

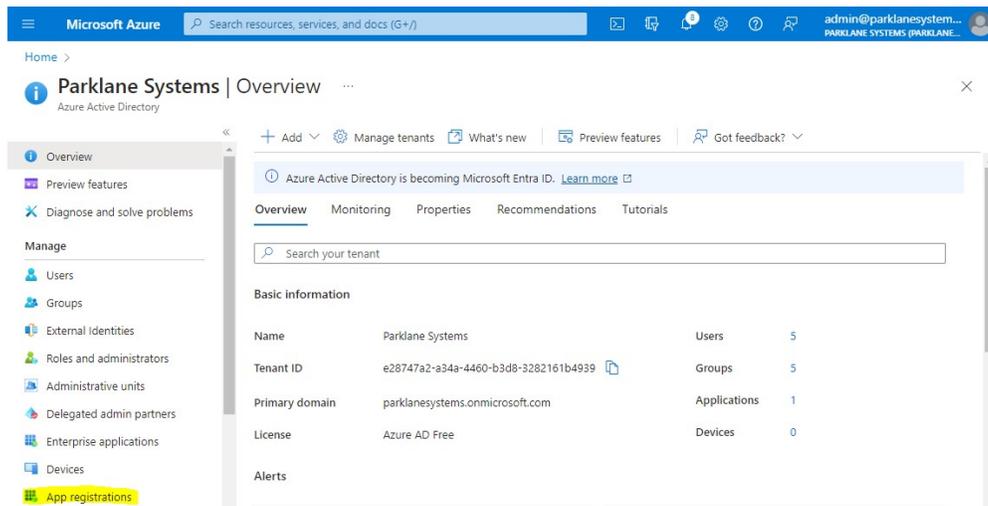
Registering KICS with Microsoft Entra ID (Azure AD)

In KICS 3.8.0, direct support was added for authentication using Microsoft Entra ID / Azure AD.

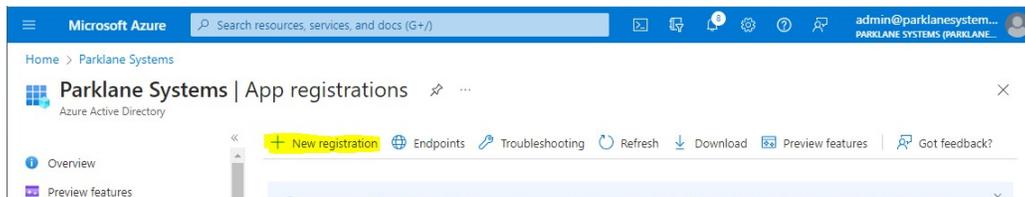
KICS utilizes SAML to authenticate with Microsoft Entra ID. To set up authentication, provisioning will need to be performed in both KICS and the Azure AD Portal.

Setting up Azure AD for KICS

Open the **Azure AD Portal** and select **App Registrations** on the left hand side



Select New Registration



Specify a name for the application such as **Parklane KICS**.

We will not configure the **Redirect URI** at this point.

Click **Register**

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

Home > Parklane Systems | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Parklane KICS ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Parklane Systems only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

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

Register

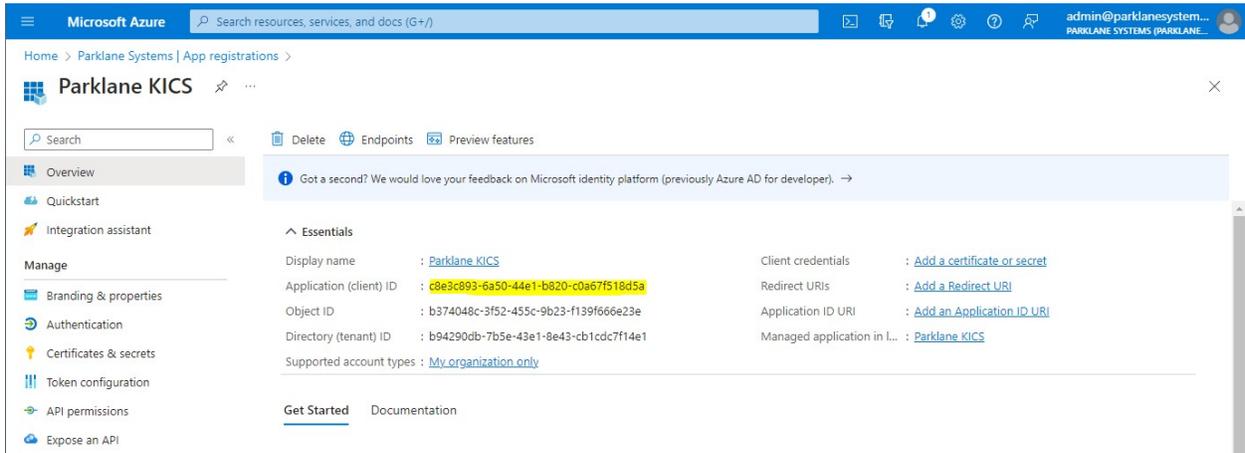
The **Parklane KICS** App Registration will now appear on the Azure AD Console

