to offer both SSO and login using a password, because if SSO is being used the password is considered unnecessary so is nullified.



Please note that this setting can only be changed by portal admins that themselves have the below permission assigned.



Current SSO enablement options are outlined below:

SSO Enablement	Description
Not Enabled	SSO is not permitted, only login with a password is allowed
Office365 Only	Only SSO using Office365/Azure AD is permitted
Okta Only	Only SSO using Okta is permitted
Any Identity Provider	SSO using Office365/Azure AD or Okta is permitted

This list will be expanded as support is added for additional SSO Identity Providers in the Kakapo partner portal.

If the SSO Enablement option is changed for an existing portal admin account then an email will be sent to notify the user of the change, as illustrated below:

Please note when SSO has been disabled the new password will also be provided in a separate email, because the previous one was nullified when SSO was enabled. The user will be prompted to change their password on first login.

3 IDENTITY PROVIDER CONFIGURATION

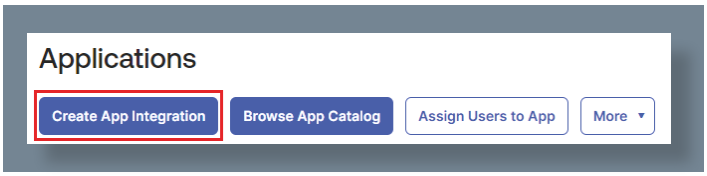
Identity Providers are objects in the Kakapo portal that provide the link into the OAuth Identity Provider platform, which is used when performing login and logout. They can be created and managed at the Group, Reseller, System Provider and System levels in the Kakapo portal, however there is already an existing Office365/Azure AD Identity Provider at the System level which is used by all SSO logins – this means that Identity Providers of this type cannot be created elsewhere in the hierarchy. Other Identity Providers must be configured in the portal as outlined below.

3.1 OKTA CONFIGURATION

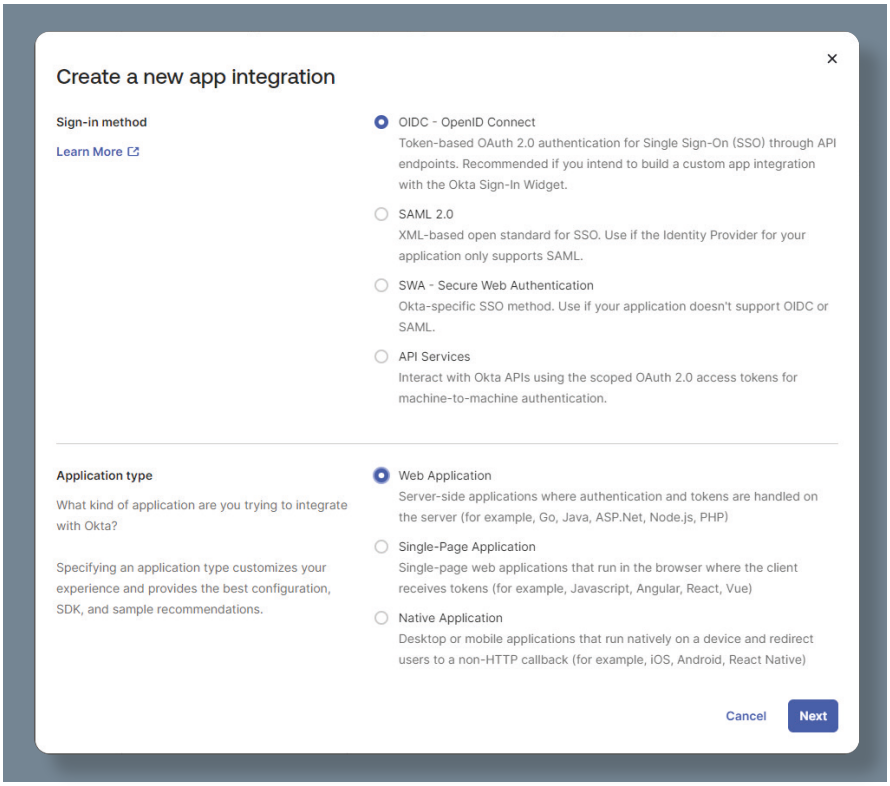
Because Okta uses a different domain per Okta customer, it is possible for an Okta Identity Provider to be created the Group level in the Kakapo portal, which can be used by any portal admins (for example contact center admin) to perform SSO into the portal. All Okta Identity Providers are created the same way, regardless of the level at which they are created at.

