

Integrating Office Timesheets with Azure Active Directory

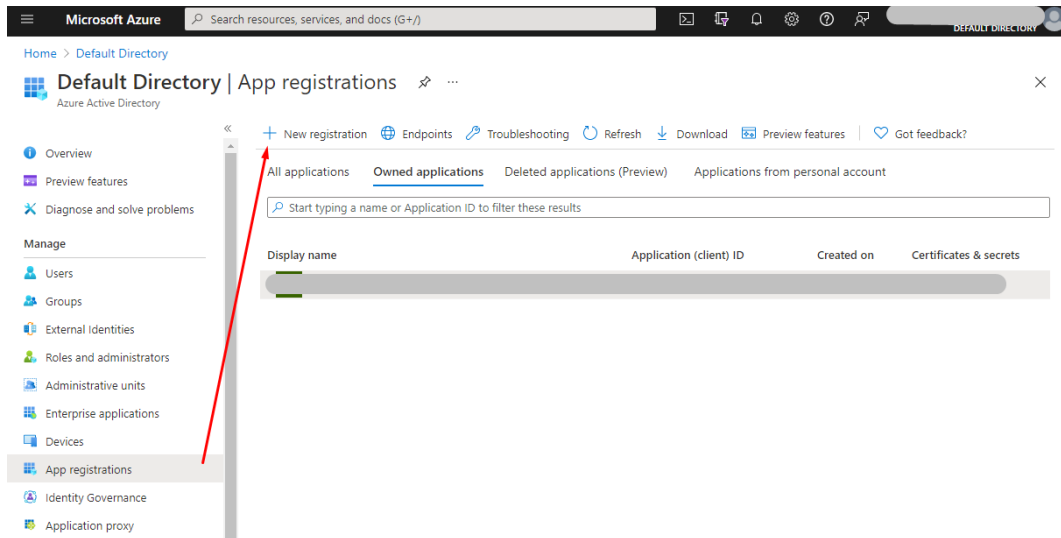
Contents

- Configuring Office Timesheets to use Azure Active Directory Authentication3
- Assigning the Azure User IDs to an Office Timesheets Employees9
 - Using Azure Principle Name (**Most Popular Method**)10
 - Using the Azure Object ID11
- Logging into Office Timesheets using Azure Authentication13
- Bypassing Azure AD Authentication13

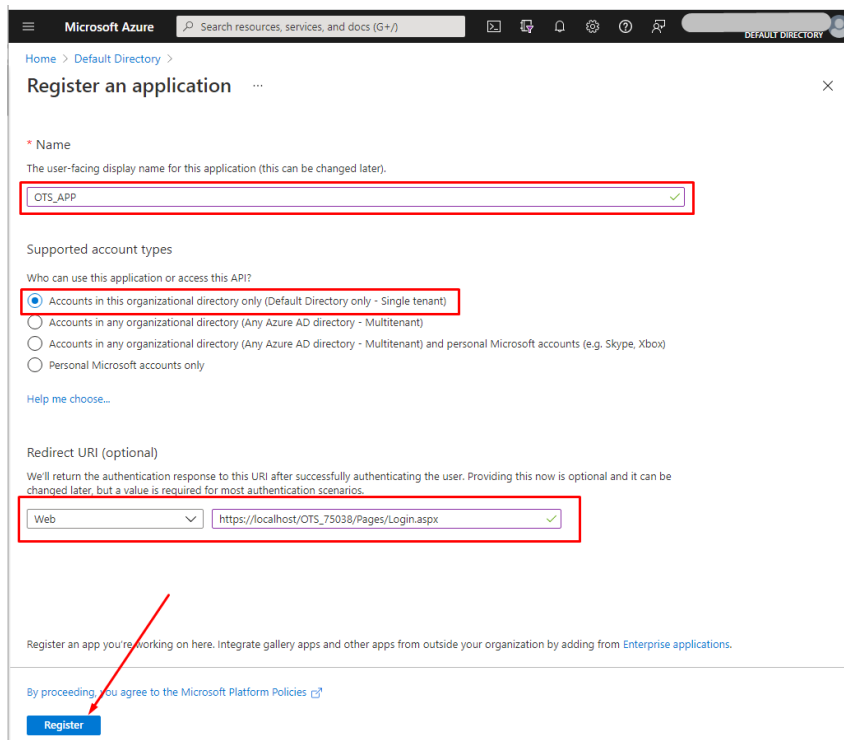
Configuring Office Timesheets to use Azure Active Directory Authentication

