Whitepaper

Whitepaper Mobile Action v2.2

EU GDPR COMPLIANT

2024-04-04

Contents

1 Introduction 3
1.1 Mobile Action Mobile Application 3
1.2 Mobile Action Web Admin application 4
1.3 Addovation Cloud 5
1.3.1 Client Service 5
1.3.2 Data Service 5
1.4 Addovation Uplink 6
1.5 Authentication Mechanisms 8
1.5.1 IFS/Oracle Authentication 8
1.5.2 Active Directory Federation Services (ADFS) Authentication 8
1.6 Logging and Diagnostics 9
1.6.1 Microsoft App Center 9
1.6.2 Monitoring the Cloud/Uplink with Windows Event Viewer 9
1.7 Technologies 9
1.8 Network Analysis and Scanning 9
1.9 Compatibility matrix 10
1.9.1 Mobile Action Mobile Application 10
1.9.2 Addovation Cloud/Uplink Applications 10
1.10 Limitations 10
2 GDPR compliance 10
3 Contact 10

1 Introduction

Mobile Action is a native client application for Android and iOS built using Addovation's Framework and Microsoft Xamarin. The client application depends on the Addovation Cloud application for communication and configuration. The client supports:

- Customer specific colors and branding options (theme)
- Working with any business object in IFS Applications
  - Including customizations
- Your phone or tablet's features such as camera/photos, barcode and QR code scanning, GPS, etc.
- Your own translations
- Multiple user interface languages
- And much more

To communicate with IFS Applications, the solution requires an instance of the Addovation Cloud and Addovation Uplink applications.

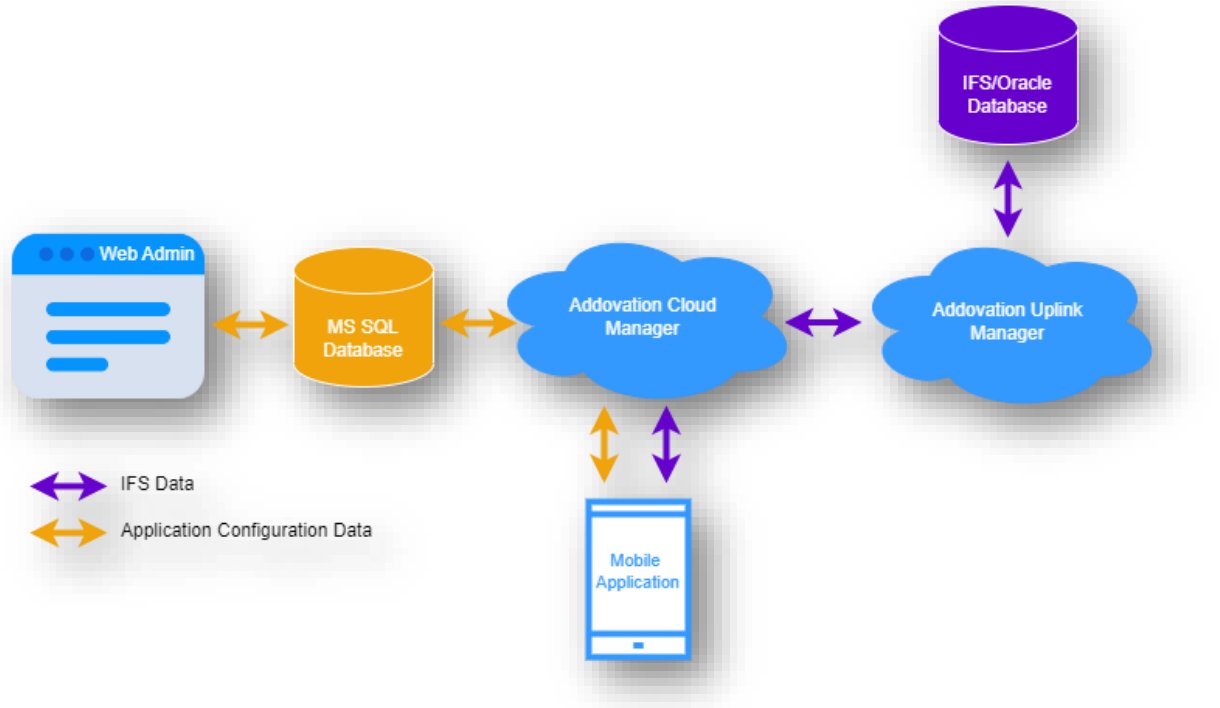

Figure 1: High Level Architecture

1.1 Mobile Action Mobile Application

Addovation Mobile Action offers functionality covering most aspects of IFS Applications.

