# FintechOS Platform 21.1.1

# Administration Guide

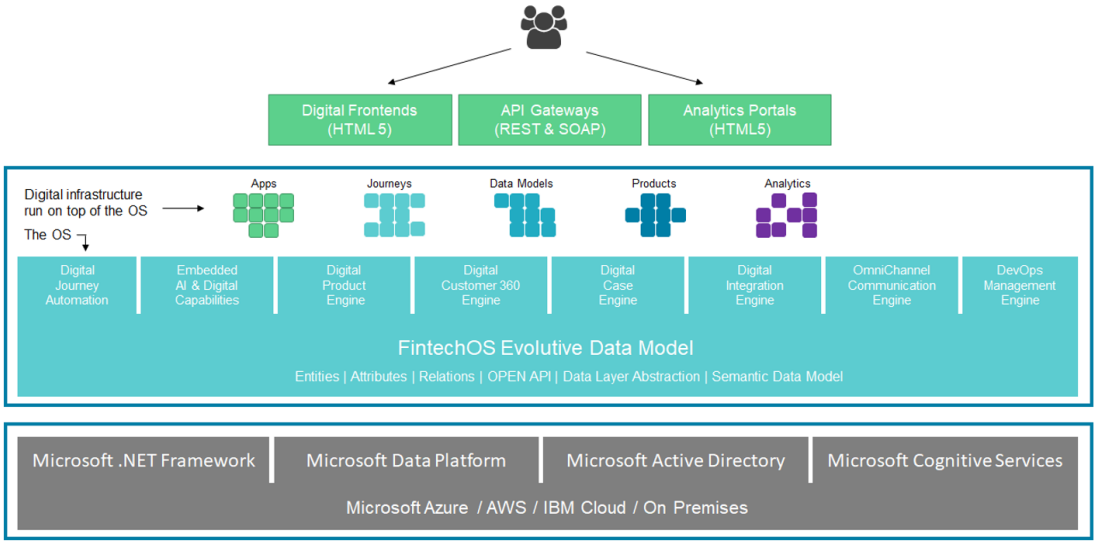
# TOC

# Overview

FintechOS is an innovation acceleration software platform that enables fast, plug & play, comprehensive digital transformation of companies that offer financial services.

FintechOS is a highly scalable technology that can be run both on premises and from the cloud.

While deployment on premises are still permitted with the current version of FintechOS we recommend using one of the enterprise cloud providers that FintechOS is compatible with. Below you can see a more detailed technological architecture on how FintechOS runs based on Microsoft, AWS or IBM.



# Installation

This section describes how to install the FintechOS Platform.

## System Requirements



### FintechOS Platform System Requirements

| Software minimum required version | 18.2.x | 20.1.x (Genie) | 20.2.x (Pulsar) |
|---|---|---|---|
| .NET Framework | 4.6.2 | 4.6.2 | 4.7.2 |
| SQL Server | SQL Server 2012 (11.x) | SQL Server 2012 (11.x) | SQL Server 2012 (11.x) |
| Windows Server | Windows Server 2012 R2 | Windows Server 2012 R2 | Windows Server 2012 R2 |

Below are details about which Windows Server roles and features are required. They were determined on a Windows Server 2012 R2. You must determine the equivalents for your particular Windows Server version.

#### Required Server Roles

Web Server (IIS)

## Required Features

- NET Framework 3.5 Features \ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- NET Framework 4.5 Features \ .NET Framework 4.5
- NET Framework 4.5 Features \ ASP.NET 4.5
- NET Framework 4.5 Features \ WCF Services \ HTTP Activation
- NET Framework 4.5 Features \ WCF Services \ TCP Port Sharing
- Windows PowerShell \ Windows PowerShell 4.0
- Windows Process Activation Service \ Process Model 17
- Windows Process Activation Service \ Configuration APIs

## Required Web Server Role (IIS) / Role Services

- Web Server \ Common HTTP Features \ Default Document
- Web Server \ Common HTTP Features \ Directory Browsing
- Web Server \ Common HTTP Features \ HTTP Errors
- Web Server \ Common HTTP Features \ Static Content
- Web Server \ Common HTTP Features \ HTTP Redirection
- Web Server \ Health and Diagnostics \ HTTP Logging
- Web Server \ Performance \ Static Content Compression
- Web Server \ Performance \ Dynamic Content Compression
- Web Server \ Security \ Request Filtering
- Web Server \ Security \ Basic Authentication
- Web Server \ Security \ URL Authorization
- Web Server \ Security \ Windows Authentication

- Web Server \ Application Development \ .NET Extensibility 4.5
- Web Server \ Application Development \ Application Initialization
- Web Server \ Application Development \ ASP.NET 4.5
- Web Server \ Application Development \ ISAPI Extensions
- Web Server \ Application Development \ ISAPI Filters
- Web Server \ Application Development \ Server Side Includes
- Web Server \ Application Development \ WebSocket Protocol
- Web Server \ Management Tools \ IIS Management Scripts and Tools

## FintechOS Portal System Requirements

FintechOS Portal can run on the following browsers, on both desktop and mobile devices:

| Browser | Operating System |
|---|---|
| Google Chrome | Windows 10 |
| Mozilla ESR | Windows 10 |
| Mozilla Firefox | Windows 10 |
| Microsoft Edge | Windows 10 |
| Internet Explorer 11 | Windows 7, 8.1, 10, Server 2016 |
| Opera | Windows 10 |
| Safari (desktop) | macOS - latest version |
| Safari (mobile) | IOS - latest version |
| Google Chrome (mobile) | Android - latest version |

**IMPORTANT!**
Please be aware that FTOS-Studio is fully compatible only with Google Chrome!

We recommend that you use the latest major version available for the browser.

# System Requirements for WebRTC Components

**NOTE**

**Components that are using WebRTC impose a series of limitations for our services to work correctly.**

**WebRTC (Web Real-Time Communication)** is a free, open-source project that provides web browsers and mobile applications with real-time communication (RTC) via simple application programming interfaces (APIs). It allows audio and video communication to work inside web pages by allowing direct peer-to-peer communication, eliminating the need to install plugins or download native apps. WebRTC is being standardized through the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF).

Its mission is to "enable rich, high-quality RTC applications to be developed for the browser, mobile platforms, and IoT devices, and allow them all to communicate via a common set of protocols".

Taking into account the versions supported by WebRTC and our 3rd party providers, please find below the list of supported browsers on different devices.

### Desktops / Laptops:

| Browser | Recommended Version | Supported Version |
|---|---|---|
| Google Chrome | Latest | 79 and greater |
| Mozilla Firefox | Latest | 71 and greater |
| Microsoft Edge | Versions 80 - 81 | 79 and greater |
| Safari | 13.1 and greater | 13.1 and greater |
| Opera | Latest | 66 and greater |
| Internet Explorer 11 | Not Supported | Not Supported |

**NOTE**

As WebRTC is in constant development, please ensure to always use the latest version.

We recommend to use Google Chrome for the best overall experience.

### Mobile Devices:

| Operating System | Browser | Supported Version |
|---|---|---|
| Android (version 6.0 and greater) | Google Chrome | Latest |
| Android (version 6.0 and greater) | Mozilla Firefox | Latest |
| Android (version 6.0 and greater) | Opera | Latest |
| iOS (version 12 and greater) | Safari | 2 most recent major versions |
| iOS | Google Chrome | Not Supported |
| iOS | Microsoft Edge | Not Supported |
| iOS | Mozilla Firefox | Not Supported |
| iOS | Opera | Not Supported |

**NOTE**
WebRTC does not support Chrome on iOS devices. On iOS you can only use the Safari engine.

# Installation Process

This guide describes how to perform the following operations:

- A first/clean install of FintechOS v18.1.9
- An upgrade from FintechOS v16.6.0 and higher to FintechOS v18.1.9

**IMPORTANT!**
In order to successfully upgrade from versions older than v16.6.0, you must first upgrade to v16.6.0 using legacy methods (not provided in this document) and then upgrade to FintechOS v18.1.9 by following the procedures explained in this guide.

**NOTE**
This chapter gives an overview of what needs to be done for both install and upgrade so make sure to read it at least down to and including How to use this guide before jumping any farther.

To follow along, we recommend you have at least the below IT professional skills:

- Windows Server administration - beginner level
- Network administration - the level required for your network
- IIS administration - beginner level
- SQL Server administration - beginner level
- Raw XML file editing - medium level

This document is available in 3 formats, all with exactly the same content. Use the format most suitable to your need, as follows:

- HTML (the .html file) if you want to read this guide on a screen. This guide looks best in this format.
- PDF (the .pdf file) if you want to print this guide.
- AsciiDoc (the .adoc file) only if you want to compare this guide with one of its previous AsciiDoc versions in order to see exactly what changed.

# Essential terms

**FintechOS (a.k.a. FTOS) release [kit]**

A **FTOS release** is a FTOS variant/build recognized by the FintechOS organization.

**HINT**
**Important FTOS release properties**

**Build id**
Unique id among all FTOS releases; e.g. CORE-RLS-Main-18.1.x b123

**Version number**
Unique id only among GOLD FTOS releases; e.g. v18.1.0

**Implicit validity**
Validity as estimated before going through QA; e.g. alpha, beta, RC

**Explicit validity**

Validity as determined after QA; e.g. GOLD (only releases supported for use in production are assigned GOLD validity)

A FTOS release kit is a set of files containing all items necessary to install or upgrade to the release associated with the kit.

#### FTOS installation [component]

A **FTOS installation** is a collection of installed **components**, including configurations, setup to work together with a sufficient level of independence from other [FTOS] installations.

> **IMPORTANT!**
> Within this guide, the term **component** is synonymous with **FTOS installation component**, unless otherwise specified.

### Example 1: FTOS Installation Component Examples

- One or more FTOS SQL Server databases
- One or more FTOS IIS web applications
- One or more FTOS Windows services
- One or more Windows/Active Directory accounts created to be used by other FTOS installation component(s) (e.g., a FTOS Windows service)
- One or more firewall/router configurations required by other FTOS installation component(s) (e.g., a route setup to let a FTOS IIS web application access a FTOS SQL Server database)

FTOS installation components are chosen with a level of granularity that ensures successful upgrade/uninstall without disturbing other [FTOS] installations which exist side-by-side (e.g., a database is a FTOS installation component, not the whole SQL Server instance; a web application or Windows service are FTOS installation components, not the whole IIS web site or machine; etc.)

FTOS installation components might be shared with other [FTOS] installations (e.g., you might account certain firewall/routing/SQL Server server-level/IIS server-level configurations as belonging to multiple [FTOS] installations).

**IMPORTANT!**
It is your responsibility to identify shared FTOS installation components and ensure they are only uninstalled when no longer used by any [FTOS] installation.

#### FTOS environment

A **FTOS environment** is a stable definition and context for a series of FTOS installations. A FTOS installation has a single associated FTOS environment (that is, a FTOS installation is installed in a FTOS environment).

The FTOS environment is defined and its context is created before any FTOS installation is installed in it, according to environment's definition. The environment continues to exist even at times when, temporarily, no associated installation exists.

**HINT**
**FTOS environment versus FTOS installation**

To better understand the difference between the two, let's assume that besides the PROD (Production) FTOS installation you have multiple side-by-side UAT (User Acceptance Testing) FTOS installations [2: It is common to have multiple FTOS installations for a large variety of reasons. Some organizations need more than one PROD installation. For a given PROD installation, most organizations need more than one UAT installation (e.g. to separate functional tests made by key business users from technical tests made by Operations (e.g. to test some security/networking change or a major version upgrade for SQL Server or Windows Server)). Some organizations need more types of installations than just UAT and PROD (DIT, SIT, etc.).]. Let's call UAT1 one of the UAT installations where you perform all final testing for a new FTOS release before you deploy it in PROD.

UAT1 will be reinstalled many times (e.g. to test successive FTOS releases) but every time in a very similar manner (i.e. on the same machines, in the same directories, with the same names for database, services and URLs) with the key point being this similarity is very desirable by everyone who uses UAT1 (keeps URLs stable, keeps db names and installation dirs stable, etc.). The FTOS environment is this stable definition and context while a FTOS installation is what is actually installed in the environment at a given time.

#### Servicing operation

Any major operation executed by following this guide, such as: first/clean install or upgrade.

#### Local path

A local path specified in Windows local path syntax, pointing to a file or directory. (such as: **C:\Program Files (x86), C:\Windows\winhlp32.exe**)

#### Windows Network share

A file or directory made accessible (a.k.a. shared) over the local Microsoft Windows Network.

#### UNC path

A network path specified in UNC syntax, pointing to a Windows Network share. (such as: **\\APPSRV02\SharedDocs, \\FILESRV2\Kit\install.exe**)

## How to use this guide

The guide is structured in chapters, each with sections and sub-sections. Each chapter is dedicated to one major FTOS installation component and details how to perform servicing operations on said component.

> **IMPORTANT!**
> It is outside this document's scope to explain FTOS' general deployment architecure. It is assumed you know the latter (i.e. you know the FTOS installation components and how they are related) and you have designed or have been handed the deployment diagram for the particular FTOS environment where you want to apply changes by following this guide.

Each chapter provides instructions as if its component is the only one that needs to be installed/upgraded in the FTOS environment. This was necessary to provide you with an easy to follow overall document structure but it means you need to slightly adjust instructions when applying a servicing operation to a FTOS environment as a whole. See the tips below for help on how to do that.

> **HINT**

- For a first/clean install go through this document in its natural order
- For an upgrade:
  - Stop/Deactivate all components (e.g., stop & switch to manual-start Windows services or Web applications) except the FTOS database.
  - Upgrade the FTOS database.
  - Upgrade each component in the order their chapters are listed in this document but in each chapter skip the instructions for starting/activating the component.
  - After you have upgraded all components, go through them again and apply the previously skipped start/activate instructions.

Even though considerable effort has been spent to provide you with a well designed document structure and instructions that are as ready to use as possible, this guide is not something to be followed 100% mechanically. Instead, you must use it as a basis for developing your Operations runbooks for FTOS and when doing so you must apply your professional skills (and common sense) to adjust the provided instructions [4: Your FTOS Operations runbooks should contain much more than just slightly adjusted instructions from this guide. Runbooks must contain step by step ready to use instructions for your FTOS environment(s) (with real machine names/IPs, directory/file paths, etc.) including instructions related to the IT infrastructure surrounding the FTOS environment (e.g. pre-upgrade backup, pre-upgrade suspend and post-upgrade resume monitoring of the FTOS environment, disaster recovery instructions in case a change runs into a major failure, pre-upgrade suspend and post-upgrade resume access to the FTOS environment via firewall rules, etc.] in order to obtain runbooks that can be followed 100% mechanically in your particular context (or you can automate runbooks through scripts or DevOps automation server jobs (e.g. Ansible Tower, RunDeck, Jenkins, etc.)).

# About doc-vars

Many instructions in this guide require you to customize them for your particular FTOS environment and then execute the customized result (e.g. customize a command line provided by FTOS by filling in an actual path to an installation directory of your choice or the name/IP of a machine of your choice).

To provide you with the most ready to use instructions, this guide uses document variables (a.k.a. doc-vars), which are a mechanism to express concise references to something that was previously associated with the referenced variables.

#### Doc-vars definition and scope

Doc-vars are always defined before they are used and their definition has a scope. With the exception of doc-vars defined in Global doc-vars definitions which apply to the whole guide, all other doc-vars are defined in special sub-sections named "Doc-var definitions" and by default apply only to the parent section and all its sub-sections.

#### Example 2: Doc-vars scope

To find the definition of a doc-var reference, you must go upwards through the parent sections looking in each "Doc-var definitions" sub-section, finishing with the special Global doc-vars definitions section.

> **NOTE**
> In most cases, the first occurrence of any doc-var in this guide - when searched as text, line by line - is that of its correct definition. This will not work for doc-vars [re]defined in multiple sections so pay attention if you run into such variables.

#### Doc-vars textual values, simple vs. complex nature and meaning vs. placeholder references

Doc-vars always have associated a meaning provided in their definition. In their definition you can find two additional optional associations:

- A **textual value** that you have to determine/choose and then replace in all the instructions where the doc-var is referenced as a placeholder for the specified value.
- A collection of sub-doc-vars

Doc-vars that have a sub-doc-vars collection are called **complex doc-vars**. Unless otherwise specified in their definition, they do not have a directly associated textual value.

Doc-vars that do not have a sub-doc-vars collection are called **simple doc-vars**. Unless otherwise specified in their definition, they have an associated textual value.

**Doc-var references** are mentions of their names written with a special style that makes it obvious in context that a doc-var is referenced, which doc-var is referenced and how the reference is to be interpreted.

Let's assume we have two doc-vars defined like this:

**ComponentX** - Complex doc-var. Represents component X installation.

**ComponentX_InstallDir** - Simple doc-var. Represents parent doc-var's installation directory.

The simplest type of doc-var reference is a **meaning reference**, which points to the meaning of the doc-var from its definition. If the doc-var has an associated textual value, it can be ignored for this kind of reference.

A meaning reference can appear anywhere and it is styled like: **ComponentX**.

#### Example 3: A more extended meaning reference example

> **IMPORTANT!**
> **ComponentX** is never to be installed on a Windows server that is an Active Directory controller. Also, you must ensure that **ComponentX_InstallDir** sits on a drive with at least 100 GB of free space.

The other kind of reference is a **placeholder reference**, which points to the textual value associated with the doc-var and demands you to replace the reference with the textual value. A placeholder reference naturally also points to the meaning of the doc-var, helping you to better understand the context where it appears.

A placeholder reference is usually embedded in text that you must otherwise use verbatim (such text has its own style in a **monospaced** font) and it is styled like: **ComponentX_InstallDir**

#### Example 4. A more extended placeholder reference example

Execute in cmd.exe:

```
MD "ComponentX_InstallDir"
xcopy.exe /I /S . "ComponentX_InstallDir"
CD /D "ComponentX_InstallDir"
```

Assuming the textual value of **ComponentX_InstallDir** is **C:\CompX**, the previous instructions must be interpreted as:

```
MD "C:\CompX"
xcopy.exe /I /S . "C:\CompX"
CD /D "C:\CompX"
```

#### Doc-var names

Names for doc-vars that are not sub-doc-vars (i.e. doc-vars that do not have a parent doc-var) are made out of only alphanumerical characters (e.g. **ComponentX**).

Names for doc-vars that are sub-doc-vars are composed from parent doc-var name, followed by an underscore, followed by their own name made out of only alphanumerical characters (e.g. **ComponentX_InstallDir**).

## Global doc-vars definitions

#### ReleaseKit

Complex doc-var. Represents the FTOS release kit associated with this guide. You must either be told where to find it or you already know if you are now reading the guide copy found in the FTOS release kit.

#### ReleaseKit_Dir

Simple doc-var. The local/UNC absolute path of ReleaseKit.

Example: **C:\kits\Fintech OS\releases\FTOS-CORE-RLS-v18.1.0.0-b123-GOLD**

#### ReleaseKit_Name

Simple doc-var. ReleaseKit_Dir directory name without path.

Example: **FTOS-CORE-RLS-v18.1.0.0-b123-GOLD**

#### ReleaseKit_VersionNo

Simple doc-var. **ReleaseKit** version number. Determine its value from **ReleaseKit_Name** by taking everything after FTOS-CORE-RLS-v until the 1st -.

