INTEGRATION

Integration section of the CONTROL CENTER allows to configure automated processes for data exchange between ScheduleInterpreter® and 3rd party platforms.

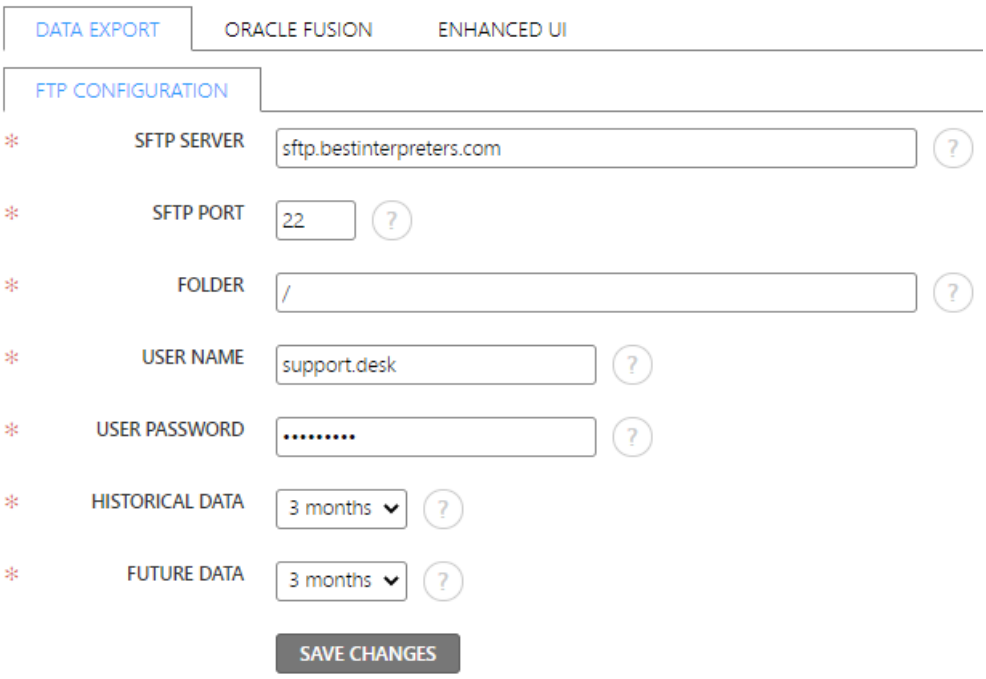
DATA EXPORT

Data export section enables your organization to setup secure and fully automated process to retrieve account information such as invoices, client and vendor profiles, assignments, etc. This process often referred as upload to a secure server. ScheduleInterpreter® supports SSH File Transfer Protocol (sFTP) as one of the most secure option available. Read more on sFTP. Information transferred via this method is encrypted using requirements of the receiving server.

All uploads are scheduled to take place after 1:00 am CST/CDT.

To configure automated process, navigate to TOOLS AND SETTINGS > Control center > ACCOUNT SETTINGS > INTEGRATION > DATA EXPORT > FTP CONFIGURATION

Below is an example of the completed form.



Provide details of your sFTP server using SFTP SERVER and SFTP PORT fields. If there is a specific folder you need to upload the data to, provide path using FOLDER field.

Windows and *nix based servers use different formats of the folders

Enter USER NAME and USER PASSWORD, authorizing ScheduleInterpreter® to login to the server. The credentials should allow the user to connect to the server, read and write to the directory listed in FOLDER field.

Using HISTORICAL DATA drop down option, provide instructions for ScheduleInterpreter® how far back retrieve the data from. FUTURE DATA option enables to export information such as upcoming assignments.