We will need the two identifiers from the Azure AD console to prepare KICS for authentication:

- **The Application (client) ID**
- **The Federation Metadata Document Endpoint URL**

To Obtain the Application ID:

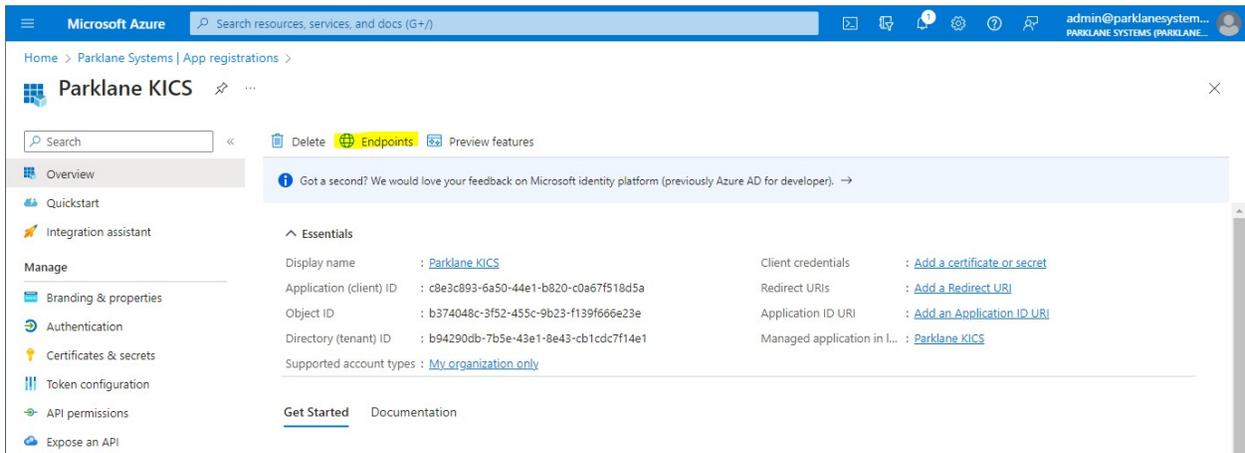
The **Application ID** is listed on the KICS Application Registration page under **Essentials**.



Make note of the Application ID. You will require this during Step 1 of setting up KICS.

To Obtain the Federation Metadata URL:

The **Federation Metadata Document** URL is listed on the KICS Application Registration page under **Endpoints**.



Make note of the Federation Metadata Document URL. You will require this during Step 2 of setting up KICS.



