



**Guardian Workplace Access
Outlook365 Plugin
Configuration Guide**

Copyright © 2008 – 2024 Alert Enterprise. All rights reserved.

Trademarks

The trademarks, service marks and logos used in this document are trademarks of Alert Enterprise Corporation, its subsidiaries (collectively, Alert Enterprise) or others. Alert Enterprise and the Alert Enterprise logo are registered trademarks of Alert Enterprise in the United States of America and other countries.

This list is not a comprehensive list of all Alert Enterprise trademarks. Any inquiries regarding these trademarks or whether any other name or logo is a trademark of Alert Enterprise should be directed to Alert Enterprise. Other brands, product names, trademarks and logos appearing in this document are the property of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to Alert Enterprise, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by Alert Enterprise.

Distribution

Use, copying, and distribution of any Alert Enterprise software described in this publication requires an applicable software license. Alert Enterprise believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ALERT ENTERPRISE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Alert Enterprise
4350 Starboard Drive
Fremont, CA 94538
USA

<http://www.AlertEnterprise.com/>

Contents

Preface	4
About this Guide	4
Getting Support	4
<i>Chapter 1. Introduction</i>	5
<i>Chapter 2. Scope</i>	5
<i>Chapter 3. Architecture</i>	6
<i>Chapter 4. Deployment & Configurations</i>	7
Prerequisites	7
Enabling Modern Authentication	7
Register SSO Plugin	8
Grant Administration consent to the Plugin	16
Installing Plugin in outlook 365	16
Uninstalling Plugin in outlook 365	19
Disabling Plugin in outlook 365	21
Enabling Plugin in outlook 365	23
<i>Chapter 5. Usage of Plugin</i>	26
<i>Chapter 6. Configurations – Alert Enterprise Agent Server & Cloud Server</i>	33
<i>Chapter 7. References</i>	41

Preface

About this Guide

This guide provides instructions to configure the Alert Enterprise Guardian Workplace Access plugin with Outlook 365. This document is intended for system and web administrators responsible for installing and configuring Plugin in your organization.

The document assumes that you are familiar with Outlook365 and the Alert Enterprise Guardian Workplace Access plugin.

Getting Support

Use the following information to get support for your installation of Alert Enterprise application.

Phone	1-855-253-7887 (1-855-ALERT ENTERPRISE-US)
Email	support@AlertEnterprise.com
Support Portal	http://support.AlertEnterprise.com
Corporate Website	http://www.AlertEnterprise.com/

Chapter 1. Introduction

The Alert Enterprise Guardian Workplace Access for Microsoft Outlook plugin effectively manages user access to the meeting location by integrating Microsoft Office 365 with the Alert Enterprise Guardian Application. The end users can open the calendar invite and request for a Badge or Access to the meeting location for which the user doesn't have access to.

Chapter 2. Scope

The scope of the project includes the following:

Develop a new Outlook Plugin called “Request Workplace Access” with the following features:

Request New Badge

- Using this option, the end user can request a new badge for a meeting location to which they don't have access. Once the user clicks on this button, a call is made to the Alert Enterprise Guardian application along with the user information and the meeting location.
- Based on the rules and policies configured within the Alert Enterprise Guardian application, a request is generated along with the next available badge and the access corresponding to the meeting location. The request will be routed through multiple approvals as per the workflow configuration, and after approval, the badge and access are assigned to the user in the access control system.

Request New Access

- Using this option, the end user can request access to a meeting location to which they don't have access. Once the user clicks on this button, a call is made to the Alert Enterprise Guardian application along with the user information and the meeting location.
- The Alert Enterprise Guardian application will verify if the user has access to the meeting location based on existing access. If the user doesn't have access, a request is generated for the access corresponding to the meeting location. The request will be routed through multiple approvals as per the workflow configuration, and after approval, access is assigned to the user in the access control system.

Provide Single Sign-On Capability

- The Plugin will use the Microsoft Entra platform to enable single sign-on (SSO). The end user should be able to access the Plugin without providing any login credentials. The Plugin should not be accessible directly to the end users; it should be accessible only from the calendar invite.

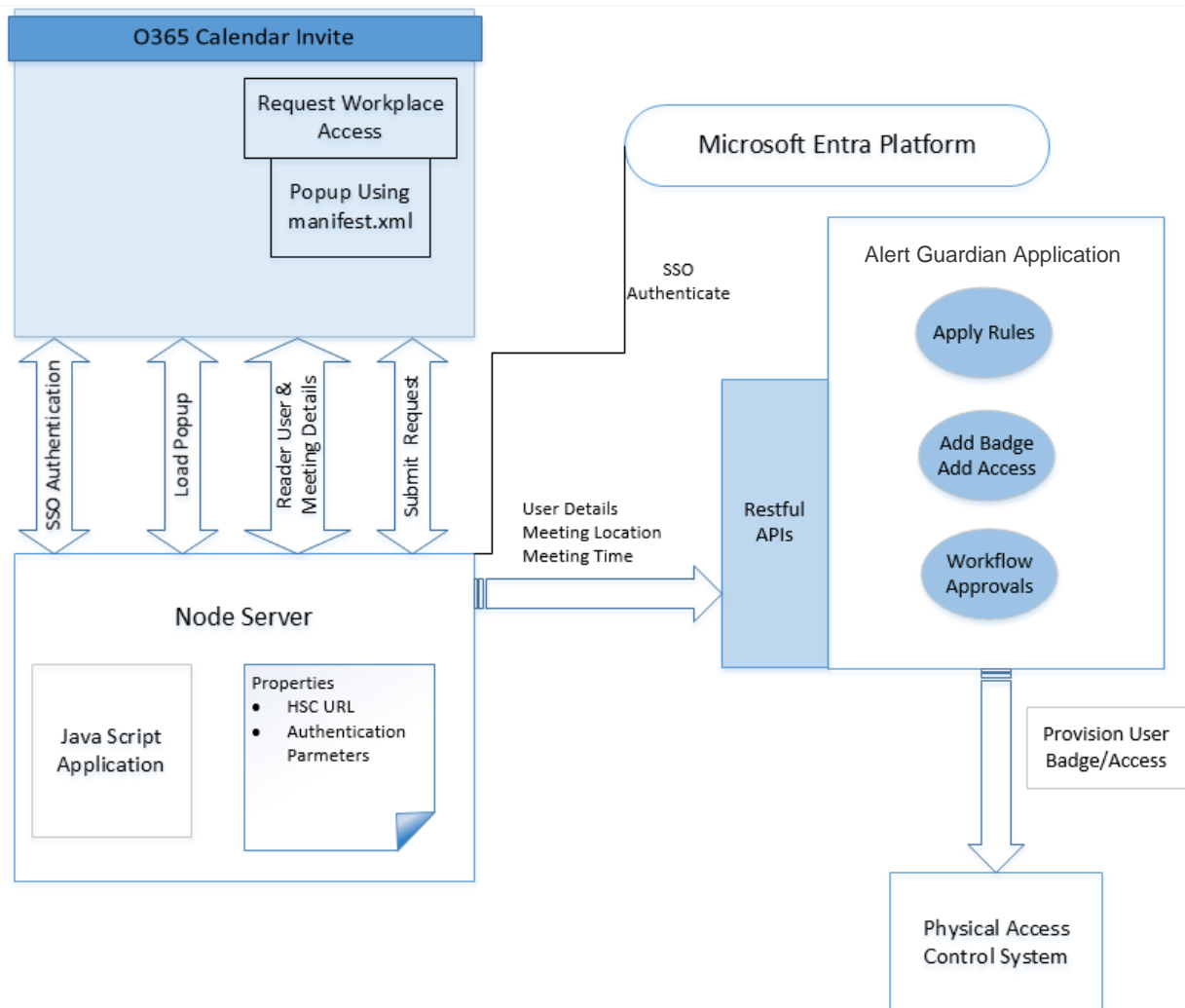
Configuration Screen

- Provide a configuration screen to define the mapping between the Outlook meeting locations and the locations defined in the Alert Enterprise application. This screen should be visible only to Outlook administrators.

Chapter 3. Architecture

The Guardian Workplace Access for Outlook Plugin architecture consists of the Alert Enterprise Guardian Application, Request Workplace Access Plugin, Outlook Calendar, and MS Entra Platform. The Guardian Workplace Access for Outlook Plugin is developed according to the standard Outlook Plugin architecture using manifest.xml. This Plugin is a JavaScript application that runs on a separate node server and is accessible through an HTTPS channel. The HTTPS URL of the application is defined as part of the manifest.xml, and when the end user clicks on the Plugin displayed on the Calendar Invite from the O365 web Outlook, this application loads as a popup.

The Plugin uses the JWT token received from the MS Entra Platform to provide single sign-on capabilities and also leverages the access token to make Graph API calls. The requests made from the Plugin are submitted to the Alert Enterprise Guardian Application using RESTful APIs, where this information is processed, approved, and finally pushed to the underlying access control systems.



Chapter 4. Deployment & Configurations

This section includes:

- **Prerequisites**
- **Enable Modern Authentication (By default it is enabled, so no need in case you create a new office 365 account)**
- **Register SSO Plugin**
- **Grant administration consent to the Plugin**
- **Installing Plugin in outlook365**
- **Uninstalling Plugin in outlook365**
- **Disabling Plugin in outlook365**
- **Enabling Plugin in outlook365**

Prerequisites

You need to have Microsoft Entra Platform Account with O365 subscription and a login account with Global Administrator Privileges.

Enabling Modern Authentication

If you already have an office365 account, you can follow below steps (till point 5) to check if it is enabled or not. This step can be skipped if it is already enabled Otherwise follow these steps to enable it.

Open Windows PowerShell in your window operating system and use below commands.

1. Set-Execution Policy RemoteSigned
2. \$UserCredential = Get-Credential
3. \$Session = New-PSSession -ConfigurationName Microsoft.Exchange - ConnectionUfice365.com/powershell-liveid/ -Credential \$UserCredential -Authentication Basic -AllowRedirection
4. Import-PSSession \$Session -DisableNameChecking
5. Get-OrganizationConfig | ft name, *OAuth*
6. Set-OrganizationConfig -OAuth2ClientProfileEnabled:\$true

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\Windows\system32> $UserCredential = Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.of
fice365.com/powershell-1liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Import-PSSession $Session -DisableNameChecking

ModuleType Name ExportedCommands
-----
Script tmp_On1kgakp.5xm {Add-AvailabilityAddressSpace, Add-DistributionGroupMember, Add-Mailb...

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Mailbox

Name Alias Database ProhibitSendQuota ExternalDirectoryObjectId
-----
DiscoverySearchMailbox... DiscoverySea... INDRP01DG011-db135 50 GB (53,687,091...
JaspreetSingh Jaspreet.s INDRP01DG020-db041 49.5 GB (53,150,2... a00bab67-6a49-4221-a6b...