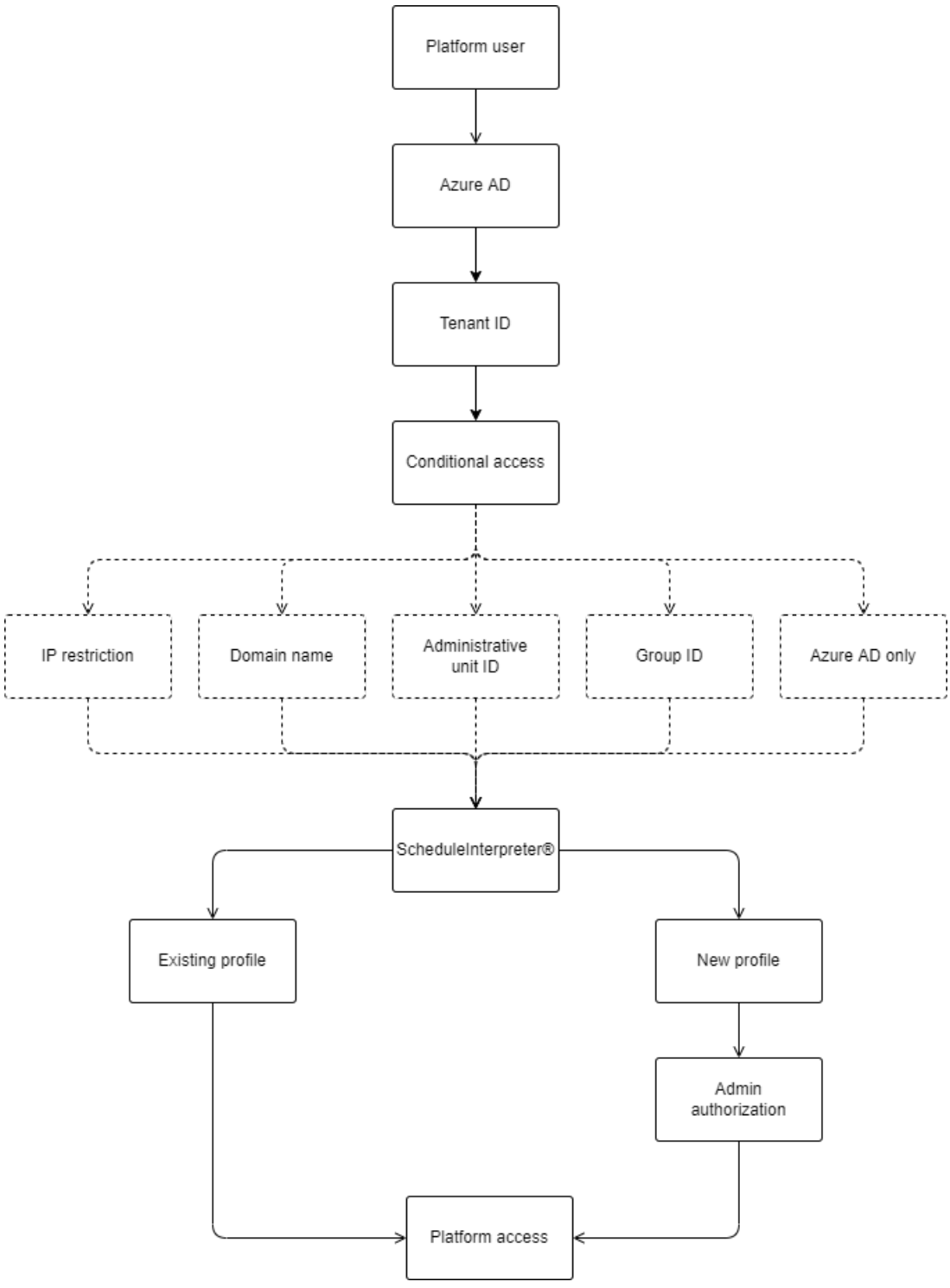
Non-time sensitive items, such as customer accounts, are always export in its entirety.

If your server is hosted in the cloud and data charges apply to ingress traffic, consider to retrieve all data on the first upload and then setting HISTORICAL DATA to 1 day.

When all settings are completed, click SAVE CHANGES button. ScheduleInterpreter® data will be uploaded to the specified server using provided instructions.

AZURE AD

Azure AD section provides set of options to activate and configure Microsoft Azure AD. Before continuing make sure to locate your organization's tenant ID.