KICS Step 1 - Preparing KICS for Azure AD

In KICS, go to **System Settings > Authentication > SAML / ADFS**

The screenshot shows the 'System Settings' interface for 'Authentication Settings'. The left sidebar contains a navigation menu with options like 'General Information', 'Authentication', 'Regional Information', 'Branding', 'Auditing', 'Email Configuration', 'Form Settings', 'Self-Hosted', 'External Forms', 'Parklane Integration', 'SQL Export', 'License', and 'Log Files'. The main content area is titled 'Authentication Settings' and includes a sub-section for 'Authentication Methods' with tabs for 'General', 'Local', 'LDAP', 'SAML / ADFS', 'Group Import', 'User Import', and 'Secondary Auth'. The 'SAML / ADFS' tab is active, showing instructions for configuring federated services. It is divided into four steps: Step 1 (KICS Service Provider (SP) Settings), Step 2 (Configure KICS for the ADFS Identity Provider (IDP)), Step 3 (Save the above ADFS Settings), and Step 4 (Create the Relaying Party Trust on the ADFS Server). Step 1 includes fields for 'KICS SP Certificate' (Certificate Not Generated), 'Requested Attributes' (Launch Attribute Editor), and 'Application Identifier' (Use Metadata URL). Step 2 includes 'Metadata URL', 'Import IDP Settings' (Query Metadata URL or Upload Metadata XML File), 'ADFS IDP Certificate' (Certificate Not Found or Invalid), and 'Entity ID / URL', 'Sign-On URL', and 'Log-Out URL'. Step 3 has a 'Save Changes' button. Step 4 provides URLs for 'Metadata URL', 'ACS URL', and 'SLS URL', and includes 'Additional Actions' for 'Display Transform'.

KICS Step 1.1 - Generate SP Certificate

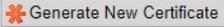
Under **Step 1**, click **Certificate Actions** beside the **KICS SP Certificate** option

KICS SP Certificate Certificate Not Generated Certificate Actions

A Dialog for the Service Provider Certificate will appear

Service Provider Certificate

 A Service Provider Certificate has not yet been generated

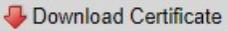
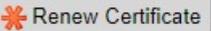
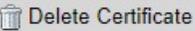




Click **Generate New Certificate**. Certificate Generation will take a couple seconds.

Service Provider Certificate

Status:	Installed
CN:	SP - pkwd1
Expiry	2020-06-11
Fingerprint	8a9f460def422264cb48075c7f32e8a7797d17c4
Fingerprint	48cfe9cf9dafde67f3b4fcb7ee6a6c46b92be24f7ebec208c9470c52cffc2437

Certificate Generated Successfully. Please review and download for your IDP

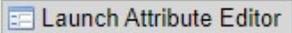
Click **Close**

KICS Step 1.2 - Setting up the Federated Services Attributes

You will need to set up KICS to use the Attributes that Azure provides during the sign-in process.

Launch the Attribute Editor

Requested Attributes



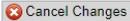
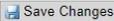
The Attribute Editor will display

ADFS Attributes

KICS requests these attributes when communicating with your ADFS server.
For most deployments, you don't need to change these values.

Setting	Value
Name ID Format	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
Account Name Attribute	<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"/>
Account Serial Attribute*	<input type="text" value="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"/>
Email Address Attribute	<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"/>
First Name Attribute	<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"/>
Last Name Attribute	<input type="text" value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"/>
Group Membership Attribute	<input type="text" value="http://schemas.xmlsoap.org/claims/Group"/>

NOTE: The Account Serial attribute uniquely identifies the ADFS account in KICS. If you change this value after ADFS is deployed, you'll need to "unlink" the existing ADFS accounts in the KICS Account Manager

KICS comes preconfigured for on-premises attributes. Please update the attributes listed below in red:

Attribute	Value
Name ID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Account Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Account Serial	http://schemas.microsoft.com/identity/claims/objectidentifier
Email Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Group Membership	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Click **Save Changes**

KICS Step 1.3 - Setting the Azure Application ID

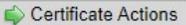
Continuing down the page, you will see the configuration parameter for the KICS application Identifier

Select **Use the following Application ID**

Paste in the **Application ID** you obtained from the Azure Console

Step 1 - KICS Service Provider (SP) Settings

You will need to generate a Service Provider (SP) Certificate for KICS to communicate with your ADFS Server. Click the **Certificate Actions** button to generate a certificate.

KICS SP Certificate Certificate Installed 

Requested Attributes 

Application Identifier Use Metadata URL (<https://tn0220.parklanesystems.com/kics/saml/metadata.php>)
 Use the following Application ID:

KICS Step 2 - Configuring Azure as the identity provider

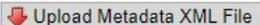
On the **System Settings > Authentication > SAML** page, **Step 2** focuses on setting up the URLs and Certificates for your Azure Environment. KICS can import this data from the Federation Metadata URL copied from your KICS App registration page above.