PS C:\Windows\system32> Get-OrganizationConfig | ft name, *OAuth*

Name OAuth2ClientProfileEnabled
-----
aedev.onmicrosoft.com True

PS C:\Windows\system32> Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true
    
```

You can also follow this link.

<https://social.technet.microsoft.com/wiki/contents/articles/32711.exchange-online-how-to-enable-your-tenant-for-modern-authentication.aspx>

Register SSO Plugin

You need this step to register your Plugin domain with Office 365, This is required for SSO authentication from Microsoft and secure your application, by not getting accessed from outside office 365 or without valid credentials. You can refer this link for complete details

<https://learn.microsoft.com/en-us/office/dev/plugins/develop/register-sso-plugin-aad-v2>

1. Go to this link <https://portal.azure.com/#home>
2. Select App registrations. If you don't see the icon, search for "app registration" in the search bar.
3. Select New registration.

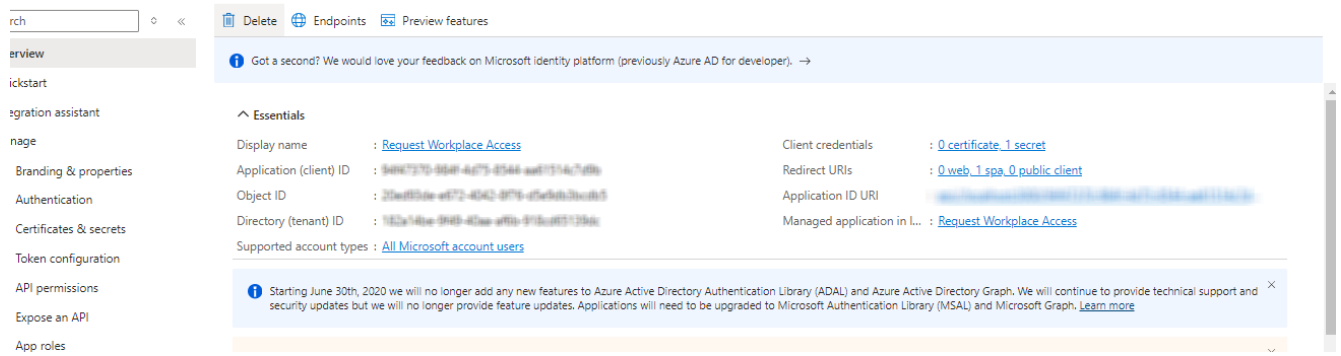
4. Set Name to the Plugin Name

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

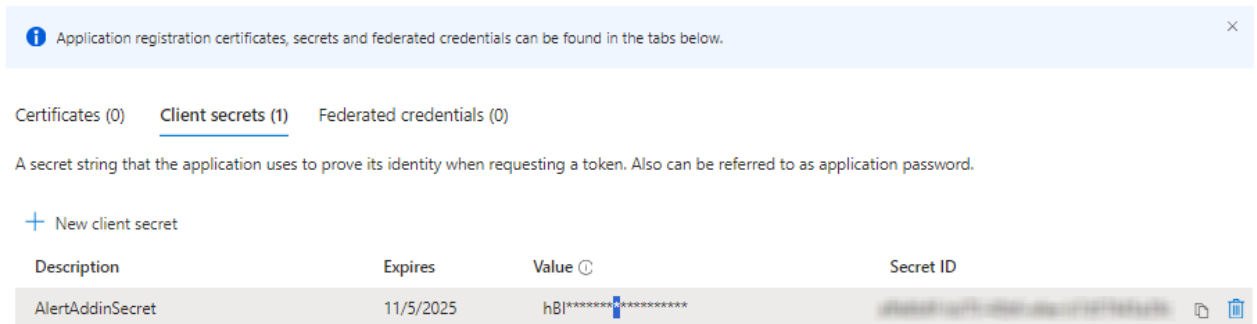
5. Select Register. A message is displayed stating that the application registration was created.
6. Copy and save the values for the Application (client) ID as it will come in use in later procedures.

Request Workplace Access



7. From the left pane, select Certificates & secrets. Then on the Client secrets tab, select new client secret.
8. The Add a client secret pane appears. Add a description for your client secret.
9. Select the Expires duration as per the requirement & Select Add. The new secret is created and the value is temporarily displayed.

Record the secret's value for use in your client application code. This secret value is never displayed again after you leave this pane.

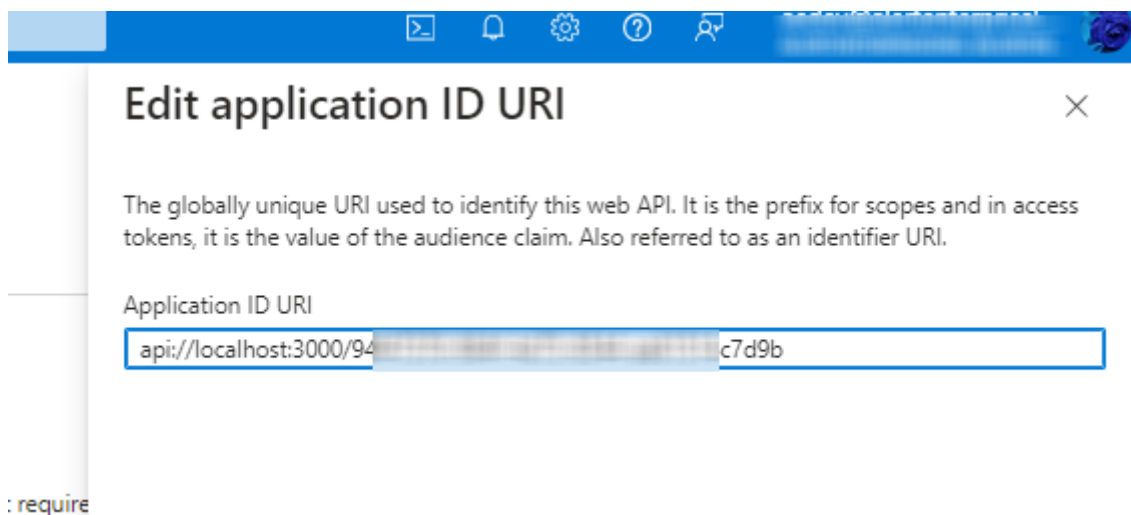


10. Navigate to the Authentication & tick the check Access Tokens & ID Tokens & hit the Save button.

11. **Expose a web API** - From the left pane, select Expose an API.
12. Select Set to generate an application ID URI.

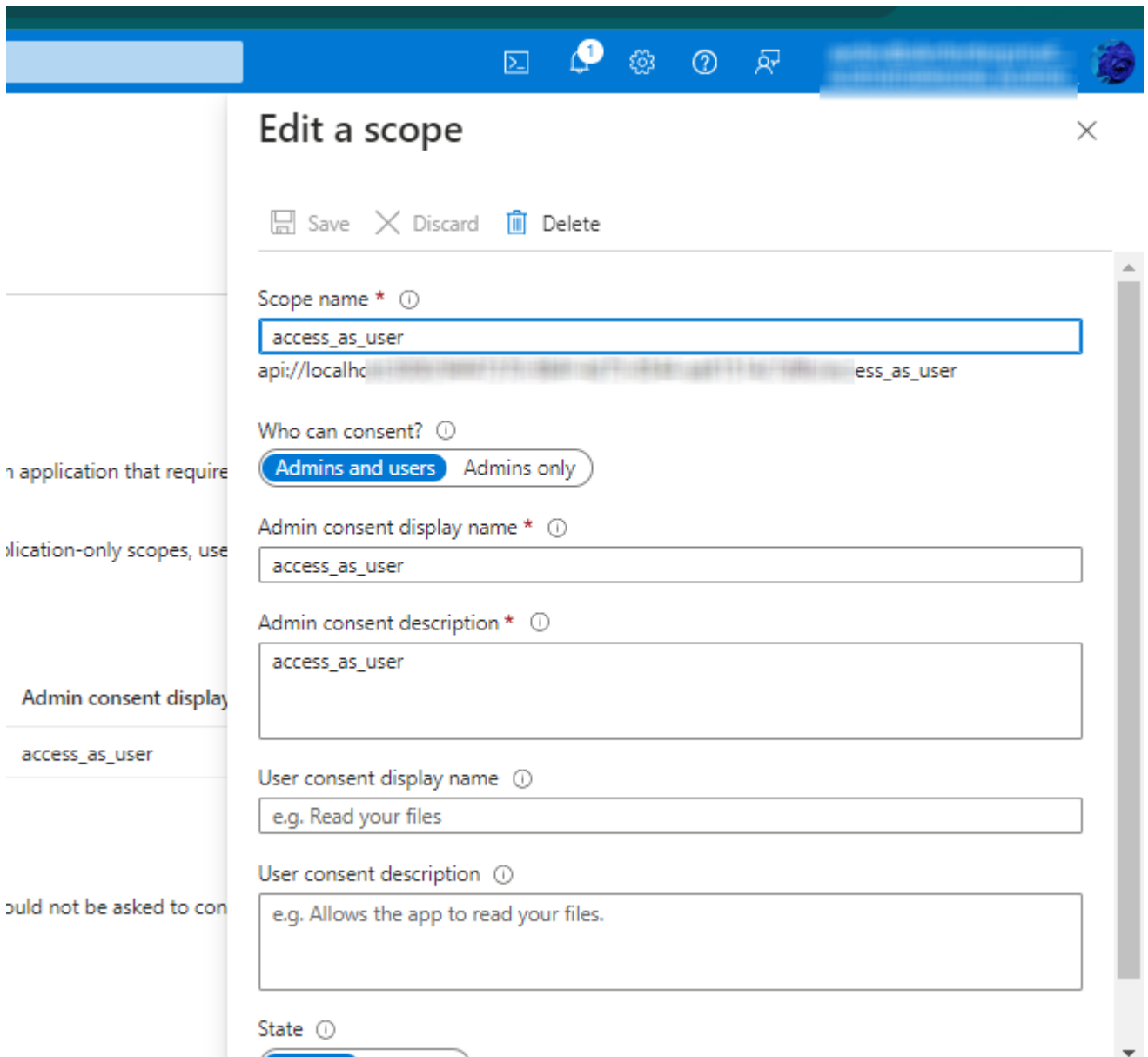
The section for setting the application ID URI appears with a generated Application ID URI in the form `api://<app-id>`.

13. Update the application ID URI to `api://<fully-qualified-domain-name>/<app-id>`



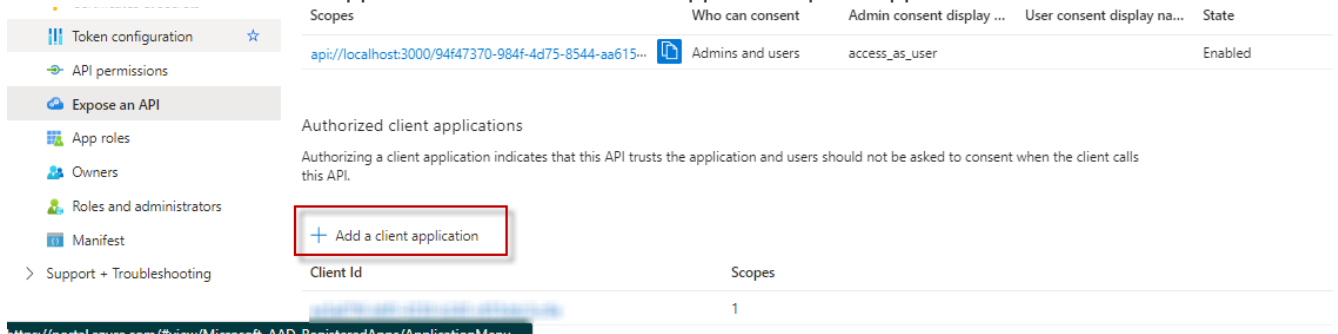
Insert the fully-qualified-domain-name between api:// and <app-id> (which is a GUID). For example, api://contoso.com/<app-id>.

14. **Add a scope** - On the Expose an API page, select Add a scope, The Add a scope pane opens.
15. Set the scope name as access_as_user, set who can consent as Admin and users, in Admin consent display name set A short description of the scope's purpose, in Admin consent description set A more detailed description of the permission granted by the scope.
16. Set the State to Enabled, and then select Add scope.



The new scope you defined displays on the pane. The domain part of the Scope name displayed just below the text field should automatically match the Application ID URI set in the previous step, with /access_as_user appended to the end; for example, api://localhost:6789/c6c1f32b-5e55-4997-881a-753cc1d563b7/access_as_user

17. Select Add a client application. The Add a client application pane appears.



18. In the Client ID enter ea5a67f6-b6f3-4338-b240-c655ddc3cc8e. This value pre-authorizes all Microsoft Office application endpoints.

19. In Authorized scopes, select the api://<fully-qualified-domain-name>/<app-id>/access_as_user checkbox. Select Add application.

Add a client application



Client ID ⓘ

Authorized scopes ⓘ

 api://localhost:44355/cfe719d7-aef3-4108-83a8-a8283f139a69/access_as_user

20. **Add Microsoft Graph permissions** - From the left pane, select API permissions. The API permissions pane opens.