Example: If ReleaseKit_Name is FTOS-CORE-RLS-v18.1.0.0-b123-GOLD then ReleaseKit_VersionNo is 18.1.0.0

#### TargetInstallation

Simple doc-var. Represents the FTOS installation you will service (install/upgrade) by following instructions from this guide.

#### TargetEnvironment

Simple doc-var. Represents the FTOS environment for **TargetInstallation**.

#### MainDb

Simple doc-var. Name you choose for the main FTOS database used by **TargetEnvironment**.

#### MainDb_OldVersionNo

Simple doc-var. **MainDb** version number as found before install/upgrade. Determine its value as follows:

If you're installing MainDb based on a new/blank database:

- Then: Leave **MainDb_OldVersionNo** undefined because its value is not needed
- Else: Determine **PortalWebApp_OldVersionNo**'s value

> **NOTE**
> If you restored **MainDb** from a backup taken from another FTOS environment, then you will need to determine **PortalWebApp_OldVersionNo** from the other environment.

- If **PortalWebApp_OldVersionNo** >= 17.1.5:
    - Then: Leave **MainDb_OldVersionNo** undefined because its value is not needed
    - Else: If **PortalWebApp_OldVersionNo** >= 17.1.0:
        - Then: Set **MainDb_OldVersionNo** to 17.1.0
        - Else: If **PortalWebApp_OldVersionNo** is 16.6.0, 16.7.0, or 17.0.0
            - Then: Set **MainDb_OldVersionNo** to **PortalWebApp_OldVersionNo**
            - Else: Stop! You can't use this guide to directly upgrade MainDb. See "Installation Process" on page 16.

#### MainDb_CompatibilityLevel

Simple doc-var. SQL Server compatibility level of **MainDb**. Determine its value as the result of the following T-SQL ran against **MainDb**:

```
SELECT compatibility_level FROM sys.databases WHERE name = 'MainDb'
```

#### MainDbServer

Simple doc-var. Full name of the SQL Server instance you choose for hosting **MainDb**, as returned by the following T-SQL when ran against it:

```
SELECT @@SERVERNAME
```

#### MainDbServer_MaxCompatibilityLevel

Simple doc-var. Maximum SQL Server compatibility level [5: For the latest information on the supported SQL Server compatibility levels, see https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-database-transact-sql-compatibility-level#arguments] supported by **MainDbServer**. Determine its value as follows:

- Determine **MainDbServer** Database Engine version as returned by the following T-SQL when ran against **MainDbServer**:

```
SELECT SERVERPROPERTY('ProductVersion')
```

- Use just the Major-part from the previously determined Database Engine version with the following table to determine **MainDbServer_ MaxCompatibilityLevel**:

| If MainDbServer Database Engine version Major-part is: | Then set MainDbServer_ MaxCompatibilityLevel to: | Note: Corresponding SQL Server version: |
|---|---|---|
| 14 | 140 | SQL Server 2017 (14.x) |
| 12 | 130 | Azure SQL Database logistical server |
| 12 | 130 | Azure SQL Database Managed Instance |
| 13 | 130 | SQL Server 2016 (13.x) |
| 12 | 120 | SQL Server 2014 (12.x) |
| 11 | 110 | SQL Server 2012 (11.x) |

#### PortalWebApp

Complex doc-var. Represents the FTOS Portal Web Application installation component.

#### PortalWebApp_Machine

Simple doc-var. The name of the Windows machine you choose to host **PortalWebApp** on.

#### PortalWebApp_InstallDir

Simple doc-var. The local absolute path on **PortalWebApp_Machine** of a not yet existent directory where you choose to install the **PortalWebApp** files in.

#### PortalWebApp_OldVersionNo

Simple doc-var. **PortalWebApp** version number as found before the install/upgrade. Determine its value as follows:

- If **PortalWebApp** is installed (i.e. you're performing an upgrade):
    - Then: On **PortalWebApp_Machine** open Windows Explorer, navigate to **PortalWebApp_InstallDir\bin**, right click on **EBS.Core.Common.dll**, click on Properties menu entry and go to Details tab. Set **PortalWebApp_**

**OldVersionNo** to the value of the File Version field.

- Else: Set **PortalWebApp_OldVersionNo** to 0.0.0.0

#### DesignerWebApp_IisAppName

Simple doc-var. Name you choose for **DesignerWebApp**'s IIS application.

#### DesignerWebApp_IisAppPoolName

Simple doc-var. Name of the IIS application pool you choose to run **DesignerWebApp_IisAppName** in. It can be a not yet existent pool as there are instructions on how to create it.

#### DesignerWebApp_IisWebSiteName

Simple doc-var. Name of the IIS web site you choose to host **DesignerWebApp_IisAppName** in.

#### DesignerWebApp_UploadEbsDir

Simple doc-var. A local/UNC absolute path usable by **DesignerWebApp_IisAppName** to access content from **PortalWebApp_UploadEbsDir**.

- If **DesignerWebApp_Machine** is the same as **PortalWebApp_Machine**:
  - Then: Set **DesignerWebApp_UploadEbsDir** to **PortalWebApp_UploadEbsDir**
  - Else: Set **DesignerWebApp_UploadEbsDir** to an UNC absolute path that maps to the same directory as **PortalWebApp_UploadEbsDir**

#### DesignerWebApp_LoginUrl

Simple doc-var. Login URL for **DesignerWebApp_IisAppName**. Determine its value based on the following format **http://DesignerWebApp_Machine/DesignerWebApp_IisAppName/Account/LogOn** which assumes the **DesignerWebApp_IisWebSiteName** works on port 80 without SSL. If the assumption is wrong, adjust the format accordingly.

#### DesignerWebApp_DbCred

Complex doc-var. The SQL Server credential you choose for **DesignerWebApp_IisAppName** to use when connecting to **MainDb** for normal operation.

#### DesignerWebApp_DbCred_Type

Simple doc-var. Determine its value as follows:

- If **DesignerWebApp_DbCred** is a SQL Server built in authentication credential:
    - Then: Value is **SqlBuiltinAuth**
    - Else (i.e. it is a Windows integrated authentication credential): Value is **WindowsAuth**

#### DesignerWebApp_DbCred_User

Simple doc-var. If **DesignerWebApp_DbCred_Type = SqlBuiltinAuth** then set **DesignerWebApp_DbCred_User** to **DesignerWebApp_DbCred**'s user name. Otherwise leave **DesignerWebApp_DbCred_User** undefined.

#### DesignerWebApp_DbCred_Password

Simple doc-var. If **DesignerWebApp_DbCred_User** is defined then set **DesignerWebApp_DbCred_Password** to **DesignerWebApp_DbCred** password. Otherwise leave **DesignerWebApp_DbCred_Password** undefined.

#### JobServer

Complex doc-var. Represents a FTOS JobServer installation component. As this component can be installed in multiple instances and configurations, **JobServer** as defined here does not represent any of them in particular. The doc-var will be reassigned a more practical meaning in later instructions. This component has been introduced starting with FTOS v18.1.0.

#### DebuggingServer

Complex doc-var. Represents the FTOS **DebuggingServer** installation component.

#### DebuggingServer_Machine

Simple doc-var. The name of the Windows machine you choose to host **DebuggingServer**.

#### DebuggingServer_InstallDir

Simple doc-var. The local absolute path on **DebuggingServer_Machine** of a not yet existent directory where you choose to install the **DebuggingServer** files.

#### DebuggingUi

Complex doc-var. Represents the **FTOS DebuggingUi** installation component.

#### DebuggingUi_Machine

Simple doc-var. The name of the Windows machine you choose to install **DebuggingUi**.

#### DebuggingUi_InstallDir

Simple doc-var. The local absolute path on **DebuggingUi_Machine** of a not yet existent directory where you choose to install the **DebuggingUi** files.

## General considerations

1. On any Windows Server machine you must operate with a Windows / Active Directory account that is in the local Administrators group, working in elevated mode (i.e. running as Administrator).

> **NOTE**
> **Consequence**
>
> Make sure you run all executables "as Administrator", including cmd.exe both when you type commands interactively or when you execute .bat files, which you should always execute by typing their names in an elevated cmd.exe window and not via mouse clicks.

2. The Windows / Active Directory account that you use must have full access rights on **ReleaseKit_Dir** (some instructions produce logs which by default are written in the **ReleaseKit_Dir**).

> **NOTE**
> A solution that covers this requirement and generally speeds up file operations is to copy **ReleaseKit_Dir** on each machine where you need to use it. This is OK as long as you compensate for the varying value of **ReleaseKit_Dir** from one machine to the next.

3. On any SQL Server instance you must operate with a SQL Server account that is in the sysadmin SQL Server role.
4. About instructions where you have to execute BasicDbUpgrader.exe

- You can execute this tool from any machine with connectivity to MainDb as long as the machine has .NET Framework >= 4.5 and SQLCMD.EXE installed. SQLCMD is auto-installed with SQL Server Management Studio but it can also be installed by itself.
- BasicDbUpgrader.exe instructions will work exactly as provided if MainDbServer uses dynamic ports and you can connect via Windows integrated authentication. If you need to connect to a specific port or with SQL Server built in authentication then you will need to slightly adjust the given instructions. Run BasicDbUpgrader.exe without any arguments to see help on how to do that (see -s, -u and -p parameters).
- The account you use with BasicDbUpgrader.exe to apply servicing operations (e.g. to apply upgrade/migration scripts) on MainDb, must be in the sysadmin SQL Server role.

5. You must edit text files (including compare and merge editing; including XML and cmd.exe batch file editing) with an editor [6: Unless you have better options, for general text file editing we recommend the freely available https://notepad-plus-plus.org while for compare-and-merge text file editing we recommend the freely available http://winmerge.org] that supports UTF8 with and without BOM and does not change file encoding on save.

**IMPORTANT!**
Do **not** use Windows' built-in notepad.exe.

6. If you have trouble when editing XML that requires XML encoding, use a specialized XML editor [7: Unless you have better options, we recommend the freely available https://github.com/Microsoft/XmlNotepad/releases].
7. You must notice if any instructions are terminated by an error signaled through common patterns (e.g. error popup window / message box, obvious terminating error message printed in a console window) and, unless specifically instructed otherwise in context or by FTOS Support or it is clear for you how to fix the problem (e.g. out of space), stop following the normal instructions and instead

abandon the servicing operation and revert TargetEnvironment to a previous good state.

**HINT**

Defining a mechanism and strategy for how to revert TargetEnvironment to a previous good state is specific to your context and part of your Operations business (e.g. some choose virtual machine snapshots, some choose uninstall and reinstall of the previous FTOS release, etc.). You should develop these steps and include them in your Operations runbooks [3: Your FTOS Operations runbooks should contain much more than just slightly adjusted instructions from this guide. Runbooks must contain step by step ready to use instructions for your FTOS environment(s) (with real machine names/IPs, directory/file paths, etc.) including instructions related to the IT infrastructure surrounding the FTOS environment (e.g. pre-upgrade backup, pre-upgrade suspend and post-upgrade resume monitoring of the FTOS environment, disaster recovery instructions in case a change runs into a major failure, pre-upgrade suspend and post-upgrade resume access to the FTOS environment via firewall rules, etc.].

8. Once you successfully went through a servicing operation where you defined/changed doc-vars you must save these values with your Operations documentation. You must retrieve the saved doc-var values before executing a servicing operation that requires them (e.g. upgrade).

**NOTE**
We recommend you to maintain the values up to date in a table-like structure where doc-vars are lines and FTOS environments are columns.

9. Where this guide mentions something as applicable for a certain chapter, section or sub-section, you must consider it applicable for all its deeper sub-sections, unless otherwise specified.

# MainDb

## Prerequisites

**MainDbServer** must be SQL Server 2012 or newer:

- With the following installed features:
    - **Database Engine Services**
    - **Client Tools Connectivity**
- With **SQL_Latin1_General_CP1_CI_AS** as server level collation, as returned by the following TSQL:

```
SELECT SERVERPROPERTY('collation');
```

## First/clean install

You should execute instructions from this section on the machine hosting **MainDbServer**. You can execute them from any machine that can execute T-SQL against **MainDbServer** but, if you need to, it will be more difficult to restore **MainDb** from a backup file.

Choose to install **MainDb** in one of the following two ways:

- Based on a main FTOS database from another FTOS environment (or an older version of **MainDb**)
    - This choice is common when **TargetEnvironment** is a clone of another environment (e.g. **TargetEnvironment** is an UAT environment and it is cloned from a PROD environment)
- Based on a new/blank database
    - This choice is common when **TargetEnvironment** is built from scratch using just resources from **ReleaseKit**

#### Based on a main FTOS database from another FTOS environment

1. Create a SQL Server backup file for the main FTOS database from the other environment.

> **NOTE**
> Unless the other environment has customizations/requirements that impact the backup process (e.g. complex database backup setup, replication configurations, custom backup software, etc.), you can closely follow these instructions: Create a Full Database Backup using SQL Server Management Studio

2. Copy/move the backup file to a location that can be accessed by MainDbServer
3. Create MainDb on MainDbServer by restoring from the backup file

> **NOTE**
> Unless **MainDbServer** has customizations/requirements that impact the restore process, you can closely follow these instructions: Restore a Database to a New Location using SQL Server Management Studio

4. If `MainDb_CompatibilityLevel < MainDbServer_MaxCompatibilityLevel`, Then: Execute the following T-SQL against MainDb:

```
ALTER DATABASE MainDb SET COMPATIBILITY_LEVEL =
MainDbServer_MaxCompatibilityLevel
```

5. Grant full access on **MainDb** for **DesignerWebApp_DbCred** and **PortalWebApp_DbCred**

#### Based on a new/blank database

1. Create **MainDb** as a new **SQL Server** database on **MainDbServer**

> **NOTE**
> Unless **MainDbServer** has customizations/requirements that impact the creation of new databases (e.g. database physical files must be located on a certain device, backup / other maintenance procedures / mechanisms must be updated, etc.), you can closely follow these instructions: Create a Database using SQL Server Management Studio

2. If `MainDb_CompatibilityLevel < MainDbServer_MaxCompatibilityLevel`, Then: Execute the following T-SQL against MainDb:

```
ALTER DATABASE MainDb SET COMPATIBILITY_LEVEL =
MainDbServer_MaxCompatibilityLevel
```

> **NOTE**
> This would only happen in the very rare case when compatibility level of **model** database was lowered for some reason.

3. Execute in cmd.exe: `"ReleaseKit\SQL\BasicDbUpgrader.exe" -s "MainDbServer" -d "MainDb" -i`

> **NOTE**
> Ignore warnings about not having specified -v or -l. In this case they are not required.

4. Follow all steps from **MainDb \ Upgrade**
5. Grant full access on **MainDb** for **DesignerWebApp_DbCred** and **PortalWebApp_DbCred**

## Upgrade

You must execute instructions from this section on a machine that can connect and execute T-SQL against **MainDbServer**.

1. Execute in cmd.exe: `"ReleaseKit\SQL\BasicDbUpgrader.exe" -s "MainDbServer" -d "MainDb"`

> **NOTE**
> You should be presented with a report on which scripts will be applied on **MainDb**.

- If the command was terminated by an error like Db is not initialized for use with BasicDbUpgrader and MainDb_OldVersionNo is between 16.6.0 and 17.1.5, Then execute in cmd.exe: `"ReleaseKit\SQL\BasicDbUpgrader.exe" -s "MainDbServer" -d "MainDb" -i -v "MainDb_OldVersionNo"`

2. Execute in cmd.exe: `"ReleaseKit\SQL\BasicDbUpgrader.exe" -s "MainDbServer" -d "MainDb" -g`

- This command will upgrade **MainDb** and it will take a few minutes to complete, depending mostly on how old **MainDb_OldVersionNo** is vs. **ReleaseKit_VersionNo**

## PortalWebApp

#### Prerequisites

On **PortalWebApp_Machine**:

- Windows Server 2008 R2 SP1 or newer

> **IMPORTANT!**
> Below are details about which Windows Server roles and features are required. They were determined on a Windows Server 2012 R2. You must determine the equivalents for your particular Windows Server version (e.g. 2008 R2, 2016)

- Required Server Roles: **Web Server (IIS)**
- Required Features:
  - .NET Framework 3.5 Features \ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - .NET Framework 4.5 Features \ .NET Framework 4.5
  - .NET Framework 4.5 Features \ ASP.NET 4.5
  - .NET Framework 4.5 Features \ WCF Services \ HTTP Activation
  - .NET Framework 4.5 Features \ WCF Services \ TCP Port Sharing
  - Windows PowerShell \ Windows PowerShell 4.0
  - Windows Process Activation Service \ Process Model
  - Windows Process Activation Service \ Configuration APIs
- Required **Web Server Role (IIS) \ Role Services**:
  - Web Server \ Common HTTP Features \ Default Document
  - Web Server \ Common HTTP Features \ Directory Browsing

    - Web Server \ Common HTTP Features \ HTTP Errors
    - Web Server \ Common HTTP Features \ Static Content
    - Web Server \ Common HTTP Features \ HTTP Redirection
    - Web Server \ Health and Diagnostics \ HTTP Logging
    - Web Server \ Performance \ Static Content Compression
    - Web Server \ Performance \ Dynamic Content Compression
    - Web Server \ Security \ Request Filtering
    - Web Server \ Security \ Basic Authentication
    - Web Server \ Security \ URL Authorization
    - Web Server \ Security \ Windows Authentication
    - Web Server \ Application Development \ .NET Extensibility 4.5
    - Web Server \ Application Development \ Application Initialization
    - Web Server \ Application Development \ ASP.NET 4.5
    - Web Server \ Application Development \ ISAPI Extensions
    - Web Server \ Application Development \ ISAPI Filters
    - Web Server \ Application Development \ Server Side Includes
    - Web Server \ Application Development \ WebSocket Protocol
    - Web Server \ Management Tools \ IIS Management Scripts and Tools
- .NET Framework 4.6.2 or newer
- Windows PowerShell 5.1 or newer

## First/clean install

You must execute instructions from this section on **PortalWebApp_Machine**.