Paste the Federation Metadata Document Endpoint URL you obtained from the Azure Console into the **Metadata URL** field and then click **Query Metadata URL**. The Azure URLs and Certificates will be imported.

Step 2 - Configure KICS for the ADFS Identity Provider (IDP)

Specify your ADFS Server's Metadata URL Below.
 You can import your IDP's certificate and URLs by querying the Metadata URL or by uploading the Metadata XML file.
 If neither option is available, the IDP settings can be specified manually

Metadata URL:
example: https://servername/FederationMetadata/2007-06/FederationMetadata.xml

Import IDP Settings  or 

You will see the Azure IDP Certificate and Endpoint URLs configured in KICS.

i The IDP Metadata has been imported, please confirm the server URLs and Certificates below

ADFS IDP Certificate	Certificate Installed	Certificate Actions
Entity ID / URL		<input type="text" value="https://sts.windows.net/b94290db-7b5e-43e1-8e43-cb1cdc7f14e1/"/> <small>example: https://servername/adfs/services/trust</small>
Sign-On URL		<input type="text" value="https://login.microsoftonline.com/b94290db-7b5e-43e1-8e43-cb1cdc"/> <small>example: https://servername/adfs/ls/</small>
Log-Out URL		<input type="text" value="https://login.microsoftonline.com/b94290db-7b5e-43e1-8e43-cb1cdc"/> <small>example: https://servername/adfs/ls/?wa=wsignout1.0</small>

Most SAML server certificates will last for 1 year. You have the option to configure KICS to query the Metadata once a day to check for certificate updates and URLs.

The **Display SAML Diagnostic Page during sign-in** option allows you to review the SAML attributes returned from Azure and make sure they line up during the authentication process. It's highly recommended to enable this feature during the initial testing of the authentication component.

Additional Options

- Automatically Check IDP Metadata Daily for new Certificates
- Automatically Check IDP Metadata Daily for new URLs
- Display SAML diagnostic page during sign-in

Click **Save** to save the current settings into KICS

Setting up URLs and Attributes for KICS within Azure

KICS can now send authentication requests to Azure, however we need to configure Azure to provide the proper attributes and send clients back to the proper URL.

On the KICS **System Settings > Authentication > SAML page**, make note of the **ACS** and **SLS** URLs.

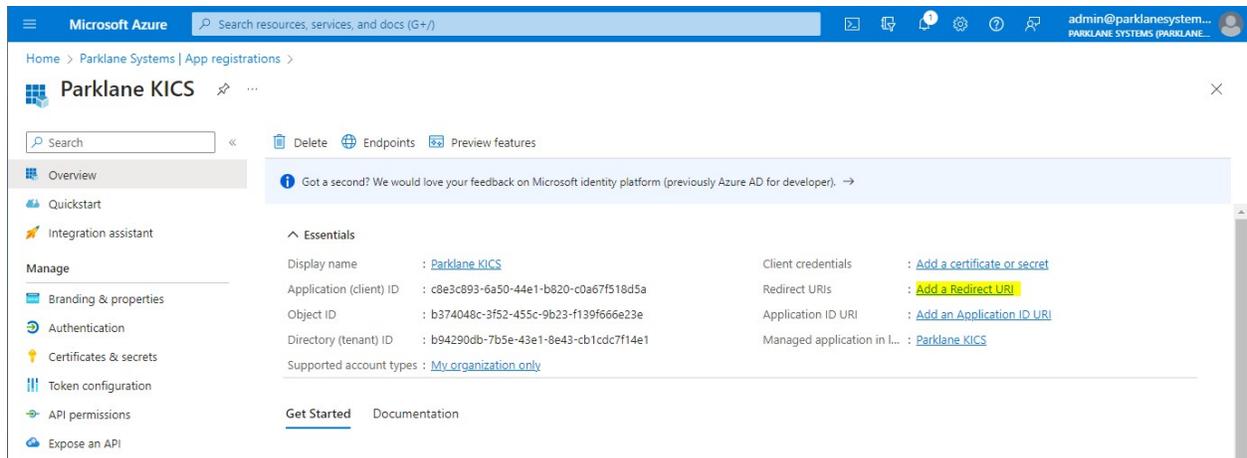
Step 4 - Create the Relaying Party Trust on the ADFS Server