To configure Office Timesheets for using Azure Active Directory Authentication you'll need to adjust Office Timesheets' Password Options and configure Azure to allow access from Office Timesheets, register the application and adjust some a few additional items:

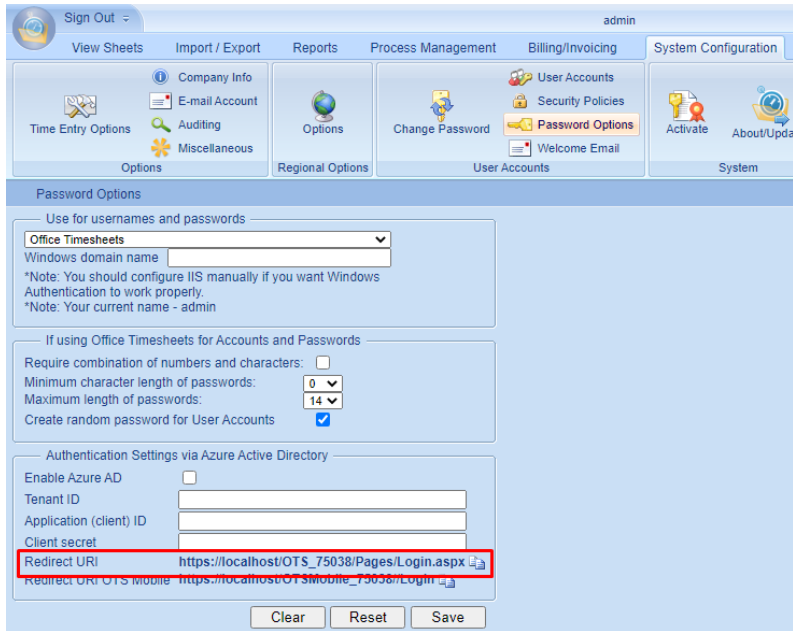
1) Log into Azure and go to **Azure Active Directory -> App Registration -> New registration**



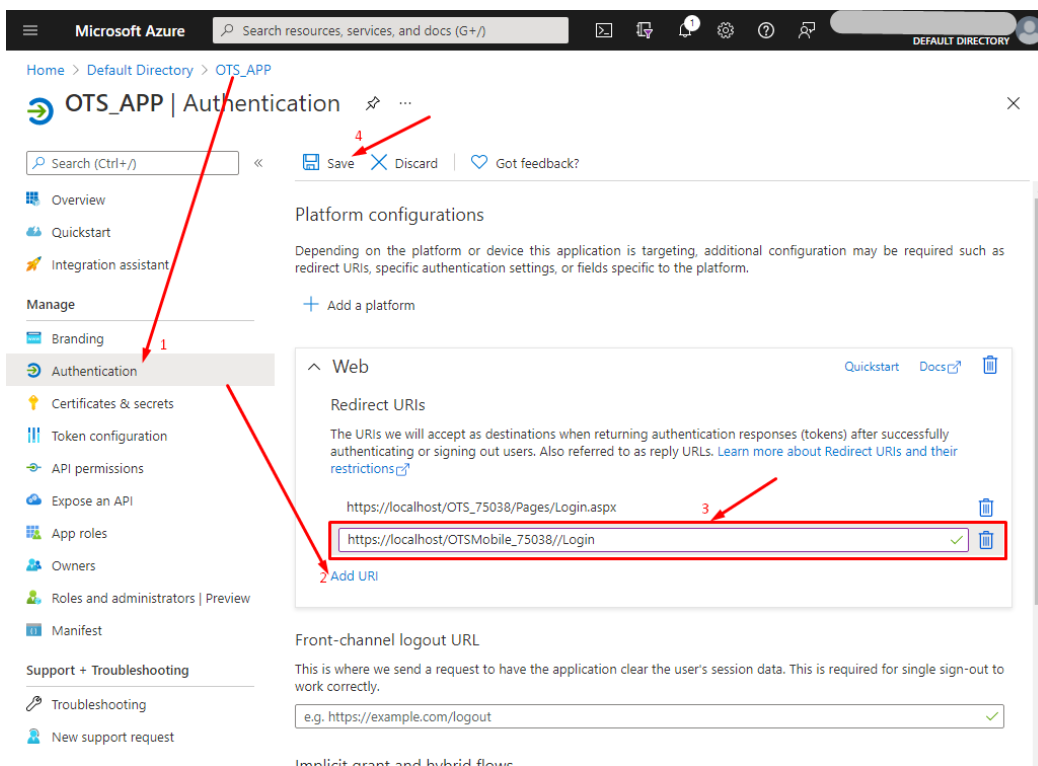
2) Register a new Application that will be used by Office Timesheets



