pitney bowes

Shipping & Mailing
Outbound and Inbound Package Management

SendSuite Tracking

Configuring Microsoft Azure Active Dreictory Authentication}

Introduction

SendSuite Tracking 14.8 supports Microsoft Azure Active Directory authentication. This guide steps the reader through registering the SendSuite Tracking collection of applications in Azure and configuring SendSuite Tracking Admin to forward login requests to Azure for authorization.

Once configured, Azure will be leveraged to authenticate users before allowing access to:

- SendSuite Tracking Admin
- SendSuite Tracking Smart Client
- SendSuite Tracking Designer
- SendSuite Mobile

Note: This article applies to SendSuite Tracking v14.8 and higher only.

Service Collateral
March 2022

Microsoft Azure AD Configuration

Prerequisites

1. A Microsoft Azure account with an active subscription. To create an Azure account, visit 'Create an account for free'.
2. Ensure the Azure account is assigned to one of the following roles which possess the necessary application management permissions:
    a. Application Administrator
    b. Application Developer
    c. Cloud Application Administrator
3. SendSuite Tracking must be installed in HTTPS mode.

Microsoft Azure App Registration

The following table displays the four individual components of SendSuite Tracking that will need to be registered in Azure:

Application	Type
Tracking Client	Desktop
Designer	Desktop
SS Mobile	Mobile
SendSuite Admin	Web

Complete these steps to register each application in Azure:

1. **Sign in** to the Azure Portal.
2. Search for and select **Azure Active Directory**.
3. In **Manage**, select **App registrations>New registration**.
4. Enter a friendly, recognizable display **Name** for the application being registered.
5. In **Sign-In Audience**, Specify the users permitted to use the application by selecting **Accounts in this organizational directory only**.
6. Leave **blank** the value for **Redirect URI (optional)**.
7. Select **Register** to complete the initial Azure App Registration.

Upon successful registration, Azure will display the app registration's Overview pane.

Platform Settings and Redirect URI

A *redirect URI* is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication. Settings for each application type, including redirect URIs, are configured in **Platform configurations** in the Azure portal. Some platforms, like **Web** and **Single-page applications**, require you to manually specify a redirect URI. For other platforms, like mobile and desktop, you can select from redirect URIs generated for you when you configure their other settings.

Complete the following additional configuration steps for each SendSuite Tracking app registered in Azure:

1. Select the app to configure in **App registrations**.
2. Under **Manage**, select **Authentication**.
3. Under **Platform configurations**, select **Add a platform**.
4. Under **Configure platforms**, select the tile for your application type (platform, e.g. mobile, web, desktop).
5. For each app being configured, apply the appropriate value from the following table:

Application Name	Platform	Redirect URI	Tokens	Allow Public Client Flows
Tracking Client	Mobile and Desktop Applications	https://login.microsoftonline.com/common/oauth2/nativeclient	N/A	N/A
Designer	Mobile and Desktop Applications	https://login.microsoftonline.com/common/oauth2/nativeclient	N/A	N/A
Mobile	Mobile and Desktop Applications	Select option for MSAL only	ID Tokens = Checked	N/A
SendSuite Admin	Web	Redirect URI should be according to the server's name configured and should also have a valid certificate on the machine. This means SendSuite Tracking Admin with Azure only works on HTTPS scheme, e.g.- *https://xxxxxx:443/Sendsuiteadmin/SecurePages/Home.aspx* For details, please refer to the following section titled **Redirect URL for SendSuite Admin**.	N/A	Yes

Redirect URL for SendSuite Admin

Also known as 'reply URLs', further details on acceptable URIs such as supported schemes, number of URIs that may be entered, and URI value length are available at:

https://docs.microsoft.com/en-us/azure/active-directory/develop/reply-url

The preceding steps are the basic minimums required for app registration. For additional details relative to your specific authentication requirements, please visit:

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

SendSuite Tracking Configuration

Once all apps have been registered in the Azure Portal, these steps must be executed to complete the authentication configuration.