**NOTE**
The next steps will fail if any of the following are true:
- **PortalWebApp_InstallDir** or **PortalWebApp_IisAppName** already exist
- **PortalWebApp_IisWebSiteName** does not already exist

1. Create a new batch file named **PortalWebAppInstaller.Install.bat** in a directory of your choice and add in a single command line as follows:

- If `PortalWebApp_DbCred_Type = SqlBuiltinAuth`
    - Then: Use this command line:

```
powershell.exe -File
"ReleaseKit\PortalWebApp\PortalWebAppInstaller.ps1" -p_MainCommand
Install -p_InstallDir PortalWebApp_InstallDir -p_IisWebSite
PortalWebApp_IisWebSiteName -p_IisApp PortalWebApp_IisAppName -p_
IisAppPool PortalWebApp_IisAppPoolName -p_DbConnServer MainDbServer
-p_DbConnSqlAuthUser PortalWebApp_DbCred_User -p_DbConnSqlAuthPass
PortalWebApp_DbCred_Password -p_DbConnDb MainDb -p_UploadEBSDir
PortalWebApp_UploadEbsDir
```

- Else: Use this command line:

```
powershell.exe -File
"ReleaseKit\PortalWebApp\PortalWebAppInstaller.ps1" -p_MainCommand
Install -p_InstallDir PortalWebApp_InstallDir -p_IisWebSite
PortalWebApp_IisWebSiteName -p_IisApp PortalWebApp_IisAppName -p_
IisAppPool PortalWebApp_IisAppPoolName -p_DbConnServer MainDbServer
-p_DbConnDb MainDb -p_UploadEBSDir PortalWebApp_UploadEbsDir
```

2. Execute in cmd.exe: `PortalWebAppInstaller.Install.bat`

**HINT**
This command does the following:

◦ Creates PortalWebApp_InstallDir and copies in PortalWebApp files from ReleaseKit
◦ Creates web.config.OriginalForReference in PortalWebApp_InstallDir, as a clone of web.config from ReleaseKit, to be used later in case there is a need to compare against the web.config as it came with ReleaseKit
◦ Configures web.config

◦ Creates PortalWebApp_IisAppPoolName if it does not already exist (if it exists it will not be changed and will just be used as is)
◦ Grants recursive full NTFS access rights on PortalWebApp_InstallDir for the Windows account used to run PortalWebApp_IisAppPoolName
◦ Creates PortalWebApp_IisAppName
◦ Creates PortalWebApp_UploadEbsDir if it's a local path and it doesn't already exist
◦ If PortalWebApp_UploadEbsDir is different from default (i.e. PortalWebApp_InstallDir\UploadEBS) then:
▪ If PortalWebApp_UploadEbsDir is a local path then:
▪ Grants recursive full NTFS access rights on PortalWebApp_UploadEbsDir for the Windows account used to run PortalWebApp_IisAppPoolName
▪ Creates an explicit /UploadEBS IIS vdir mapped on PortalWebApp_UploadEbsDir
◦ [Re]Starts PortalWebApp_IisAppPoolName

3. If **PortalWebApp_UploadEbsDir** is an UNC path, then:

- Modify Windows network share access rights on **PortalWebApp_UploadEbsDir** and grant full rights for the Windows account used by **PortalWebApp_IisAppPoolName** to access it.

**NOTE**
If **PortalWebApp_IisAppPoolName** uses the default IIS app pool identity configuration (i.e. **ApplicationPoolIdentity**, as is the case if **PortalWebAppInstaller.ps1** created **PortalWebApp_IisAppPoolName** for you) then you need to grant rights for **PortalWebApp_Machine**'s own Windows account (i.e. a Windows / Active Directory account that has the same name as **PortalWebApp_Machine** Windows machine name).

- Modify NTFS access rights on the directory behind **PortalWebApp_UploadEbsDir** Windows network share and grant full access for the Windows account used by **PortalWebApp_IisAppPoolName** to access it.

4. Open in a web browser **PortalWebApp_LoginUrl** and check the page appears as expected.

## Upgrade

You must execute instructions from this section on **PortalWebApp_Machine**.

1. Create a new batch file named **PortalWebAppInstaller.Upgrade.bat** in a directory of your choice and add in the following single command line:
`powershell.exe -File "ReleaseKit\PortalWebApp\PortalWebAppInstaller.ps1" -p_MainCommand Upgrade -p_InstallDir PortalWebApp_InstallDir`
2. Execute in cmd.exe: `PortalWebAppInstaller.Upgrade.bat`

> **HINT**
> This command does the following:
>
> ◦ Overwrites all files from **PortalWebApp_InstallDir** with **PortalWebApp** files from **ReleaseKit**, except for web.config which is not overwritten in case you customized it
> ◦ [Re]Starts **PortalWebApp_IisAppPoolName**

3. Open in a web browser **PortalWebApp_LoginUrl** and check the page appears as expected.

## DesignerWebApp

#### Prerequisites

On **DesignerWebApp_Machine**: Same as on **PortalWebApp_Machine** (See PortalWebApp \ Prerequisites)

#### First/clean install

You must execute instructions from this section on **DesignerWebApp_Machine**.

> **NOTE**
> The next steps will fail if any of the following are true:
> • **DesignerWebApp_InstallDir** or **DesignerWebApp_IisAppName** already exist
> • **DesignerWebApp_IisWebSiteName** does not already exist

1. Create a new batch file named **DesignerWebAppInstaller.Install.bat** in a directory of your choice and add in a single command line as follows:

- If `DesignerWebApp_DbCred_Type = SqlBuiltinAuth`, then use this command line:

```
powershell.exe -File
"ReleaseKit\DesignerWebApp\DesignerWebAppInstaller.ps1" -p_
MainCommand Install -p_InstallDir DesignerWebApp_InstallDir -p_
IisWebSite DesignerWebApp_IisWebSiteName -p_IisApp DesignerWebApp_
IisAppName -p_IisAppPool DesignerWebApp_IisAppPoolName -p_
DbConnServer MainDbServer -p_DbConnSqlAuthUser DesignerWebApp_
DbCred_User -p_DbConnSqlAuthPass DesignerWebApp_DbCred_Password -p_
DbConnDb MainDb -p_UploadEBSDir DesignerWebApp_UploadEbsDir
```

- Else, use this command line:

```
powershell.exe -File "
ReleaseKit\DesignerWebApp\DesignerWebAppInstaller.ps1" -p_
MainCommand Install -p_InstallDir DesignerWebApp_InstallDir -p_
IisWebSite DesignerWebApp_IisWebSiteName -p_IisApp DesignerWebApp_
IisAppName -p_IisAppPool DesignerWebApp_IisAppPoolName -p_
DbConnServer MainDbServer -p_DbConnDb MainDb -p_UploadEBSDir
DesignerWebApp_UploadEbsDir
```

2. Execute in cmd.exe: `DesignerWebAppInstaller.Install.bat`

**HINT**

This command does the following:

◦ Creates DesignerWebApp_InstallDir and copies in DesignerWebApp files from ReleaseKit
◦ Creates web.config.OriginalForReference in DesignerWebApp_InstallDir, as a clone of web.config from ReleaseKit, to be used later in case there is a need to compare against the web.config as it came with ReleaseKit
◦ Configures web.config
◦ Creates DesignerWebApp_IisAppPoolName if it does not already exist (if it exists it will not be changed and will just be used as is)
◦ Grants recursive full NTFS access rights on DesignerWebApp_InstallDir for the Windows account used to run DesignerWebApp_IisAppPoolName
◦ Creates DesignerWebApp_IisAppName
◦ Creates DesignerWebApp_UploadEbsDir if it's a local path and it doesn't already exist
◦ Note: This is very unusual considering DesignerWebApp_UploadEbsDir definition
◦ If DesignerWebApp_UploadEbsDir is different from default (i.e. DesignerWebApp_InstallDir\UploadEBS) then:
▪ Note: This is the expected case considering DesignerWebApp_UploadEbsDir

definition
▪ If DesignerWebApp_UploadEbsDir is a local path then:
▪ Grants recursive full NTFS access rights on DesignerWebApp_UploadEbsDir for the Windows account used to run DesignerWebApp_IisAppPoolName
▪ Creates an explicit /UploadEBS IIS vdir mapped on DesignerWebApp_UploadEbsDir
◦ [Re]Starts DesignerWebApp_IisAppPoolName

3. If **DesignerWebApp_UploadEbsDir** is an UNC path, then:

- Modify Windows network share access rights on **DesignerWebApp_UploadEbsDir** and grant full rights for the Windows account used by **DesignerWebApp_IisAppPoolName** to access it.

> **NOTE**
> If **DesignerWebApp_IisAppPoolName** uses the default IIS app pool identity configuration (i.e. **ApplicationPoolIdentity**, as is the case if **DesignerWebAppInstaller.ps1** created **DesignerWebApp_IisAppPoolName** for you) then you need to grant rights for **DesignerWebApp_Machine**'s own Windows account (i.e. a Windows / Active Directory account that has the same name as **DesignerWebApp_Machine** Windows machine name).

- Modify NTFS access rights on the directory behind **DesignerWebApp_UploadEbsDir** Windows network share and grant full rights for the Windows account used by **DesignerWebApp_IisAppPoolName** to access it.

4. Open in a web browser **DesignerWebApp_LoginUrl** and check the page appears as expected.

#### Upgrade

You must execute instructions from this section on **DesignerWebApp_Machine**.

1. Create a new batch file named **DesignerWebAppInstaller.Upgrade.bat** in a directory of your choice and add in the following single command line:
`powershell.exe -File "ReleaseKit\DesignerWebApp\DesignerWebAppInstaller.ps1" -p_MainCommand Upgrade -p_InstallDir DesignerWebApp_InstallDir`
2. Execute in cmd.exe: `DesignerWebAppInstaller.Upgrade.bat`

**HINT**
This command does the following:

◦ Overwrites all files from **DesignerWebApp_InstallDir** with **DesignerWebApp** files from **ReleaseKit**, except for web.config which is not overwritten in case you customized it
◦ [Re]Starts **DesignerWebApp_IisAppPoolName**

3. Open in a web browser **DesignerWebApp_LoginUrl** and check the page appears as expected.

## JobServer

Any FTOS JobServer instances come with a set of standard jobs configured and enabled by default. You can disable standard jobs and install additional jobs via plugins (e.g. MessageBus (OCS) plugin, MessageComposer plugin).

If **JobServer_JobConfig** is:

- **StandardJobCfg** then:
  - Go to section JobServer \ Standard job configuration
- **MessageBusJobCfg** then:
  - Go to section JobServer \ MessageBus (OCS) job configuration
- **MessageComposerJobCfg** then:
  - Go to section JobServer \ MessageComposer job configuration
- **MessageBusMessageComposerJobCfg** then:
  - Go to section JobServer \ MessageBus (OCS) + MessageComposer job configuration

## Doc-var definitions

#### JobServer

Complex doc-var. Represents the FTOS JobServer installation component instance that you're currently servicing.

#### JobServer_Id

Simple doc-var. Alphanumerical id you choose for **JobServer**. It must be unique across all **JobServer** instances in **TargetEnvironment**.

Examples: `1, Standard1, MessageBusMessageComposer2`

#### JobServer_Machine

Simple doc-var. Name of the Windows machine you choose to install **JobServer** on.

#### JobServer_InstallDir

Simple doc-var. The local absolute path on **JobServer_Machine** of a not yet existent directory where you choose to install the **JobServer** files.

#### JobServer_WinSvcName

Simple doc-var. Name of the Windows service that runs **JobServer**. Set **JobServer_WinSvcName** to **FtosJobServer-JobServer_Id**.

#### JobServer_JobConfig

Simple doc-var. Determine its value depending on the job configuration you choose for **JobServer**:

| If you choose this job configuration: | Then set `JobServer_JobConfig` to: |
|---|---|
| Standard (i.e. standard jobs enabled and no plugin jobs installed) | StandardJobCfg |
| MessageBus (OCS) (i.e. standard jobs disabled and MessageBus (OCS) plugin jobs installed and enabled) | MessageBusJobCfg |
| MessageComposer (i.e. standard jobs disabled and MessageComposer plugin jobs installed and enabled) | MessageComposerJobCfg |
| MessageBus (OCS) + MessageComposer (i.e. standard jobs disabled, MessageBus (OCS) + MessageComposer jobs installed and enabled) | MessageBusMessageComposerJobCfg |

#### JobServer_UploadEbsDir

Simple doc-var. A local/UNC absolute path usable by **JobServer_WinSvcName** to access content from **PortalWebApp_UploadEbsDir**.

If **JobServer_JobConfig** is **MessageBusJobCfg** or **MessageBusMessageComposerJobCfg**, then:

- If **JobServer_Machine** is the same as **PortalWebApp_Machine**
  - Then: Set **JobServer_UploadEbsDir** to **PortalWebApp_UploadEbsDir**
  - Else: Set **JobServer_UploadEbsDir** to an UNC absolute path that maps to the same directory as PortalWebApp_UploadEbsDir
- Else: Leave **JobServer_UploadEbsDir** undefined because its value is not needed

#### JobServer_DbCred

Complex doc-var. The SQL Server credential you choose for **JobServer** to use when connecting to **MainDb** for normal operation.

## Prerequisites

On **JobServer_Machine**:

- .NET Framework 4.6.1 or newer
- Windows PowerShell 5.1 or newer

## Standard job configuration

#### First/clean install

You must execute instructions from this section on **JobServer_Machine**.

1. Create directory **JobServer_InstallDir**
2. Copy all files from **ReleaseKit_Dir\JobServer** to **JobServer_InstallDir**
3. Edit XML file **JobServer_InstallDir\connections.config** as follows:

- In XML node `/connectionStrings/add[@name='EbsSqlServer']` set XML attribute **connectionString** to a SQL Server connection string [8: For SQL Server connection string syntax see https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connectionstring-syntax] pointing to **MainDb**, using **JobServer_DbCred**.
- Snippet from connection.config showing where you must edit:

```
<add name="EbsSqlServer" connectionString="Data Source=...;Initial
Catalog=...;
User ID=...;Password=...; Persist Security Info= true;"
providerName="System.Data.SqlClient" />
```

4. Execute in cmd.exe: `JobServer_InstallDir\FTOS.JobServer.Service.Install.bat JobServer_WinSvcName`

#### Upgrade

You must execute instructions from this section on **JobServer_Machine**.

1. Execute in cmd.exe: `sc.exe stop JobServer_WinSvcName`
2. Copy with overwrite all files from **ReleaseKit_Dir\JobServer** to **JobServer_InstallDir** except for the following files:
   - connections.config
   - FTOS.JobServer.Service.exe.config
   - schedule.config
   - services.config
   - serviceSettings.config
3. For each of the files excepted at the previous step, analyze the differences between version from **ReleaseKit_Dir** and that from **JobServer_InstallDir** using a text file compare tool and merge changes into the version from **JobServer_InstallDir** without breaking existing customizations
4. Execute in cmd.exe: `sc.exe start JobServer_WinSvcName`

## MessageBus (OCS) job configuration

#### First/clean install

You must execute instructions from this section on **JobServer_Machine**.

1. Follow all steps from JobServer \ Standard job configuration \ First/clean install
2. Execute in cmd.exe: `sc.exe stop JobServer_WinSvcName`
3. Copy with overwrite all files from **ReleaseKit_Dir\JobServer.Plugins\MessageBus (OCS)** to **JobServer_InstallDir**
4. Edit XML file **JobServer_InstallDir\connections.config** as follows:

- In XML node `/connectionStrings/add[@name='FtosConnection']` set XML attribute **connectionString** to a SQL Server connection string [8: For SQL Server connection string syntax see https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connectionstring-syntax] pointing to **MainDb**, using **JobServer_DbCre**
- Snippet from **connections.config** showing where you must edit:

```
<add name="FtosConnection" connectionString="Data
Source=...;Initial
Catalog=...; User
ID=...;Password=...;MultipleActiveResultSets=True;"
providerName="System.Data.SqlClient" />
```

5. Edit XML file **JobServer_InstallDir\serviceSettings.config** as follows:

- In XML node `/appSettings/add[@name='AttachmentPath']` set XML attribute value to **JobServer_UploadEbsDir**
- Snippet from **serviceSettings.config** showing where you must edit:

```
<add key="AttachmentPath" value="...\EBS.Core.Web.MVC\UploadEBS"/>
```

6. If **JobServer_UploadEbsDir** is a local absolute path:

- Then: Modify NTFS access rights on **JobServer_UploadEbsDir** and grant full rights for the Windows account used to run **JobServer_WinSvcName**. ↖By default this account is **LocalSystem**.
- Else (i.e. it is an UNC path):

- Modify Windows network share access rights on **JobServer_UploadEbsDir** and grant full rights for the Windows account used by **JobServer_WinSvcName** to access it. By default this account is **JobServer_Machine**'s own Windows account (i.e. a Windows / Active Directory account that has the same name as **JobServer_Machine** Windows machine name).
- Modify NTFS access rights on the directory behind **JobServer_UploadEbsDir** Windows network share and grant full rights for the Windows account used by **JobServer_WinSvcName** to access it.

7. Execute in cmd.exe: `sc.exe start JobServer_WinSvcName`

#### Upgrade

You must execute instructions from this section on **JobServer_Machine**.

1. Follow all steps from JobServer \ Standard job configuration \ Upgrade
2. Execute in cmd.exe: `sc.exe stop JobServer_WinSvcName`

- Copy with overwrite all files from **ReleaseKit_Dir\JobServer.Plugins\MessageBus (OCS)** to **JobServer_InstallDir** except for the following files:
  - connections.config
  - schedule.config
  - services.config
  - serviceSettings.config

3. For each of the files excepted at the previous step, analyze the differences between version from **ReleaseKit_Dir** and that from **JobServer_InstallDir** using a text file compare tool and merge changes into the version from **JobServer_InstallDir** without breaking existing customizations.
4. Execute in cmd.exe: `sc.exe start JobServer_WinSvcName`

## MessageComposer job configuration

#### First/clean install

You must execute instructions from this section on **JobServer_Machine**.

1. Follow all steps from JobServer \ Standard job configuration \ First/clean install
2. Execute in cmd.exe: `sc.exe stop JobServer_WinSvcName`
3. Copy with overwrite all files from **ReleaseKit_Dir\JobServer.Plugins\MessageComposer** to **JobServer_InstallDir**
4. Edit XML file **JobServer_InstallDir\connections.config** as follows:

- In XML `node /connectionStrings/add[@name='FtosConnection']` set XML attribute **connectionString** to a SQL Server connection string [8: For SQL Server connection string syntax see https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connectionstring-syntax] pointing to **MainDb**, using **JobServer_DbCred**.
- Snippet from **connections.config** showing where you must edit:

```
<add name="FtosConnection" connectionString="Data
Source=...;Initial
Catalog=...; User
ID=...;Password=...;MultipleActiveResultSets=True;"
providerName="System.Data.SqlClient" />
```

5. Execute in cmd.exe: `sc.exe start JobServer_WinSvcName`

#### Upgrade

You must execute instructions from this section on **JobServer_Machine**.

1. Follow all steps from JobServer \ Standard job configuration \ Upgrade
2. Execute in cmd.exe: `sc.exe stop JobServer_WinSvcName`
3. Copy with overwrite all files from **ReleaseKit_Dir\JobServer.Plugins\MessageComposer** to **JobServer_InstallDir**, except for the following files:

- connections.config
- schedule.config
- services.config

- serviceSettings.config

4. For each of the files excepted at the previous step, analyze the differences between version from **ReleaseKit_Dir** and that from **JobServer_InstallDir** using a text file compare tool and merge changes into the version from **JobServer_InstallDir** without breaking existing customizations.
5. Execute in cmd.exe: `sc.exe start JobServer_WinSvcName`

## MessageBus (OCS) + MessageComposer job configuration

#### First/clean install

You must execute instructions from this section on **JobServer_Machine**.

1. Follow all steps from JobServer \ MessageBus (OCS) job configuration \ First/clean install
2. Follow all steps from JobServer \ MessageComposer job configuration \ Upgrade starting at step 2

#### Upgrade

1. Follow all steps from JobServer \ MessageBus (OCS) job configuration \ Upgrade
2. Follow all steps from JobServer \ MessageComposer job configuration \ Upgrade starting at step 2

## DebuggingServer

#### First/clean install

You must execute instructions from this section on **DebuggingServer_Machine**, unless otherwise specified.

> **IMPORTANT!**
> You can use a single **DebuggingServer** instance for multiple **PortalWebApp** instances from multiple FTOS environments.

1. Create directory **DebuggingServer_InstallDir**
2. Copy all files from **ReleaseKit_Dir\DebuggingServer** to **DebuggingServer_InstallDir**
3. Execute in cmd.exe: `powershell.exe -File "DebuggingServer_InstallDir\setup-as-service.ps1"`

> **HINT**
> ◦ This will install and start a Windows service named RavenDB that will listen for incoming connections on port 8080
> ◦ A web browser will open, pointing to the web interface for RavenDB. You can ignore and close this browser window.