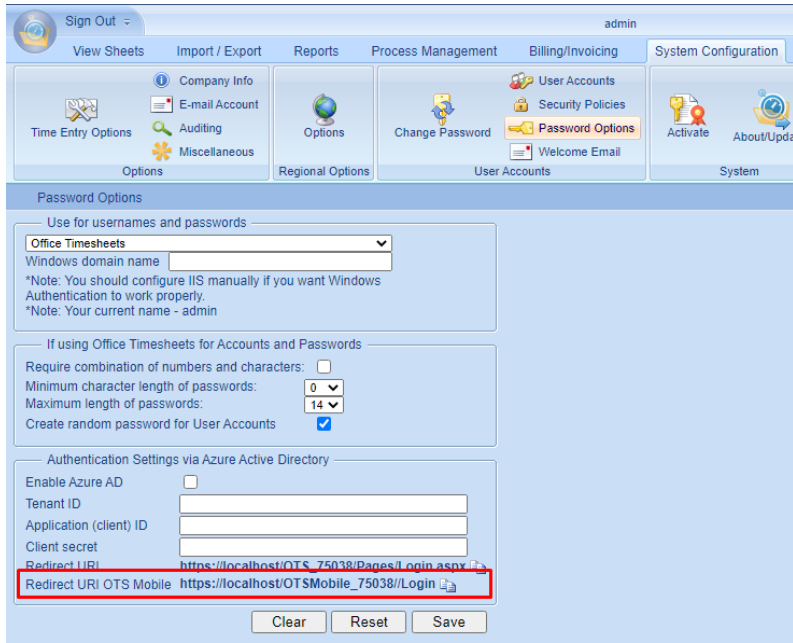
The **Redirect URL** should correspond to the Office Timesheets login page, and can be found within the **Password Options** page in the *System Configuration* tab here:



- 3) If your Office Timesheets installation (including OnDemand accounts) has a mobile instance then you'll need to add a **Redirect URL** for the mobile site as well...

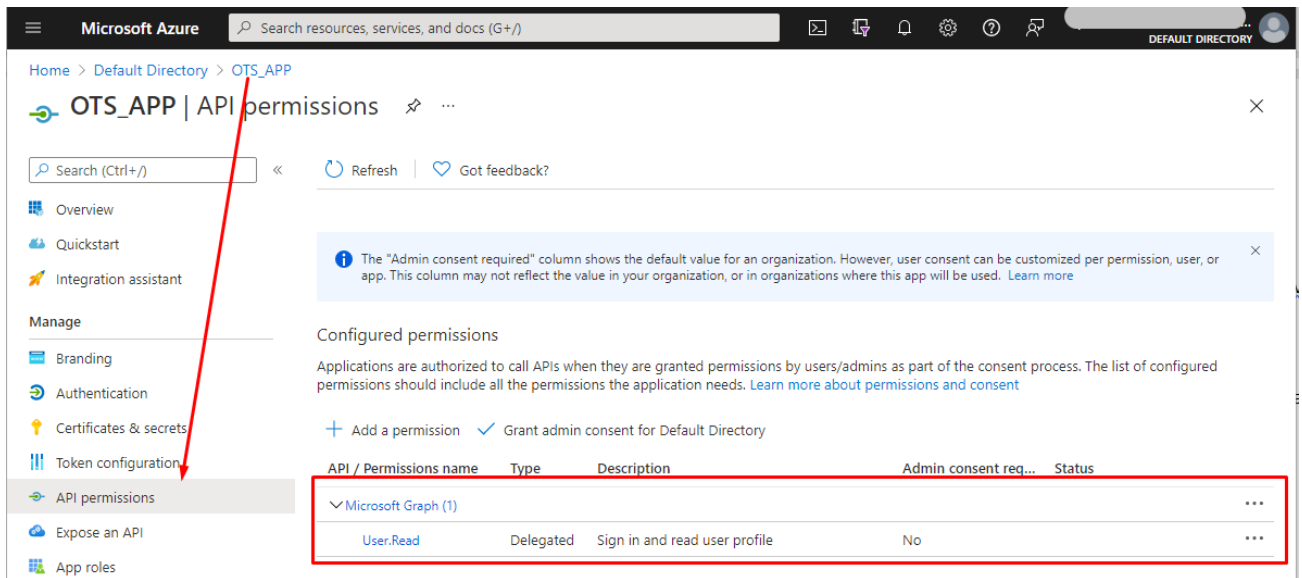


The **Redirect URL** should correspond to the Office Timesheets Mobile login page, and can be found on the Office Timesheets **Password Options** page in the *System Configuration* tab here:



- 4) Next, you'll need to assign the **User.Read** permission to the application you added. This permission is typically assigned automatically upon creation of the application. However, you'll need to make sure the permission is correct.