Home > App registrations > Request Workplace Access

Request Workplace Access | **API permissions** ✎ ...

Refresh
Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators

⚠ Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted may be affected.

ℹ The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This can be done in the consent policy, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✔ Grant admin consent for AlertEnterpriseEng

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (15)				
Files.Read	Delegated	Read user files	No	✔ Granted for all users


21. Select Add a permission. The Request API permissions pane opens. Select Microsoft Graph.

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 Rights Management Services
Allow validated users to read and write protected content



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



Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

22. Select Delegated permissions.

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.

23. In the Select permissions search box, search for the permissions your plugin needs. For example, for an Outlook plugin, you might use profile, openid, Files.ReadWrite, and Mail.Read. Attaching below screenshots & add all the below mentioned permissions.
24. Select the checkbox for each permission as it appears. Note that the permissions will not remain visible in the list as you select each one. After selecting the permissions that your plugin needs (choose the required permission based on the requirement), select Add permissions.
25. Select Grant admin consent for [tenant name]. Select Yes for the confirmation that appears.

Home > App registrations > Request Workplace Access

Request Workplace Access | API permissions

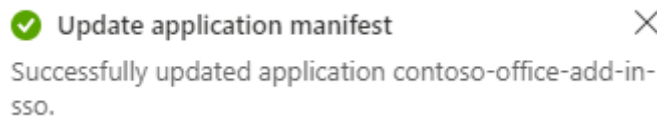
Refresh
Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

+ Add a permission
✓ Grant admin consent for AlertEnterpriseEng

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (15)				
Files.Read	Delegated	Read user files	No	✔ Granted for AlertEnterpr... ***
Files.Read.All	Delegated	Read all files that user can access	No	✔ Granted for AlertEnterpr... ***
Files.Read.Selected	Delegated	Read files that the user selects (preview)	No	✔ Granted for AlertEnterpr... ***
Files.ReadWrite	Delegated	Have full access to user files	No	✔ Granted for AlertEnterpr... ***
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✔ Granted for AlertEnterpr... ***
Files.ReadWrite.AppFolder	Delegated	Have full access to the application's folder (preview)	No	✔ Granted for AlertEnterpr... ***
Files.ReadWrite.Selected	Delegated	Read and write files that the user selects (preview)	No	✔ Granted for AlertEnterpr... ***
Mail.Read	Delegated	Read user mail	No	✔ Granted for AlertEnterpr... ***
Mail.Read.Shared	Delegated	Read user and shared mail	No	✔ Granted for AlertEnterpr... ***
Mail.ReadWrite	Delegated	Read and write access to user mail	No	✔ Granted for AlertEnterpr... ***
Mail.ReadWrite.Shared	Delegated	Read and write user and shared mail	No	✔ Granted for AlertEnterpr... ***
Mail.Send	Delegated	Send mail as a user	No	✔ Granted for AlertEnterpr... ***
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?...	Delegated	Sign users in	No	✔ Granted for AlertEnterpr... ***

26. From the left pane, select Manifest. The Azure Active Directory application manifest appears.
27. Enter 2 as the value for the accessTokenAcceptedVersion property. Select Save. A message pops up on the browser stating that the manifest was updated successfully.



Grant Administration consent to the Plugin

This is required to grant Azure Active Directory permissions. You can refer this link <https://docs.microsoft.com/en-us/office/dev/plugins/develop/grant-admin-consent-to-an-plugin>

- In the following string, replace the placeholder “{application_ID}” with the Application ID that you copied when you registered the plugin. Navigate the link in browser.