Log into your AD FS Management Console and create a Relaying Party Trust using the Metadata URL below. You can either use the Metadata URL, or download the Metadata XML file

Metadata URL	https://tn0220.parklanesystems.com/kics/saml/metadata.php
ACS URL	https://tn0220.parklanesystems.com/kics/saml/index.php?acs
SLS URL	https://tn0220.parklanesystems.com/kics/saml/index.php?sls

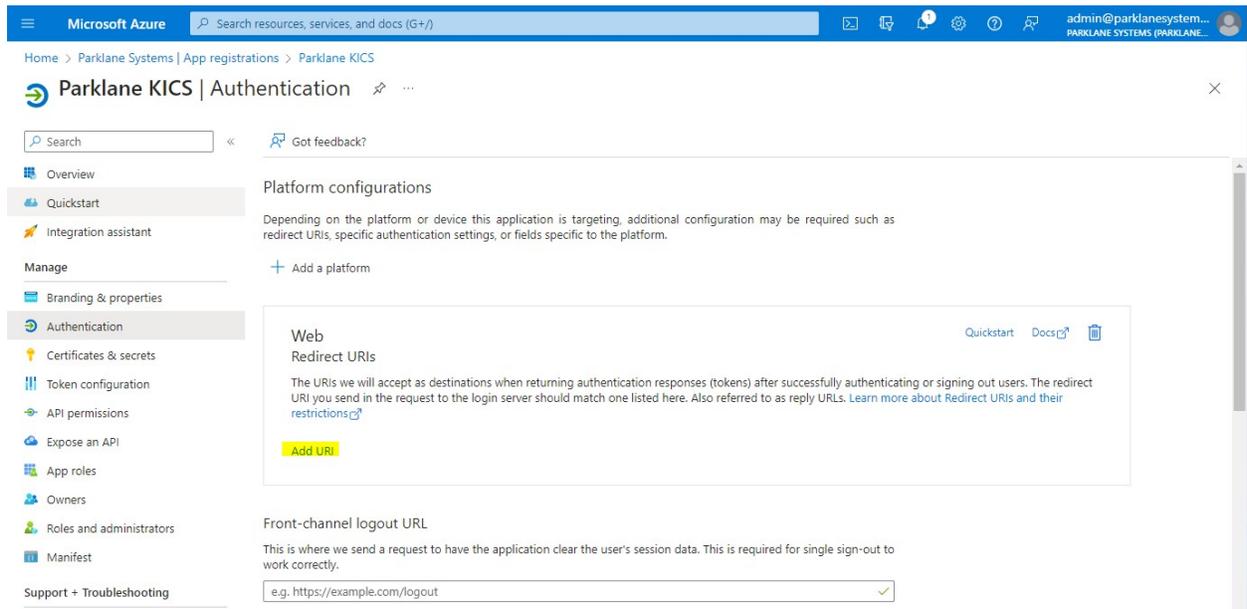
Once the Relaying Party Trust is created, add two Claim Rules to the Trust

Open the **Azure AD Portal > App Registrations > Parklane KICS** configuration page.



Select **Add a Redirect URI**

The **Authentication** page will open.



Under **Web - Redirect URIs**, select **add URI** and paste in the ACS URL obtained from KICS.

Under **Front-channel logout URL**, paste the SLS URL obtained from KICS.

Web Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

[Add URI](#)

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and

Save Discard

Click **Save**

Next, we will set up the Attribute Tokens for KICS. KICS accepts the default tokens that Azure AD provides, however if you wish to pass Group Membership, you will need to configure the Group Token Attribute.

On the left side of the Azure Portal, select **Token Configuration**

Select **Add Groups Claim**

The **Edit Groups Claim** dialog will appear on the right side of the screen.

Choose which groups would like to pass into KICS. If you're unsure, select **All Groups**

Edit groups claim ✕

i Adding the groups claim applies to Access, ID, and SAML token types. [Learn more](#)

Select group types to include in Access, ID, and SAML tokens.