4. On **PortalWebApp_Machine**, edit XML file **PortalWebApp_InstallDir\web.config** and add a new child XML node named add under **/configuration/appSettings**:

- Add two XML attributes to the new node:
  - 1st XML attribute named key with value **feature.development-debugging-server**
  - 2nd XML attribute named value with value **http://DebuggingServer_Machine:8080**
- Snippet from web.config showing how you must edit:

```
<appSettings>
  <add key="feature.development-debugging-server" value="..." />
  ...
</appSettings>
```

## DebuggingUi

#### First/clean install

You must execute instructions from this section on **DebuggingUi_Machine**.

1. Create directory **DebuggingUi_InstallDir**
2. Copy all files from **ReleaseKit_Dir\DebuggingUi** to **DebuggingUi_InstallDir**

3. Execute in cmd.exe: `DebuggingUi_InstallDir\FTOS.Debugger.exe`
4. In the newly opened **Fintech-OS Debugger** application click on main menu entry **Server \ Connect to debug server…** and type in the URL **http://DebuggingServer_Machine:8080**

- Alternatively, if you always use the same **DebuggingServer** URL, edit XML file **DebuggingUi_InstallDir\FTOS.Debugger.exe.config** and set the value of the XML attribute `/configuration/appSettings/add [@key='feature.development-debugging-server']/@value` to **http://DebuggingServer_Machine:8080**
- Snippet from **FTOS.Debugger.exe.config** showing how you must edit:

```
<add key="feature.development-debugging-server" value="..." />
```

# DevOps

DevOps is a set of processes that unifies development (Dev) and processes (Ops) to complement software development. Unlike traditional software development methodologies, DevOps enables companies to create and improve products and go to market at a faster pace.

This section covers the following topics:

---

## Configure the File Upload Folder

When building a web application that requires users to upload or download files (documents, images, etc.), file storage can be an important aspect of the application architecture.

### Where Should I Store Files?

FintechOS platform supports multiple storage providers for storing the uploaded or generated user files. When building web applications using FintechOS technology, you've got a few choices for where to store your files:

- "Local File System Storage" on the next page
- "Azure Blob Storage" on page 55
- "Amazon S3 Buckets Storage" on page 57

The local file system refers to either a local path on the application server or a shared folder on the network containing the application server. While it is the default storage provider, you might be running out of disk space or you might find it a very challenging task to ensure that files are properly backed up and available at all times.

If you'll be storing large blobs of content, you might want to consider one of the other options. Storing files in a file storage service like Amazon S3 Buckets or Azure Blob is a great option if you'll be storing large blobs of content. Not only you stay rest assured that your data is replicated and backed up, but they also ensure scalability and high availability.

This section walks you through the steps needed to configure the "UploadEbs" storage provider /location as needed.

## Local File System Storage

There are no special configurations that have to be made in order to use it other than setting the name of the root folder.

To set the name of the root folder, go to the **web.config** file, open it and to the **appSettings** node, add the application setting **UploadFolder**, as described below:

```
<configuration>
 ...
 <appSettings>
       ...
       <add key="UploadFolder" value="path_to_root_folder" />
  </appSettings>
  </configuration>
```

Depending on where the root folder resides, make sure that you properly set the value of the UploadFolder setting:

- subfolder of the application folder: "~/path/to/uploadfolder/";
- local folder on application server, the full path to local folder, like:

  "c:\path\to\uploadfolder"

- network shared folder: "\\server\path\to\uploadfolder";

> **NOTE**
> If in the **web.config** file you do not set the **UploadFolder** setting, it is automatically set to the default value, that is, "~/UploadEBS/".

### Automatically Create File Upload Subfolders

> **IMPORTANT!**
> This feature is available only for local file system storage. It is not available for Azure Blob Storage or Amazon S3 Buckets Storage.

You can automatically group uploaded files into folders based on the last three characters in their file name (excluding the file extension). To do so, add an **feature-uploadfolder-autocreate-subfolders** key with a value of **1** in the web.config file:

```
<add key="feature-uploadfolder-autocreate-subfolders" value="1">
```

This will save each uploaded file in a `-.files\`*xyz* subfolder of the upload folder, where *xyz* represents the last three characters of the file name. For example, a file called MyDoc_0caf99b6-549d-48f7-8747-5e3eb82753fd.txt will be saved in a folder structure similar to:

```
...\
    UploadEBS\
        -.files\
            3fd\
                MyDoc_0caf99b6-549d-48f7-8747-5e3eb82753fd.txt
```

Setting the feature-uploadfolder-autocreate-subfolders key value to **0** disables the feature.

This feature is backward compatible. If a requested file is not stored in the above folder structure, it will be read from the main upload folder or the entity specific upload folder respectively.

## Azure Blob Storage

To configure FintechOS to store user files in Azure Blob, follow these steps:

1. Go to the web.config file and open it.
2. Add a `ftosStorageService` section to the **<configSections>** element:

```
<configuration>
        <configSections>
            ...
            <section
name
=
"ftosStorageService"

type
="EBS.Core.Utils.Services.Config.StorageServiceConfigSection,
EBS.Core.Utils"/>
        </configSections>
<configuration>
```

3. Add a `ftosStorageService` section (note the AzureBlob type) as child of **<configuration>** element:

```
<configuration>
 ...
 <ftosStorageService type="AzureBlob">
       <settings>
            <setting
name="connectionString" value="connection_string"/>
            <setting name="rootContainer" value="root_
container"/>
       </settings>
  </ftosStorageService>
</configuration>
```

where:

- *connectionString* is the connection string FintechOS is using to connect to an Azure Blob container;
- *rootContainer* is the root container name where the user files will be stored.

## Azure Resource Manager templates support

To enable automatic deployment through ARM templates, the `connectionString` and `rootContainer` settings must be configured in the **<appSettings>** element of the web.config file:

```
<appSettings>
...
    <add key="ftosStorageService-AzureBlob-
connectionString" value="connection_string" />
    <add key="ftosStorageService-AzureBlob-
rootContainer" value="root_container" />
</appSettings>
```

**IMPORTANT!**
Values set in the **<appSettings>** keys take precedence over the values set in the **<ftosStorageService>** settings node.

## Amazon S3 Buckets Storage

To configure FintechOS to store user files in Amazon S3 Buckets, follow these steps:

1. Go to the web.config file and open it.
2. To the <configSections> element, add the following two sections: ftosStorageService and aws, as described below:

```
<configuration>
        <configSections>
        ...
            <section
name
=
"ftosStorageService"

type
="EBS.Core.Utils.Services.Config.StorageServiceConfigSection,
EBS.Core.Utils"/>
            <section name="aws" type="Amazon.AWSSection,
AWSSDK.Core"/>
        </configSections>
 <configuration>
```

3. Add <ftosStorageService> tag (note the AmazonS3Bucket type) as child of configuration element:

```
<configuration>
        ...
        <ftosStorageService type="AmazonS3Bucket">
            <settings>
                <setting name="AWSAccessKey" value="access_
key" />
                <setting name="AWSSecretKey" value="secret_
key" />
                <setting name="BucketName" value="bucket_
name"/>
            </settings>
        </ftosStorageService>
</configuration>
```

where:

`AWSAccessKey` and `AWSSecretKey` are used by FTOS to sign the requests made to AWS. For more information, see Access Keys (Access Key ID and Secret Access Key).

**BucketName** is the root bucket name where the user files will be stored.

4. Add the **aws** section as child of the configuration element:

```
<configuration>
...
        <aws region="aws_region">
        </aws>
</configuration>
```

> **NOTE**
> The only required attribute is **region**. For a complete list of available regions, see Amazon documentation, section *Regions, Availability Zones, and Local Zones*. The region attribute must have one of the values from the column "Region". E.g.: `<aws region="eu-central-1"></aws>`

For a list of allowed elements in the AWS section, see Configuration Files Reference for AWS SDK for .NET.

# Importing and Exporting Deployment Packages

In FintechOS, users with elevated privileges (admin users) can export metadata from an environment and import it into another environment, using deployment packages.

Deployment packages are text-based so they can be version controlled to have their history inspectable with text-diff tools.

In FintechOS, you have three options for importing and exporting deployment packages, as follows:

- In FintechOS Studio, from the DevOps menu > Deployment Packages. For more information, see the FintechOS Studio, section Deployment Packages.
- Using the customization set methods of the API. For information on how to import and export packages using customization sets), see FintechOS API documentation.
- From the command line by using the **FtosPkgDeployer** tool.

The **FtosPkgDeployer** tool is available in the release subdirectory, *Tools**FtosPkgDeployer*, It allows you to do the following from the command prompt:

- list the customization sets found in a FTOS server.
- import / export in / from server a customization set from / in a local file.

> **NOTE** :In order to use the tool, make sure to run the command prompt as admin.

For information on how to use the **FtosPkgDeployer** tool , see the built-in help by running the command prompt as admin and executing `FtosPkgDeployer.exe` without arguments. The tool is using the POST CUSTOMIZATION SET method of the FintechOS API.

# File-Type Upload Control

In FintechOS, you can control what types of files users can upload into the system.

This feature is particularly useful in preventing users from uploading wrong file types, thus saving time from investigating what went wrong and having to resubmit the files.

> **NOTE** The file-type upload control feature has been added to the previous existing validations: file extension validation, content size validation etc. For a content to be uploaded all validations must pass.

## Enable the file-type upload control

By default, the file-type upload control is disabled. To enable it, on the server where the FintechOS installation package resides, go to the **web.config** file, open it and add the following setting:

```
<appSettings>
    ....
    <add key="feature.upload.filetype-check" value="true" />
</appSettings>
```

## File-Type Upload Processing

Once the File-Type Upload control is enabled, upon file uploads using client scripts (using the ebs.upload function) or server automation scripts (using the uploadFile function), the system verifies the uploaded content against the file extension. The system will try to match the uploaded content (the bytes) with the provided file extension based on a list of files signatures.

Files signatures are available for the following file types: pdf, docx, xlsx, pptx, odt, ods, jpg/jpeg, doc, xls, ppt, rtf, xml, png, gif, bmp.

**No match, the file is uploaded**

If the matching process does not find any match between the file content and the available file signatures then the upload is allowed.

The user uploads an Autocad file.

**Match, but the signature's extension is not what the file says it is**

if the matching process finds a match between the file extension and the available file signature, the system further checks the file internal type (that's is, MIME type) which serves as an integrity check. If there is a mismatch between the two, that means that the internal type of the file does not correspond to what the file extension says it is and the file upload is not allowed. An error will be returned.

The user tries to upload a PNG file (the content has a PNG signature) that has a ".jpg" extension

**Executable files**

By design, if the matching process identifies that the uploaded content has an EXE or DLL signature then the upload is not allowed. An error will be returned.

# FintechOS API a Standalone Web App

FintechOS gives you the ability to set the FintechOS API as a standalone web app, which means that the API it will work in exclusive API server mode. This is particularly useful when you want to get data from FintechOS using API calls and use it within your own web apps. The following controllers are available via the API standalone app: WCF Services, API and Authorization.

> **NOTE** The Portal functionality is disabled, that means that the API web app will not be available to end users.

To configure the API as a standalone app, go to the **web.config** file and enable the API server, as provided below:

```
<configuration>
        <appSettings>
            ...
            <add key="feature-api-server" value="1" />
            </appSettings>
```

```
...
</configuration>
```

# Activating Localization Debug Mode

FintechOS supports the localization of static and dynamic elements, as well as the localization of customized messages and metadata.

Before localizing in a new language, you need to prepare your environment to easily identify the resources to be localized. To do so, open the **Web.config** file of your application and change the value of the following key:

From:

```
<add key="ebs:debugLocalization" value="0" />
```

To:

```
<add key="ebs:debugLocalization" value="1" />
```

The table below lists the localization keys:

| Key | Description |
|---|---|
| ebs:uiLocalization | Toggles dynamic UI localization (HTML templates, after generate JavaScript).<br><br>The immediate result visible in the user interface is the dynamic generation of HTML templates in the optimum format for localization. |
| ebs:dataLocalization | Toggles metadata (data) localization and automatically creates database support for each language. |
| ebs:debugLocalization | Toggles the debug mode. |
| ebs:localizationSchedulerTimeSpan | Interval in milliseconds when checking for external resource updates in the database. |

Once the localization debug mode is activated, the following markers are displayed for both the user interface and the metadata localized values:

✓✓ - To indicate the localized values.

 - To indicate that values are localizable, but no localization has been provided.

 - To indicate that the fields allow localization of the data inside the field.

# Configure SMTP Server

In the FintechOS Platform it is possible to have receive notifications for operations. This is done by ticking the **Send Notification On Error** check box when you create a step. For this to properly function, the email settings need to be configured in the **mail.config** file, as follows:

- Navigate to the **JobServer** folder inside the FintechOS Platform installation folder (for example: `C:\FintechOS\MyProject\JobServer`). Please note that the **JobServer** folder is in the folder with the name of your project.
- Open the **mail.config** file with a text editor (such as Notepad++). It needs to contain the following:

```
<mailSettings>
  <server>test@fintechos.com</server>
  <port>587</port>
  <auth>true</auth>
  <user>test@fintechos.com</user>
  <password>insertPasswordHere</password>
  <from>test@fintechos.com</from>
  <to>test@fintechos.com</to>
  <cc>test@fintechos.com</cc>
  <bcc></bcc>
  <replyTo>test@fintechos.com</replyTo>
</mailSettings>
```

- Fill in the parameters, as follows:
  - `<server>FintechServer</server>` - the server from which FintechOS operates
  - `<port>587</port>` - the port corresponding to the server
  - `<auth>true</auth>` - set the value to **true** if the authentication requires username and password
  - `<user>test@fintechos.com</user>` - the username corresponding to the server
  - `<password>insertPasswordHere</password>` - the password of the provided user
  - `<from>test@fintechos.com</from>` - the email address which appears in the **From** field
  - `<to>test@fintechos.com</to>` - the email address to send the notification to
  - `<cc>test@fintechos.com</cc>` - optional; an additional address to send the notification to
- Save and close the **mail.config** file.

# Integrations

This section explains how to integrate the FintechOS platform with third party services, such as payment processors, electronic signature providers, or digital profile reviews:

---

## Connect to Azure Notification Hubs

The server SDK sendMobileNotifications function allows you to send notifications to subscribed user devices via the Azure Notifications Hub push engine. To connect FintechOS with the Azure Notifications Hub, follow the steps below:

1. Configure your notifications hub on the Microsoft Azure cloud computing service. For details, see the Azure Notification Hubs documentation.

   > **NOTE**
   >
   > You have to create one notification hub per mobile app, per environment.

2. In the <appSettings> node of the *web.config* file, add keys for the hub name and endpoint settings of each client application, based on the model below:

```
<appSettings>
    ...
    <add key="azure-mobile-notifications-myApp1-
hubname" value="xxxhubname1">
    <add key="azure-mobile-notifications-myApp1-
endpoint" value=
"Endpoint=sb://xxxnamespace1.servicebus.windows.net/;SharedA
ccessKeyName=DefaultFullSharedAccessSignature1;SharedAccessK
ey=xxxxxxxxx1">
    ...
```

```
    <add key="azure-mobile-notifications-myApp2-
hubname" value="xxxhubname2">
    <add key="azure-mobile-notifications-myApp2-
endpoint" value=
"Endpoint=sb://xxxnamespace2.servicebus.windows.net/;SharedA
ccessKeyName=DefaultFullSharedAccessSignature2;SharedAccessK
ey=xxxxxxxxx2">
</appSettings>
```

In the example above:

- We set up two client applications that will receive notifications: **myApp1** and **myApp2**.
- The notifications are sent using the **xxxhubname1** and **xxxhubname2** Azure notifications hubs respectively.
- The endpoints for the two hubs are **sb://xxxnamespace1.servicebus.windows.net/** and **sb://xxxnamespace2.servicebus.windows.net/**.
- The shared access key names are **DefaultFullSharedAccessSignature1** and **DefaultFullSharedAccessSignature2**.
- The shared access keys are **xxxxxxxxx1** and **xxxxxxxxx2**.

## Push Notifications Log

Sent notifications are saved in the FTOS_DPA_MessageQueue table. The table contains an entry for each notification sent to each user. This message queue can be viewed at the http://localhost:57123/Main#/entity/FTOS_DPA_MessageQueue/list link:

| Attribute | Description |
|---|---|
| ToAddress | Mobile app name. |
| UserId | ID of the user that received the notification. |
| Subject | Message queue subject set in the sendMobileNotifications function call that initiated the notification push. |
| Body | Message received by the recipient. |

| Attribute | Description |
|---|---|
| ChannelProvider | Provider with the same name as the Mobile App Name. |
| CommunicationChannel | Hardcoded to **AzureNotificationHub**. |
| ChannelProviderParams | Recipient filter used when sending the notification (example: "role: developer"). |
| MessageStatus | Hardcoded to **Sent**. If notifications were not successfully received, check the logging in the Azure Portal. |

# FAQs

## What happens if the messages are added to the FintechOS message queue, but are not sent by the Azure notification hub?

The messages remain in the Sent status. The main purpose of the message queue logging is to track notification attempts. For troubleshooting, the main place to check statuses is the Azure portal.

## Is there a limit to the number of notifications sent at once?

No. The Azure Notification Hubs support a maximum of 20 tags on a notification command, but FintechOS automatically splits the notification into batches if this number is exceeded.

## If my role contains 5 users, but only 3 are registered to the notification hub, how many push notifications are going to be sent?

In the FintechOS message queue, there are going to be 5 entries (one for each user). On the Azure notification hub, after sending the request from FintechOS, the outcome will be: 3 Success, 0 Failed.

## Can I have only one notification hub for 2 client apps ?

It is recommended to have 1 hub per app. In the Azure portal > Notification Hub setup, you can set only one key, which is normally associated to only one app.

There are exceptions such as Android-FCM where the API key corresponds to the Firebase project. In this case, you can:

- Add multiple apps on the same Firebase project, resulting in a single API key.
- Create a project for each App, resulting in separate API keys/hubs.

# CertSign Integration for electronic signature

Certsign is a digital certification for digital signatures. It will provide the user with the capability to use the Esign processor in the Studio and Portal. This makes possible to sign contracts and other documents by a client. The existing integration provides two types of signature:

- Remote signature (with authorization code sent through sms)
- Automatic signature (with an existing certificate)
- Automatic signature with qualified electronic sign.

After the installation of the ESign provider package, you should add the following configuration in FTOS Portal web.config, section appSettings or JobServer serviceSettings.config:

```
<add
key
=
"FTOSServicesESignProvider2Endpoint"
 value="https://aztestapi01.azure-api.net/certSign"/> <!-- This is
the test env url -->
<add key="FTOSServicesESignProvider2AppId" value=""/><!-- the
subscription key -->
<add key="ESignProvider2CertName" value="certSignTest"/> <!-- the
mapping for the certificate provided by FTOS-->
```

If you have to configure also, the automatic signature, please add the following keys:

```
<add key="ESign2AutomaticNumber_{ProfileName}" value=""/> <!--this
will contain the serial number provided for the specific profile-->
<add key="ESign2AutomaticName_{ProfileName}" value="cn=certSIGN CA
Class 2 G2,ou=certSIGN CA Class 2 G2,o=certSIGN,c=RO"/> <!--this
will contain the issuer information for the profile-->
```

**IMPORTANT!**
The token {ProfileName} must be replaced with a profile name that will be used when requesting the signature process.