3.1.1 Create SSO Application in Okta

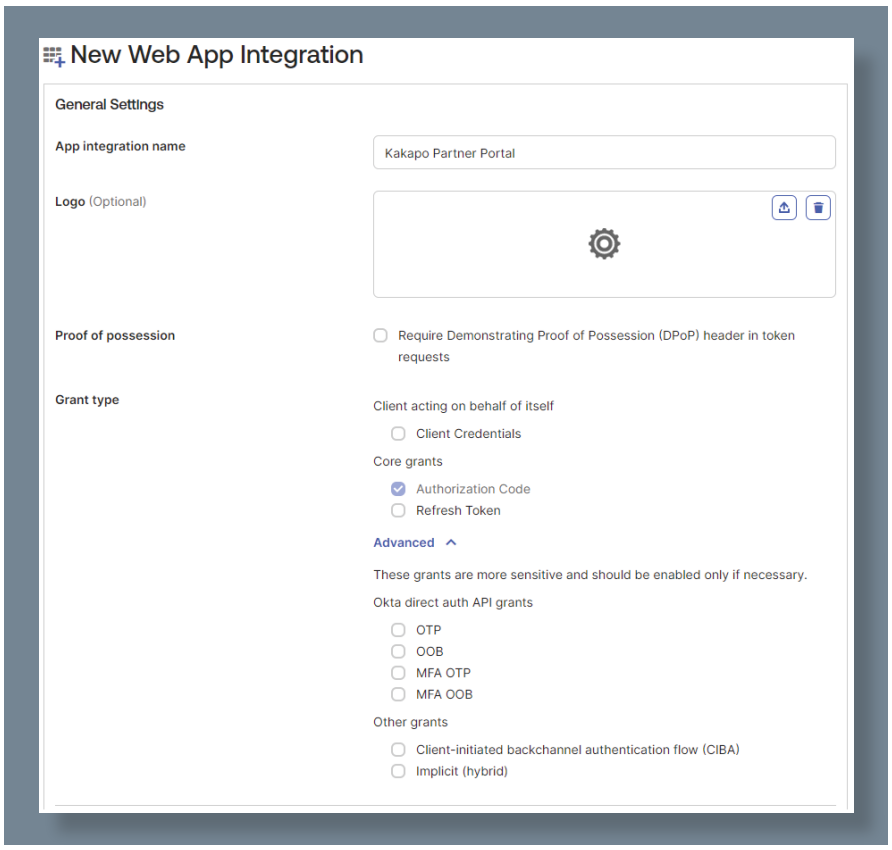
Use the Create App Integration wizard from within Okta to create the OAuth app.



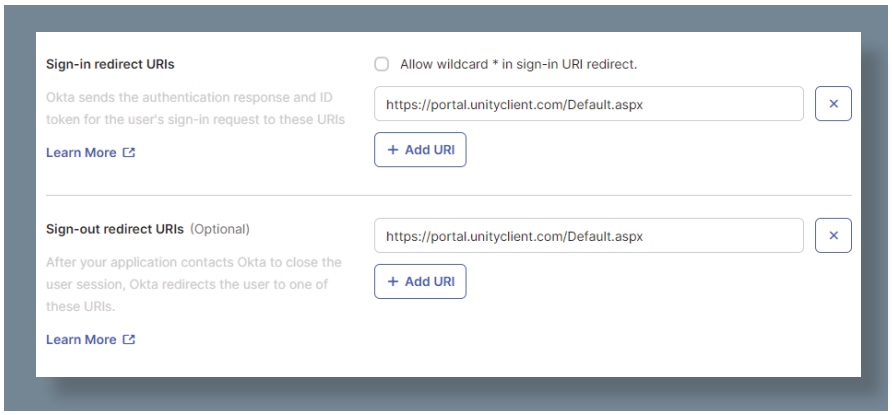
The application should be configured as an OpenID Connect web application.