The permission should be as follows:



If this permission is not present on the page as shown above then you'll need to remove all existing permissions, and add the correct permission that the Office Timesheets app needs: (**Microsoft Graph User.Read**)...

Microsoft Azure | Search resources, services, and docs (G+)

Home > OTS_APP

OTS_APP | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners

Configured permissions

Applications are authorized to call APIs: all the permissions the application needs

+ Add a permission Grant access

API / Permissions name

No permissions added

To view and manage permissions and...

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Office 365 Management APIs

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

More Microsoft APIs

Microsoft Azure | Search resources, services, and docs (G+)

Home > OTS_APP

OTS_APP | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners

Configured permissions

Applications are authorized to call APIs: all the permissions the application needs

+ Add a permission Grant access

API / Permissions name

No permissions added

To view and manage permissions and...

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Microsoft Azure | Search resources, services, and docs (G+)

Home > OTS_APP

OTS_APP | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs: all the permissions the application needs

+ Add a permission Grant access

API / Permissions name

No permissions added

To view and manage permissions and...

Request API permissions

< All APIs

- UserNotification
- UserTimelineActivity
- User (1)**

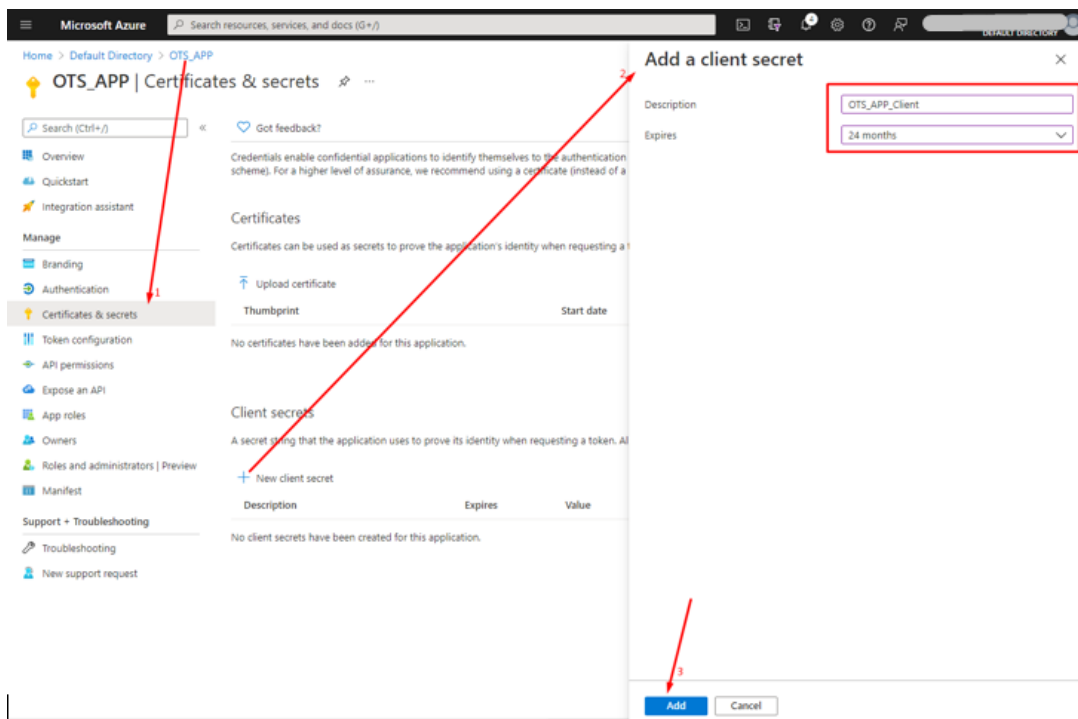
<input type="checkbox"/>	User.Export.All	Export users' data	Yes
<input type="checkbox"/>	User.Invite.All	Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All	Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read	Sign in and read user profile	No
<input type="checkbox"/>	User.Read.All	Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadBasic.All	Read all users' basic profiles	No
<input type="checkbox"/>	User.ReadWrite	Read and write access to user profile	No
<input type="checkbox"/>	User.ReadWrite.All	Read and write all users' full profiles	Yes