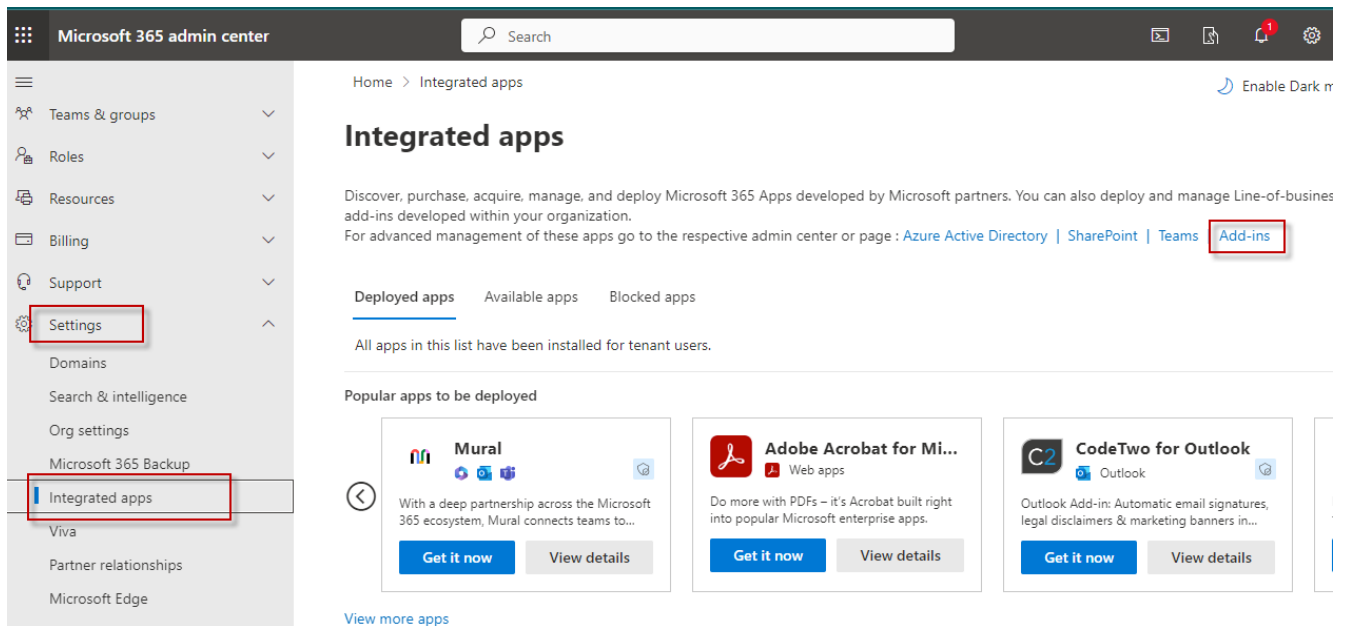
`https://login.microsoftonline.com/common/adminconsent?client_id={application_ID}&state=12345`

- When prompted, sign in with the credentials to your Office 365.
- You are then prompted to grant permission for your plugin to access your Microsoft Graph data. Click Accept.
- The browser window/tab is then redirected to the Redirect URL that you specified when you registered the plugin.

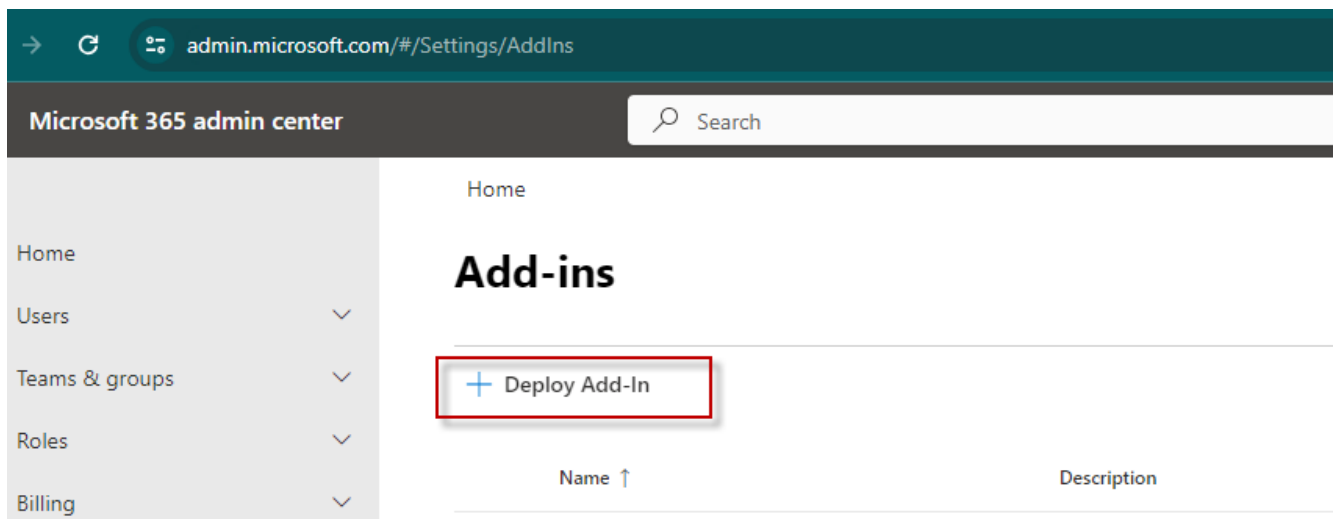
Installing Plugin in outlook 365

Here are the steps that need to be performed to install the AddIn.

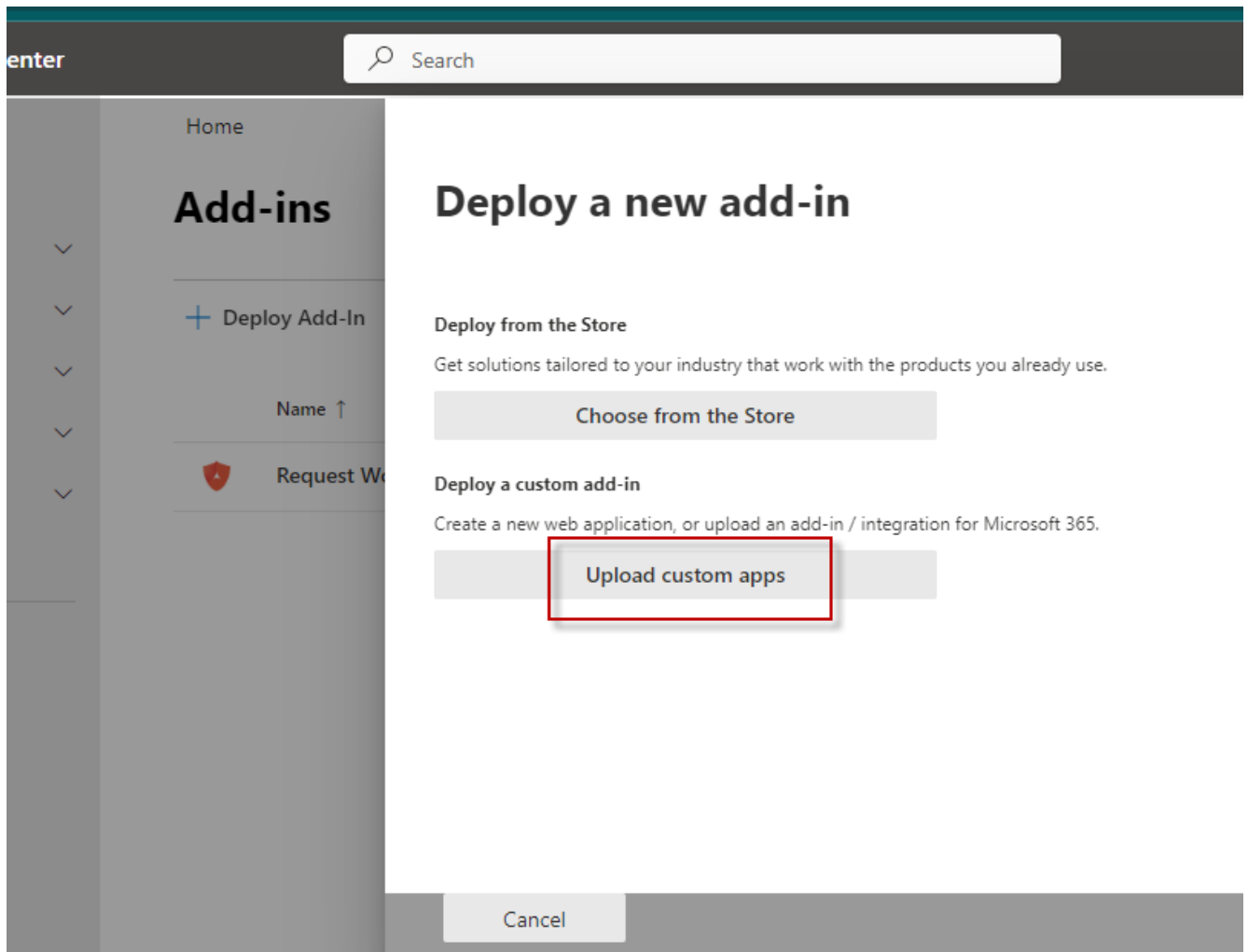
1. Login to Microsoft 365 admin center from a browser - <https://admin.microsoft.com/>
2. Navigate to the Settings → Integrated apps & click the Plugins icon as shown below:



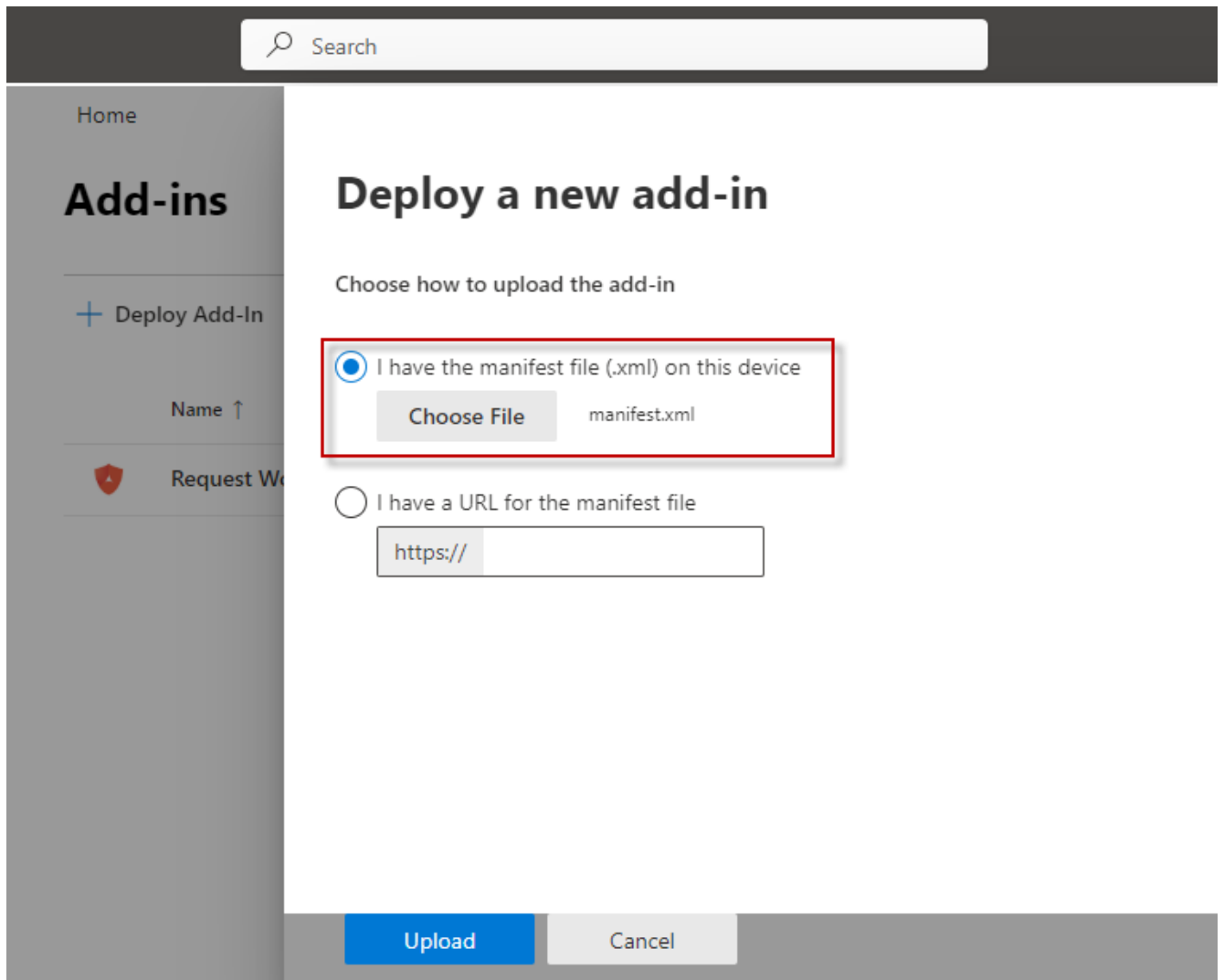
3. Plugins home screen opens up. Now, Click Deploy Plugin & a new pop up opens up as Deploy a new plugin.



4. Once Deploy a new Plugin screen shows up, click Next button then click Upload custom apps button as shown below.




5. Under Deploy a new plugin, we have 2 options to get our plugin deployed. First says, I have a manifest file (.xml) on this device & another option says, I have a URL for the manifest file.
6. Select the first option & upload the xml manifest file which can be found in the source code repository & hit the save button.



- Once the request workplace access plugin for Outlook 365 is added, a confirmation dialog will be displayed. And, same can be tracked under the plugins pane as shown below:

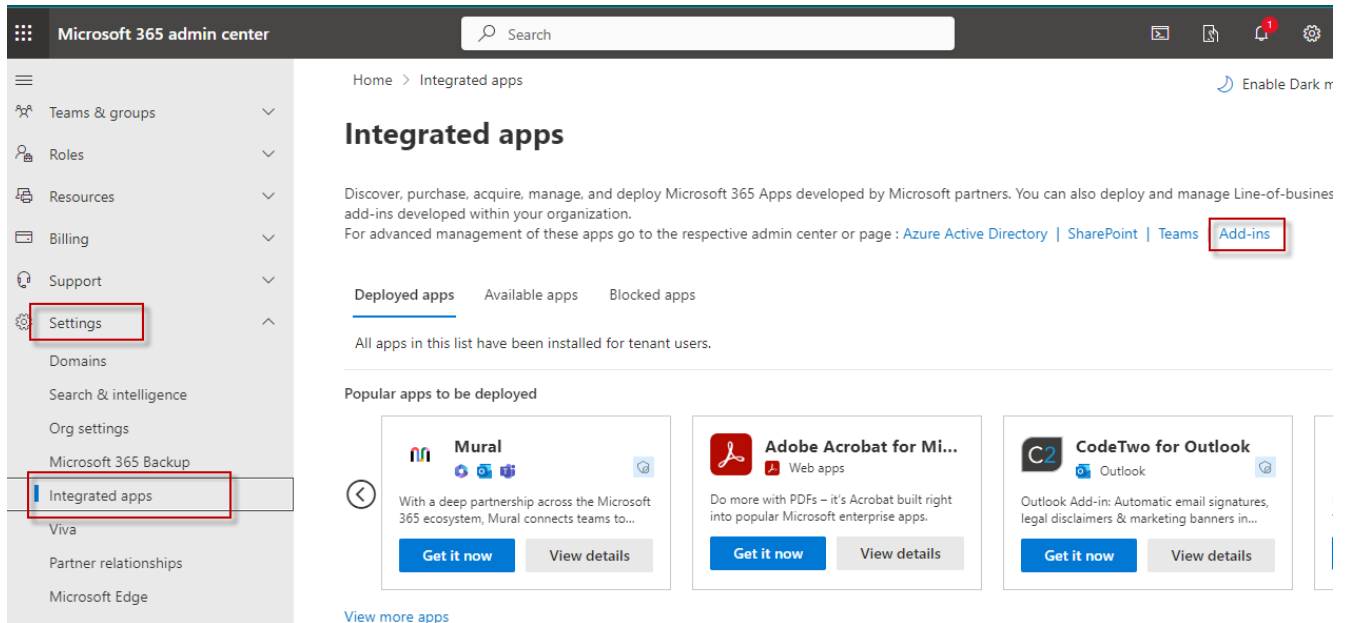
Add-ins

+ Deploy Add-In		Search	≡
Name ↑	Description	Host Apps	
 Request Workplace Access	Request Workplace Access	Outlook	

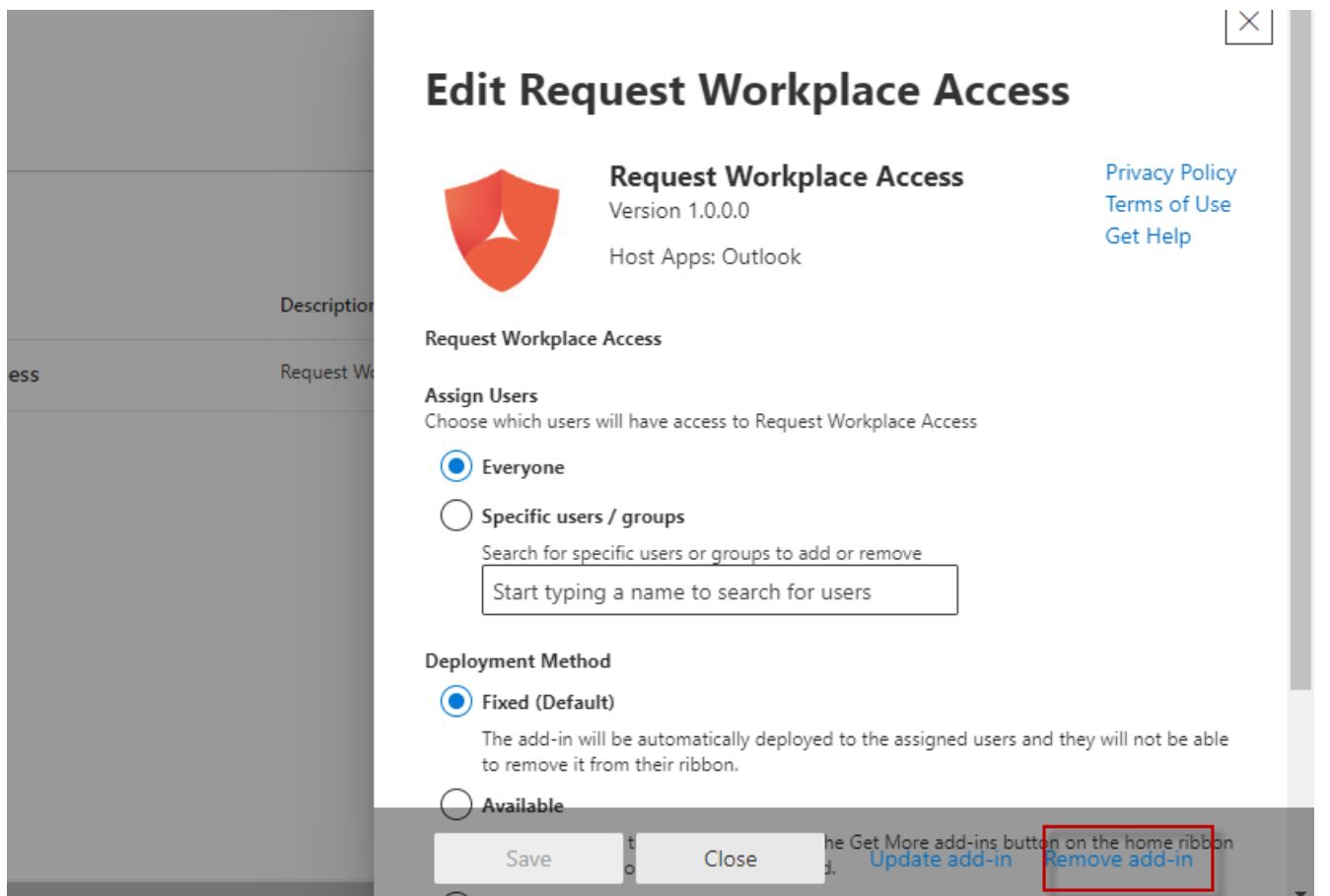
Uninstalling Plugin in outlook 365

Below are the steps that need to be performed to uninstall the Plugin.

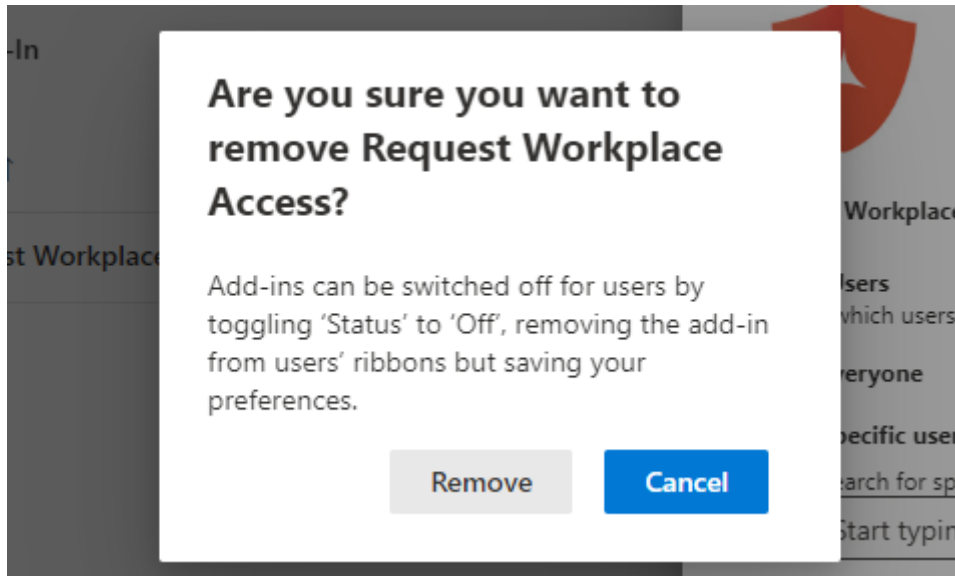
1. Login to Microsoft 365 admin center from a browser - <https://admin.microsoft.com/>
2. Navigate to the Settings → Integrated apps & click the Plugins icon as shown below:



3. Plugins home screen opens up. Select the deployed plugin from the list of plugins.



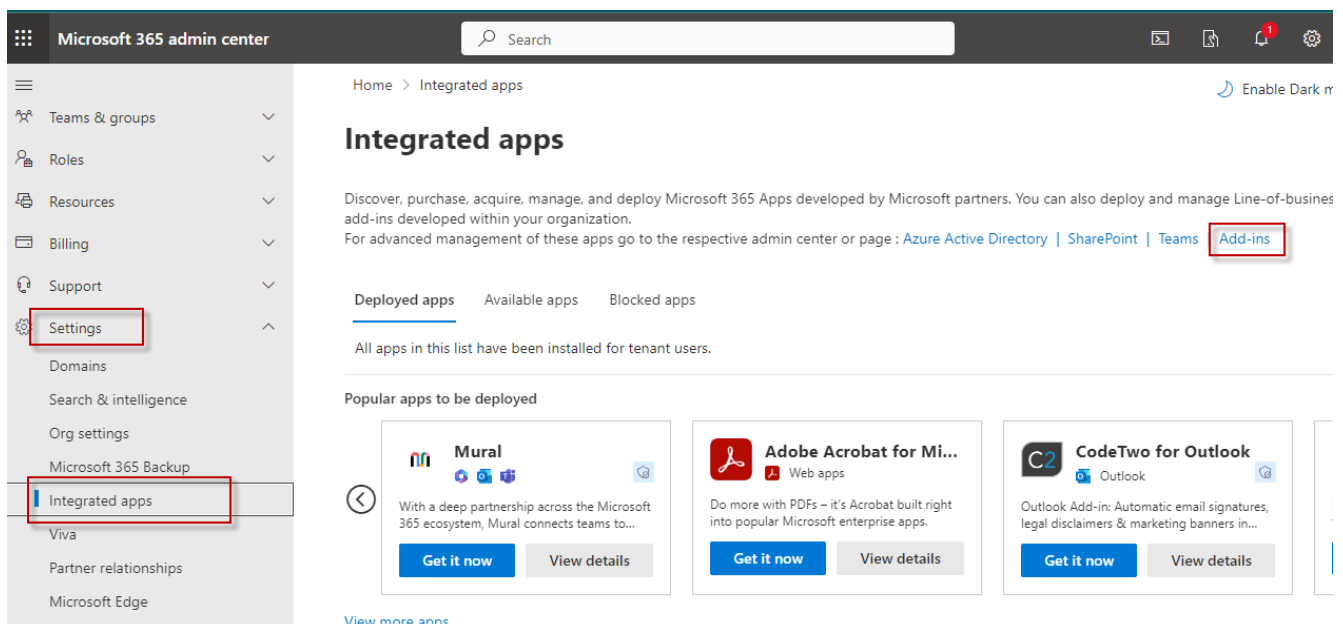
4. Click on the Remove plugin button at the bottom of the pop-up screen as shown above.
5. Now, click on the Remove button which triggered when clicked on Remove plugin button & the plugin will be uninstalled completely.



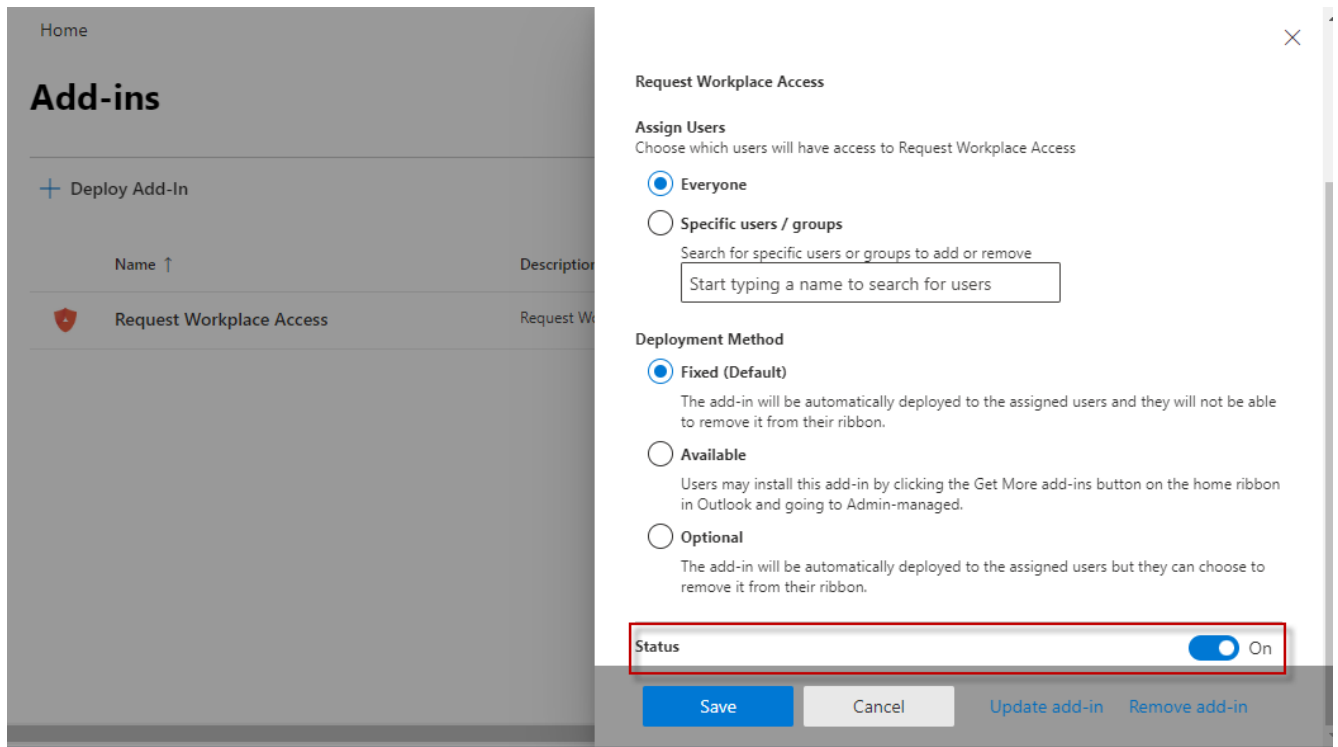
Disabling Plugin in outlook 365

Below are the steps that need to be performed to disable the Plugin.

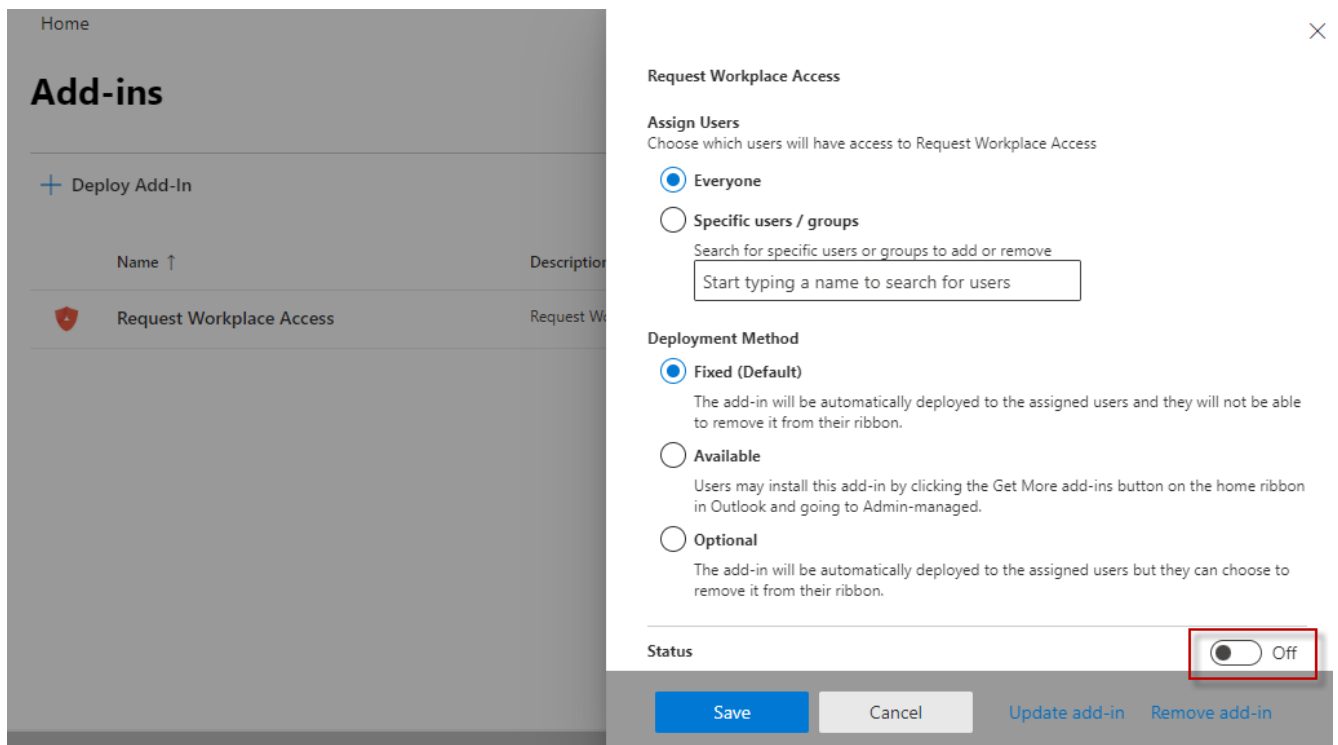
1. Login to Microsoft 365 admin center from a browser - <https://admin.microsoft.com/>
2. Navigate to the Settings → Integrated apps & click the Plugins icon as shown below:



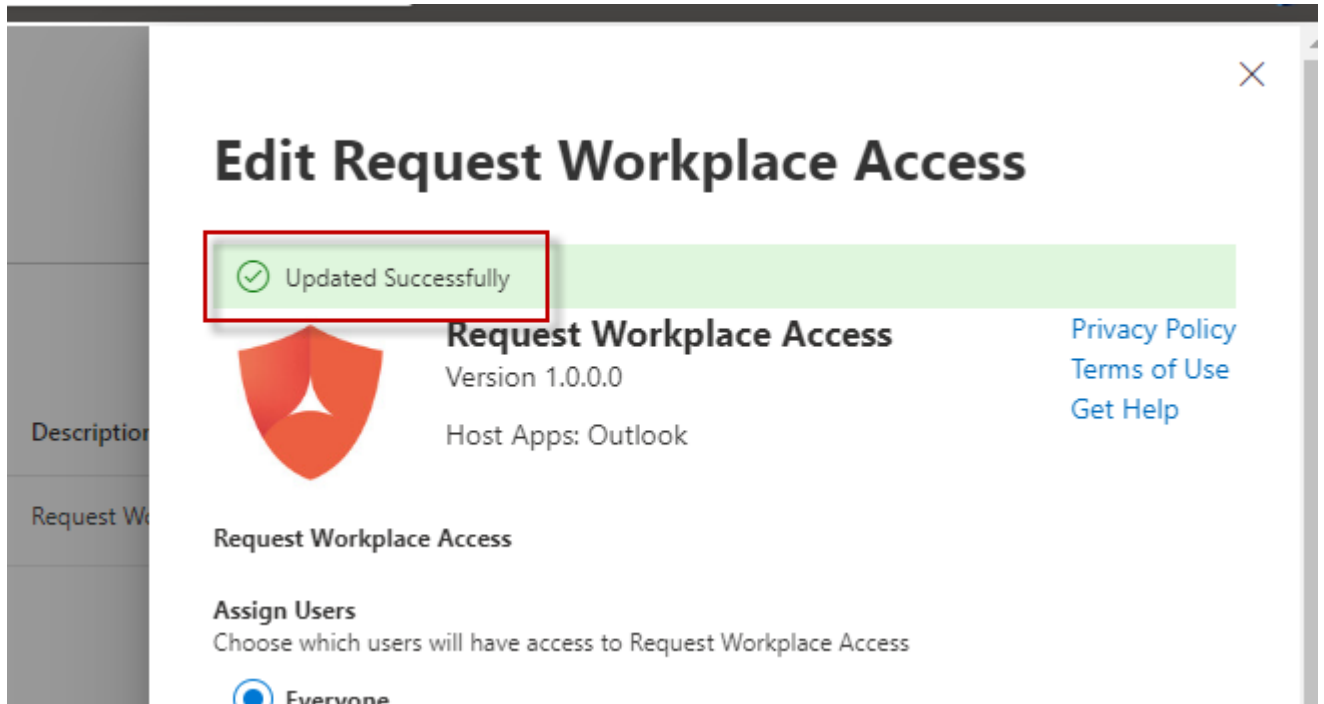
3. Plugins home screen opens up. Select the deployed plugin from the list of plugins & scroll it down when you see status.



- Now, untick the Status field at the bottom of the plugin pop-up screen & hit the save button.



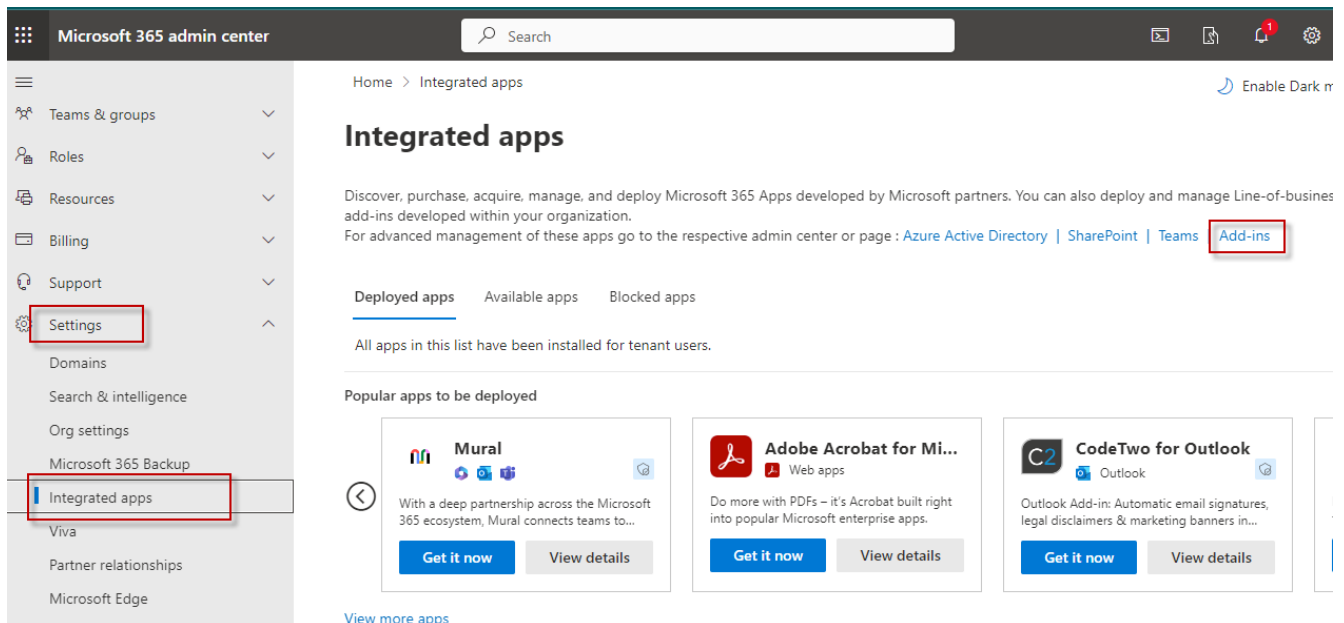
- Once you hit the save button, a text message will get displayed which says Updated Successfully that means the plugin is disabled.



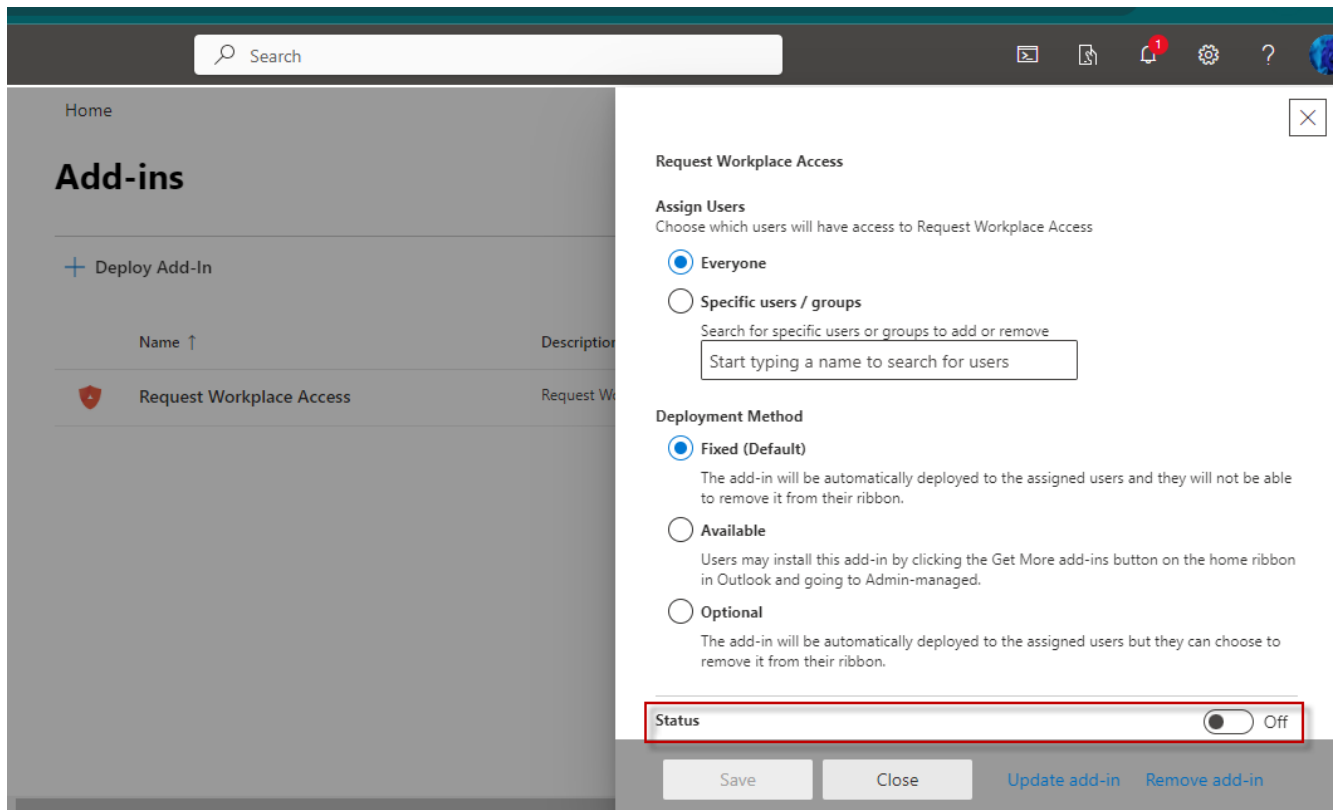
Enabling Plugin in outlook 365

Below are the steps that need to be performed to enable the Plugin.

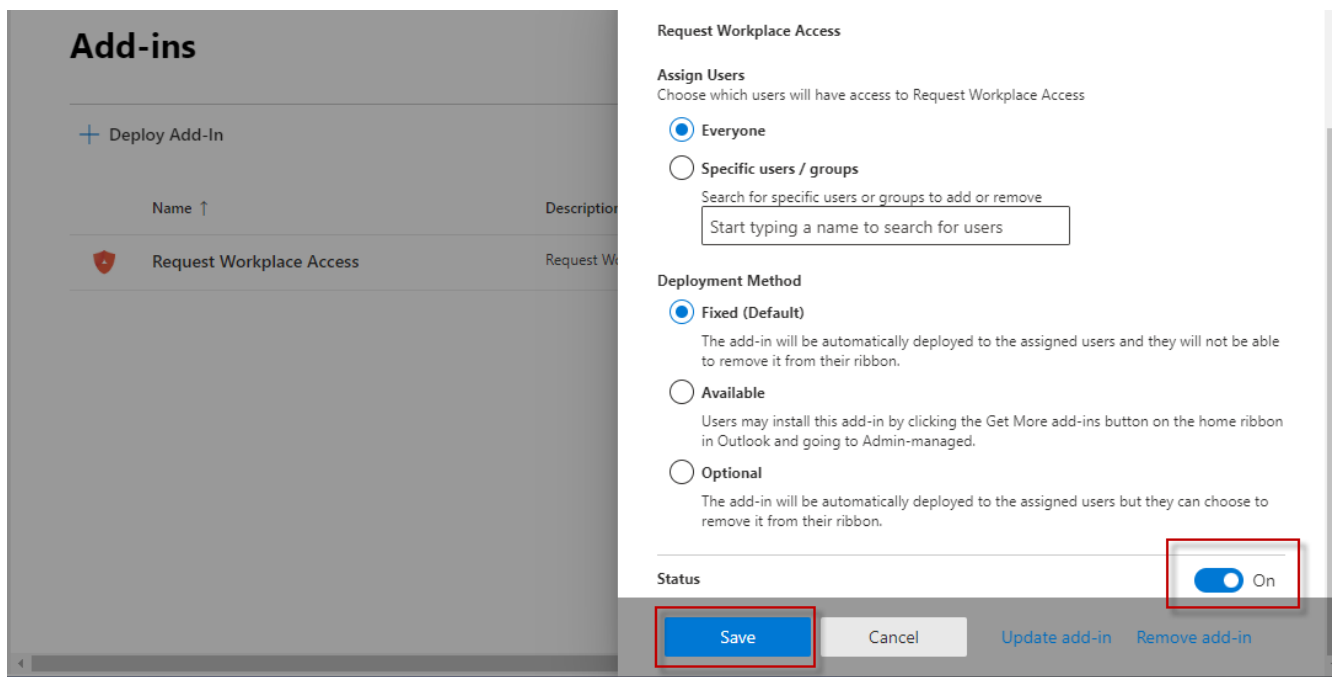
1. Login to Microsoft 365 admin center from a browser - <https://admin.microsoft.com/>
2. Navigate to the Settings → Integrated apps & click the Plugins icon as shown below:



3. Plugins home screen opens up. Select the deployed plugin from the list of plugins & scroll it down when you see status.