Addovation Mobile Action uses standard components from our library to configure solutions for customer need. Our platform generates interfaces for different mobile clients such as iOS & Android. It enables secure and efficient transfer of any type and quantity of data. It will eliminate inefficiencies and deliver your workforce with the information they need, when and where they need it.

Mobility is not only a matter of mobile application. Selection of the mobile hardware, over-the-air connectivity technologies, device security should be considered in a mobile project. Depending on your area of business, and the level of security your company requires, Addovation will be able to tailor apps to suite your needs, regardless of the technology you want to use.

An SQLite database is used by the Mobile Action client to store the information related to the application configurations that are requested from the Addovation Cloud. The applications can be configured using the Mobile Action Web Admin web application.

1.2 Mobile Action Web Admin application

Mobile Action Web Admin is a web application that supports maintaining the Customers, Users, Themes, Document Management, Applications, Pages, Risk Libraries, and Presentation Objects.

Users can create many applications and each application can have several pages. Also, each page can have several rows but Maximum two columns for each row. After adding a row or column to the application, users can drag tools (columns, textboxes, labels, buttons or panels) to each row or column.

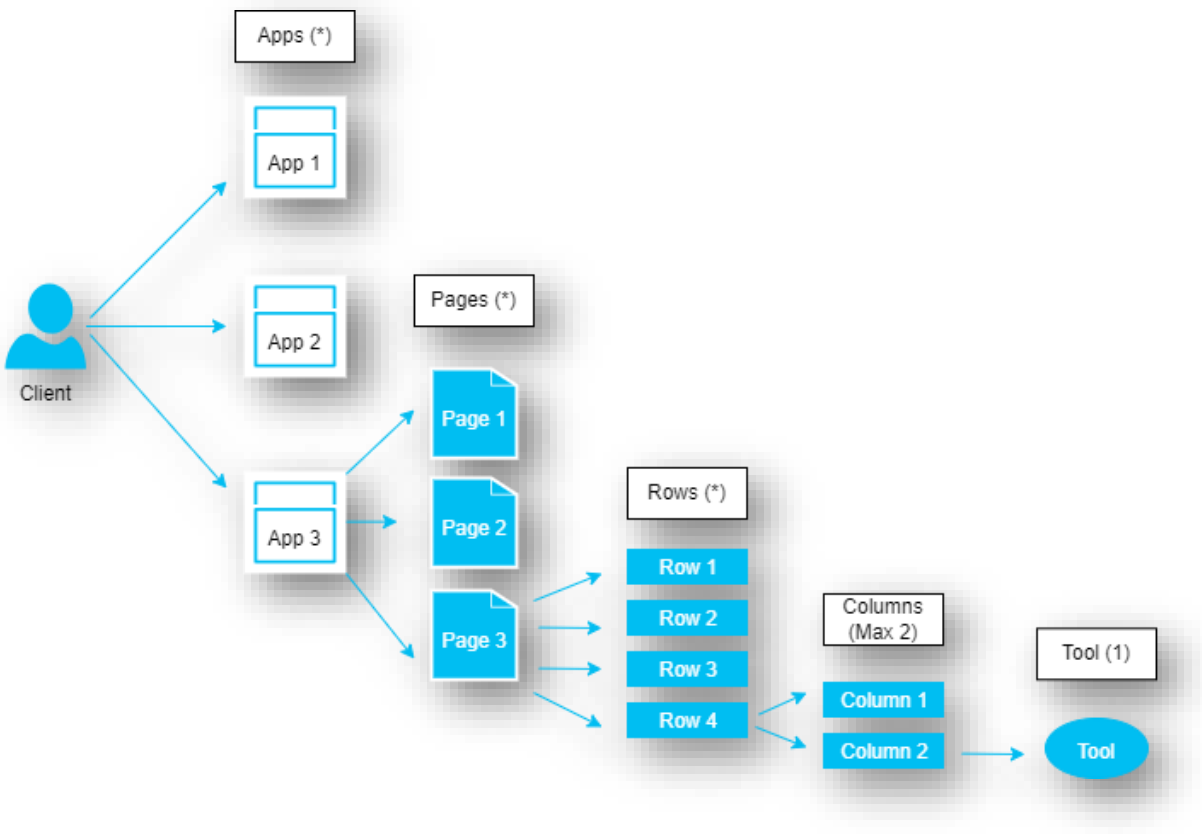

Figure 2: Application Configuration Flow

1.3 Addovation Cloud

Addovation provides a cloud service integration platform that is located either in a professional hosted environment, located within the borders of Norway or Sweden, Microsoft Azure or in your local in-house environment. All that is required is an Internet Information Server and an SQL Server database (2008+). All communication is done via REST-based interfaces; hence it is perfect for enabling collaboration between IFS and the outside world. No passwords are stored in Addovation Cloud, and all communication through the Cloud is encrypted.