Configure the Azure AD Header

1. Open **SendSuite Tracking Admin** and login with an **Admin** user.
2. Navigate to **Setup>Enterprise>Login Settings**.
3. Select the **Azure Active Directory Authentication** radio button.
4. Enter the **Directory (tenant) ID** from Azure:
    a. Sign in to the Azure Portal.
    b. Select **Azure Active Directory**.
    c. Select **Properties**.
    d. Scroll to the **Tenant ID** field and copy the value to the system clipboard.
5. Select one of the available **Object Identifier Types** from the drop-down:
    a. **Preferred_username**: If selected, the User from Azure AD will be mapped to the User in SendSuite Tracking by **email address**. Administrators must use users' email addresses in Azure AD as the identifier to map the user in SendSuite Tracking.
    b. **http://schemas.microsoft.com/identity/claims/objectidentifer**: This represents the object identifier for the user in Azure AD. This value is the immutable and non-reusable identifier of the user. Every user, without exception, in Azure AD is assigned. If this option is selected, the Administrator must enter the object Identifier of users in the Users table so that users in Azure AD can be mapped to users in SST.
6. Remain on the SendSuite Tracking Admin Login Settings page and continue to the next section.

For additional information on user mapping, please refer to the section of this document titled 'User Mapping: Azure-to-SendSuite Tracking'.

Configure the Azure AD Details (Components)

1. While on the Login Settings page of SendSuite Tracking Admin, select **Add Components**.
2. For each component:
    a. Select the Component Name to configure:
        i. **SSTTrackingClientID**: SendSuite Tracking Smart Client
        ii. **SSTDesignerClientID**: SendSuite Tracking Designer
        iii. **SSAdminClientID**: SendSuite Tracking Administrator web-client
        iv. **SSMobileClientID**: SendSuite Mobile
    b. Using the following table, complete the available fields for each component record:

Component Name	Component Description	Component Client ID	Component Redirect URL	Component Logout URL
SSTTrackingClientID	Friendly description indicating that details are for Tracking Client	Client ID of App registered in Azure for Tracking Client.*	Redirect URL of App registered in Azure for tracking Client.*	N/A
SSTDesignerClientID	Friendly description indicating details are for Designer	Client ID of App registered in Azure for Tracking Client.*	Redirect URL of App registered in Azure for Designer.*	N/A
SSMobileClientID	Friendly Description indicating details are for SS Mobile	Client ID of app registered in azure for SS Mobile.*	Redirect URL of App registered in Azure for Sendsuite Mobile*	N/A
SSAdminClientID	Friendly Description indicating details are for SS Admin.	Client ID of app registered in azure for SS Admin.*	Redirect URL of App registered in Azure for SS Admin. https://xxxxx:xxxx/Sendsuiteadmin/SecurePages/Home.aspx.*	https://xxxxx:xxx/Sendsuiteadmin/LogOut.aspx

*Value must be acquired from the app registration record in the Azure Portal.

3. Select **Update** after each component record is added followed by **Add Components** to create and complete the next component record.
4. Once all components have been added, Select **Save**.

Disable Windows Authentication for the SendSuite Tracking Admin

Note: The following steps require knowledge of Internet Information Services (IIS) Manager and therefore may require involvement from your IT department.

1. While logged into the server hosting the SendSuite Tracking solution using an account having sufficient permissions, navigate to **IIS Manager**.
2. Navigate to **Sites>Default Web Site>SendSuiteAdmin**.
3. Select **Authentication**.
4. Change **Windows Authentication** to **Disabled**.
5. Close IIS Manager.
6. Restart IIS.

Upon completion of the aforementioned steps, SendSuite Tracking Admin will require AAD authentication, including MFA, if applied.

User Mapping: Azure-to-SendSuite Tracking

This section explains how users in Azure are mapped to users in SendSuite Tracking.

- Users in Azure AD are mapped to users in SendSuite Tracking by 2 fields:
  - Preferred_username
  - ObjectIdentifier
- A new column – AZUREUSERIDENTIFIER – has been added to the Users table. The column is represented in the **SendSuite Admin>Support>Users** UI by way of a new field in a user's record labeled 'AAD Unique Identifier'. All users must have a value entered for this field in their record (see the following table).
  - **Preferred_username**: Requires that the 'AAD Unique Identifier' field contains the user's email address.
  - **ObjectIdentifier**: Requires that the 'AAD Unique Identifier' field contains the user's unique GUID value from Azure AD.