- Now, tick the Status field at the bottom of the plugin pop-up screen & hit the save button.




- Once you hit the save button, a text message will get displayed which says Updated Successfully that means the plugin is disabled.

✕

Edit Request Workplace Access

✓ Updated Successfully



Request Workplace Access

Version 1.0.0.0

Host Apps: Outlook

[Privacy Policy](#)

[Terms of Use](#)

[Get Help](#)

Request Workplace Access

Assign Users

Choose which users will have access to Request Workplace Access

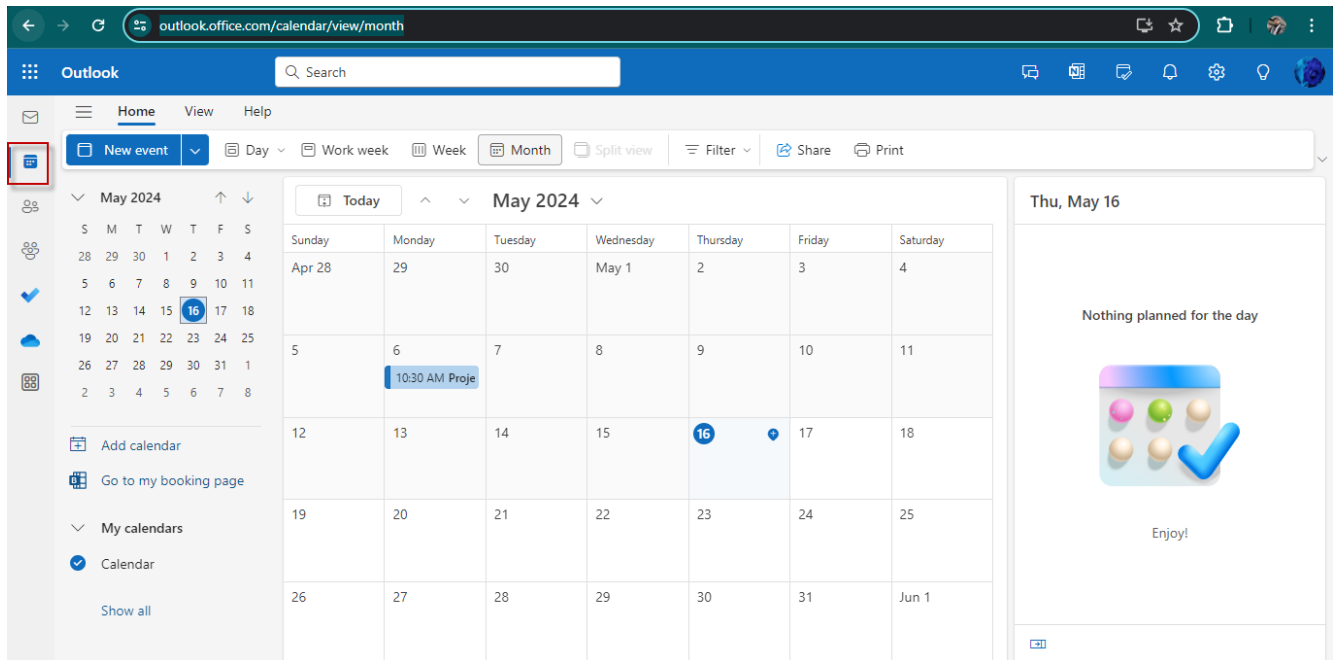
Everyone

Chapter 5. Usage of Plugin

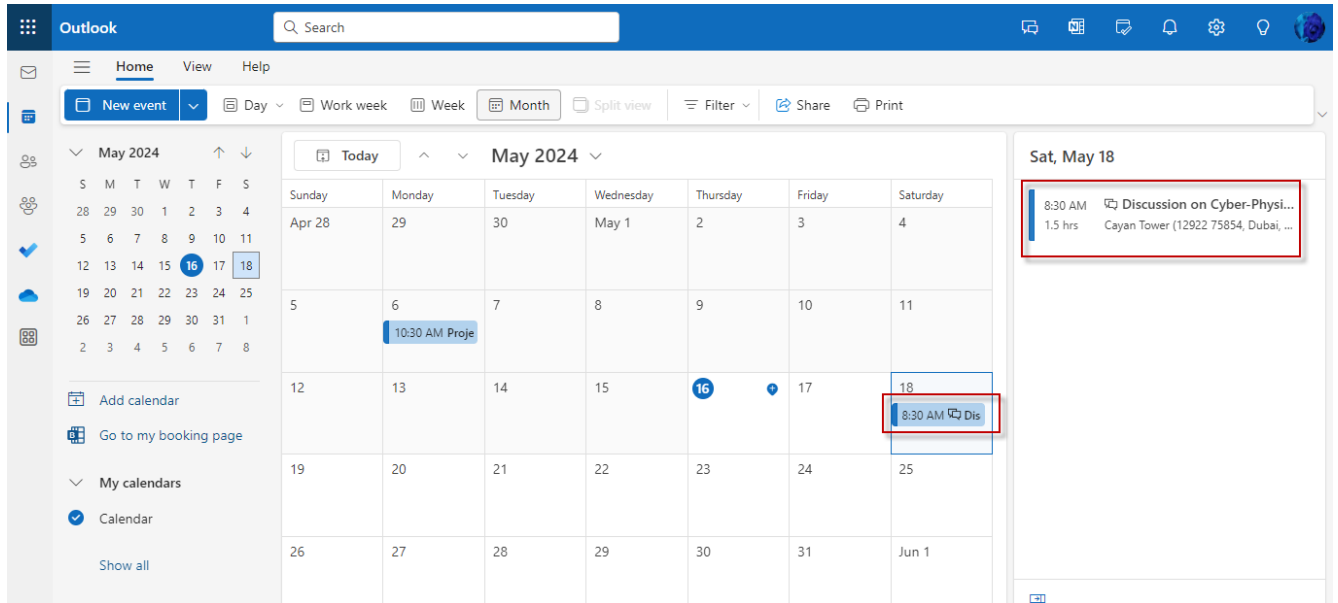
Alert Enterprise Request Workplace Access plugin provides functionality where logged-in users to the outlook account can request for badges & location or meeting room access using the outlook calendar screen windows. This feature works by automatically fetching the location or meeting room from the scheduled calendar invite once the Request New Access button is clicked & furthermore making calls to AE GUARDIAN APIs.

Below is the UI representation of the Request Workplace Access Plugin that highlights the different screens & functionality -

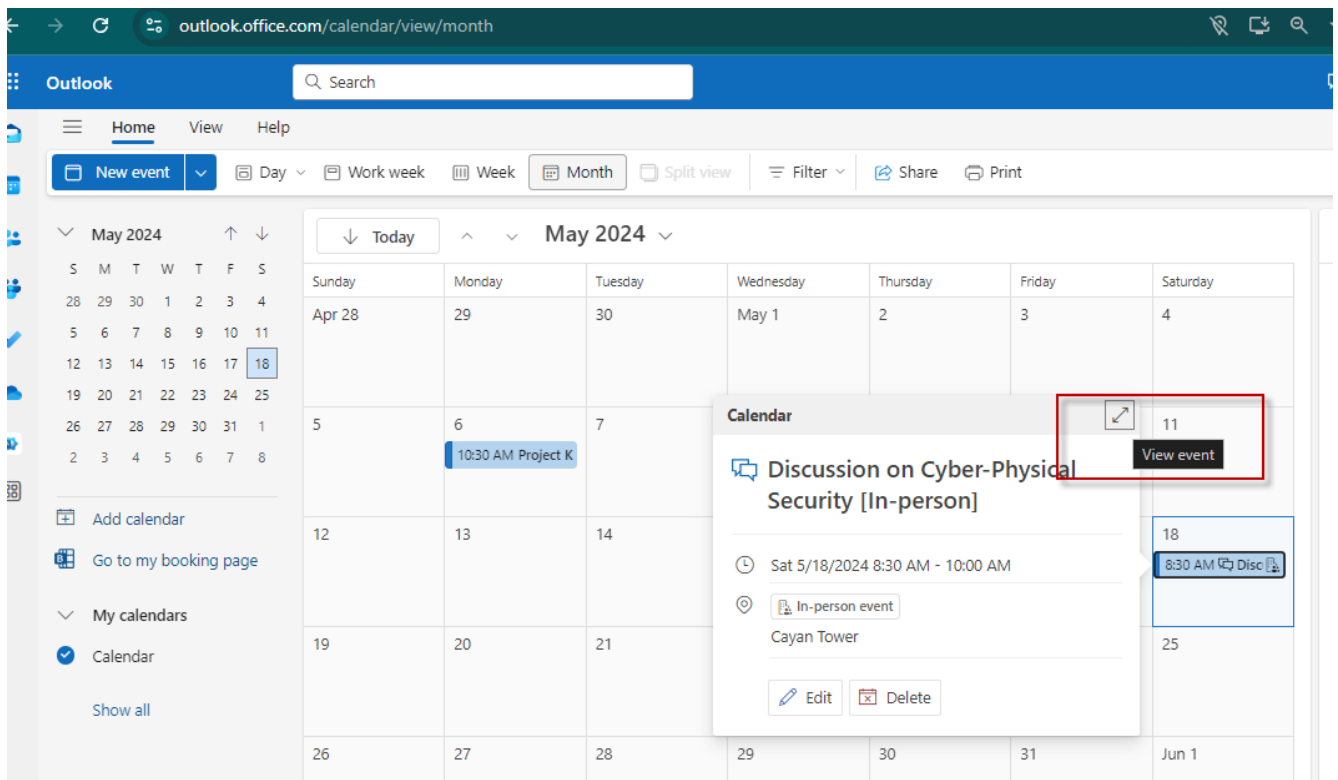
1. Logon to the URL <https://outlook.office.com/calendar/view/month> & calendar view of the outlook opens up.



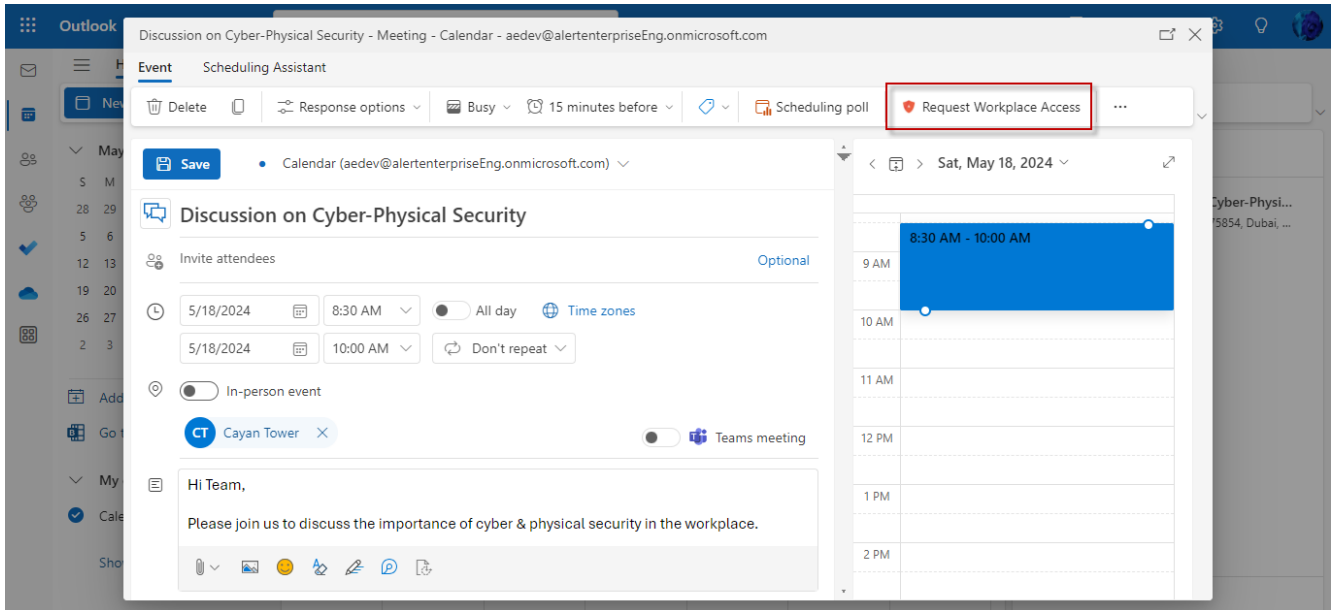
2. Click on the scheduled meeting from the calendar view of outlook.



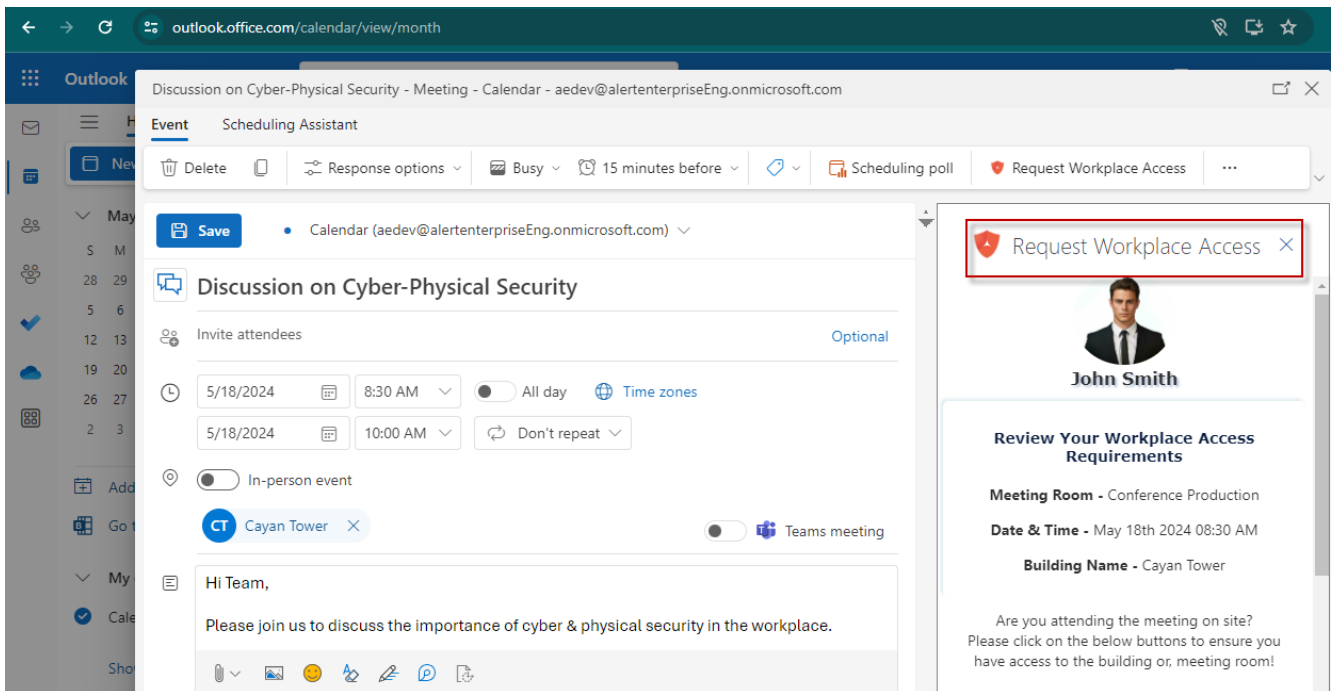
3. A small pop-up window opens up when the calendar invite is clicked. Now, on the same pop-up window, click on the **View Event** icon present at top-right of the window.

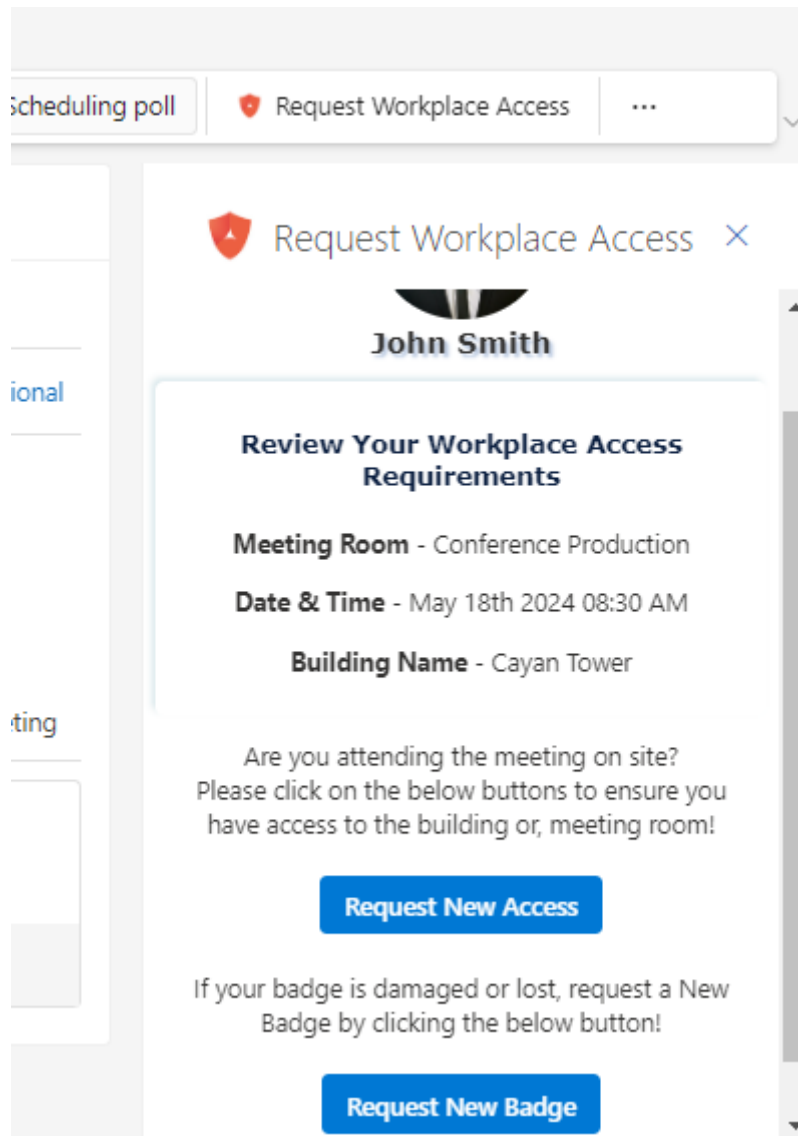


4. Detailed view of scheduled meeting invites will open up in a large pop-up window screen. Now, click on the Request Workplace Access button in the Horizontal navigation bar as shown below.

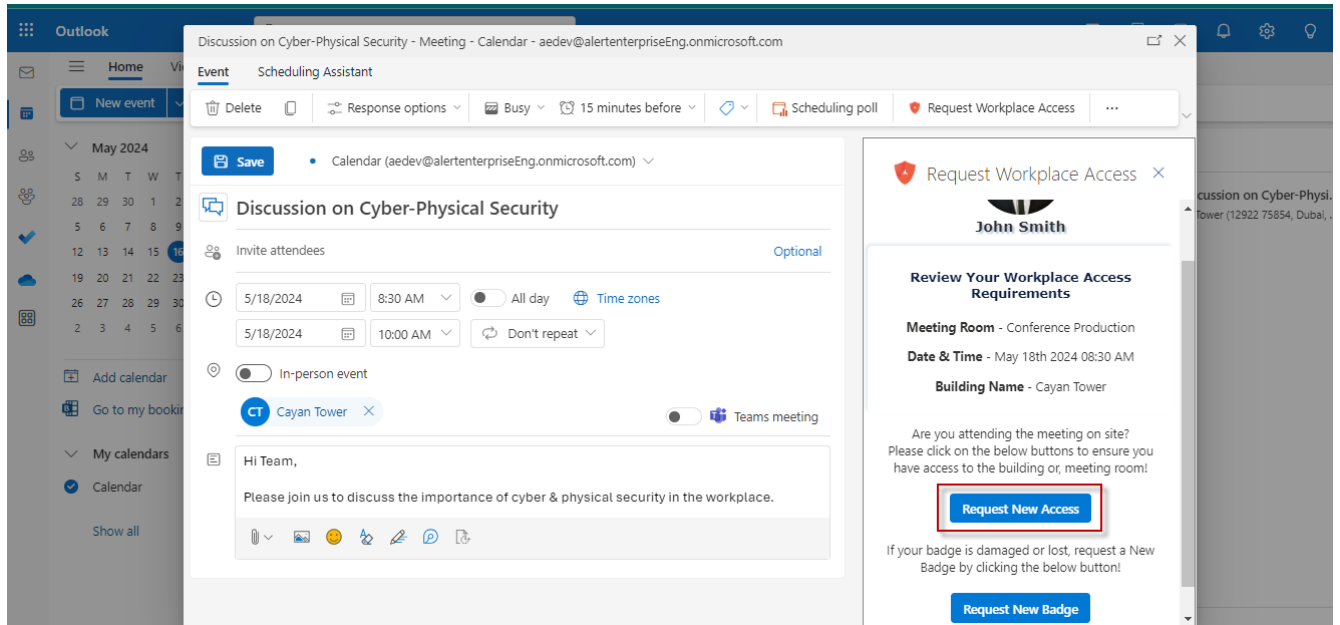


- Once the Request Workplace Access button is clicked, a new sliding window will open up on the same meeting invite pop-up screen highlighting the logged-in users details along with operations to request for the access & badges.

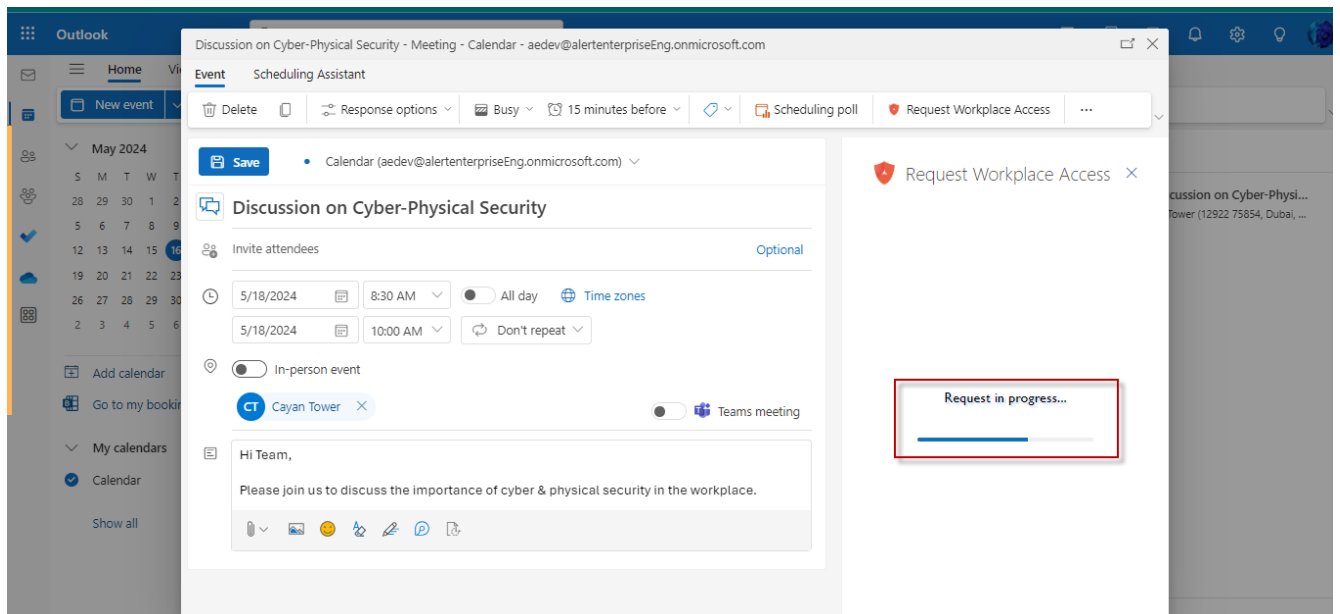




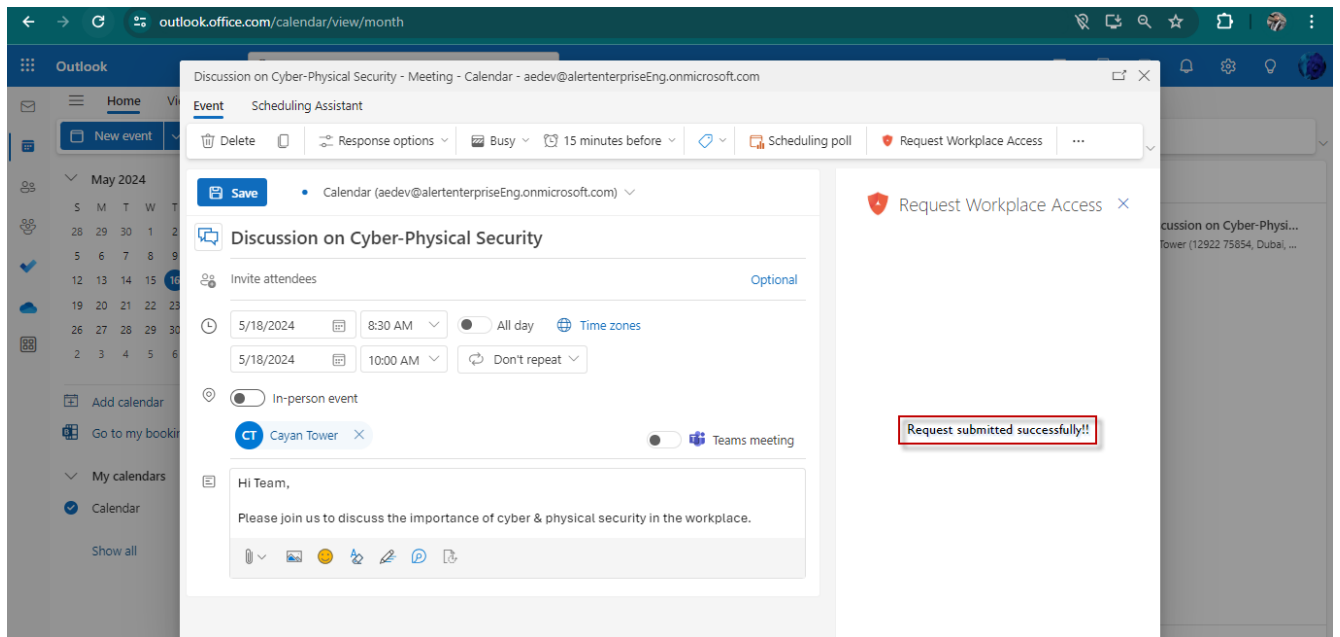
6. As the Request Workplace Access screen shows 2 buttons which has different functionality so if you want to request for the Access / Locations / Meeting Rooms where meeting is scheduled or would require access if you want to join the meeting then click on the button **Request New Access**.



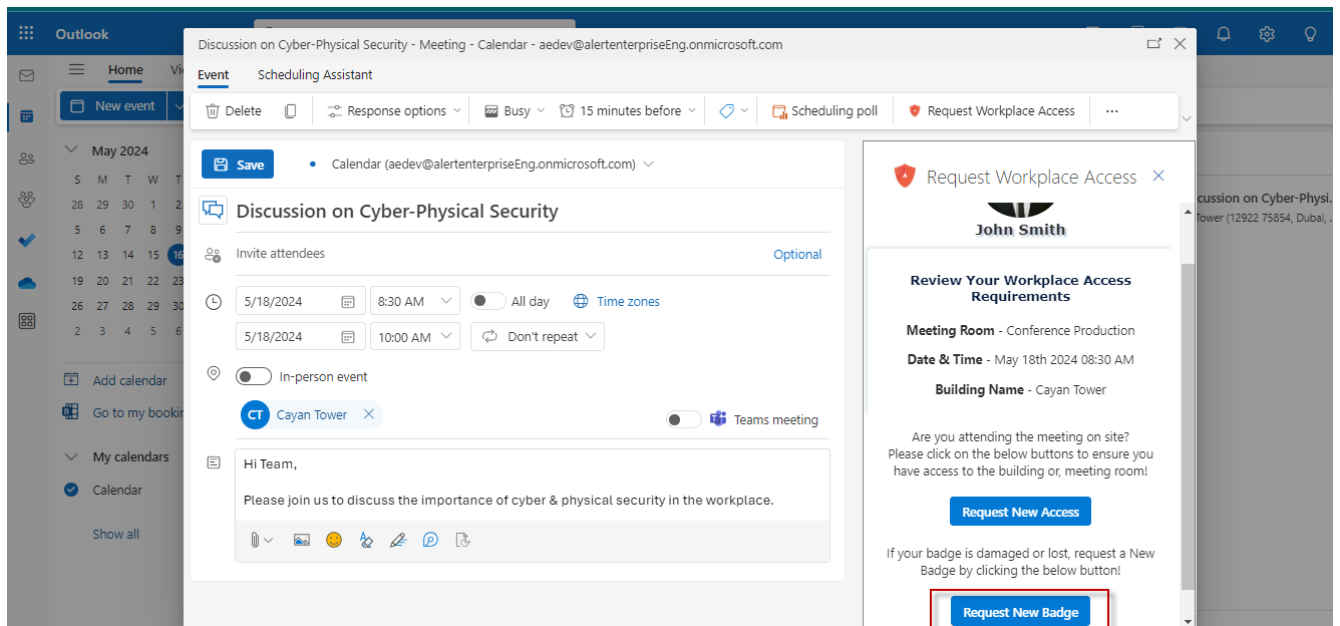
7. When the Request New Access button is clicked, the request will get submitted to the Alert Enterprise GUARDIAN application which will provide the required access to the user.



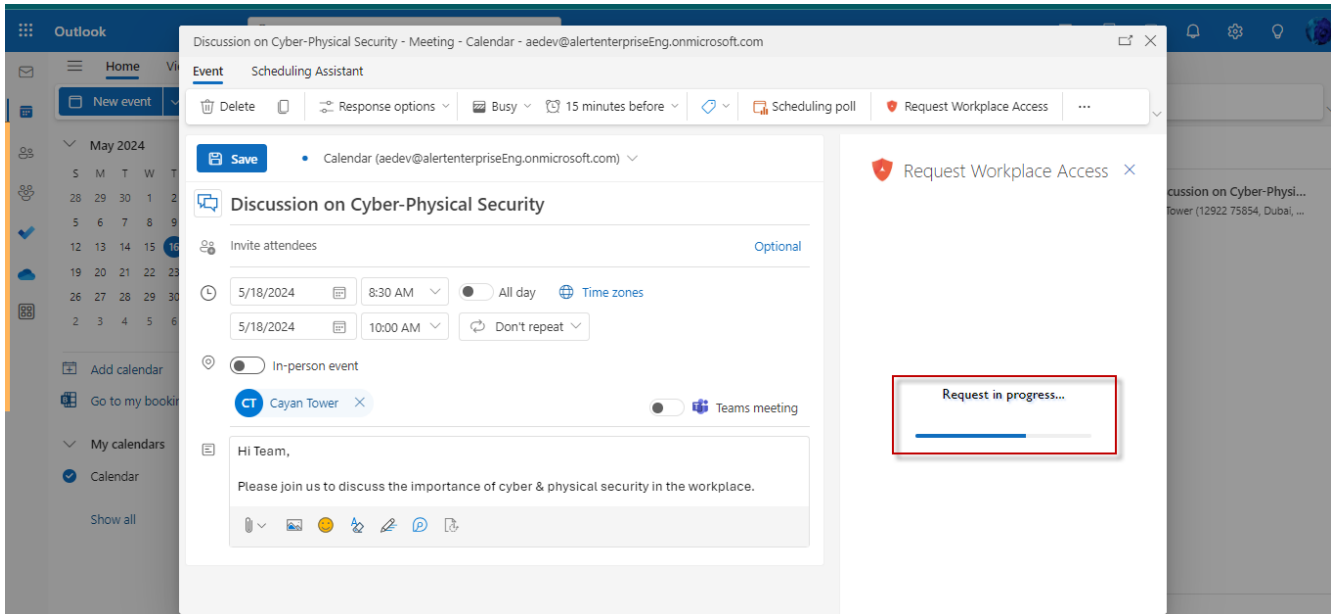
8. On the same Request Workplace Access window, it will show the text message highlighted that the request is submitted successfully.



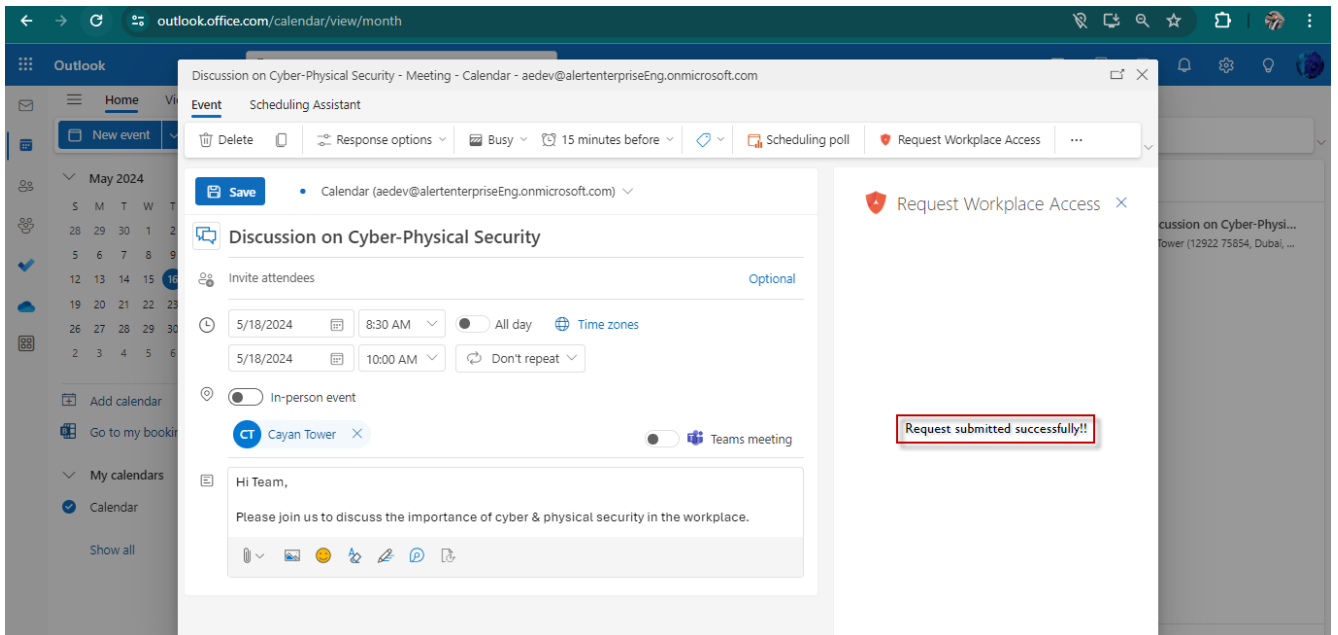
9. Now, if you want to request a new badge to this user then just click another button as **Request New badge**.



10. When the Request New Badge button is clicked, the request will be submitted to the Alert Enterprise GUARDIAN application which will assign the badge to the user.



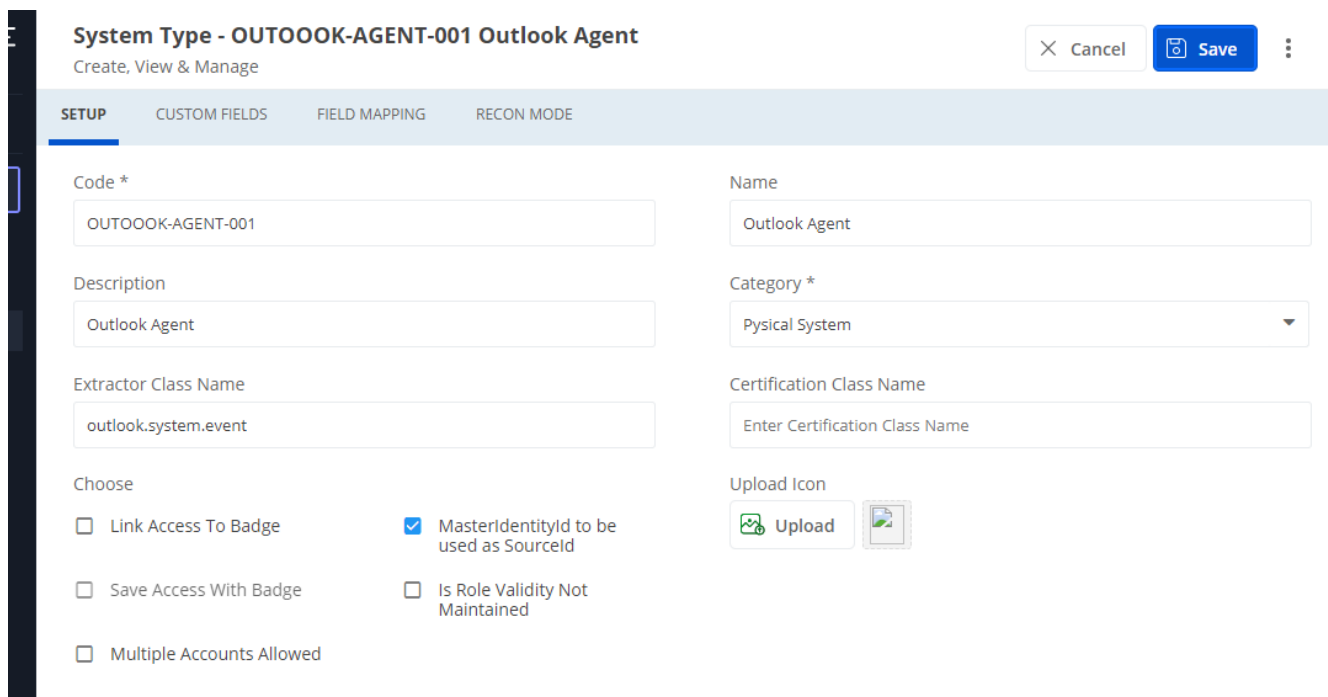
11. On the same Request Workplace Access window, it will show the text message highlighted that the request is submitted successfully.



Chapter 6. Configurations – Alert Enterprise Agent Server & Cloud Server

This section comprises the configurations required to be done on Alert Enterprise Agent & GUARDIAN Cloud application. It mainly focuses on creating new system type, new system, configuring system field mappings, adding event types, executing few SQL scripts on the agent side & changes in the environment configurations files. Below are the steps to follow to make these configurations –