WindowsUpdates

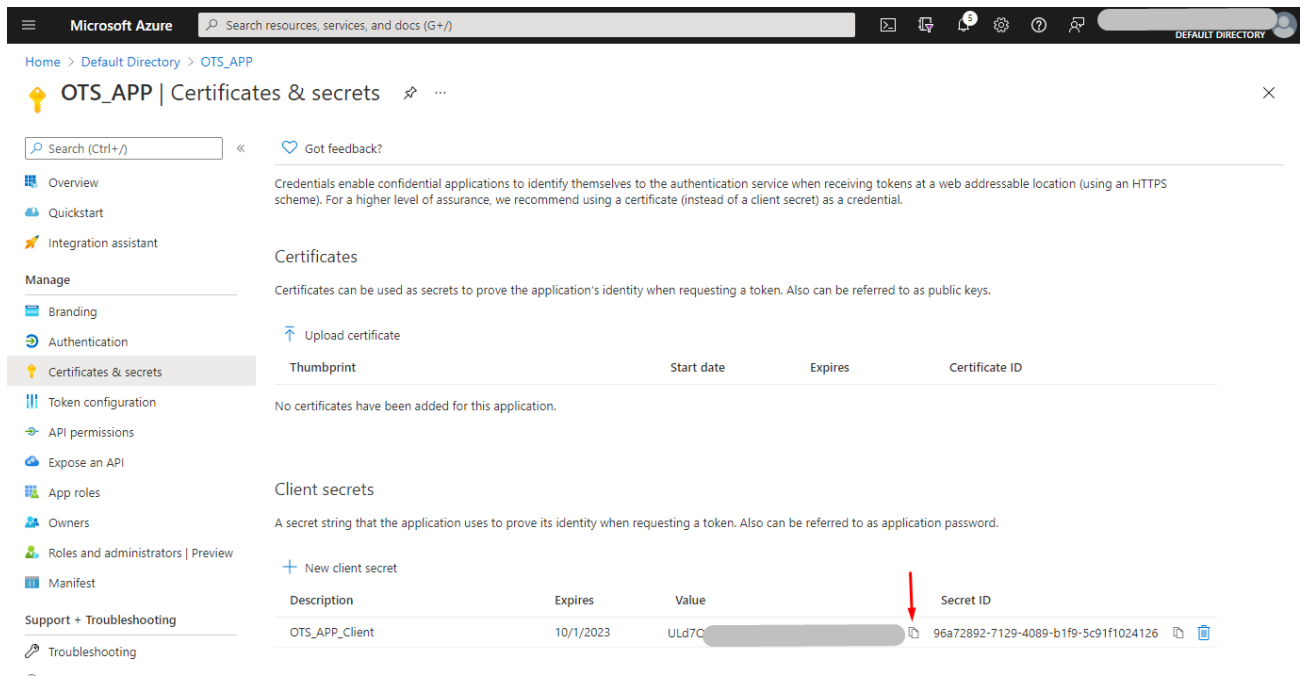
Workforceintegration

Add permissions Discard

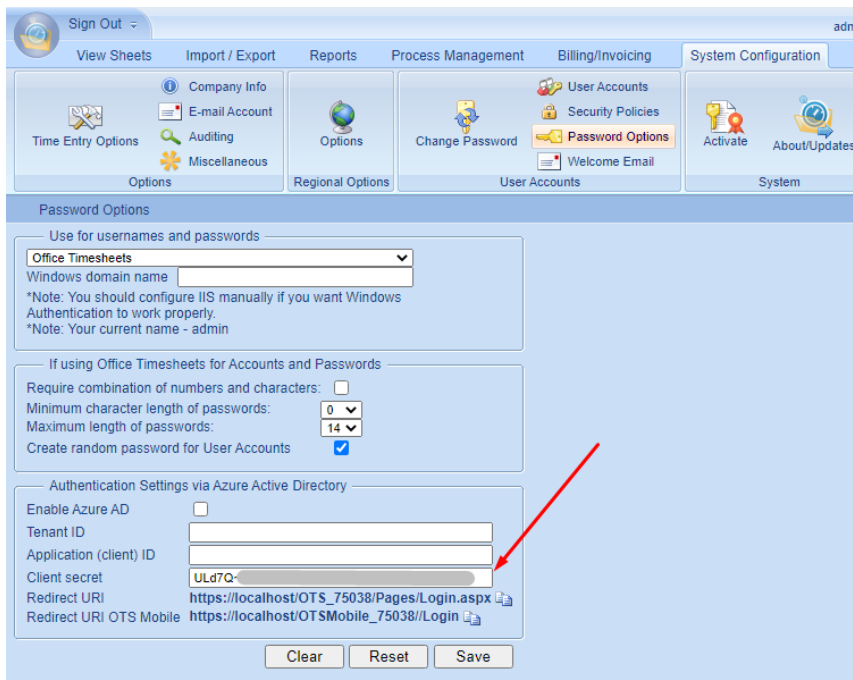
5) Next, you'll need to create a **Client Secret** and save the secret key to the Office Timesheets application...