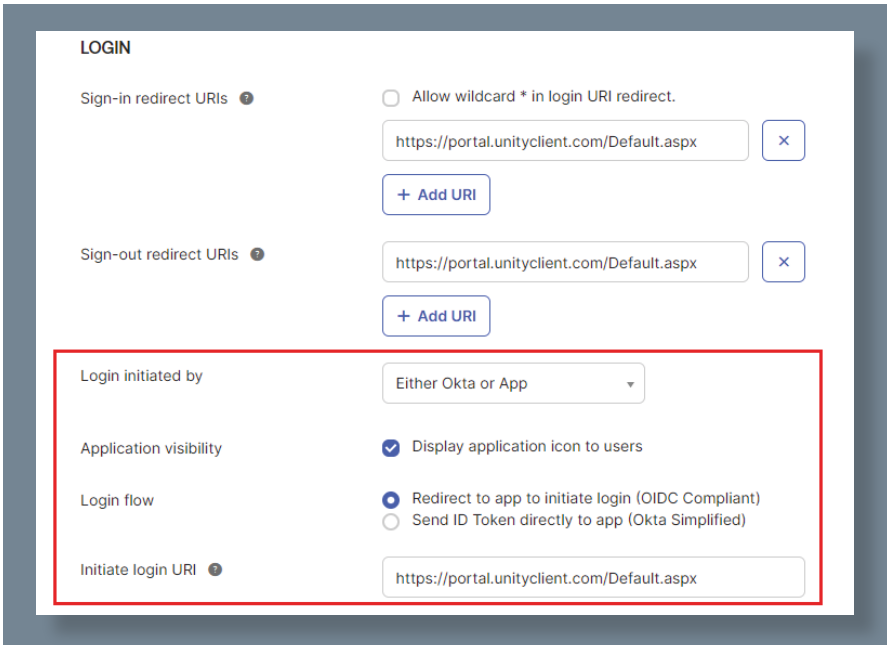
The application can have any name and logo (optional), only the Authorization Code grant needs to be checked.



In most cases the URL to use will be https://portal.unityclient.com/Default.aspx which must be entered correctly or the OAuth handshake will fail. The only time this URL may be different will be if portal customization has been performed, in which case the URL will have been confirmed by Kakapo Systems as part of the customization project.



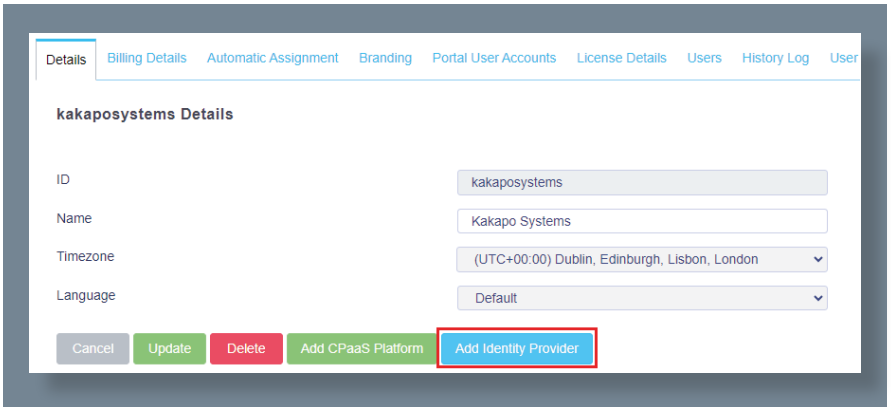
Once the application has been created it can be configured so that users can perform SSO into the Kakapo portal directly from the Okta dashboard, as shown below:



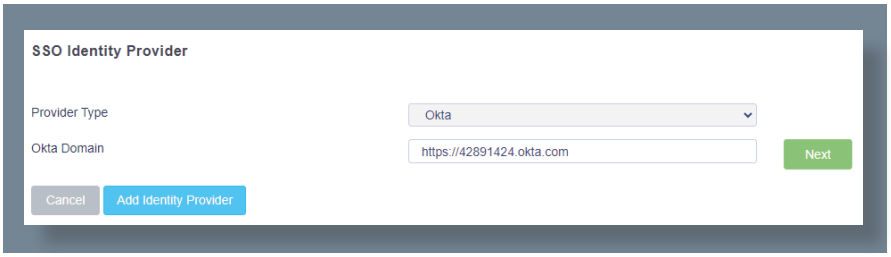
3.1.2 Create Identity Provider in Kakapo Partner Portal

Once the SSO application has been created in Okta it can be referenced in the Kakapo portal.