1. Logon to the agent and navigate to System Type & hit the Create button.
2. Add the required details as shown below in screenshot –



System Type - OUTOOOK-AGENT-001 Outlook Agent
Create, View & Manage

Cancel Save

SETUP CUSTOM FIELDS FIELD MAPPING RECON MODE

Code *
OUTOOOK-AGENT-001

Name
Outlook Agent

Description
Outlook Agent

Category *
Physical System

Extractor Class Name
outlook.system.event

Certification Class Name
Enter Certification Class Name

Choose

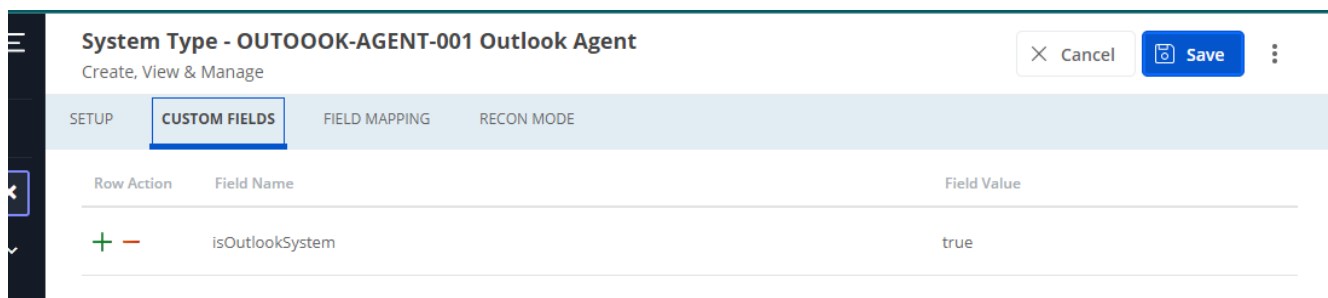
Link Access To Badge MasterIdentityId to be used as SourceId

Save Access With Badge Is Role Validity Not Maintained

Multiple Accounts Allowed

Upload Icon
Upload

3. On the same screen, switch to Custom Fields tab & add the below mentioned details –



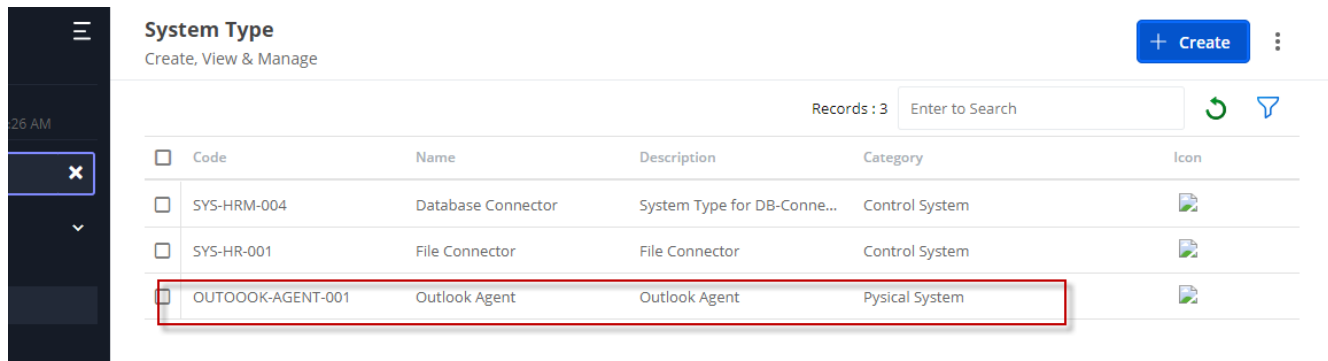
System Type - OUTOOOK-AGENT-001 Outlook Agent
Create, View & Manage

Cancel Save

SETUP CUSTOM FIELDS FIELD MAPPING RECON MODE

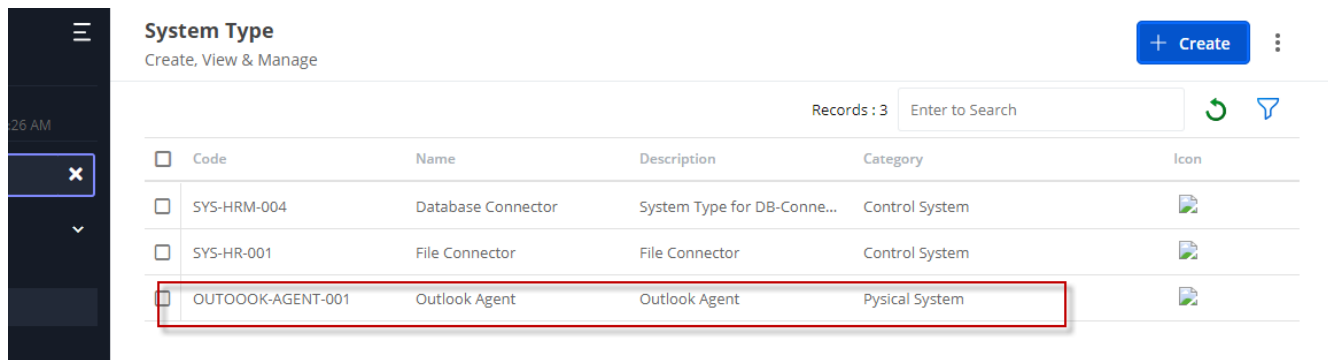
Row Action	Field Name	Field Value
+ -	isOutlookSystem	true

4. Once all the mentioned details are added in the system type, Hit the Save button. This should save the newly created system type & should get displayed in the grids layout of the screen.

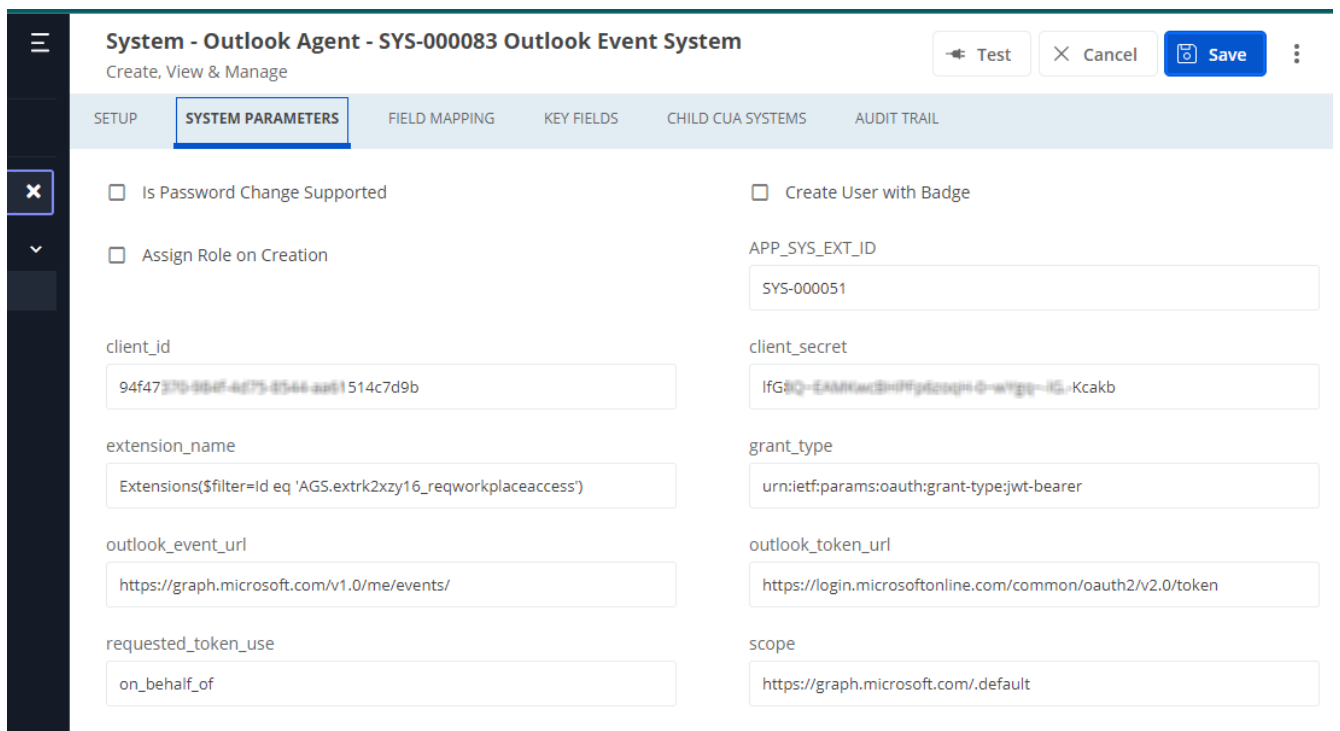


5. Now, navigate to System, click on the Create button & this will open up the System screen layout.

6. Under the SETUP tab of the system screen, add the following details as mentioned below –



7. Now, switch to System Parameters tab of this system screen & add the following parameters –



NOTE: In case SCS is not created of this system, then you may see a blank screen when switched to System Parameters. So, in such a case please create the required SCS of this

system type & then add these parameters in the SCS. Field Id in SCS will be the same as mentioned above in the labels of system parameters.

ATTENTION: Some data in the system parameter will be dynamic for different customers. Here, the value of client_id, client_secret, extension_name & APP_SYS_EXT_ID will be different & as per the customer environment. Value of the APP_SYS_EXT_ID is the connector Ext-ID of the system created on the api server in the later part of this document. Other details are static only & will remain the same on any environment as mentioned below –

grant_type - urn:ietf:params:oauth:grant-type:jwt-bearer

outlook_event_url - https://graph.microsoft.com/v1.0/me/events/

outlook_token_url - https://login.microsoftonline.com/common/oauth2/v2.0/token

requested_token_use - on_behalf_of

scope - <https://graph.microsoft.com/.default>

Extension Name Used Internally

extension_name - Extensions(\$filter=Id eq 'AGS.extrk2xzy16_reqworkplaceaccess')

8. Once the necessary details are provided in the system parameter. Hit the save button.
9. Now, Go to System open the recently create outlook system switch to field mapping tab & add the below mappings.

Mapping Type	Entity	AE Field Name	System Field Name
Recon	User Event Data	description	subject
Recon	User Event Data	validFrom	start_dateTime
Recon	User Event Data	areaName	location_displayName
Recon	User Event Data	fullName	name
Recon	User Event Data	lastName	name
Recon	User Event Data	firstName	name
Recon	User Event Data	subdevice_id	organizer_emailAddress_address
Recon	User Event Data	domain	preferred_username
Recon	User Event Data	userId	oid
Recon	User Event Data	validTo	end_dateTime
Recon	User Event Data	eventId	id
Recon	User Event Data	eventType	eventType
Recon	User Event Data	eventSerialNum	outlook_request_badge

NOTE: AE Field Name can be different as per the requirement & can be mapped accordingly.

10. Once added all the field mappings as mentioned in the above table, hit the Save button.
11. Also, make sure in the environment configuration file of Agent Server, the following entry is added –