## Set up for the automatic signature with qualified electronic sign

After the installation of the ESign provider package, you should add the following configuration in JobServer serviceSettings.config:

```
<add
key
="FTOSServicesESignProvider2Endpoint"
 value="https://aztestapi01.azure-api.net/certSign"/> <!-- This is
the test env url -->
    <add key="FTOSServicesESignProvider2AppId" value=""/><!-- the
subscription key -->
    <add
key
="ESignProvider2AutomaticQESCertName"
 value="certSignTestAutomatic"/> <!-- the mapping for the
certificate provided by FTOS for the Automatic QES signature-->
```

Insert a record in the business entity **FTOS_DDM_ESignQueue**, this record will contain the configurations that will be used for automatic qualified electronic sign.

ProfileName, choose a name for this automatic profile, make sure it is unique if you have multiple configurations:

- ExternalId, this value should be provided CertSign, it will be the externalId of the user that is enrolled to sign with automatic QES
- Seed, this value will be read by the agent from his CertSign acount (he will receive an email with steps to follow)
- WorkstepsBulkNo, this represents the number of worksteps that will be sent in the request to be signed with automatic QES.

## Calling the automatic signature with qualified electronic sign

The request for automatic QES will be sent together with the rest of the worksteps. The signing processes will be made in the order provided in the request. It is recommended that this signature to stay at the end because it will be processed async by Job Server.

The workstep with automatic QES should be like:

```
{
      "signatureTag": "#tagAgentQES#",
      "signatureType": FTOSServices.DDM.signatureType.AutomaticQES,
      "automaticProfile": "ProfileNameDefinedInQueue", //defined in
FTOS_DDM_ESignQueue
      "signatureStamp": { //this is for the signature stamp
        "SignerName":"Sign name",
        "Reason": "Credit loan", //this will appear in signature
details
        "Subject": "Bank signature",
        "ShowTimeStamp": true, //show date in signature stamp
        "FontSize": "12"
      }
    }
```

## Example

```
var signRequest = {
  "workstepConfigs": [
    {
      "signatureTag": "#tagClient#",

"signatureType"
:FTOSServices.DDM.signatureType.QualifiedElectronicSign,
      "recipient": {
        "Country": "RO",
        "Email": "@fintechos.com",
        "ExternalId": "", //an unique id representing the
customer (ex: Accoountid)
        "FirstName": "M",
        "LastName": "C",
        "PhoneMobile": "+407",
        "SocialSecurityNumber": "", //PIN
        "IdPhoto": "", // ftos file attribute value
representing the id picture

      },
      "signatureStamp":{
        "Reason": "Client reason",
        "Subject": "Credit loan",
        "SignerName":  "TestFirstName TestLastName",
        "FontSize": "12"
      }
    },
    {
      "signatureTag": "#tagAgentQES#",
      "signatureType":
FTOSServices.DDM.signatureType.AutomaticQES,
      "automaticProfile": "ProfileNameDefinedInQueue",
      "signatureStamp": { //this is for the signature stamp
        "SignerName":"Sign name",
        "Reason": "Credit loan", //this will appear in
signature details
        "Subject": "Bank signature",
        "ShowTimeStamp": true, //show date in signature
stamp
        "FontSize": "12"
      }
    }
  ],
  "signedDocumentName": "test.pdf",
  "files": [
```

```
    {
      "ftosFile": "" //ftos file attribute value
representing the pdf that needs to be signed
    }
  ]
}
```

**NOTE**

The automatic QES signing has to be processed by Job Server, so you must configure a schedule trigger with a server side script. Please make sure that you won't use the same ExternalId on multiple instances of FintechOS. Also, the scheduled trigger should be configured to run with a frequency of at least 30 seconds. The recommended cron expression should be to start at second 0 or at second 30 and to run from 30s in 30s (or a multiple of 30s = 1min, 2min, etc).

In the server side script you have to call the following method with the parameter ProfileName that you've defined in FTOS_DDM_ESignQueue:

```
//This method returns the list with processed eSignId and the
workstepId that has been finished
//As input you shoul pass the Name that you've configured in  FTOS_
DDM_ESignQueue
var result = FTOSServices.DDM.ESign2.processPendingAutomaticQESSign
("ProfileNameDefinedInQueue");


// if success the result will look like:
/*
{
  "isSuccess": true,
  "isFinished": true,
  "eSignProcesses": [
    {
      "eSignId": "e2f2bc20-de1f-41f1-851b-5c0279cc4cb7",
      "eSignWorkstepId": "13b2ea4e-f5cb-491a-a32a-268741e7da2a"
    },
    {
      "eSignId": "ac42d532-88a3-4db6-932c-9d0888e2fd0e",
      "eSignWorkstepId": "6830d22a-9309-4a11-9e9a-05ab7ac8807b"
```

```
    }
  ]
}
*/
```

## FTOS ESign Services API

In order to sign a document you must call the following methods:

1. RequestSign (for the configuration of the automatic signature)

   For client signature with remote method with authorization code sent through sms:

2. AcceptTermsAndConditions
3. Authorize signature
4. Resend code

## RequestSign

Firstly, add a reference to the library FTOSServices. To request with qualified electronic signature and automatic, use the following example:

```
var signRequest = {
    "workstepConfigs": [{
        "signatureTag": "#tagClient#",
        "signatureType":
FTOSServices.DDM.signatureType.QualifiedElectronicSign,
        "recipient": {
            "Country": "RO",
            "Email": "@fintechos.com",
            "ExternalId": "", //an unique id representing the
customer (ex: Accoountid)
            "FirstName": "M",
            "LastName": "C",
            "PhoneMobile": "+407",
            "SocialSecurityNumber": "", //PIN
```

```
            "IdPhoto": "", // ftos file attribute value
representing the id picture
        },
        "signatureStamp": {
            "Reason": "Client reason",
            "Subject": "Credit loan",
            "SignerName": "TestFirstName TestLastName"
        }
    }, {
        "signatureTag": "#tagBank#",
        "signatureType":
FTOSServices.DDM.signatureType.AutomaticSign,
        "automaticProfile": "Profile1",
        "signatureStamp": { //this is for the signature stamp
            "Reason": "Credit loan", //this will appear in
signature details
            "Subject": "Bank signature",
            "ShowTimeStamp": true //show date in signature stamp
        }
    }],
    "signedDocumentName": "test.pdf",
    "files": [{
        "ftosFile": "" //ftos file attribute value representing the
pdf that needs to be signed
    }]
}
Optionally, you can add to the recipient property the following
information.It will appear in terms and conditions file......
"workstepConfigs": [{
        "signatureTag": "#tagClient#",
        "signatureType":
FTOSServices.DDM.signatureType.QualifiedElectronicSign,
        "recipient": {......
            "DocumentIssuedBy": "splcid", "DocumentIssuedOn":
"2020-01-20", "DocumentExpiryDate": "2050-01-25", "DocumentNumber":
"123456", "DocumentSeries": "xa", "County": "Braila", "City":
"Braila", "Street": "asd", "StreetNo": "12", "Block": "asd",
"Entrance": "q", "ApartmentNo": "123", "ZipCode": "123453",
        }
```

**HINT**

If you have a request with multiple signatures, please keep in mind that the signing processes is sequentially and the client signature must have manual input (accept terms and conditions and authorize signing using the code received via sms).

You should save the eSignId in order to track the status of the eSign process using the method GetESignStatus.

## AcceptTermsAndConditions

Add a reference to the client script library FTOS_DDM_ESignProvider2.

```
/**
* Accepts terms and conditions for emtitting the certificate
* @param termsId is the id returned by requestSign method
(entityId property)
* @param accepted should be set on true, if the user accepts
the terms and conditions
* @return documentId that will be used for authorize signing
*/
acceptTermsAndConditions(termsId: string, accepted:
boolean): Promise<any>
```

Example:

```
var ddmESign = ebs.importClientScript("FTOS_DDM_
ESignProvider2");
ddmESign.acceptTermsAndConditions(termsId, true).then
(function(result) {
    console.log(result);
    //output should be{isSuccess: true, entityId: "12437-
34873"}
}, function(error) {
    console.log(error);
});
```

## Authorize signature

Add a reference to the client script library FTOS_DDM_ESignProvider2.

```
// @param documentId is the id returned by
acceptTermsAndConditions method (entityId property)
// @param code should be the code sent via sms for the
signing process

authorizeSign(documentId: string, code: string): Promise <
any > ;
```

```
// Example:

var ddmESign = ebs.importClientScript("FTOS_DDM_
ESignProvider2");
ddmESign.authorizeSign(documentId, code).then(function
(result) {
    console.log(result);
    //output should be {isSuccess: true}
}, function(error) {
    console.log(error);
});
```

Example:

```
var ddmESign = ebs.importClientScript("FTOS_DDM_
ESignProvider2");
ddmESign.authorizeSign(documentId, code).then(function
(result) {
    console.log(result);
    //output should be {isSuccess: true}
}, function(error) {
    console.log(error);
});
```

## Resend sms code

As before, add a reference to the client script library FTOS_DDM_ ESignProvider2.

```
/**
* @param documentId is the id returned by
acceptTermsAndConditions method (entityId property)
*/
resendCode(documentId: string): Promise<any>
```

Example:

```
var ddmESign = ebs.importClientScript("FTOS_DDM_
ESignProvider2");
ddmESign.resendCode(ebs.getCurrentEntityId()).then(function
(result) {
    console.log(result);
```

```
    //output should be {isSuccess: true}
}, function(error) {
    console.log(error);
});
```

Async methods, can be used with JobServer:

## Update statuses

This method should be called using Job Server scheduler. It will update the status of the in progress eSign processes.

FTOSServices.DDM.ESign2.updateStatusESignProcess();

## ProcessAutomaticSign (sign with automatic signature)

This method should be called using Job Server scheduler. It gets the in progress esign processes that must be signed with automatic signatures.

FTOSServices.DDM.ESign2.processPendingAutomaticSign();

## Get ESign Status

This method returns the status of the eSign process. If the status is Finished, then you can get the signed document name to use it in your digital journey.

```
/**
 * @param eSignId is the id returned by requestSign
 */
FTOSServices.DDM.ESign2.getESignStatus(eSignId): any
Example: var eSignStatus =
FTOSServices.DDM.ESign2.getESignStatus(eSignId);
log(toJson(eSignStatus));
/*should print:
{
"isSuccess": true,
"status": "Finished",
```

```
"documents": "[\r\n  {\r\n    \"Name\":
\"contract1.pdf\",\r\n    \"RealName\": \"contract1_
42dfa5ba-c1f4-4328-b095-
b6075d0c12ee.pdf\",\r\n    \"IsSuccess\":
true,\r\n    \"Message\": null,\r\n    \"ClientScript\":
null,\r\n    \"Serialized\": null,\r\n    \"ErrorCode\":
0,\r\n    \"UIResult\": null\r\n  }\r\n]"
}
/*
```

Example:

```
var eSignStatus = FTOSServices.DDM.ESign2.getESignStatus
(eSignId);
log(toJson(eSignStatus));
/*should print:
{
"isSuccess": true,
"status": "Finished",
"documents": "[\r\n  {\r\n    \"Name\":
\"contract1.pdf\",\r\n    \"RealName\": \"contract1_
42dfa5ba-c1f4-4328-b095-
b6075d0c12ee.pdf\",\r\n    \"IsSuccess\":
true,\r\n    \"Message\": null,\r\n    \"ClientScript\":
null,\r\n    \"Serialized\": null,\r\n    \"ErrorCode\":
0,\r\n    \"UIResult\": null\r\n  }\r\n]"
}
/*
```

# Configure the CData Sync Service

The CData Sync service is required for the FintechOS Data Pipes data replication feature. CData Sync must be installed on the same machine as the FintechOS platform. The service is shared between FintechOS instances. If you have multiple platform instances running on the same machine, install the CData Sync service only once.

## System Requirements

- Windows Vista/Windows Server 2008 or higher.
- .NET Framework 4.5 or higher.
- 500 MB RAM required. 1+ GB recommended.
- Adequate free disk space for job logging.

## Installation

1. Copy the CData Sync installation kit provided by FintechOS to your local machine.
2. Open Windows PowerShell as administrator and navigate to the installation kit folder.
3. Run the following command in Windows PowerShell:

```
.\FtosCDataSyncInstaller.ps1 -p_MainCommand Install -p_
InstallDir <installation path>
```

4. This will start the installer. At the command line prompt, type **GO!** and press **Enter**.

The CData Sync server will be installed in the specified directory. The default credentials are:

- username: admin
- password: admin

For more details about managing the CData Sync server, see the CData official documentation.

## Upgrade

To upgrade the CData Sync server, follow the same "Installation" on the previous page instructions, but replace the Windows PowerShell command with:

```
.\FtosCDataSyncInstaller.ps1 -p_MainCommand Upgrade -p_InstallDir
<installation path>
```

## Uninstall

To uninstall the CData Sync server, follow the same "Installation" on the previous page instructions, but replace the Windows PowerShell command with:

```
.\FtosCDataSyncInstaller.ps1 -p_MainCommand Uninstall -p_InstallDir
<installation path>
```

# Configure the Payment Processor Service Provider

If you wish to enable online payments in your digital journeys, you need to partner with a payment processor and configure the link to their service in the FintechOS Studio *web.config* file.

## Define a new type of section in the web.config file for the payment processor

Opent the FintechOS Studio *web.config* file in a text editor and add a new entry inside the **<configSections>** node:

```
<section
name
="ftosPaymentProcessor"

type="EBS.Core.Utils.Services.Config.PaymentProcessorConfigSection,
EBS.Core.Utils"/>
```

## Add the connection settings for your payment processor

Opent the FintechOS Studio *web.config* file in a text editor and add a new entry inside the **<configuration>** node (after <configSections>):

```
<ftosPaymentProcessor type="Netopia">
    <definition>
        <settings alias="conf1">
            <setting
name="environment" value="http://sandboxsecure.mobilpay.ro"/>
            <setting name="publicCertificate" value="C:\\PATH_TO_
CERT\\sandbox.cer"/>
            <setting name="privateKey" value="C:\\PATH_TO_
CERT\\sandbox.key"/>
            <setting name="signature" value="XXX"/>
            <setting
name="redirectUrl" value="http://localhost/test_redirect.html"/>
            <setting
name="confirmUrl" value="http://localhost/test_confirm.html"/>
        </settings>
    </definition>
</ftosPaymentProcessor>
```

**NOTE**

- Currently, only the *Netopia* payment processor type is supported, which will link to a mobilPay service provided by Netopia Payments. Additional payment processors may be available in the future.
- The *alias* will identify the payment processor service when initiating payments using the getPaymentToken function.

# Configure FTOSApiSMS provider

The FTOSApiSMS does not come out-of-the-box with the FintechOS Studio. Add the configuration elements in web.config for the provider.

Add section

```
<configSections>
...
  <section name="ftosApiSmsProvider" type=
"EBS.Core.Data.Services.CommunicationProviders.Sms.FtosApiSmsProvid
erConfig, EBS.Core.Data.Services"/>
</configSections>
```

Add configuration element

```
<ftosApiSmsProvider
xmlns="urn:EBS.Core.Data.Services.CommunicationProviders.Sms"
        serviceUrl="insertyourURL"
        subscriptionKey="insertyourkey"
        from="SantaClaus"
    />
```

where:

- serviceUrl - the URL to FintechOS SMS gateway;
- subscriptionKey;
- from - a text representing the sender of the message.

### Add support for customizing the text for messages sent through SMS on Multi-Factor Authentication process:

- web.config - add a new attribute on multiFactorAuthentication/providers/provider section.

  Name: “messageTemplate“. Its value should be one of the FTOS_CMB_ ActionTemplate records;

- identify the correct template - find FTOS_CMB_ActionTemplateContent child of FTOS_ CMB_ActionTemplate (with name equal to the value of messageTemplate attribute) that has a FTOS_CMB_CommunicationChannel (Channel) that has FTOS_DPA_ ChannelProvider (Bus Communication Provider) with name equal to the name of the channel provider set on the MFA provider. The template also depends on user culture → try to find the template using the user culture (from EbsMetadata.UserSettings with fallback to default system culture);
- if a proper template cannot be identified → error;
- the message (the body of the sms) will be customizable with 2 tokens: {{otp}} (the generated OTP) and {{user_display_name}} (DisplayName of the current user);
- if “messageTemplate” is missing the message will contain just the OTP code (as it is now);

# Configure the OneyTrust Digital Review service

The OneyTrust Digital Review service analyzes the information in a user's profile (email, telephone number, address, etc.) and calculates a reliability score for that information. This allows companies to detect potentially problematic profiles and act accordingly (for instance, by deciding to direct them to a manual review process instead of accepting them automatically).

To set up a connection to the OneyTrust service, add the following keys in the FintechOS Portal web.config file:

```
    <add key="FTOSServicesOneyTrustEndpoint" value="exposed
endpoint url"/>
    <add key="FTOSServicesOneyTrustAppId" value="the subscription
key"/>
```

Once the connection to the OneyTrust service is set up, you can use the createReview and getReview Server SDK functions to review user profiles.

# Security

FintechOS was built on 4 pillars of security: data encryption, authentication, authorization and logging. With a keen focus on security critical aspects, such as: access rights, segregation of duties, data ownership, it also provides you with comprehensive audit trail of what happened at any given time and who performed the action.

For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type). We recommend you to implement security best practices provided by your cloud provider.

This section covers the following topics:

---

## Data Encryption and Security

One of the keys to data protection is accounting for the possible states in which your data may occur, and what controls are available for that state:

- **Data in transit**. When data is being transferred between components, locations or programs, such as over the network, across a service bus, or during an input/output process, it is thought of as being in-transit.
- **Data at rest**. This includes all information storage objects, containers, and types that exist statically on physical media, be it magnetic or optical disk.

Data in transit is encrypted using the industry standard AES-128 encryption algorithm.

To establish identity and trust between FintechOS web-based platform and the web browser, the connection is secured via SSL certificates.

The SSL-secured communication between FintechOS and the client is done using the symmetric encryption keys that are established during the authentication process.

The data model and all scripts defined within FintechOS can be exposed through REST APIs to enable integration with 3rd party systems / solutions. FintechOS APIs are secured through OAuth 2.0 and follow the OWASP security standards.

You can encrypt the data at rest using security best practices provided by the infrastructure provider of choice where you install and deploy FintechOS (Microsoft Azure, AWS, IBM Cloud, other).

## XSS Prevention

To prevent Cross-Site Scripting (XSS) and keep FintechOS users safe, all user input data is sanitized by default, except for the following attributes: JavaScript, HTML and XML.

In FintechOS, the XSS prevention secures your web apps by escaping user input of type JavaScript, HTML and XM. It censors the data received by the web pages in a way which disallows the following characters: ”<”, “</”, “>”, “<” and “>” (e.g., <text, </text, <text or >text) from being rendered.

> **IMPORTANT!** When importing deployment packages or adding new metadata in FintechOS versions which have XSS prevention enabled, you have to eliminate the following tags from metadata and packages: ”<”, “</”, “>”, “<” and “>”; otherwise, you will get an error message and you will not be able to import them.

### XSS prevention when upgrading to FintechOS 20.1

When upgrading FintechOS to version 20.1, you should enable the request validation to the latest version; otherwise you will be vulnerable to cross-site scripting attacks. To do so, go to the **web.config** file and set the request validation version to **4.5**:

```
<httpRuntime targetFramework="4.6.2" requestValidationMode="4.5"
... />
```

# Authentication

The second pillar of security, authentication is the process of verifying the identity of a user based on a set of credentials.