Addovation Cloud can work as self-hosted service or as Windows service.

The cloud solution requires that TCP-connections is allowed on port 8080 on full duplex towards:

- cloud.addovation.com
  - IP: 217.65.228.51
- testcloud.addovation.com
  - IP: 217.65.228.50

1.3.1 Client Service

Client service is a WCF REST service, which receives all the mobile clients' requests. It uses HTTP binding with transport-level security (HTTPS communication provides confidentiality and integrity protection for the messages that are transmitted over the wire). It will be available on address https://server:48081/Addovation.Cloud/ClientService/ by default.

1.3.2 Data Service

Data service is a WCF service, which provides possibility to perform requests to IFS databases. It uses NET TCP binding (socket endpoints) and NET HTTPS binding (websocket endpoints) with both transport and message security configured and duplex communication (duplex contracts are supported) with Uplink service. It will be by default available on address "net.tcp://server:48080/Addovation.Cloud/DataService/" for NET TCP binding and on address "wss://server:48079/Addovation.Cloud/DataServiceWss/" for NET HTTPS binding.

1.4 Addovation Uplink

Addovation Uplink is a WCF service installed on the client side. The uplink service initiates connection to the Cloud service, so no ports on client side need to be opened. Uplink service has access to the configured database through IFS DataAccess Provider (provided by IFS) that ensures that all business logic is being preserved.

The communication is being illustrated in the following picture:

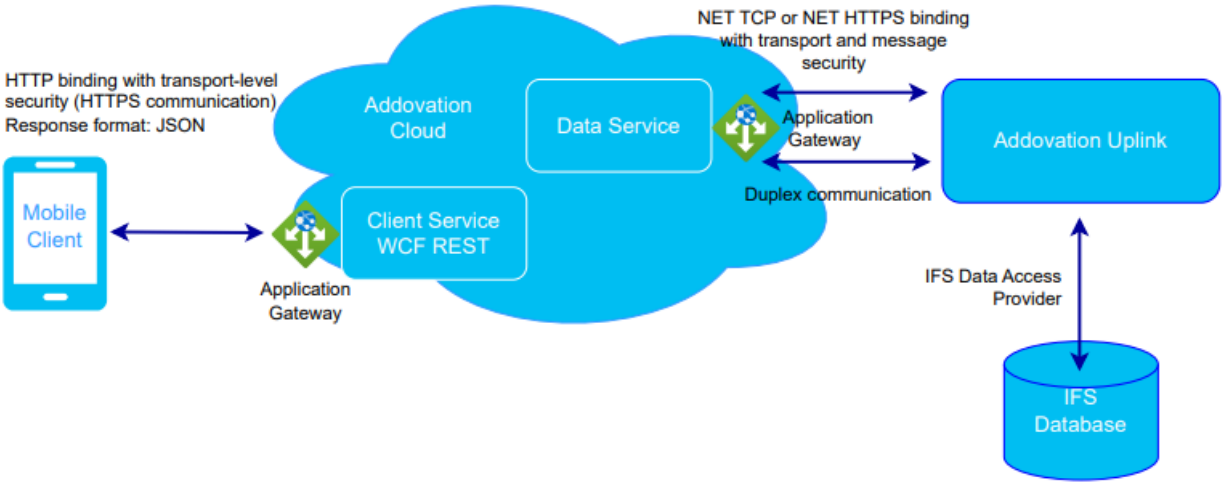

Figure 3: Communication among Mobile Client, Addovation Cloud, Addovation Uplink, and IFS Database

Every instance of the Uplink service must provide certificate generated for the specific Customer/SystemID. Duplex connection will be established only if correct certificate is provided.

Mobile clients are to request the public key of generated certificate from the Addovation Cloud. This key is used to encrypt all the messages to send to the Cloud service.