Click on the Group, Reseller or System Provider where you want to create the integration, then click 'Add Identity Provider' – please note this requires the 'Can Create Objects' permission.

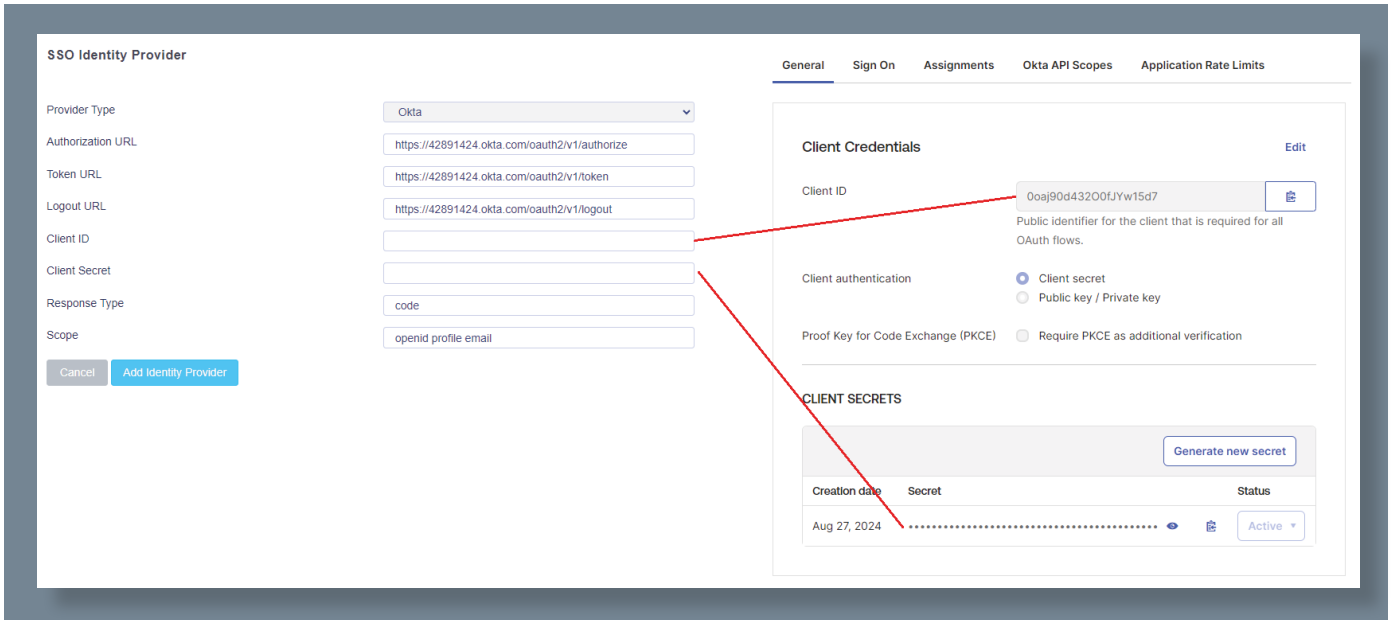


Select Okta from the list of available provider types, then enter the domain of your Okta account. All Okta accounts have their own domain, please contact your security administrator if you are unsure what this is.