FintechOS provides the following authentication mechanisms:

## FintechOS Authentication

You can log into FintechOS using the account credentials provided to you by your FintechOS administrator.

FintechOS provides you with extensive security measures to protect users access: ensure password security and unauthorize inactive users.

## Microsoft Active Directory Authentication

Access within the platform is granted through authentication with FintechOS account credentials (username and password). The built-in integration with Microsoft Active Directory (AD) allows you to access FintechOS using your AD credentials.

## Azure Active Directory Authentication

If your organization is using Azure Active Directory (Azure AD) for identity and access management, you can map Azure groups to FintechOS "Security Roles" on page 141 using the OpenID authentication protocol. This allows users to log in to FintechOS using their existing Azure AD credentials.

## OpenID Connect Authentication

OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 specifications which uses straightforward REST/JSON message flows. It enables developers authenticate the users across their apps without having to own and manage password files. OpenID Connect securely identifies the identity of the person that is using an app.

The FintechOS built-in integration with Okta (a certified OpenID Connect provider) provides user authentication and single sign-on (SSO) functionality.

SSO means being able to access all the applications and resources that you need to do business, by signing in only once using a single user account. Once signed in, you can access all of the applications you need without being required to authenticate (for example, type a password) a second time.

## Active Directory Federation Services

This service provided by Microsoft manages the user sign-in information for members of a platform. If your organization is using ADFS for identity and access management of your users, it is possible to map the users already existing in ADFS to FintechOS.

## Multi-Factor Authentication

Multi-Factor Authentication is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions. Multi-Factor Authentication helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of verification options: phone calls, text messages, or mobile app notifications or verification codes and third-party OAuth tokens.

# FintechOS Auth Provider

For the authentication process, it is possible to implement if needed within the web.config file a special request upon logging into the FintechOS Portal or FintechOS Studio. The full password is never requested in order to log in successfully, but only random characters contained in the password of a user.

---

# Microsoft Active Directory Authentication

If your organization is using Microsoft Active Directory (AD) as central user repository, you can configure FintechOS to give users the possibility to log in FintechOS using their existing AD credentials.

FintechOS supports interoperability with AD using two configurations: AD standard configuration and AD configuration using a configuration file in which you map the business units and the security roles from FintechOS with the ones in AD.

To avoid unnecessary traffic across domains and return results promptly with maximum speed, you can limit the scope of Active Directory queries. For more information, see Limiting scope of the query on Active Directory.

This section covers the following topics:

---

## AD Standard Login Configuration

In order to change the default FintechOS authentication with the Microsoft Active Directory authentication, go to the **web.config** file of your WebApp (Portal/Designer) and add/edit the following setting:

```
<appSettings>
...
<add key="EBSDefaultAuthentication" value="AD"/>
...
</appSettings>
```

You are still able to log in using the administrator host credentials (using the password fromFintechOS authentication).

**NOTE**

- When adding system users in FintechOS who will be using AD credentials for logging in, in the **UserName** field, you should provide the username in the following format: **[Domain]\[Username]**. When logging in FintechOS, users should provide the username in the format previously mentioned.
- Every AD has different security roles, so make sure that the Application Pool Identity of the FintechOS WebApp has the privileges to search into the directory entry nodes, otherwise, when trying to log in FintechOS using AD credentials, privileges related errors might occur.

## Automatically Adding Users from AD

You can automatically create / update users from Microsoft AD in FintechOS using a configuration file.

**NOTE** Automatically creating users from AD will remove the existing business units and security roles from FintechOS and add the ones from AD as provided in the configuration file. If you want to keep the system user as is, you should make additional settings. For information on the additional settings, see Preserve System User's Business Unit and Security Roles.

**IMPORTANT!** In FintechOS versions prior 18.2.8, ,getting from the Active Directory (AD) the groups to whom a user belongs to did not work smoothly; therefore, there might be situations in which wrong security roles were applied to users. With version 18.2.8, the existing configurations for mapping AD groups-roles (specified in the **~\ADUserConfiguration.xml** file) might not work as it worked in previous versions of FintechOS.

To automatically create/update users in FintechOS using a configuration file, follow these steps:

1. In the **web.config** file fo your WebApp, add the following setting:

```
<appSettings>
...
<add key="EBSADAuthAutoCreateUsers" value="true"/>
...
</appSettings>
```

2. In an xml file, create the mapping between the AD groups and the security roles and business units fromFintechOS. Name the file **ADUserConfiguration.xml**.

   Overwrite the Business Unit from FintechOS with the business unit from AD

```
<ADUserConfiguration>
    <SecurityGroup>
          <Name>`AD Group Name`</Name>
           <DefaultBusinessUnitName>`FTOS Business Unit
Name`</DefaultBusinessUnitName>
           <SecurityRoleName>`FTOS Security Role
Name`</SecurityRoleName>
    </SecurityGroup>
</ADUserConfiguration>
```

3. In the root of the WebApp, add the **ADUserConfiguration.xml** file previously created.

## Preserving System Users

To preserve the system user's business unit from FintechOS, go to the **web.config** file and add the following key:

```
<appSettings>
...
<add key="ADOverwriteBusinessUnit" value="false"/>
...
</appSettings>
```

To preserve the system user's security roles from FintechOS and merge them with the ones provided in the **ADConfiguration.xml** file, go to the **web.config** file and add the following key:

```
<appSettings>
...
```

```
<add key="ADOverwriteUSerRoles" value="false"/>
...
</appSettings>
```

## Limiting Query Scope on AD

By default, the Lightweight Directory Access Protocol (LDAP) queries are performed on the entire Active Directory (AD).

To avoid unnecessary traffic across domains and return results promptly with maximum speed, limit the scope of active directory queries by adding the following appSettings keys in the web.config file:

- for queries related to users, add the key `core-setting-adauth-users-container`
- for queries related to groups, add the key `core-setting-adauth-groups-container`.

When AD authentication is enabled, the FintechOS platform will use the values provided in the appSettings keys in the web.config file.

The keys are optional, if they are not provided the search will be performed on the entire directory.

Setting the users and groups containers:

```
<appSettings>
    <add key="core-setting-adauth-users-
container" value="OU=Utilizatori,DC=acme,DC=ro"/>
    <add key="core-setting-adauth-groups-
container" value="OU=Grupuri,DC=acme,DC=ro"/>
    ....
</appSettings>
```

In the example above, the LDAP queries will be performed against the following AD containers:

**Users**:

- Organizational Unit (OU): Utilizatori
- Domain Component (DC): ro

**Groups**:

- Organizational Unit (OU): Grupuri
- Domain Component (DC): ro

# Azure Active Directory Authentication

If your organization is using Azure Active Directory (Azure AD) for identity and access management, you can map Azure groups to FintechOS "Security Roles" on page 141 using the OpenID authentication protocol. This allows users to log in to FintechOS using their existing Azure AD credentials.

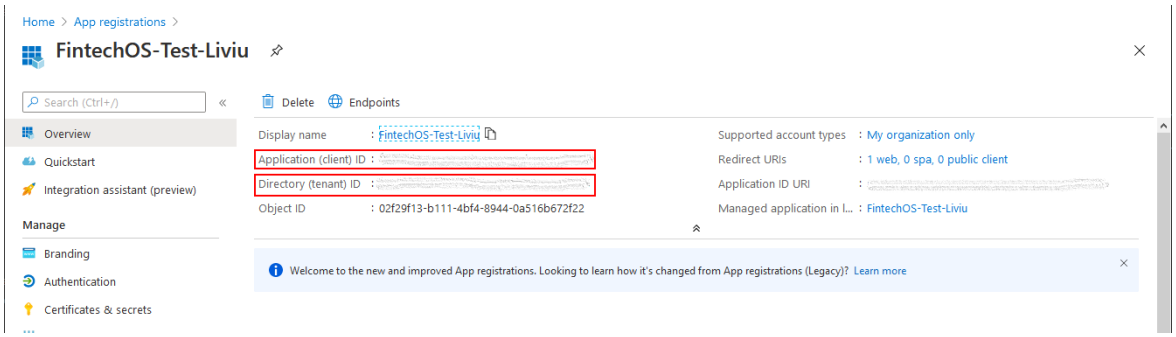
## Configure OpenID Settings

Add the following keys to the `<appSettings>` node in the *web.config* file of your web service (Portal/Studio):

```
<add key="EBSDefaultAuthentication" value="AzureAD" />
<!-- BEGIN AzureAD IDOPEN ID CONFIGURATION -->
<add key="openid-client-id" value="Azure directory (tenant) id
(GUID)" />
<add key="openid-application-id" value="Azure application id
(GUID)"/>
<add key="openid-client-secret" value="Azure application secret"/>
<add key="openid-callback-
url" value="http://${portalRoot}/Account/LogonCallback" />
<add key="openid-discovery-
endpoint"
 value="https://login.microsoftonline.com/${tenantId}/.well-
known/openid-configuration" />
<!-- USER MAPPING SETTINGS -->
<add key="openid-auto-user-roles" value="Registered User,My default
role" />
<add key="openid-auto-user-organization" value="ebs" />
<add key="openid-auto-user-businessunit" value="root" />
<add key="openid-auto-user-type" value="Back Office" />
<add key="openid-auto-user-remote-roles-add" value="0 or 1"/>
<add key="openid-auto-user-remote-roles-sync" value="0 or 1"/>
<!-- END AzureAD IDOPEN ID CONFIGURATION -->
```

To find the *Azure directory (tenant) id (GUID)* and the *Azure application id (GUID)*:

1. Open the **Azure Portal**.
2. Select the **App registrations** service.
3. Select the application you wish to use as a source for identity credentials.
4. The *Azure directory (tenant) id (GUID)* and the *Azure application id (GUID)* will be displayed in the Overview section of the application.




### Configuration Keys

| Parameter | Value |
|---|---|
| `openid-auto-user-roles` | Platform role names, separated by colons. These roles will be added automatically when the Azure AD user is mapped to a FintechOS user. |
| `openid-auto-user-organization` | Platform organization name. The mapped user will be added in this organization. |
| `openid-auto-user-businessunit` | Platform business unit name. The mapped user will be added in this business unit. |
| `openid-auto-user-remote-roles-add` | When set to 1, the roles from Azure AD will be added to the mapped user on user creation, adding the roles found in the values for web.config key="openid-auto-user-roles" (has effect only at user creation). See below how to expose the Azure AD roles in custom claims consumable by FintechOS. Azure AD will be added to the mapped user, |
| `openid-auto-user-remote-roles-sync` | When set to 1, the roles from Azure AD and the default roles are always synchronized at login. Any roles manually added to Azure AD user are lost. |

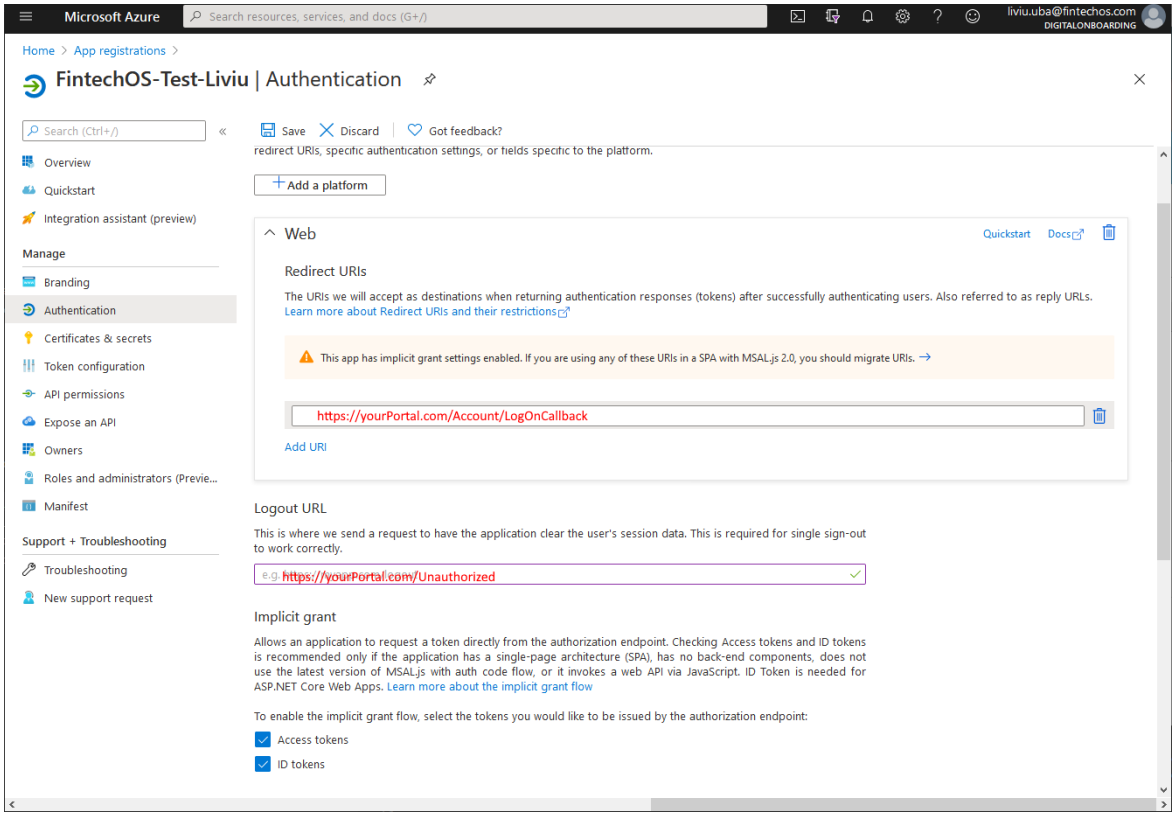
**Parameters**

| Parameter | Value |
|---|---|
| `${portalRoot}` | Root URL for the FintechOS web service. |
| `${tenatnId}` | Azure tenant ID. |

## Set up Login/Logout Redirect URIs

In the Azure Portal, in the Authentication section of your registered application, fill in the:

- Login redirect URI: `{$portalRoot}/Account/LogonCallback`
- Logout redirect URI: `{$poratalRoot}/Unauthorized`

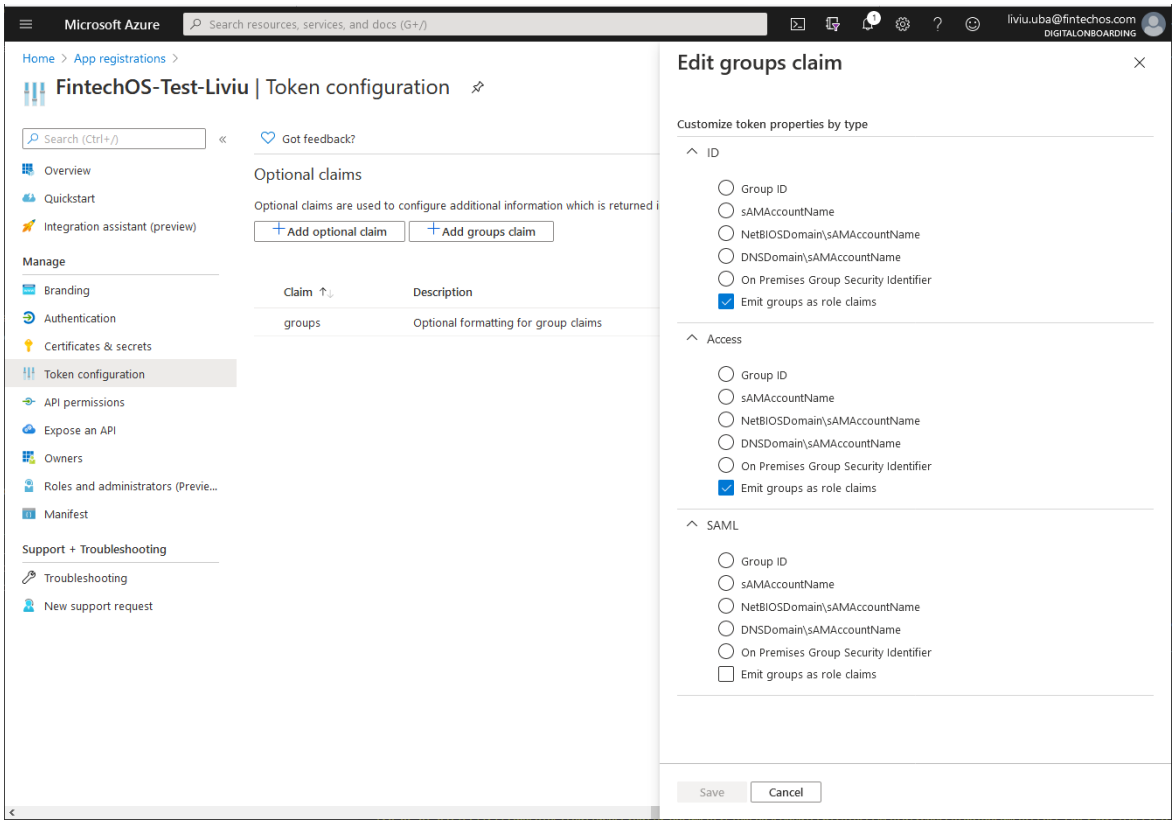



## Groups Mapping

When a user is authorized with Azure AD, a corresponding system user is created in FintechOS. Default roles for this user, organization, business unit, and user type can be configured in *web.config*. Any Security Role which has not already been created in

the system and is mentioned in OpenIdUserConfiguration.xml it will be automatically created.

To synchronize groups created in Azure AD with FintechOS, the administrator of the Azure AD application must include an optional claim named **groups** in the token configuration.




To configure the mappings, an XML file named *OpenIdUserConfiguration.xml* must be placed in the root folder of the web application. Azure AD sends group IDs with the OpenID token, so the mapping must be done between the Azure Group ID and QWPlatform security roles.

```
<root>
    <SecurityGroup>
        <Name>b681734a-5601-435c-b817-465f8e20b7fb</Name>
        <DisplayName>GROUP1</DisplayName>
        <DefaultBusinessUnitName>root</DefaultBusinessUnitName>
        <SecurityRoleName>Registered Users</SecurityRoleName>
    </SecurityGroup>
        ...
```

```
    <SecurityGroup>
        <Name>84d47d54-0956-4f9a-b37d-81880374fd46</Name>
        <DisplayName>GROUP2</DisplayName>
        <DefaultBusinessUnitName>root</DefaultBusinessUnitName>
        <SecurityRoleName>Developer,Registered
Users</SecurityRoleName>
    </SecurityGroup>
</root>
```

**IMPORTANT!**
Any changes to `OpenIdUserConfiguration.xml` require a manual Application Domain restart.

## Logging to Azure AppInsights

This authentication method makes it possible to write the logs in the cloud and no longer store them in the local file **trace.log**. For this process to be possible you need a Azure AppInsights subscription is needed beforehand. The logs can arrive from several machines in a cluster and be put in the same place.

Logs with level <= Warning: Information, Debug,etc are saved to traces.

Logs with level = Exception or Fatal are saved to exceptions.