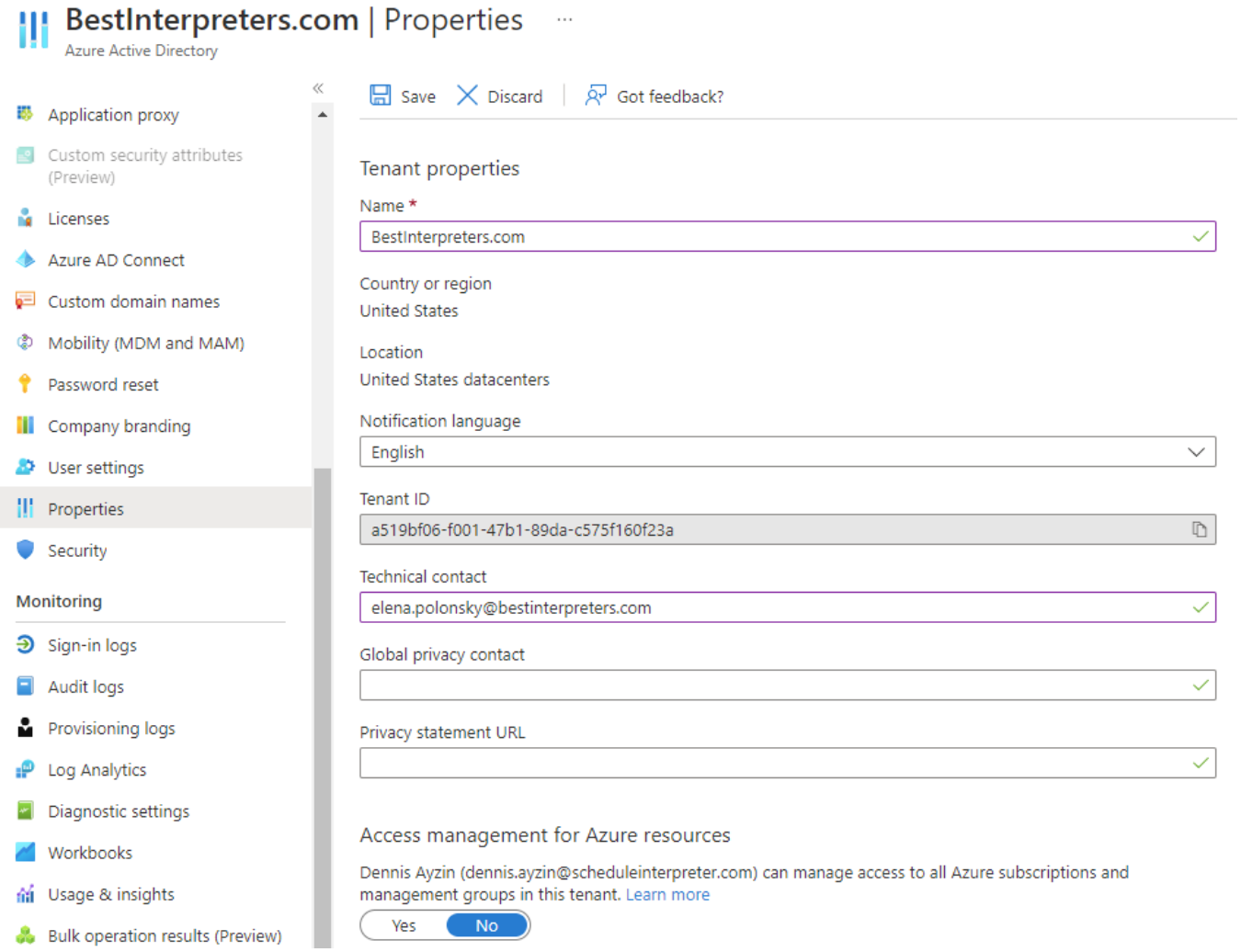
HOW TO FIND YOUR AZURE ACTIVE DIRECTORY TENANT ID

Azure subscriptions have a trust relationship with Azure Active Directory (Azure AD). Azure AD is trusted to authenticate users, services, and devices for the subscription. Each subscription has a tenant ID associated with it, and there are a few ways you can find the tenant ID for your subscription.

FIND TENANT ID THROUGH THE AZURE PORTAL

Sign in to the Azure portal.