```
STAGING_REDISSTREAM_QUEUES=["Alert Enterprise:mock","Alert Enterprise:outlook"]
```

12. This completed most of the configurations required on the Agent server. Now, we have to make some configuration onto the GUARDIAN Alert Enterprise API server.
13. Logon to the API server, go to manage class definition & hit the create button.
14. Add the new entity in the class def with name EventType as mentioned below –

Manage Class Definition - Entity - EventType EventType

Create, View & Manage

Cancel Save

SETUP ATTRIBUTES FIELDS ADDITIONAL APIS PURGE CONFIGURATIONS

Type * Entity

Name * EventType

Business Object * EventType

Class Name * com.alnt.event.domain.EventType

Service Class com.alnt.event.service.EventTypeServiceImpl

Code * EventType

Description EventType Desc

Table Name * event_type

Controller Class com.alnt.event.controller.EventTypeController

Import Job Class Enter Import Job Class

Manage Class Definition - Entity - EventType EventType

Create, View & Manage

Cancel Save

SETUP ATTRIBUTES FIELDS ADDITIONAL APIS PURGE CONFIGURATIONS

Tenant Name Enter Tenant Name

Validation Rule Set Select Rule Set

Auth Exempted Fields Select Field Name

Before Save Rule Validation Select Before Save Rule Validation

Before Save UI Validation Enter Validation text

Key Field Enter Key Field

Suggest Default Rule Set Select Rule Set

Post Save Rule Set Select Post Save Rule Set

Delete Check:	Delete with warning:	Doc Number Supported:	Validation Enabled:	Is Translatable:
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Workflow Enabled:	No Workflow On Update:	Rule Applicable:	Disable History:	Is Undelete Not Allowed:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Once added all the details in the class def, hit the save button. This should add the new class def in the grid.
- Now, navigate to Document Number Range & hit the Create button. It opens up the screen layout of the doc number. Now, add the following details as mentioned below & hit the save button.

Document Number Range - EventType

Create, View & Manage

Cancel Save

SETUP TYPES

Document Field type:
 Ext ID Others

Document Range ID *

Business Object Category *

Generation Field

Systems

Validation Systems

Exclusion Rule

Length

Range Start *

Range End *

Range Format *

Choose
 Remove Leading Zeros Duplicate Check Use External Document Range

Pattern

17. Now, go to Manage Access search for Admin User Role & open the same. Switch to the MENU tab & add the below entry & once added, hit the Save button.

Manage Access - Application - ACS-002812 Admin User Role

Create, View & Manage

Print QR Code Cancel Save

SETUP **MENU** AUTHORIZATION LOCATION ORGANIZATION IDENTITY PREREQUISITES OWNERS CARDS SCHEDULES

Action	Menu ID	Label	Sub-menu Label	Url Hash	Activity ID	Sequence	Hidden	Is
+ [Folder]	Reports_ID001	Reports					<input type="checkbox"/>	
+ [Folder]	sentry_adminU...	Sentry				9	<input type="checkbox"/>	
+ [Folder]	home_admin_a...	Home				1	<input type="checkbox"/>	
+ [Folder]	settings_admin...	Settings				8	<input type="checkbox"/>	
- [Folder]	identity_eventT...	Event					<input type="checkbox"/>	
+ [Folder]	eventType	Event Type Set...			identitymgmt.e...	10	<input type="checkbox"/>	
+ [Folder]	adminUserRole...	VIM					<input type="checkbox"/>	

18. Now, go to System Type & click on the Create button. Add the below mentioned details & hit the save button.

System Type - OUTLOOK-001 Outlook Addin Cancel Save

Create, View & Manage

SETUP CUSTOM FIELDS FIELD MAPPING RECON MODE

Code *

Name *

Description

Category *

Extractor Class Name

Certification Class Name

Choose

Link Access To Badge MasterIdentityId to be used as SourceId

Save Access With Badge Is Role Validity Not Maintained

Upload Icon

19. Now, Go to system, Hit Create button & this should open the System screen layout. Add the details as mentioned below & hit the Save button. Make sure to use the same system type which we created above.

System - SYS-000054 Outlook Plug-In System Test Cancel Save

Create, View & Manage

SETUP SYSTEM OWNERS SYSTEM PARAMETERS FIELD MAPPING KEY FIELDS CHILD CUA SYSTEMS DISCREPANCY ACTION COMMENTS ATTACHMENTS AUDIT TRAIL

Type *

Code *

Name

Description

Environment *

Timezone

System Group *

Provisioning Sequence

Login Sequence

External System Code

Choose

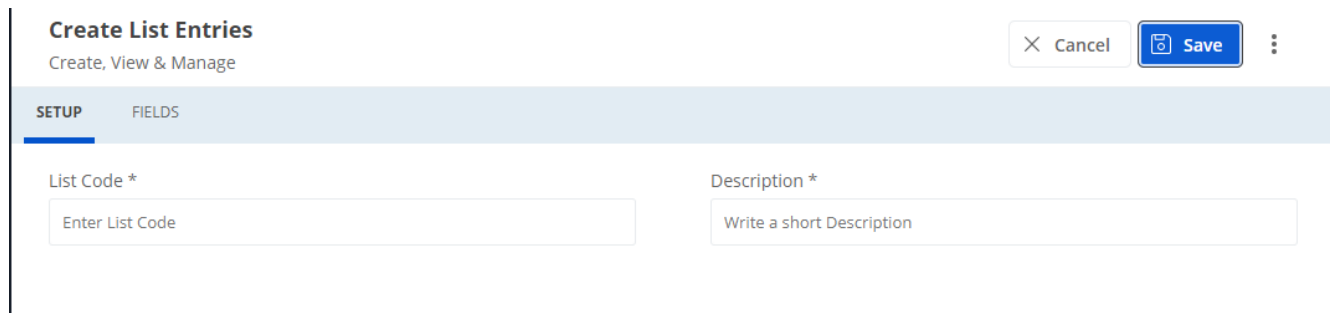
Provisioning Is Master Auth System Is Role Validity Not Maintained Do Not Update Identity For Provisioning Is Watchlist

20. Now, Switch to System Field Mapping tab, add the following mappings –

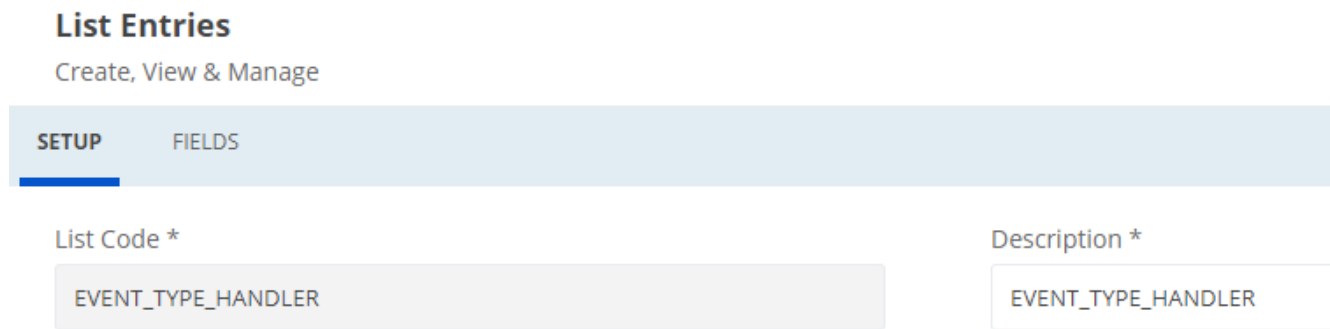
Mapping Type	Entity	AE Field Name	System Field Name
Recon	User Event Data	fullName	fullName
Recon	User Event Data	lastName	lastName
Recon	User Event Data	validFrom	validFrom
Recon	User Event Data	description	description
Recon	User Event Data	eventType	eventType
Recon	User Event Data	event_subtype	outlook_request_badge

21. Once added all the field mappings, hit the Save button.

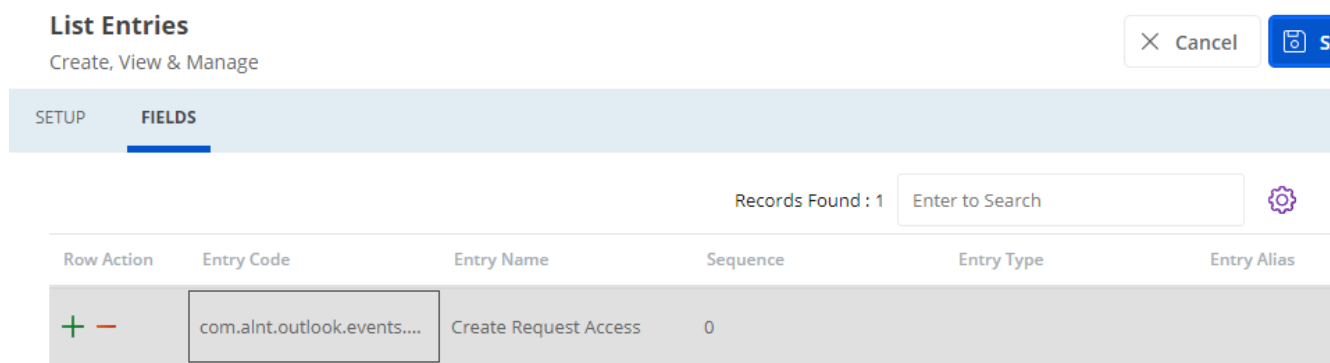
22. Navigate to List Entries, Hit the Create button. It opens up list entries screen layout.



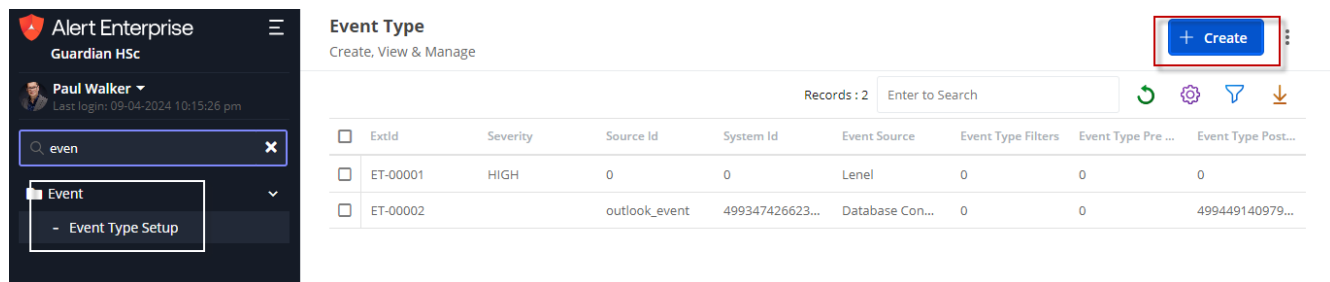
23. Add the following details in the list entry setup layout –



24. Switch to the FIELDS tab on the same screen & add the Entry Code as com.alnt.outlook.events.service.OutlookEventsServiceImpl & Entry Name as Request Workplace Access & hit the save button.



25. Now, go to Event Type & Hit the Create button.



26. Add the following details in the Event Type & once added all the required details, hit the Save button.

Create Event Type

Create, View & Manage

✕ Cancel
Save
⋮

SETUP

Ext Id

System Id
 Add the System Hibernate ID of the System created in API server

Source Id *

Filter rule set

Post Feed Rule Set

Severity

Event Source
 Add the same handler create in the previous step

Handler *

Pre Feed Rule Set

Async

27. Now, Go to the jobserver.conf file in the present the build inside jobserver\conf & update the entry of consumer-enabled as true & save the file.