- Security groups
- Directory roles
- All groups (includes 3 group types: security groups, directory roles, and distribution lists)
- Groups assigned to the application (recommended for large enterprise companies to avoid exceeding the limit on the number of groups a token can emit)

Customize token properties by type

∨ ID

∨ Access

∨ SAML

Add

Cancel

Click **Add**

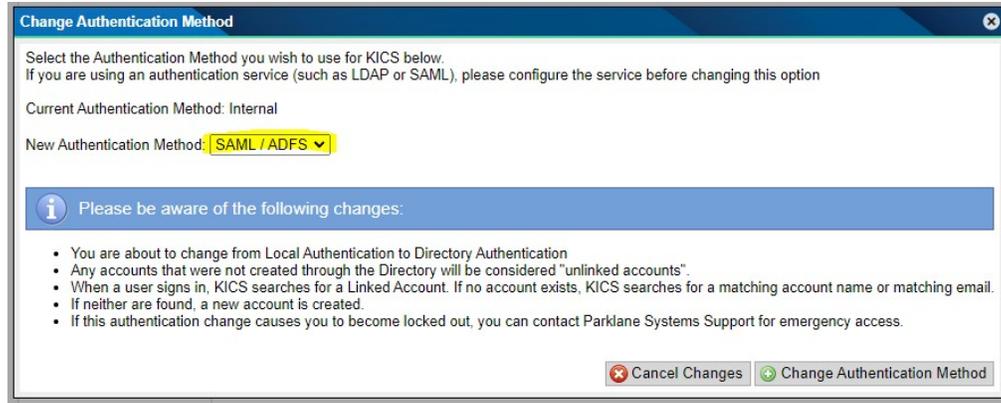
Configure KICS to Authenticate with Azure

At this point, the provisioning of SAML in KICS and Azure is complete. To configure KICS to send login requests to Azure, we need to change the primary login method in KICS.

In KICS, go to the **System Settings - Authentication - General** page

The screenshot shows the 'System Settings' interface for 'Authentication Settings'. The left sidebar contains a navigation menu with items like 'General Information', 'Authentication', 'Regional Information', 'Branding', 'Auditing', 'Email Configuration', 'Form Settings', 'Self-Hosted', 'External Forms', 'Parklane Integration', 'SQL Export', 'License', and 'Log Files'. The main content area is titled 'Authentication Settings' and includes a description: 'The following settings define how users can authenticate to KICS. Each Authentication method has its own properties you can assign. Once the Authentication Method is configured, you can change the authentication method below'. Below this is a 'Authentication Methods' section with a tabbed interface. The 'General' tab is active, showing 'Session Timeout' settings (Enable Session Timeout: No, Session Timeout: 60 Minutes) and 'Primary Authentication' settings (Primary Authentication Method: Internal, with a 'Change' button).

Under the **Primary Authentication** section, click **Change**



Select **SAML/ADFS** and then click **Change Authentication Method**

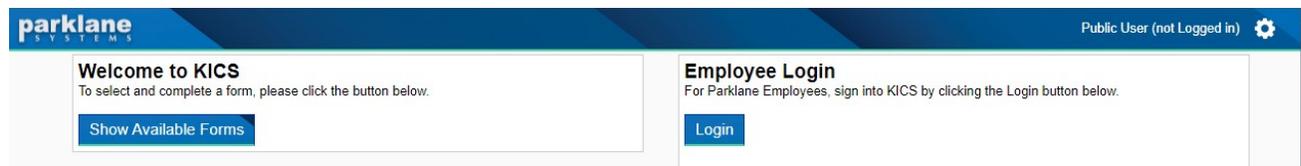
Primary Authentication

Primary Authentication is used by employees and managers within your organization. Depending on the size of your organization, you can choose to use Local Authentication have KICS manage the user accounts, or you can select Directory Authentication and have KICS utilize your organization's directory server for account management and authentication

Primary Authentication Method: **SAML / ADFS**

The primary authentication method will now be listed as **SAML/ADFS**.

The login page will now show a login button to redirect users to the Azure AD login page.