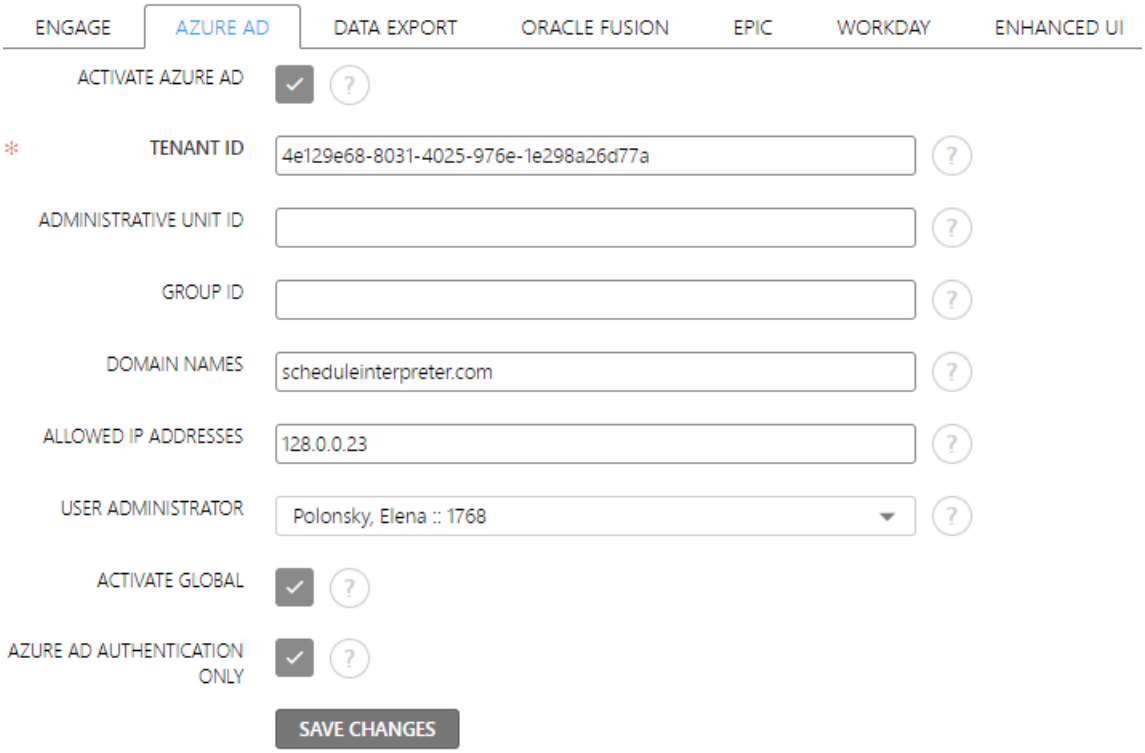
1. Select Azure Active Directory.
2. Select Properties.
3. Scroll down to the Tenant ID field. Your tenant ID will be in the box.
4. Selecting ACTIVATE AZURE AD option will open the set of fields.



Locate Tenant ID field and use copy icon on the right side to copy your organization's Tenant ID.

CONFIGURE AZURE AD

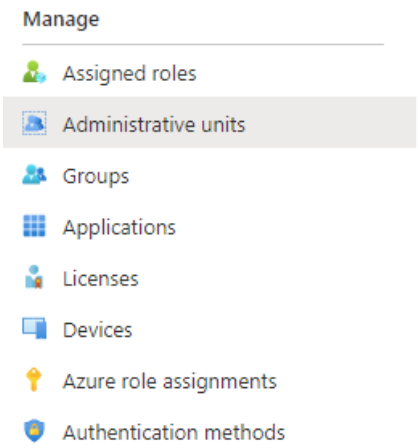
Navigate to Tools and settings > Account center > Account settings > Integration Azure AD. Click on Activate Azure AD option to open the rest of the configuration fields. Start by filling TENANT ID field by pasting Tenant ID copied from Microsoft Azure AD portal.



ScheduleInterpreter® offers additional options, known as conditional access, to provide more precise access rights to the users. When necessary, using ADMINISTRATIVE UNIT ID and GROUP ID fields access can be limited to a specific group of Azure AD users.

> Creating a security group is recommended as a best business practice.

This information can be obtained from the same Azure AD portal.



DOMAIN NAMES field activates a requirement for user to be part of the same domain. Several domains can be listed using comma as a separator.

> Domain names option allows to fine tune the group of users for organizations with multiple domains and unified administrative units or groups.

Microsoft Azure AD offers option to manage conditional access for users and applications. If conditional access is

configured in Microsoft Azure AD, there is no need to configure it in ScheduleInterpreter®.

ALLOWED IP ADDRESSES activates conditional access offered by ScheduleInterpreter® and is based on user's network IP address. This is the most restrictive setting in Azure AD configuration, proceed with caution. Make sure external IP address of the computer used to make changes is in the IP pool added to the list, failing to do so will block your account and will prevent you from completing configuration. Add one or multiple IP addresses using comma as a separator.

ScheduleInterpreter® is a closed platform. Authenticated users are not automatically granted right to access the platform. Their profile is created and notification is sent to the administrator who can then assign the role and activate the profile. This regulates the access rights and guarantees secondary validation by authorized individual.

USER ADMINISTRATOR field allows to select an individual on the management team who will receive a notification when new users is added through Azure AD authentication.

ACTIVATE GLOBAL will require all users to be authenticated using Azure AD. This will include users in all accounts and sub-accounts. When left unchecked, only members of the administrative team will be authenticated using Azure AD.

AZURE AD AUTHENTICATION ONLY, when activated, will prevent options to login to ScheduleInterpreter® using traditional method of user name and password.

Revision #9
★Created Thu, Jun 18, 2020 3:51 PM by manual admin
Updated Sun, Sep 4, 2022 6:22 PM by Dennis Ayzin