Note that in the case of using proxy, the Data service should use WebSocket connection type. The proxy server should have SSL termination switched off. This needs to be handled via the customer proxy configuration (these settings vary between different proxy software).
Important! The cloud uplink uses local Internet Explorer proxy configuration so it's possible that the following setting needs to be enabled and configured:

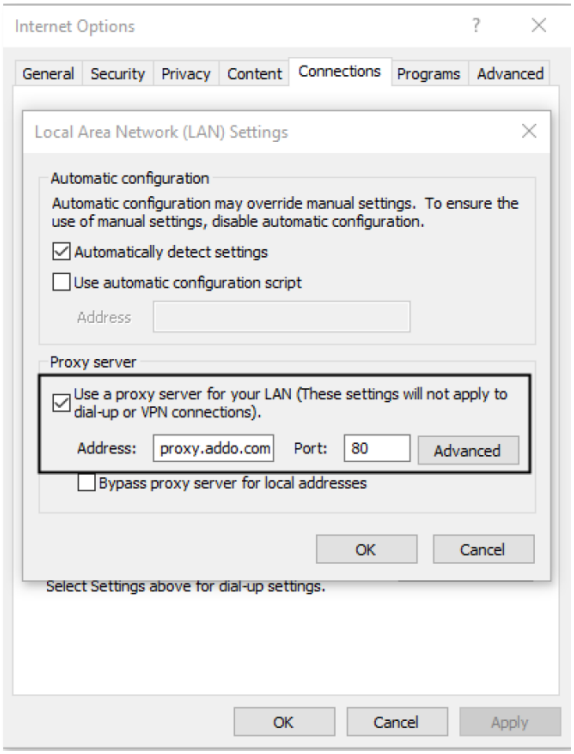

Figure 4: Proxy Configuration

The security communication can be illustrated by the following drawing:

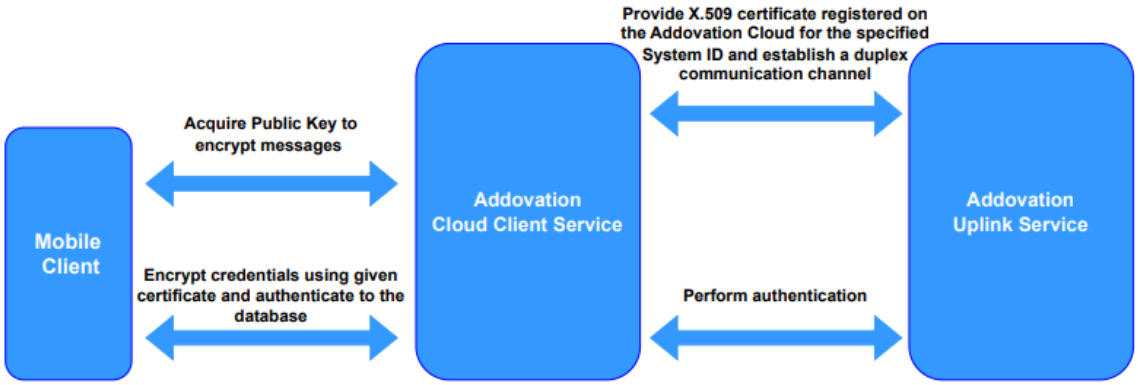

Figure 5: Secure Communication

1.5 Authentication Mechanisms

Mobile Action supports two authentication mechanisms:

- IFS/Oracle Authentication
- Active Directory Federation Services (AD FS)

1.5.1 IFS/Oracle Authentication

Users can log in to the Mobile Action mobile application by providing the relevant Cloud URL, System ID, Username, and the Password.

Then the mobile application requests an X509-formatted system certificate from the Addovation Cloud in order to generate an authentication token. The System ID, Username, and the Password are used to generate the token. The public key for encrypting the password is extracted from the system certificate and it is used to encrypt the user's password while generating the authentication token.

The authentication token is used to initiate a session with the Addovation Cloud. The user authentication is taken place at the Addovation Uplink via the Addovation Framework and the IFS Access Provider using the login credentials.

1.5.2 Active Directory Federation Services (ADFS) Authentication

Mobile Action supports Microsoft Active Directory Federation Services (ADFS) Authentication with some configurations in the Addovation Cloud and the Addovation Uplink applications.

The Addovation Cloud must be configured as follows in order to use ADFS authentication:

1. Open the File menu and select Manage Resources.
2. Expand the Customer and select the configured ADFS environment.
3. Select the version and right-click to open the context menu and select the Configure Resource.
4. Fill in the following information in ADFS Settings section:
    a. ADFS URL
    b. Client ID
    c. Resource URL
    d. Return URL
5. And make sure to check the Use ADFS checkbox.