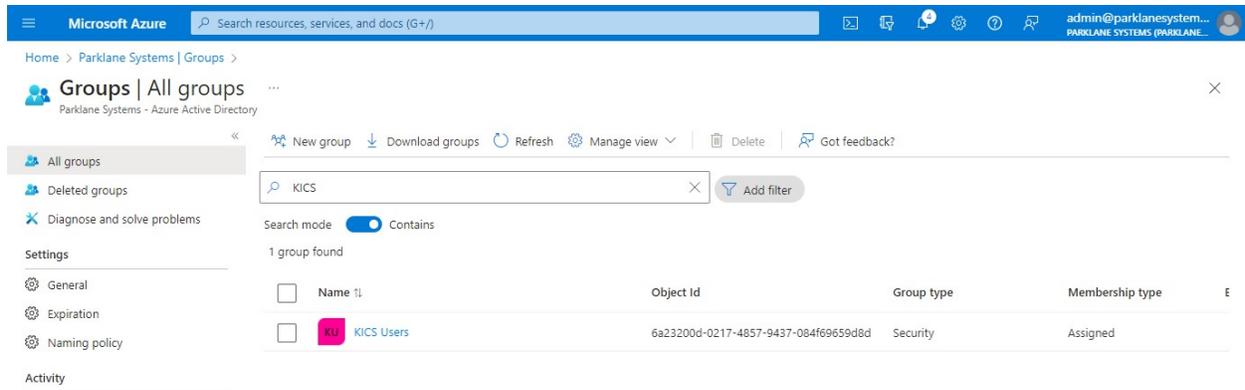


Importing Groups into KICS from Azure

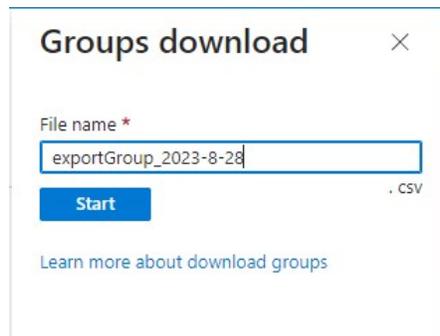
In KICS, we can import a list of groups that are exported from the Azure AD console. These groups can be assigned role permissions in KICS.

When users authenticate, they can be automatically granted permissions to templates and functions within KICS if they are a member of the appropriate group.

From the **Azure AD Console**, open the **Groups Panel**



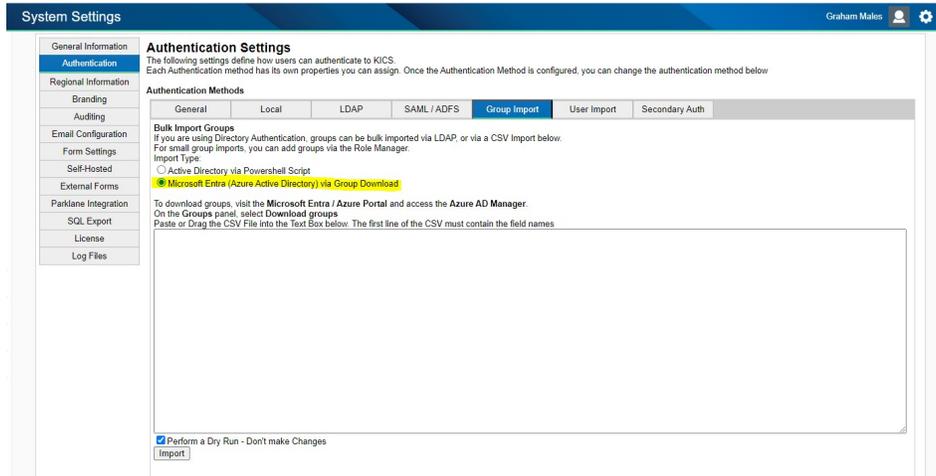
Select **Download Groups**.



Click **Start**. Azure will generate an export of Azure AD groups as a CSV file.

In KICS, go to the **System Settings - Authentication - Group Import** page

Select **Microsoft Entra (Azure Active Directory) via Group Download**



Paste the contents of the CSV file into the text box.

You have the option to perform a **dry run** of the import to ensure the import will be successful without making changes.

Click **Import**

You will see a status result of the import

Line Number	Import Success	Group Name	Import Details
1	Yes	KICS Users	Group not found, creating

If this was a dry run and everything looks successful, uncheck the **dry run** option and re-run the import to add the groups to KICS.

The Group Import is now successful. If you access the Role Manager, you can now search for and see the groups you imported.