Copy the Secret Key **Value**...

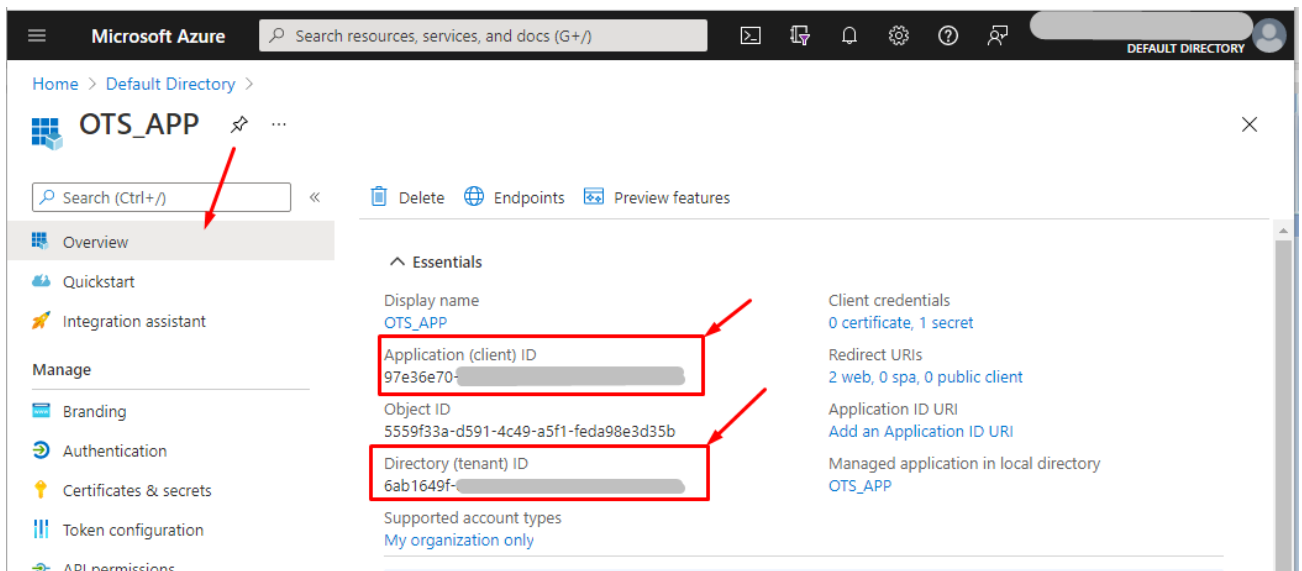


Insert the secret key's **Value** into the **Client secret** field of Office Timesheets' *Password Options*...