The Addovation Uplink must be configured with the user credentials in the Integration User for ADFS Login section.

Mobile Action mobile client opens the ADFS login page when sign on to the app and obtains the User Principal Name (UPN) upon successful sign in. Then the UPN is passed to the Addovation Cloud and then to the Addovation Uplink to impersonate the integration user in order to perform the user authentication via the IFS Access Provider.

1.6 Logging and Diagnostics

1.6.1 Microsoft App Center

Mobile Action mobile client uses the Microsoft App Center Software Development Kit (SDK)s for monitoring the application health. It uses the Analytics and the Crashes SDKs for the application logging and diagnostic purposes.

App Center Analytics helps to understand the user behavior and customer engagement to further enhance the application. The SDK captures the session count, device properties like model, OS version, etc. And the App Center Crashes SDK generates the crash logs every time the app crashes. The crash logs are first written to the device's storage and when the user starts the app again, the crash log will be sent to the App Center.

1.6.2 Monitoring the Cloud/Uplink with Windows Event Viewer

Windows Event Viewer can be used to monitor the issues in the Addovation Cloud and the Addovation Uplink applications.

Addovation Cloud related logs can be found in Event Viewer → Windows Logs → Application. Logs can be filtered using "Addovation.Cloud" in the Source.

Logs related to the Addovation Uplink can be found in Event Viewer → Applications and Services Logs → <Name of the corresponding Uplink System ID>.

1.7 Technologies

Application	Technologies/Frameworks	Version(s)
Mobile Action Mobile Application	Xamarin.Forms	Xamarin.Forms 5.0.0.2083
Mobile Action Web Admin	ASP.NET MVC	.NET Framework 4.6.2
Addovation Cloud/Uplink	Windows Communication Foundation (WCF)	.NET Framework 4.6.2
Mobile Action Configuration Database	DACPAC (Data-tier application package)	DACPAC 2.11.0.0
IFS Access Provider	.NET based add-ins for IFS development.	IFS Access Provider 10.13.20.0

1.8 Network Analysis and Scanning

Wireshark (https://www.wireshark.org/) is one of the best network protocol analyzers. It supports checking everything that is going on within a network, troubleshoot different problems, analyze and filter your network traffic using various tools, etc.

Wireshark can be utilized to capture the network traffic among different components in Mobile Action application setup. The Addovation Uplink communicates with Addovation Cloud via ether Net TCP or Web Socket while the Mobile Application communicates with the Addovation Cloud via a Web Socket. Filters can be defined in Wireshark with the configured port numbers in Mobile Action.

1.9 Compatibility matrix

1.9.1 Mobile Action Mobile Application

Operating systems:

- Minimum Android version supported: Android 11 (API level 30)
- Target Android version supported: Android 13 (API level 33)
- Minimum iOS version support: iOS 9

IFS Applications:

- Tested with IFS Applications 10 Update 21

1.9.2 Addovation Cloud/Uplink Applications

Supports/Requires	Version/Bitness	Cloud/Uplink
WINDOWS SERVER 2019	32 and 64	✓
WINDOWS SERVER 2022	32 and 64	✓
WINDOWS 10	32 and 64	✓
WINDOWS 11	32 and 64	✓
IFS APPLICATIONS	10 Upd 21	✓

1.10 Limitations

- Mobile Action does not support automatic device font size adjustments
  - Font size is controlled in the configuration stored in the Addovation Cloud app's database
- Working offline is not supported, a working network connection is required
- Barcode scanning on colored backgrounds is not supported or recommended
  - High contrast gives better results
- Single sign-on (SSO) is not currently supported
- App linking
  - The root of the link (URL) must always start with https://applink.addovation.com/
  - In iOS, Email Sending is only allowed with the iOS default mail app
  - On android you need to add the applink base url in App Info.

2 GDPR compliance

Mobile Action is built with GDPR regulations in mind and communicates in the same way as IFS Applications Enterprise Explorer 10.
The Mobile Action client uses Microsoft App Center. The only information that is stored in the App Center logs is cloud server URL, environment name (system id), and username. This log information enables Addovation to track crashes and warnings for specific sessions and to analyze the relevant stack trace. The information is automatically erased after 90 days.

3 Contact

Visit www.addovation.com for further information.