Technical requirements MediusFlow Cloud

ⓘ This document describes technical requirements for clients that uses MediusFlow Cloud.

This document was last updated May 15:th 2018

End user client requirements

Software requirements

The following operating systems are supported in combination with the web browsers mentioned below:

- Windows 7, Windows 8, Windows 8.1
- Windows 10
- Mac OS X Lion and later

The following Web browsers are recommended:

- Google Chrome, most recent stable version
    - Chrome applies updates automatically. Medius makes every effort to test and support the most recent version.
- Mozilla Firefox, most recent stable version
    - By default Firefox is set to update automatically but it can be changed to manual. Medius makes every effort to test and support the most recent version.
- Apple Safari, version 8.x or later

The following Web browsers are supported:
- Microsoft Edge, most recent stable version
- Microsoft Internet Explorer - version 11.0
    Updates can be done automatically through Windows Update.

Use this link to check overall browser usage statistics, it can be filtered on versions, regions, time intervals etc: http://gs.statcounter.com/

ⓘ **Supported vs recommended browsers**
By Recommended browser, we mean the browsers where XI performs the best in terms of:

- User experience
- Performance
- Robustness
- Maturity

Supported browsers can be used, but they perform less well in the areas described above. For example:

- Manual tests have been executed for a shorter time, meaning that minor quirks can still exist
- Browsers that are not actively developed any longer and the vendor has set an End Of Life date (for example, Internet Explorer 11).
- Statistics based on usage (how much is a particular browser used by our customers)
- Noticeable degradation in terms of performance etc.

Hardware requirements

Below are the requirements on a local machine to make the user experience as good as possible.

- Processor: Dual-core Intel i5, 2GHz or better

- RAM: 4 GB
- Screen resolution: Minimal supported screen resolution is 1280x720. Recommended resolution is 1920x1080 or higher

⚠️ **Desktop virtualization**
If possible, avoid running MediusFlow on Citrix or any other desktop virtualization platform. If it cannot be avoided, make sure the thin clients are (at least) configured according to the requirements above. Otherwise, end-users might experience performance problems.

Office 365 user integration service

ⓘ The Office 365 integration service handles user authentication and user transfer from Office 365 (Azure AD). The service is a cloud service that is integrated with Mediusflow and Azure AD.

Note that this is an add-on to MediusFlow and below requirements are not valid if Office 365 integration is not in scope for your implementation of MediusFlow.

To be able to run the Office 365 user integration against a MediusFlow XI Cloud tenant, please go through the prerequisites below:

Azure AD application

MediusFlow is registered as a globally available application in Azure and is enabled in the Azure AD for the customer. By enabling the application MediusFlow get's access to read users and groups, this is done through Microsoft Graph API(https://developer.microsoft.com/en-us/graph).

Medius provides an admin consent link that Microsoft have invented to simplify activation of an application, the customer clicks that link to approve access.

ⓘ **Example of admin consent link**
Below is how the admin consent link looks. Replace tenantId with the Azure AD tenant id.

https://login.microsoftonline.com/**[tenantId]**/adminconsent?client_id=9625c4b9-1361-442d-a68f-e7d8a3655ebc&state=1&redirect_uri=https://office365.cloudapp.mediusflow.com/success

An example link is seen below:

https://login.microsoftonline.com/8e717190-f5dc-4b69-892e-bc74f89a8ec7/adminconsent?client_id=9625c4b9-1361-442d-a68f-e7d8a3655ebc&state=1&redirect_uri=https://office365.cloudapp.mediusflow.com/success

MediusFlow needs access to the following resources in Azure AD to synchronize users:

- Group/Directory read
- User read all

Read more about it here:

- https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added
- https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent

Office 365/Azure AD version

All versions of Azure AD are supported, there exists though limitations in how many applications and configuration possibilities for subscription/plan for Free and Basic Azure AD.

Please ensure to verify your Azure AD subscription:

https://www.microsoft.com/en-us/cloud-platform/azure-active-directory-features

User provisioning

Some Azure AD applications use something called user provisioning where Azure AD pushes the users and changes to the other system.

MediusFlow do not use the user provisioning feature from Azure AD, instead users are extracted by specifying the group. This makes configuration more flexible and allows for faster deployment with less impact in Azure AD. After initial user transfer, the delta endpoint from Azure AD is used to get the changed users.

> ⊘ To be able to read from groups that are created in Active directory, they need to be synced to Azure AD. Otherwise only groups created in Azure AD can be used.

Relevant properties

Office 365/Azure AD	Mediusflow XI	Supported
GivenName	FirstName	Yes
Surname	LastName	Yes
Id	identityprovider identifier / externalsystemId	Yes
mail	Email	Yes
accountEnabled	IsActive	Yes
mailNickname (If the user is transferred from Active Directory this is usually the same as SAMAccountName. If the user is created in Azure it is usually the same as name or the text before @ in UPN)	UserName	Yes
Manager	Responsible(UserConfiguration, this needs to be configurable)	No
Authorization groups	AuthorizationGroup on User configuration	No

MediusFlow related properties such as Default company, TimeZone, Language, Format, Roles etc. is set in the user integration service UI.

Known limitations

- One Mediusflow tenant can only be connected to one Azure AD instance
- Pointing directly to the Azure AD tenant when logging in is not supported
  - The service uses the Office 365 common endpoint, this means in practise that we let Microsoft decide when logging in what tenant and what account it is.
- Guest users is not supported
  - Guest users gets a new global id when they are created in the "foreign" tenant, this makes it impossible to retrieve that id when logging in.
- Deleting a user
  - MediusFlow cannot delete a user through the integration. This is mainly due to that it can be transactions connected to it. It's important to deactivate the user in Azure AD first, to ensure that the user is inactivated in MediusFlow before it's being removed in Azure AD.
  - If a user is removed by mistake it's possible to inactivate it manually in MediusFlow
- Inactivation by removing the user from a group
  - To inactivate a user in MediusFlow XI, the user must be inactivated. The user is not inactivated when it's removed from the group. This due to that it can be in more groups that are configured with the same user.

> ⊘ **Official URL to Mediusflow XI**
> Ensure that users are using official url when logging to their Mediusflow XI tenant - the official URL is https://cloud.mediusflow.com/customer. Addresses like https://cloudXX.mediusflow.com/customer does not work.

Integration to on premise Active Directory

Medius provides the possibility to integrate MediusFlow to on premise versions of Active Directory to facilitate user synchronization and single sign on. Separate requirements apply to this integration and will be provided upon request.

Other Integration requirements

For technical requirements and prerequisites for other integrations, such as ERP integrations and data capture software integrations, please see product definition of each product respectively.