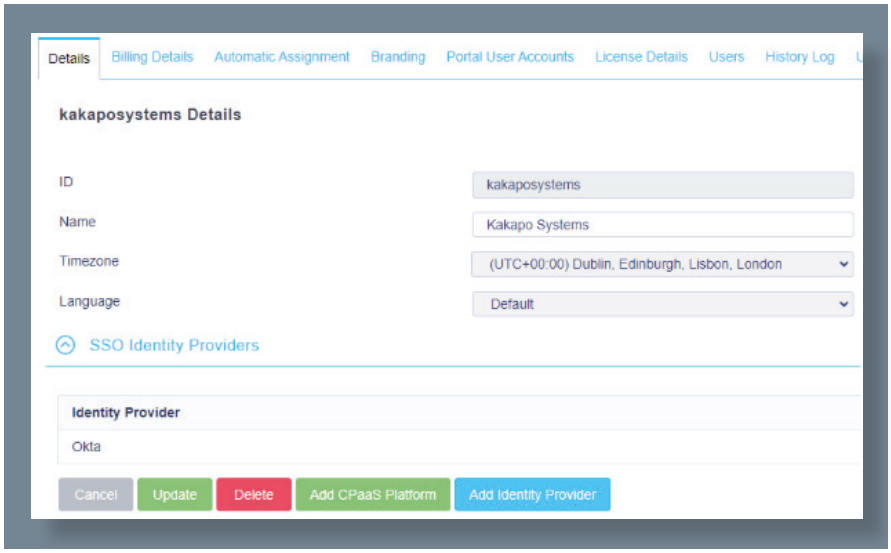
When you click Next all URLs will be completed based on the Okta domain entered, all fields can be modified but these are values known to work correctly so should only be changed if you are certain they are incorrect for your customer account in Okta.

The client ID and secret should be copied directly from Okta and pasted into the fields shown below:



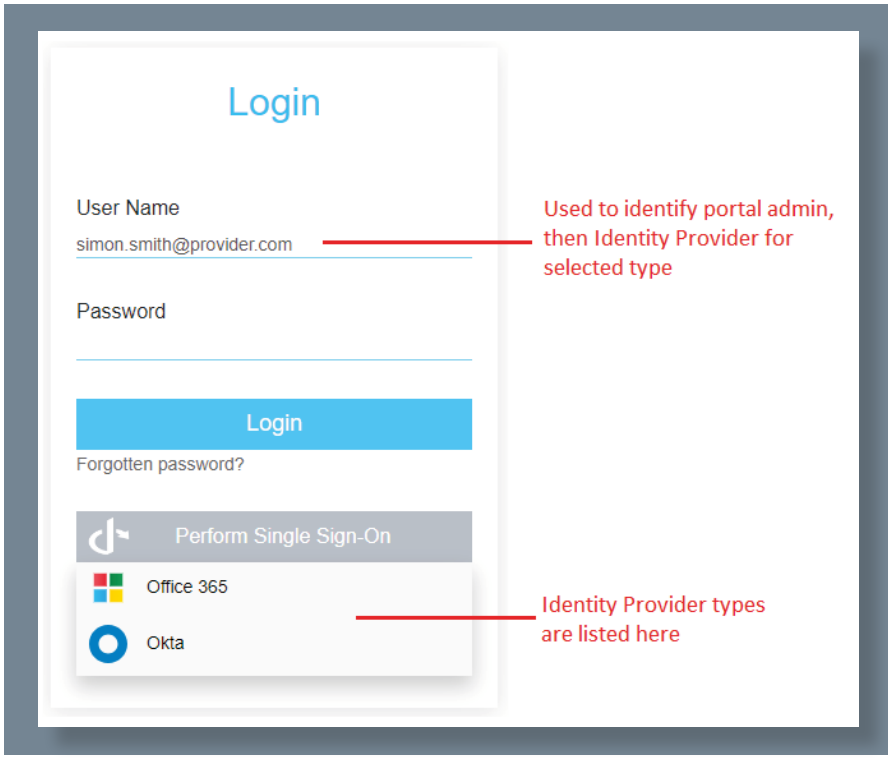
Please note that a Group, Reseller or System Provider can only reference one Okta app, and the Okta domain can only be used once throughout the Kakapo hierarchy, therefore it is imperative that the Identity Provider is created at the correct level in the portal.

Once the Identity Provider has been created it will be displayed in the profile page for the Group, Reseller or System Provider that it was created for. Clicking on the Identity Provider will allow all settings to be modified, or for the Identity Provider to be deleted.