Application specific information saved with the log message as part of custom dimensions:

MachineName

CorrelationId

Language

AutomationScript

AutomationScriptLibrary

SQL

ExtraErrorDetails

# Example

To write the logs in the cloud:

```
<appSettings>
...
<add key="feature-logging-azure-appinsights"
value="enabled=1; apiKey=API_KEY; logLevel=Warning; flushInterval=1m">
...
</appSettings>
```

| Field | Default value | Description |
|---|---|---|
| enabled | boolean | 0 (enables or disables Azure logging, to be specified as truthy or falsy values: true, false, on, off, 0, 1). |
| apiKey | guid string | empty (Instrumentation Key provided by your Azure AppInsights subscription). |
| logLevel | string | Error (Minimum log level for the application. Possible values: Fatal, Error, Warning, Information, Debug, Verbose). |
| flushInterval | timespan | 1m (delay between message batches sent to Azure, to be specified in .NET Timespan format or in 1h, 1d, 1h30m etc.). |

# Authentication with Okta

Okta is a standards-compliant OAuth 2.0 authorization server and a certified OpenID Connect provider.

FintechOS built-in integration with Okta enables users to log in to the Digital Experience Portal using the Okta single-sign on (SSO).

## How to Set up the Okta Authentication

To set up the Okta authentication for your Experience Portal, follow these steps:

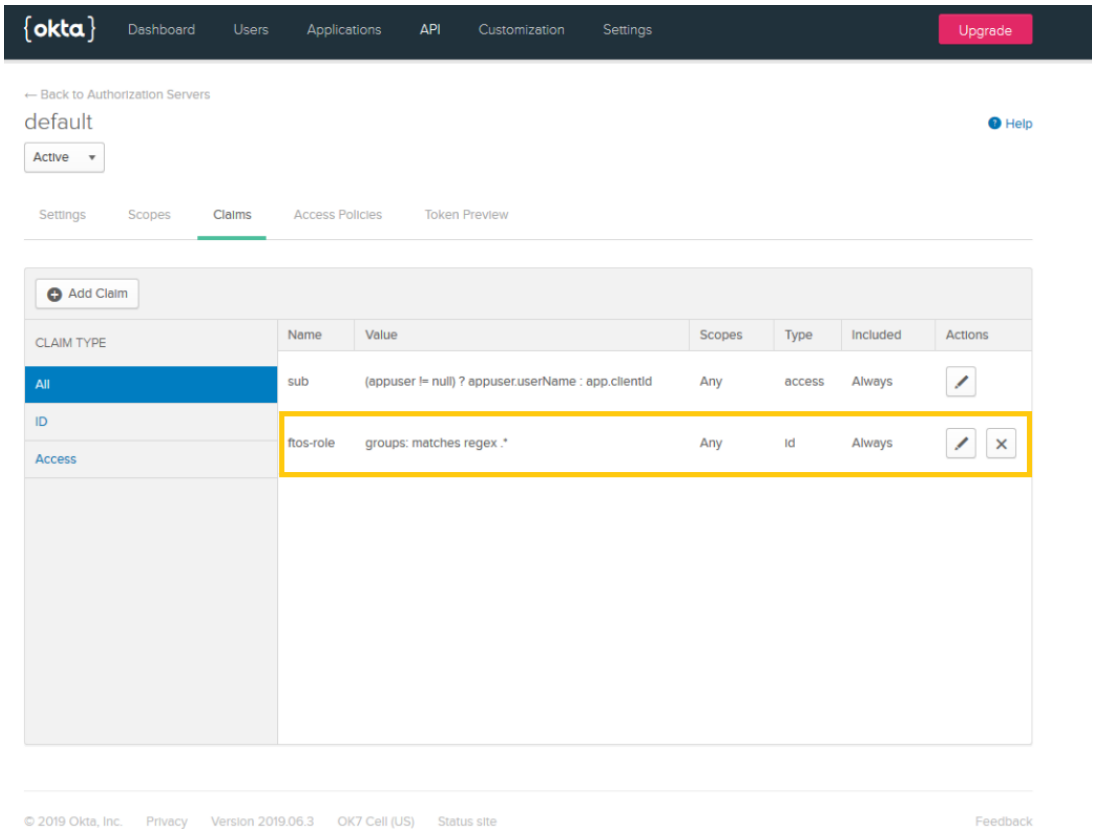
#### Step 1. Create and configure the Okta app

1. Using an Okta admin account, log into Okta and create an Okta application (Application tab > Web > OpenID Connect).
2. From the Applications tab > General > Login, set up the FintechOS callbacks by configuring both the login and the logout redirect URLs, as follows:

| | |
|---|---|
| login redirect uri | **{$portalRoot}/Account/LogonCallback** |
| logout redirect uri | **{$portalRoot}/Unauthorized** |

3. From the **API** tab > **Authorization Servers**, create an authorization server for the Okta application.
4. Expose the Okta roles in custom claims consumable by FintechOS. To do so, synchronize the user groups created in Okta with FintechOS by creating a custom claim named **ftos-role** mapped to the group metadata in Okta. For more information on how

to create a custom claim in the Okta app, see Okta Documentation.




When a user is authorized with Okta, a corresponding system user will be created in FintechOS . In the **web.config** file you can configure default roles for this user, organization, business unit and user type.

#### Step 2. Configure the Experience Portal

**Prerequisite**:

Make sure that you know the following values:

- Client ID (from the Okta app, General tab)
- Client Secret (from the Okta app, General tab)
- Discovery Endpoint (from the Okta app, API section > Authorization Servers > Metadata URL)

In the **web.config** file, go to the <appSettings> section and add the configuration of your Okta appplication:

```
<!-- 1. Set Okta authentication-->
<add key="EBSDefaultAuthentication" value="Okta" />

<!-- 2. Replace these values with your Okta configuration: -->
<add key="openid-client-id" value="{ClientId}" />
<add key="openid-client-secret" value="{ClientSecret}" />
<add key="openid-callback-
url" value="http://${portalRoot}/Account/LogonCallback" />
<add key="openid-discovery-
endpoint"

value
="https://${oktaApplication}.okta.com/oauth2/${authServerId}/.well-
known/oauth-authorization-server" />

<!-- 3. Map user settings: -->
<add key="openid-auto-user-roles" value="Guest,Developer,Registered
Users" />
<add key="openid-auto-user-organization" value="ebs" />
<add key="openid-auto-user-businessunit" value="root" />
<add key="openid-auto-user-type" value="Back Office" />

<add key="openid-auto-user-remote-roles-add" value="0|1"/>
<add key="openid-auto-user-remote-roles-sync" value="0|1"/>
```

The table below describes the Okta app configuration keys:

| Key | Description |
|---|---|
| ${portalRoot} | The root URL of the Experience Portal. |
| ${authServerId} | The ID of the authorization server associated with the Okta application (default value is default). |
| ${oktaApplication} | The ID of the Okta application. |
| Key | Description |

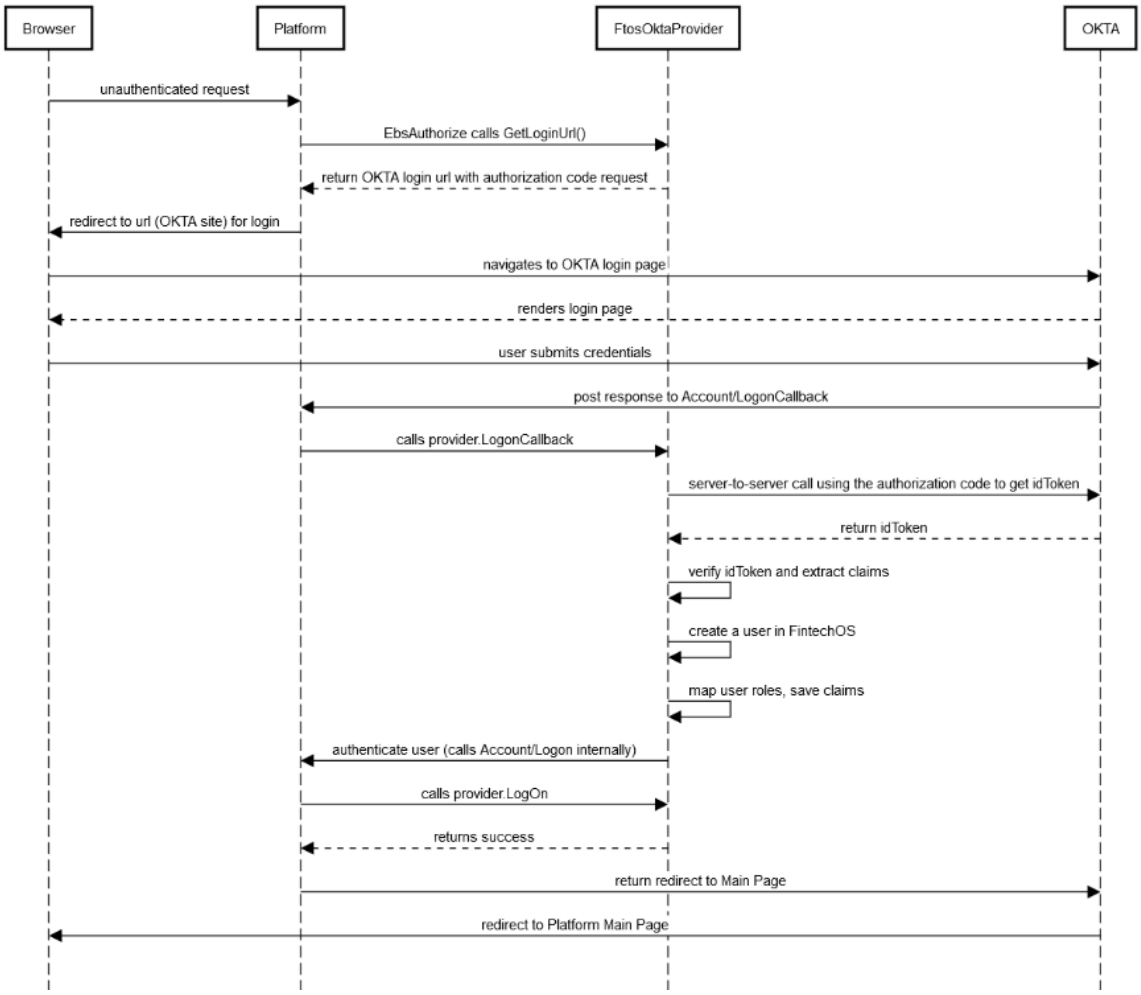
The table below describes the user mapping configuration keys.

| Parameter | Value |
|---|---|
| openid-auto-user-roles | The platform role names, separated by colon. These roles will be added automatically when the Okta user is mapped to a platform user. |
| openid-auto-user-organization | The platform organization name. The mapped user will be added in this organization. |
| openid-auto-user-businessunit | The platform business unit name. The mapped user will be added in this business unit. |

| Parameter | Value |
|---|---|
| openid-auto-user-remote-roles-add | If set to 1, the roles from the Okta app will be added to the mapped user. |
| openid-auto-user-remote-roles-sync | If value is 1, the roles from Okta and the default roles are always synchronized at login. Any roles manually added to a Okta user are lost. |

## How it Works

The diagram below describes the FintechOS login flow when using Okta authentication.



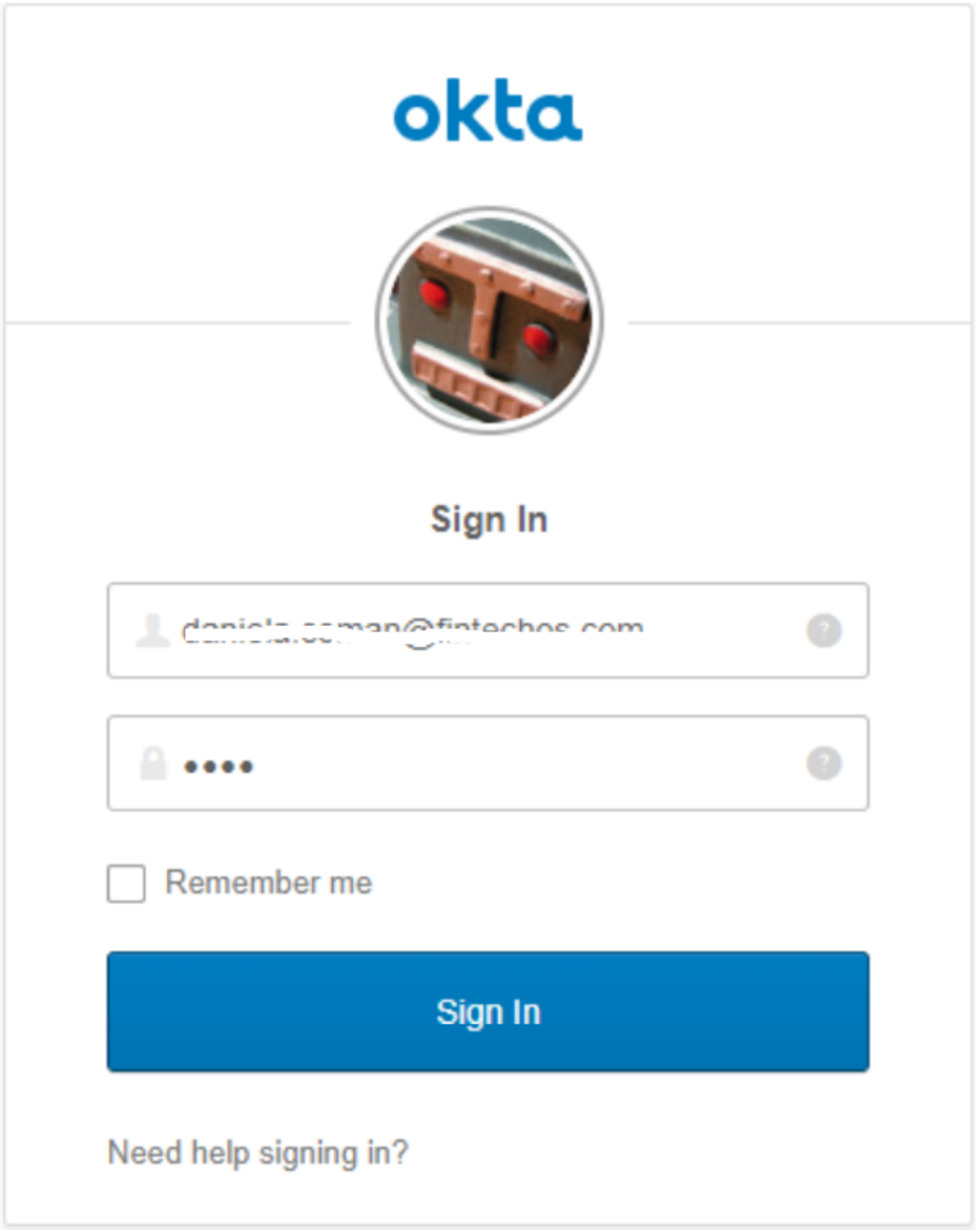
## Group mapping in FintechOS

When a user is authorized with Okta, a corresponding system user is created in FintechOS. In web.config file of the FintechOS instance, default roles for this user, organization, business unit and user type are added.

Create a custom claim named **ftos-role** mapped to the group metadata in Okta. This configuration is done for the authorization server associated with the Okta application.

## How users log in the Portal

When accessing the Digital Experience Portal URL, users will be redirected to the URL of the authorization server associated with the Okta app. The Okta login page appears.




Once they provide Okta account credentials, they will be logged into the Digital Experience Portal.

When new users are created, they will receive an email notification from Okta which contains instructions and Okta credentials.

# Troubleshooting Okta Redirect Error

### Error

UnhandledException: System.Web.HttpException (0x80004005): Server cannot set status after HTTP headers have been sent.

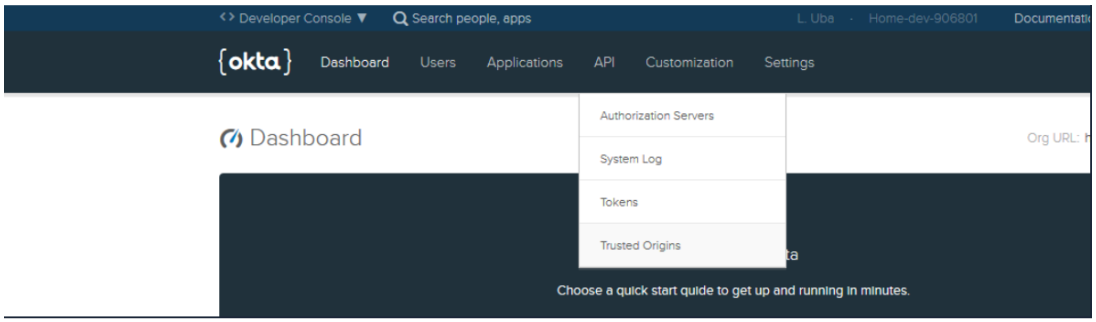
### Cause

FTOS OpenID provider does not redirect when the user is still logged in due to the OpenID cookie not being expired too.

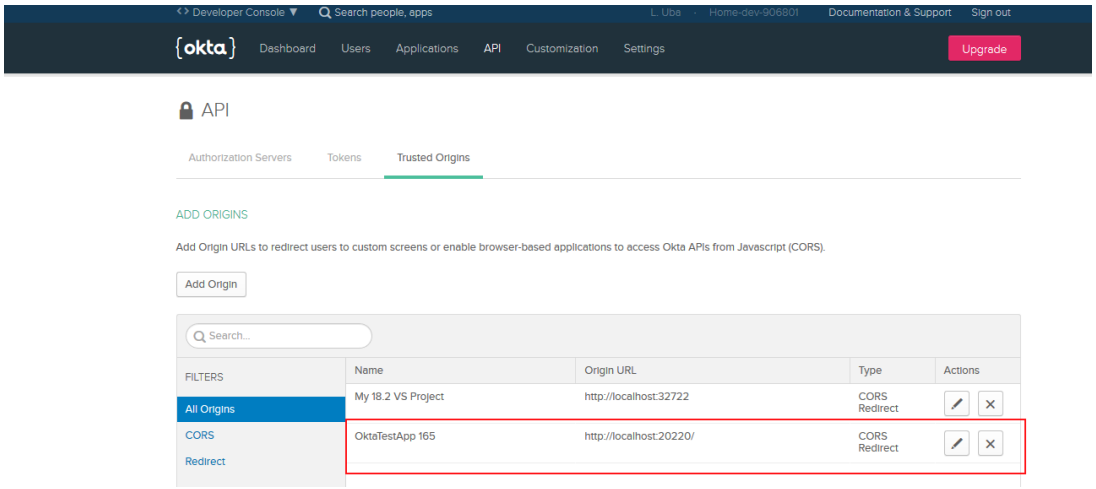
### What should I do?

For session expiration to work seamlessly, follow these steps:

1. Using an Okta admin account, log into Okta.
2. Click API tab > Trusted Origins.




3. Allow CORS and Redirect for FTOS portal host.



# Authentication with Active Directory Federation Services

This service provided by Microsoft manages the user sign-in information for members of a platform. If your organization is using ADFS for identity and access management of your users, it is possible to map the users already existing in ADFS to FintechOS Security Roles. When a user is authorized with ADFS, a corresponding system user is created in FintechOS. Through ADFS OpenId, users to log in to FintechOS using their existing ADFS credentials.