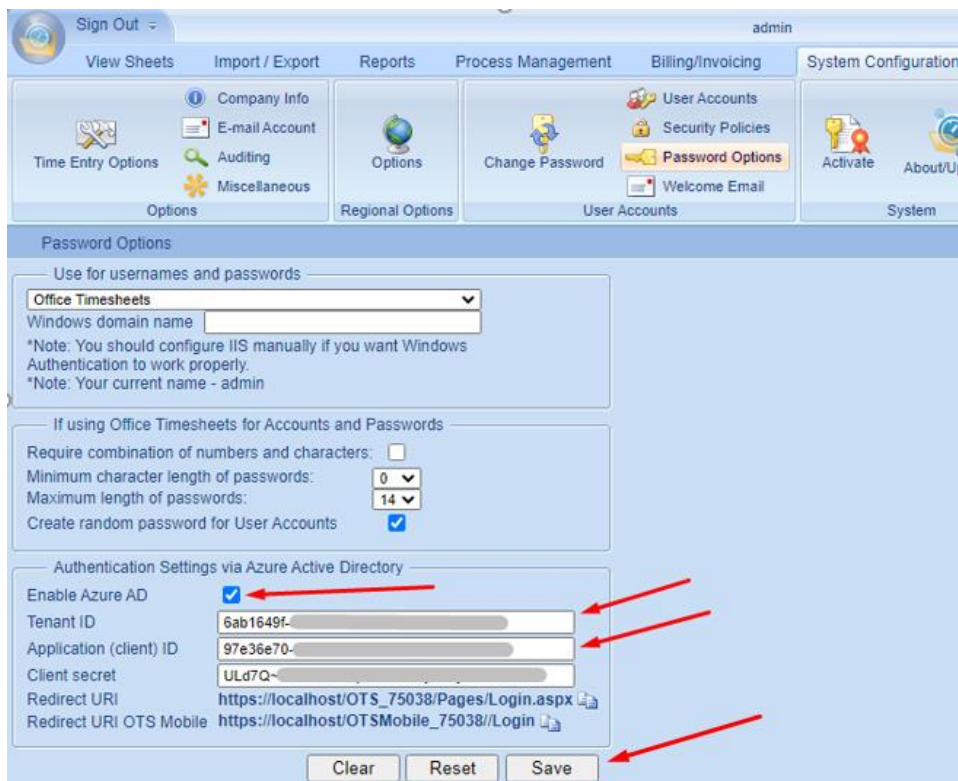


Be sure to **Save** the any changes to this options page.

6) Next, copy the Office Timesheets **Application ID** and **Tenant ID**...



Insert these copied values into Office Timesheets' Password Options; and check **Enable Azure AD** and **Save** the settings.



Assigning the Azure User IDs to an Office Timesheets Employees

To allow an Azure user to log into Office Timesheets, the user must be assigned to an Office Timesheets employee record.

There are two methods that can be used to assign an Azure User Account to an Office Timesheets Employee record.

The first method that can be used to assign an Azure User Account to an Office Timesheets Employee record is by using the Azure User's "User Principle Name". In most cases the Azure User's Principle Name is the same as their email address. When this is the case, then this typically makes the assignment much easier, as the Timesheet administrator doesn't require access to the Microsoft Azure Active Directory Portal; and they can simply apply the employee email address (that's associated with the Azure User Account). Also, this can be done in mass if the email address is already populated in the Office Timesheets employee record as there is a built-in tool to copy all employee's email addresses into their employee Azure ID field with a single click command.

The second method that can be used to assign an Azure User Account to an Office Timesheets Employee record is by using the Azure User's Azure "Object ID". This will require the Office Timesheet Administrator to have to access to the Microsoft Azure Active Directory Portal to obtain each user's Azure Active Directory Object ID.

Using Azure Principle Name (**Most Popular Method**)

Using the Azure User's User Principle Name is the most commonly used method of association with an Office Timesheet Employee, because it's often the same as the employee's email address. If this is the case, then you'll definitely want to use this option.

If you decide to use this option, you'll need to go to **System Configuration -> Password Options** in Office Timesheets; and check the box **Use User Principal Name as Azure ID**. Also, assuming the email field has been populated for all employee records in Office Timesheets, you'll also want to check the box **Copy Email To Azure ID**. Once these options have been activated press the **Save** button.

The screenshot displays the 'System Configuration' menu with 'Password Options' selected. The 'Password Options' section is expanded, showing three main configuration areas:

- Use for usernames and passwords:** A dropdown menu is set to 'Office Timesheets'. Below it are fields for 'Windows domain name' and two notes: '*Note: You should configure IIS manually if you want Windows Authentication to work properly.' and '*Note: Your current name - James Bone'.
- If using Office Timesheets for Accounts and Passwords:** Includes a checkbox for 'Require combination of numbers and characters' (unchecked), dropdowns for 'Minimum character length of passwords' (0) and 'Maximum length of passwords' (14), and a checked checkbox for 'Create random password for User Accounts'.
- Authentication Settings via Azure Active Directory:** This section is highlighted. It contains:
 - 'Enable Azure AD' checked.
 - 'Use User Principal Name as Azure ID' checked and highlighted in yellow.
 - 'Copy Email To Azure ID' checked and highlighted in yellow.
 - 'Tenant ID' field with a value ending in '1181'.
 - 'Application (client) ID' field with a value ending in '153'.
 - 'Client secret' field with a value ending in 'Msq5Y4J'.
 - 'Redirect URI' field with the value 'http://localhost/OTS/Pages/Login.aspx'.
 - 'Redirect URI OTS Mobile' field with the value 'http://localhost/OTSMobile/Login'.