4 PORTAL ADMIN LOGIN & LOGOUT

When logging into the partner portal, the Identity Provider type must be selected from the SSO drop down, as illustrated below:

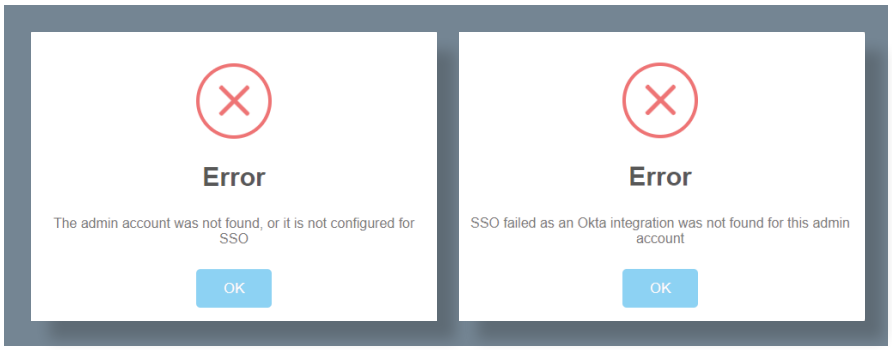


Once selected, the partner portal will use the email address entered to find the portal admin, then look for an Identity Provider of the selected type. Identity providers created at lower levels in the portal hierarch will be considered first, as outlined in the below table.

Portal Admin Level	Identity Provider Search Performed At
Group level admin	Group level Then Reseller level Then System Provider level Then Parent Provider level (if applicable) Then System level
Reseller level admin	Reseller level Then System Provider level Then Parent Provider level (if applicable) Then System level
System Provider level admin	System Provider level Then Parent Provider level (if applicable) Then System level
Parent Provider level admin	Parent Provider level Then System level
System level admin	System level only

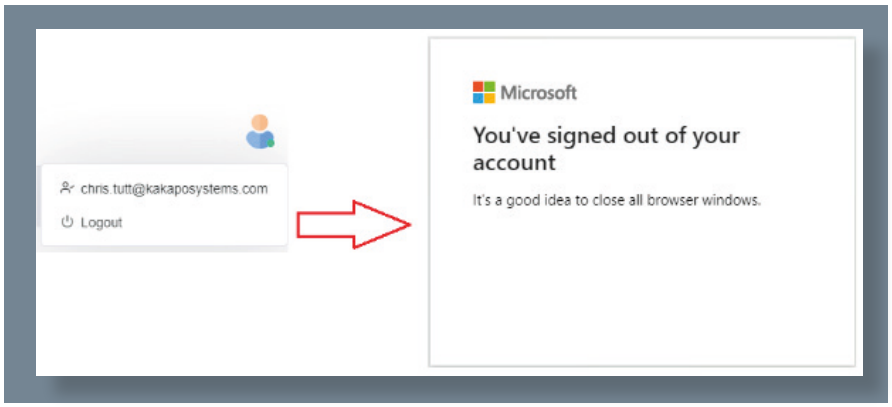
Please note the email address doesn't need to be entered when using Office 365 for SSO because this Identity Provider exists at the System level, so is available to all.

If the portal admin account was not found based on the email address entered (when not using Office 365) or if an Identity Provider was not found for the selected type, then the portal will display an error.



Otherwise the web page will be automatically redirected using the configuration of the Identity Provider found. The user may or may not be prompted to login, based on if they are already logged in. Once login is complete (or is not required) the web page will be automatically redirected back to the Kakapo portal, where OAuth handshake will be completed. If there are any issues when performing the OAuth handshake the user will be alerted, otherwise they will be logged into the Kakapo portal with the permission set of their portal admin account.

Once the user is logged into the Kakapo portal through SSO, if they click Logout they will be logged out of the SSO Identity Provider as well, this is accepted best practice when implementing SSO.



KAKAPO
SYSTEMS

T +44 (0)207 084 6845
E tellmemore@kakaposystems.com
W www.kakaposystems.com
International House | 36-38 Cornhill | London | EC3V 3NG

FIND US ON