Setting Applied in SendSuite Admin	Value be present in 'AAD unique Identifier' Field
Preferred_username	Email address of Azure User
ObjectIdentifier	GUID Object ID of User from Azure AD

Logging in to SendSuite Admin

Upon successful configuration of Azure AD authentication in SendSuite Tracking Admin, users logging in to SendSuite Admin will be required to authenticate and complete any Multi-Factor Authentication (MFA) identification checks before being granted access to the app.

Logging in to SendSuite Tracking Smart Client, Designer and Mobile

Note: Tracking Assistants having SendSuite Mobile installed and already paired with SendSuite Tracking will need to be un-paired then re-paired before the AAD authentication workflow will take effect.

Upon successful configuration of Azure AD authentication in SendSuite Tracking Admin, users will be required to authenticate with Microsoft before being granted access to the configured apps. The following details the typical login workflow:

1. Upon launching the Smart Client, Designer, or Mobile, the user will be presented the Microsoft login form.
2. Users will enter their AD credentials.
3. Upon successful authorization, the user will be granted access to the application.

Note: If enabled in AD, Multi-Factor Authentication (MFA) will not be triggered for the Smart Client, Designer, and Mobile.

Azure Active Directory and SendSuite Link

AAD configuration is stored in the SendSuite Tracking database and may be retrieved using the following request:
http://<ServerName>:<port>/link/rest/mobile/azurecomponent/SSMobileClientID?apikey=<apikey>

- <ServerName> = Name of the server hosting SendSuite Link.
- <port> = The port being used by SendSuite Link (default is 8080).
- <apikey> = The API Key value generated in SendSuite Admin.

Additional Information and Troubleshooting

- A user must already exist in the SendSuite Tracking Users table before they may be authenticated via Azure AD. It is recommended that all users have been imported with AAD-specific data prior to completing the AAD configurations.
- Service accounts are not currently supported.
- AAD is implemented only for authentication. A user's configuration profile, layout assignment, and other SendSuite Tracking-specific profile information will be recalled from the SendSuite Tracking database only.

Database Changes

In support of Azure AD, the following changes have been made to the SendSuite Tracking database:

New Tables

AzureRegisteredAppDetails

Table Schema

Column Name	Type	Description
CompId	[PK] nvarchar(200)	Component Id
CompDesc	nvarchar(200)	Component Description
CompClientId	nvarchar(500)	Application Id used in Azure
CompRedirectURL	nvarchar(max)	Redirection URL used in Azure
CompLogoutURL	nvarchar(max)	Logout URL used in Azure
UPDDATE	datetime	Updated date and Time

New Stored Procedures

- ins_AzureRegisteredAppDetails
- get_AzureRegisteredAppDetails
- get_AzureRegisteredAppDetailsbyID
- del_AzureRegisteredAppDetails
- upd_AzureRegisteredAppDetails

Tables Modified

- USERS

Table Modifications:

Column Name	Type	Description
Azureuseridentifier	nvarchar(1000)	Azure unique ID for mapping to a SendSuite Tracking user.

Stored Procedures Modified

- ins_USERS
- get_USERS
- get_USERSbyID
- upd_USERS
- get_USERSbyAzureUserID

Resetting SendSuite Tracking Authentication to Default 'Product'

To return to the OEM Forms authentication mode.

1. Execute the following query against the SendSuite Tracking SQL database:

```
use <SST_database_Name>
update ConfigurationSettings
set KeyValue = 'APP'
where KeyName = 'LoginMode' and Category = 'System'
```

   Note: Replace <SST_database_Name> with the name of the SendSuite Tracking database against which to execute the script.

2. Return to the section of this article titled **Disable Windows Authentication for the SendSuite Tracking Admin** then execute the steps, making sure to change **Windows Authentication** to **Enabled** in step 4.