Active Directory Service

Fleetistics offers customers the ability to share secure user rights management (URM) access information between existing systems and the MyFleetistics portal providing a single sign on experience. This Active Directory integration also provides immediate user access and denial based on centrally managed Active Directory changes completed as part of routine processes with your organization. This provides additional security and a significant reduction in user maintenance time for the telematics platform program manager.

If your organization has Azure AD or ADFS but does not have the IT skills to complete the setup, www.IGTech365.com can assist you for a set project free. IGTech365 can also provide managed IT services, backups, employee help desk and other IT networking and administration services. **866.365.7798**

If your organization utilizes a different URM services and would like to discuss an integration project contact your account manager. (OAuth, OpenID, SAML, LDAP, LenAuth, HTTP Basic, etc)

Submit any corrections or suggestions to contact@fleetistics.com

Azure AD Setup

1. Enable the appropriate Active Directory service in MyFleetistics>Account>Services>Services Admin
    a. Sign into your Azure portal.
    b. Choose the Directory by selecting your account in the top right corner of the page, followed by selecting the Switch Directory navigation and then selecting the appropriate Directory.
    c. In the Azure portal, search for and select Azure Active Directory.
    d. In the Azure Active Directory left menu, select App Registrations, and then select New registration.
    e. Follow the prompts and create a new application: - Name: My Fleetistics - Supported account types: "Accounts in this organizational directory only" or "Accounts in any organizational directory" (if you have several directories) - Platform configuration (Optional): "Client Application (Web, iOS, Android, Desktop+Devices)" then click "Register"
    f. On the next page click "+ Add platform". If you accidentally close the next page after register - select the "My Fleetistics" application and click "Add a Redirect URI" select "Web application" - "Web" - Redirect URIs: "https://my4.myfleetistics.com/complete-azure-ad-login" - Logout URL: leave empty - Implicit grant: check "ID tokens" checkbox then click "Configure"

   g. On the application page select "Token configuration (preview)" at the left menu click "+ Add optional claim" and select "ID" as the Token type. Check: - email - family_name - given_name - nickname then click "Add" click "+ Add groups claim", check "Security groups" at "Select group types to include in Access, ID, and SAML tokens.", open "ID" section in "Customize token properties by type" and choose "Group ID" then click "Add"
   h. If you plan to grant the MyFleetistics application with the rights to read User Info to in order to provide the Users' phones On application page select "Certificates & secrets" at the left menu click "+ New client secret", fill the "Description" with any descriptive text like "user info access". Copy the secret value so you can assign it on the service settings page later - On application page select "API permissions" at the left menu click "+ Add a Permission", choose "Microsoft Graph" and "Application permission" then check "User.Read.All" and click "Add permissions". You can revoke this grant any time or disable reading User Info on service settings page.
2. Enable "Azure AD Single Sign On" on Company Services Admin page, then open settings of this service and assign: - Directory ID - Directory (tenant) ID from Azure AD My Fleetistics Application page - Application ID - Application (client) ID from Azure AD My Fleetistics Application page - Application Client secret - Generated Client secret Azure AD User of your Company will be only allowed to login to My Fleetistics if was assigned to application role or group. If you want that any Azure AD User of your Company will be allowed to login to My Fleetistics - you should select "Default Permission Role" that will be used for user without assigned role or group Unique login URL is a link to special login page that should be used by users of your company - https://www.fleetistics.com/login/?azureAdCompanyID=[your companyID] Debug login URL link will show Azure AD token payload without the actual login to be able to check what is sent by Azure AD to My Fleetistics
3. If you plan to use Application Roles to manage MyFleetistics User Roles
   a. Declare roles for My Fleetistics application select "Manifest" at the left menu of My Fleetistics application page and replace node "appRoles" with list from file: app_roles.txt then click "Save"
   b. You can assign roles to users/groups as described in documentation (https://docs.microsoft.com/en-us/azure/active-directory/develop/how to-add-app-roles-in-azure-ad-apps#assign-users-and-groups-to-roles)
4. If you plan to user Azure AD Groups to manage My Fleetistics User Roles
   a. Create new groups: FLT-Administrator, FLT-Supervisor, FLT-DefaultUser, FLT-Dispatcher, FLT-DriveAppUser, FLT-ViewOnly, FLT-Nothing, FLT-Inactive or use your own groups
   b. Map Azure AD groups (by group Object ID) to My Fleetistics User role on the "Azure AD Single Sign On" settings page If User have more than one group assigned - will be used the first matched group in the order you created the groups mapping 5. Both - Application Roles and Azure AD Groups can be used together at the same time: - if User has assigned Application Role - it will be used - if no Application Role - Azure AD Groups will be used - if no Roles or Groups - Default Permission Role will be used - if no Default Permission Role was

assigned - user won't be allowed to login.

ADFS Setup

1. On your server open AD FS Administration and open Add Relying Party Trust Wizard by clicking “Add Relying Party Trust…” at the Action menu:
    a. “Select Data Source” - Choose “Enter data about the relying party manually”
    b. “Specify Display Name” - Enter a display name for the relying party. This name won’t be shown to user and is for Admin only
    c. “Choose profile” - Choose “AD FS Profile”
    d. “Configure Certificate” - Skip this step
    e. “Configure URL” - Skip this step
    f. “Configure Identifiers” – add Relying Party Trust Identifier that lately will be assigned on "Active Directory - ADFS User Authentication & SSO Service" admin page
    g. “Configure Multi-factor Authentication Now?” – choose “I do not want to configure multi-factor ….”
    h. “Choose Issuance Authorization Rules” – choose “Permit all users to access this relying party”
    i. “Ready to Add Trust” – skip this step
    j. Finish

Add:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (select or type to add more) Custom name in blue
Required field	
User-Principal-Name	UserPrincipalName
Display-Name	DisplayName
E-Mail-Addresses	E-Mail Address
Optional fields	
Surname	Surname
Given-Name	Given-Name
Telephone-Number	PhoneNumber
Employee-ID	Employee

3. To assign MyFleetistics permission roles to your users you can create special groups: FLT-Administrator, FLT-Supervisor, FLT-DefaultUser, FLT-Dispatcher, FLT-DriveAppUser, FLT-ViewOnly, FLT-Nothing, FLT-Inactive or use your own groups. After this you have 2 options:

3.1. You can map AD Groups to MyFleetistics permission roles in the MF Admin page To do so you should select Relying Party Trust and click “Edit Claim Rules…”,

Select rule name “UserInfo” and click “Edit Rule…

Add:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (select or type to add more) Custom name in blue
Token-Groups as SIDs	Group SID

It will send the list of all User group SIDs to MyFleetistics on the "Active Directory - ADFS User Authentication & SSO Service" admin page map each used group to MyFleetistics permission roles by assigning Group SID and selecting permission role from the list

3.2. You can map AD Groups to MyFleetistics permission roles in the AD FS Management. To do so you should select Relying Party Trust and click “Edit Claim Rules…”, For each group click “Add Rule…”, choose “Send Group Membership as Claims” in “Claim rule template”, assign “Claim rule name” that will be used just to name the rule, select AD Group in “User’s group”, assign “Outgoing Claim Type” as “flt-role” and “Outgoing claim value” as one of MyFleetistics permission roles Supervisor, Default, Dispatcher, Driver, ViewOnly, Nothing, Inactive

This way allows you to not send all User group SIDs to MyFleetistics but requires to assign claim type and value manually for each mapped group.

Unique solution ID: #1024
Author: n/a
Last update: 2021-05-06 18:51