At the bottom of the form are three buttons: 'Clear', 'Reset', and 'Save' (highlighted in yellow).

Again, assuming the email field has already been populated for each employee record in Office Timesheets, then skip ahead to the topic [Logging into Office Timesheets using Azure Authentication](#).

If an employee's record did not contain the employee email address, then you'll need to manually enter the email address in to the Employee's record in Office Timesheets. To do this, click Process Management ->

Employee. Next, open the employee's record and enter the employee's email address into the *Azure ID* field; and click **Save & Close**.

The screenshot shows the 'Employee' record form. The 'Azure ID' field is highlighted in yellow and contains the email address 'cindy.anderson@lookoutsoftware.com'. Other fields include Full Name, First Name (Cindy), Last Name (Anderson), Display Name/ID (Cindy Anderson), E-Mail, Windows Login, Status (Active), Reporting Period (Weekly), Holiday Group, Manager, Company Code, and ADP File Number / Pay ID. There are also sections for Lock Dates, Time Entry, Expense Entry, and Approval Start Date.

Repeat this for each employee record as needed.

Using the Azure Object ID

Using the Azure User's Object ID is typically used as the method of association with an Office Timesheet Employee when the User Principal Name is not the same as the user's email address within the Azure Active Directory User Profile. If this is the case, then you'll want to use this option.

To use this method, select the desired Azure User with the Azure Active Directory Portal and copy its "**Object ID**"...

Microsoft Azure | Search resources, services, and docs (G+)

Home > Default Directory > Users > [Redacted]

Profile

Diagnose and solve problems

Manage

- Profile
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

Troubleshooting + Support

- New support request

User Sign-ins

Group memberships

Creation time: 8/4/2017, 5:00:41 AM

Identity

Name: James

User Principal Name: [Redacted]

Object ID: 2190e2c6-fcd6-46f3-b53f-c21... [Copy icon]

User type: Member

Issuer: [Redacted] [Manage B2B collaboration](#)

View more

Job info

Next, Insert the "Object ID" into the **Azure ID** field of the corresponding Office Timesheets employee record...

Sign Out - admin

View Sheets | Import / Export | Reports | Process Management | Billing/Invoicing | System Configuration

Employee

Full Name: System

First Name: Administrator

M.I.: admin

Last Name: [Redacted]

Display Name/ID: [Redacted]

E-Mail: [Redacted]

Windows Login: [Redacted]

Azure ID: 2190e2c6-fcd6-46f3-b53f-c21b65583ee

Status: Active

Reporting Period: (No selection)

Holiday Group: (No selection)

Manager: (No selection)

Company Code: (No selection)

ADP File Number / Pay ID: [Redacted]

Lock Dates

Time Entry: [Redacted]

Expense Entry: [Redacted]

Do not allow Time and/or Expense Entries prior to these dates.

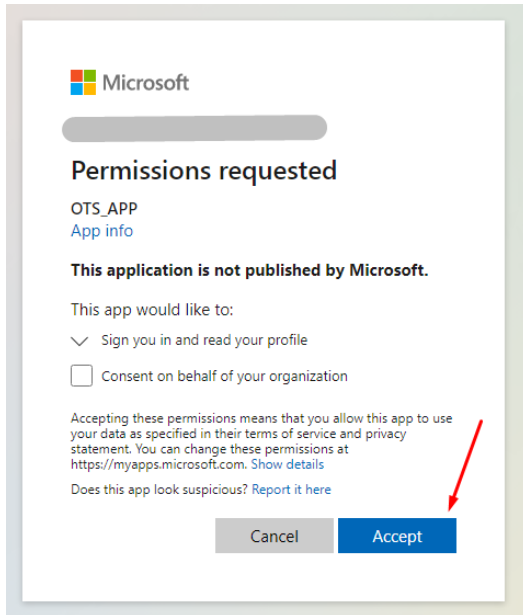
Approval Start Date: 07/29/2011

Do not show Time and/or Expense Sheets prior to this date.

Repeat the steps above for all users.

Logging into Office Timesheets using Azure Authentication

- 1) Log out Office Timesheets; and close your browser session. Next, open a new browser session and type in the URL you use to access your Office Timesheets account. Upon the first login, you'll see the following permission request, which you'll need to **Accept**...



- 2) Done!

Bypassing Azure AD Authentication

If you wish to bypass Microsoft Azure Active Directory Authentication, and authenticate through Office Timesheets simply type of the following text after the URL you use to access Office Timesheets:
?code=IgnoreAzure.