Technical requirements MediusFlow Cloud

This document describes technical requirements for clients that uses MediusFlow Cloud and was last updated March 1st 2016.

1 End user client requirements

1.1 Software requirements

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

- Windows 7, Windows 8, Windows 8.1
- 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 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/

1.2 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 below. Otherwise, end-users will experience performance problems.

2 Integration requirements

MediusFlow Cloud can integrate to local services within customer networks. The most common integrations are:

- ERP integration
  - Data exchange between MediusFlow and the ERP system
- Active Directory integration
  - Being able to import users from AD to MediusFlow
  - Being able to authenticate (log in) with AD credentials on MediusFlow Cloud

3 General Integration Requirements

These are general requirements to be able to setup integrations with Mediusflow.

3.1 Integration Server

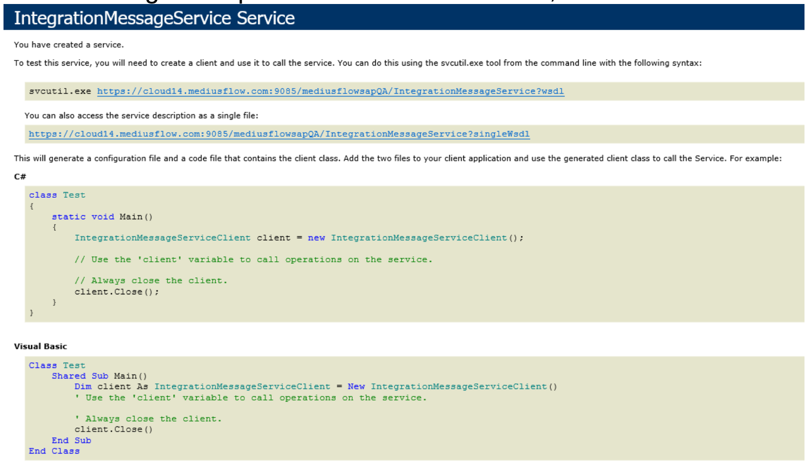
The ERP integration needs to send and fetch data to/from the ERP system. To do this there is a need to setup a Medius Integration Client in the local network (on premise at customer) that performs the data exchange between MediusFlow Cloud and the ERP system. The Integration Client is a Windows application that can be installed on any server fulfilling the following requirements (server can be shared with other applications):

Component	Requirement
OS	Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2
CPU	2 GHz
RAM	4 GB
Disk	2 GB

3.2 Access

Access	Comment
VPN	VPN credentials to integration server
Server account	Administration rights on integration server
ERP access	ERP credentials and access to ERP server/services from integration server
MediusFlow XI	Integration server needs to have access to MediusFlow XI SOAP services. • Cloud environment ○ Port 9085 for outbound traffic • On premise ○ Network communication between the Integration Server and the Mediusflow server ○ Default port: 19308 (could be different in your project) • Verify access on https://cloud14.mediusflow.com:9085/mediusflowIBSQA/IntegrationMessageService

- You should get this picture in the web browser,



IntegrationMessageService Service

You have created a service.

To test this service, you will need to create a client and use it to call the service. You can do this using the svcutil.exe tool from the command line with the following syntax:

```
svcutil.exe https://cloud14.mediusflow.com:9085/mediusflowsapQA/IntegrationMessageService?wsdl
```

You can also access the service description as a single file:

```
https://cloud14.mediusflow.com:9085/mediusflowsapQA/IntegrationMessageService?singleWsdl
```

This will generate a configuration file and a code file that contains the client class. Add the two files to your client application and use the generated client class to call the Service. For example:

C#

```
class Test
{
    static void Main()
    {
        IntegrationMessageServiceClient client = new IntegrationMessageServiceClient();

        // Use the 'client' variable to call operations on the service.

        // Always close the client.
        client.Close();
    }
}
```

Visual Basic

```
Class Test
    Shared Sub Main()
        Dim client As IntegrationMessageServiceClient = New IntegrationMessageServiceClient()
        ' Use the 'client' variable to call operations on the service.

        ' Always close the client.
        client.Close()
    End Sub
End Class
```

FTP	Medius Consultants to transport deployment files to the Integration server • Port 21 need to be opened for outbound traffic

For Cloud environment: In addition, these ports need to be open in the customer firewall for the Medius Integration Client:

Binding	Connectivity mode	Port
WSHttp2007RelayBinding	HTTPS, outbound	9085

3.3 Software Installed

Software	Comment	Download
.NET Framework 4	To be able to run integration enginee	http://www.microsoft.com/en-us/download/details.aspx?id=17851
Notepad++ or SharpDevelop	Consultant tool for XML configuration	http://notepad-plus-plus.org/download/ http://www.icsharpcode.net/OpenSource/SD/Download/
Winmerge	Consultant tool for diff configuration files during upgrades etc	http://winmerge.org/downloads/
Chrome	Preferred web browser for MediusFlow	https://www.google.com/chrome/browser/desktop/index.html
Powershell version 4.0 or later	Used during deployment of integration packages	http://social.technet.microsoft.com/wiki/contents/articles/21016.how-to-install-windows-powershell-4-0.aspx

3.4 Active Directory integration requirements

The Active Directory (AD) integration is used to keep the customer's local Active Directory users in sync with MediusFlow Cloud. The benefits are that the customer can import AD users and end users can log in with the AD user name and password.

The integration consists of two parts:

- User synchronization service
  - This service keeps the Mediusflow users in sync with the local Active Directory, this is provided by Medius
- ADFS (Active Directory Federation Services) installation provided and configured by the customer

To be able to use this feature there are some requirements that needs to be fulfilled on premise.

- On a Windows Server (This can be done on the integration server mentioned above.)
  - Being able to install a local Windows service to synchronize users with the MediusFlow cloud environment.

Depending on the security requirements on how to authenticate against the local ADFS server there are two options:

- Expose it on Internet
  - When exposing over Internet SSL/HTTPS should be used and a valid certificate is needed for the exposed host. This certificate is maintained and bought by the customer.
- Expose it internally

- When exposing it internally end users need a VPN to company network to be able to log in to MediusFlow even though it's a Cloud service, or you need to be located within your company network.

3.4.1 Server requirements for ADFS

Windows Server 2008 to 2012 uses ADFS 2.0. Read the full requirement specification from Microsoft here: https://technet.microsoft.com/en-us/library/cc771145.aspx

Windows server 2012 R2 and later uses ADFS 3.0. Read the full requirement specification from Microsoft here: https://technet.microsoft.com/en-us/library/dn554247.aspx

Windows Server 2008 supports ADFS 2.0, however the SSO features are incompatible with modern browsers. (it works with Firefox up to 3.5, Internet Explorer, but it does not work with Chrome). It is possible to use it, but users will need to enter their credentials for each login session.

3.5 Iphone Authentication Configuration

The following authentication protocols are supported if MediusFlow XI Iphone application is to be used:

Mobile Identity Provider: Local, ADFS:

- Local IP – form authentication
- ADFS – configured on IWA (Integrated Mode) with NTLM authentication

*Please note that other authentication protocols (e.g.,Kerberos, forms) are **not supported**.*