```

truststorepath:${STAGING_REDIS_TRUSTSTOREPATH}
truststorekey:${STAGING_REDIS_TRUSTSTOREKEY}
ssl : ${STAGING_REDIS_SSL}
stream {
    consumer-enabled : true
    queues : ${STAGING_REDISSTREAM_QUEUES}
}
    
```

28. Go to environment.conf file & add the outlook queue in the STAGING_REDISSTREAM_QUEUES as ["Alert Enterprise:mock","Alert Enterprise:outlook"] & save the file.

```

210 STAGING_REDIS_SSL=false
211 STAGING_REDIS_USERNAME=""
212 STAGING_REDIS_CONNECTION_TIMEOUT=3000
213 STAGING_REDIS_KEYSTOREPATH=""
214 STAGING_REDIS_KEYSTOREKEY=""
215 STAGING_REDIS_TRUSTSTOREPATH=""
216 STAGING_REDIS_TRUSTSTOREKEY=""
217 STAGING_REDISSTREAM_QUEUES=["alert:mock","alert:outlook"]
218 STAGING_REDISSTREAM_THREAD_POOL=10
219 STAGING_REDIS_JEDISMAXTOTAL=16
220 STAGING_REDIS_JEDISMAXIDLE=16
221 STAGING_REDIS_JEDISMINIDLE=8
222 STAGING_REDIS_LIBRARY="jedis"
223
224 SOCKS_PROXY_HOST=""
    
```

29. Once done with all the configuration changes, restart the api server first then job server & after that agent server.

Chapter 7. References

Outlook Plugins tutorial/documentation

<https://learn.microsoft.com/en-us/office/dev/plugins/outlook/>

<https://learn.microsoft.com/en-us/office/dev/plugins/outlook/one-outlook>

Plugin Deployment

<https://admin.microsoft.com/Adminportal/Home#/Settings/IntegratedApps>

<https://admin.microsoft.com/Adminportal/Home#/Settings/AddIns>

Outlook Plugins APIs

<https://learn.microsoft.com/en-us/office/dev/plugins/outlook/apis>

© 2024 Alert Enterprise Inc. All rights reserved. Alert Enterprise and Guardian are trademarks of Alert Enterprise Inc. Other names and logos mentioned herein may be the trademarks of their respective owners.