## Add keys to the web.config file

```
<add key="EBSDefaultAuthentication" value="ADFS" />

    <!-- BEGIN ADFS OPENID CONFIGURATION -->

    <add key="openid-client-id" value="Client identifier configured
in ADFS" />

    <add key="openid-application-id" value=" this value is not used
"/>
    <add key="openid-client-secret" value="ADFS Web API shared
secret"/>

    <add key="openid-callback-url" value="http://
{portalRoot}/Account/LogonCallback" />

    <add key="openid-discovery-endpoint" value="{adfs server
uri}/adfs/.well-known/openid-configuration" />

    <!-- USER MAPPING SETTINGS -->

    <add key="openid-auto-user-roles" value="Registered User,My
default role" />
    <add key="openid-auto-user-organization" value="ebs" />
    <add key="openid-auto-user-businessunit" value="root" />
    <add key="openid-auto-user-type" value="Back Office" />

    <add key="openid-auto-user-remote-roles-add" value="0|1"/>
    <add key="openid-auto-user-remote-roles-sync" value="0|1"/>

    <!-- END ADFS OPENID CONFIGURATION -->
```

**Configuration Keys:**

| Key | Value |
|---|---|
| openid-auto-user-roles | Platform role names, separated by colon. These roles will be added automatically when the AD user is mapped to a platfrom user |
| openid-auto-user-organization | Platform organization name. The mapped user will be added in this organization |
| openid-auto-user-businessunit | Platform business unit name. The mapped user will be added in this business unit |
| openid-auto-user-remote-roles-add | when value is 1 the roles from AD will be added to the mapped user on user creation. See below how to expose the AD roles in custom claims consumable by FintechOS |
| openid-auto-user-remote-roles-sync | when value is 1 the roles from AD and the default roles are always synchronized at login. Any roles manually added to a AD user are lost |

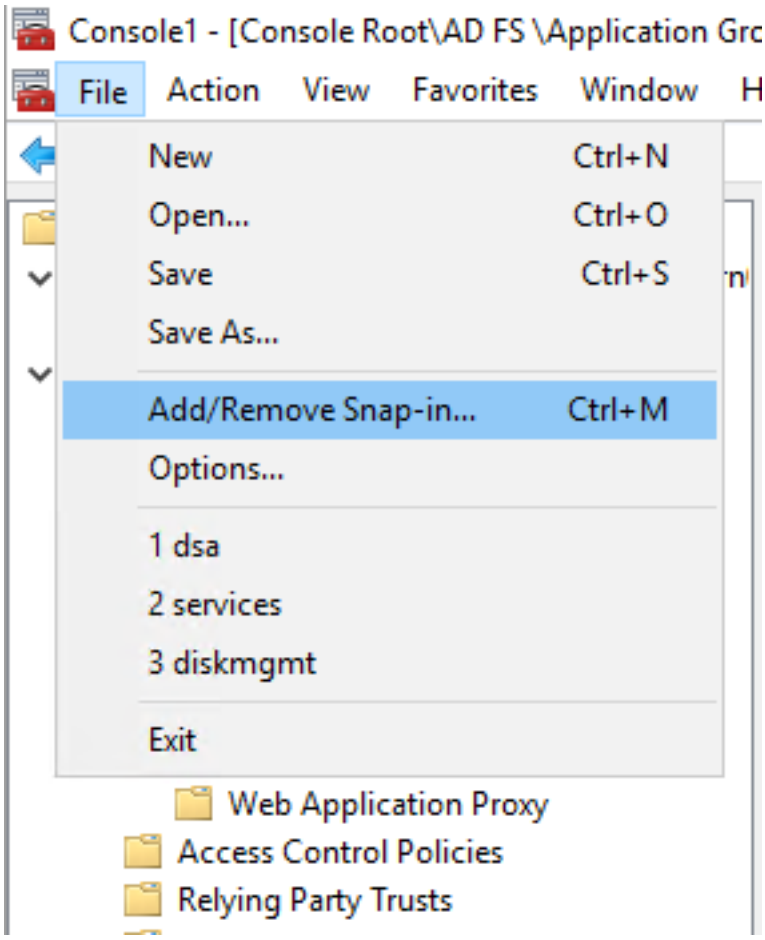
**Parameters:**

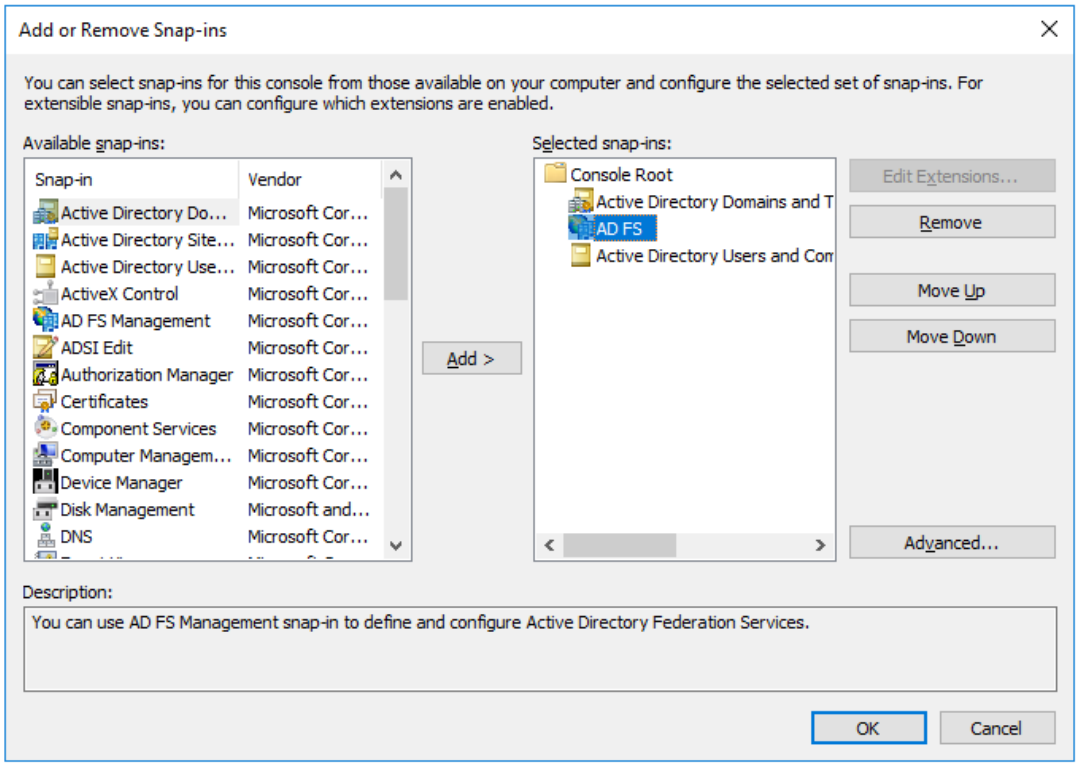
| Parameter | Value |
|---|---|
| {portalRoot} | root url for FintechOS portal |
| {adfs server url} | ADFS server url |

## ADFS configuration

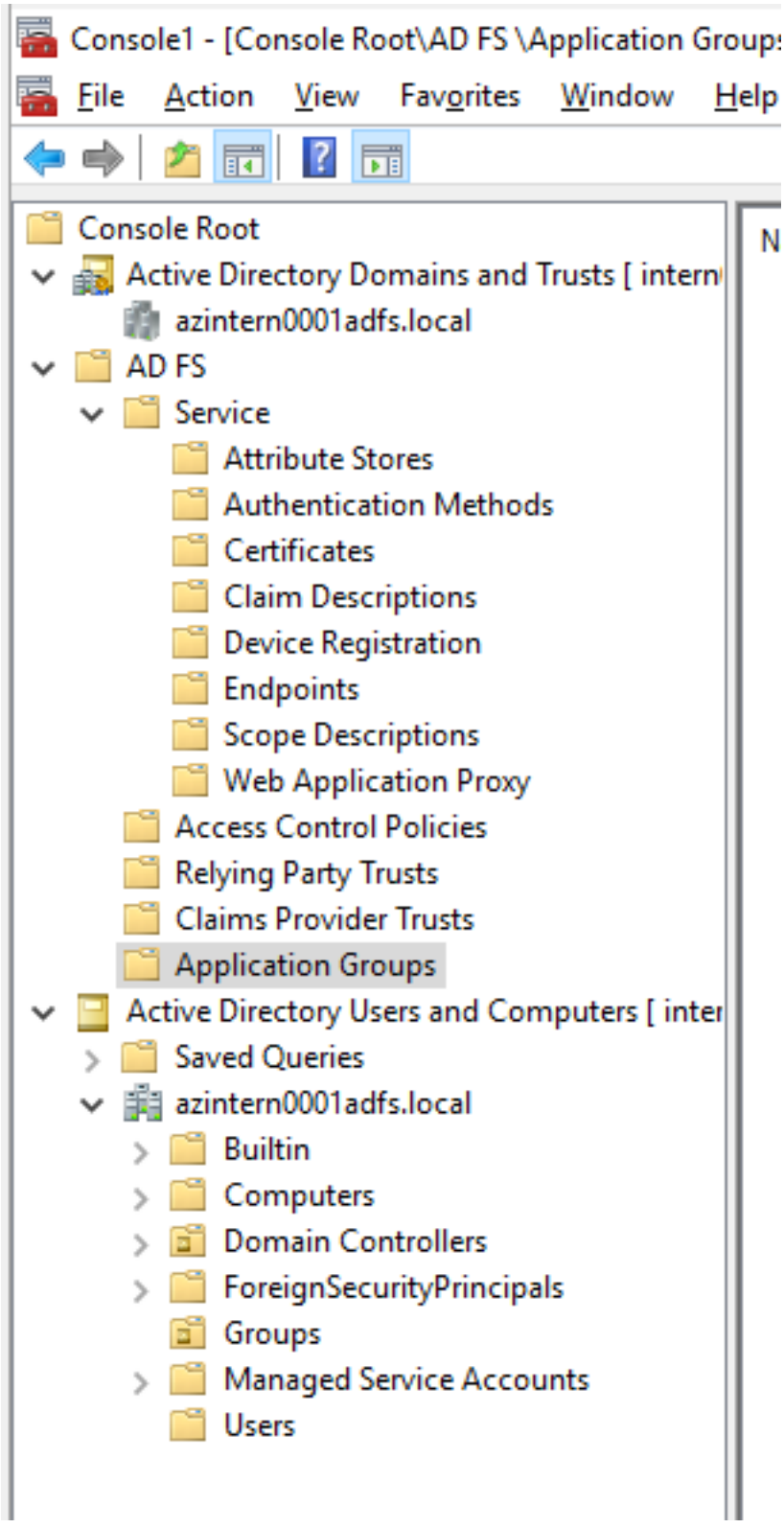
1. On a Windows Server 2016+, on the ADFS server open the Microsoft Management Console (mmc).

2. Add the ADFS snap in if not already added.

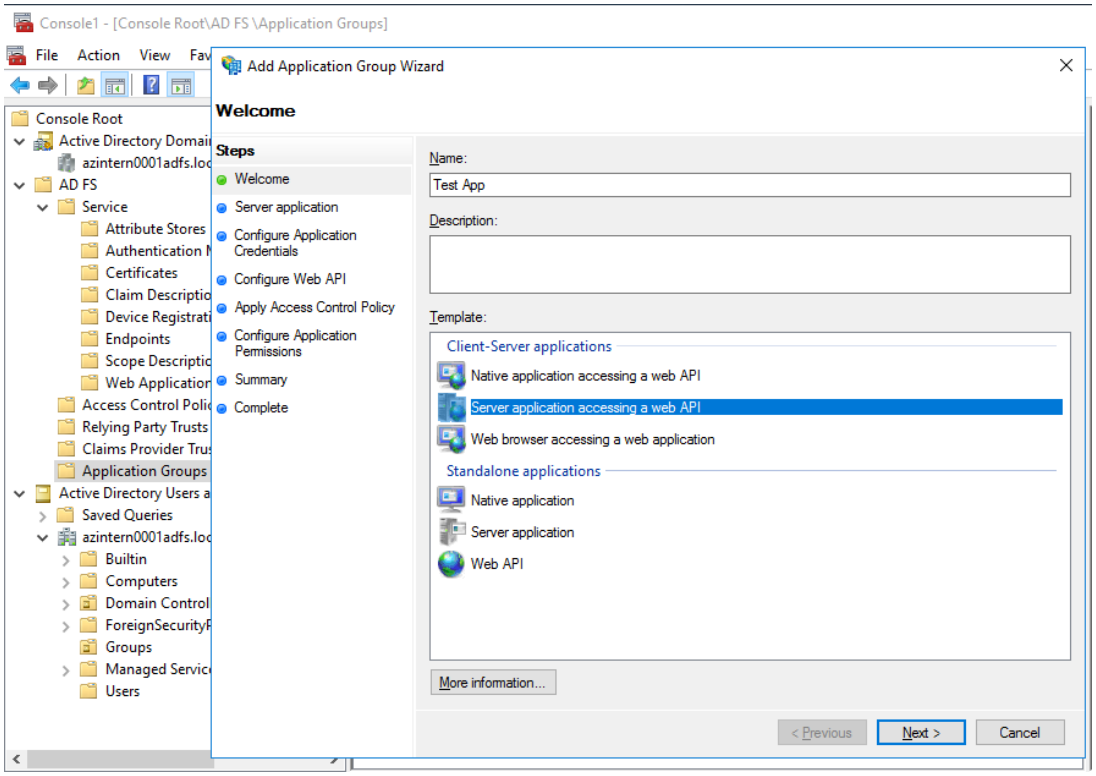





3. Open the ADFS MMC plugin and select the node Application Groups.

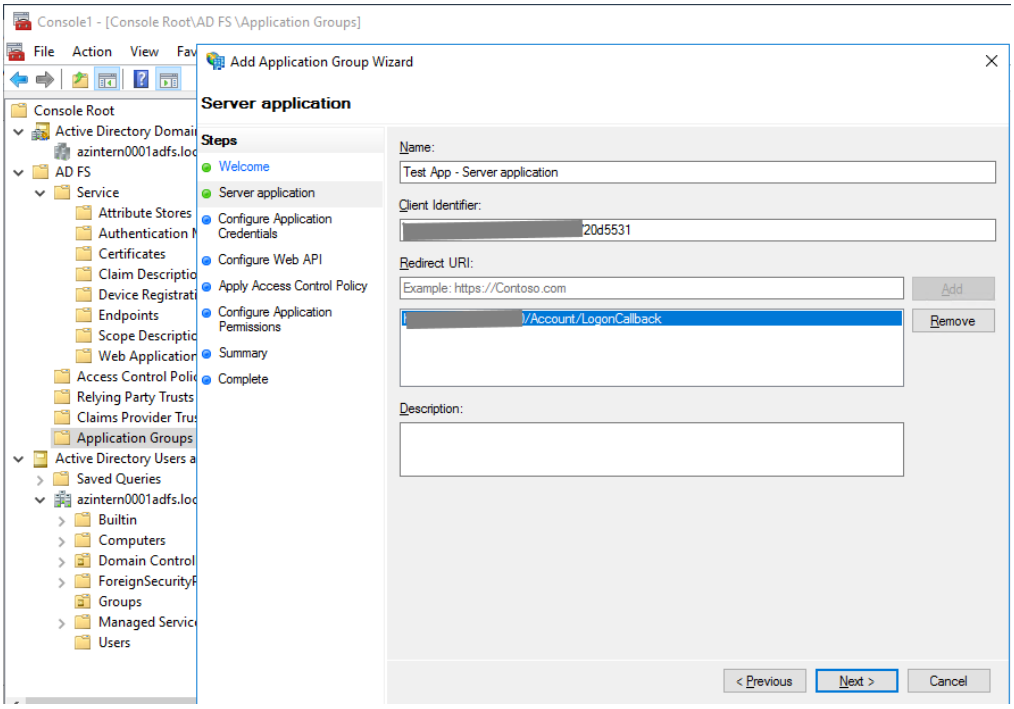

Console1 - [Console Root\AD FS \Application Groups
File Action View Favorites Window Help
Console Root
Active Directory Domains and Trusts [ intern
azintern0001adfs.local
AD FS
Service
Attribute Stores
Authentication Methods
Certificates
Claim Descriptions
Device Registration
Endpoints
Scope Descriptions
Web Application Proxy
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Active Directory Users and Computers [ inter
Saved Queries
azintern0001adfs.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Groups
Managed Service Accounts
Users

4. Right click and select Add application group. In the template list select Server application accessing a web API.

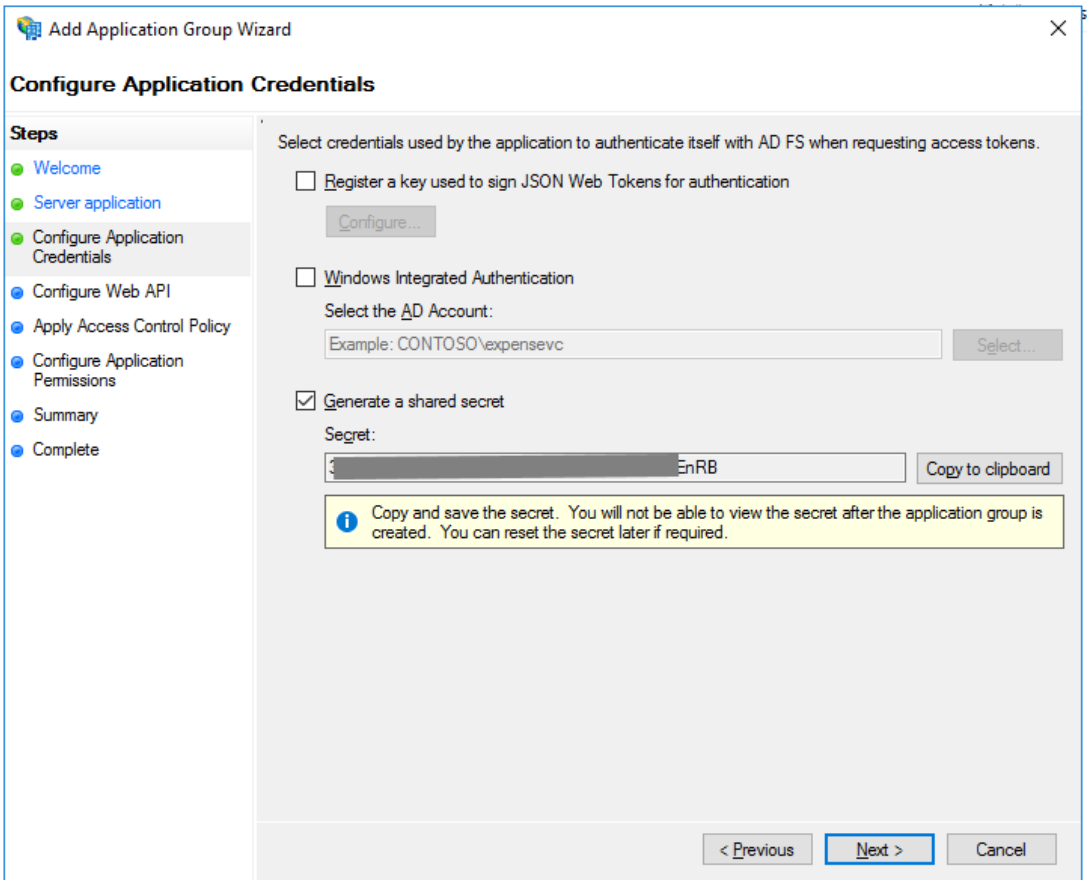



- Configure the client identifier and the redirect (callback) Url.
- Client identifier should be an global unique identifier. This value must be set in the openid-client-id configuration item in FintechOS.
- Redirect (callback) Url must be also be set in the openid-callback-url

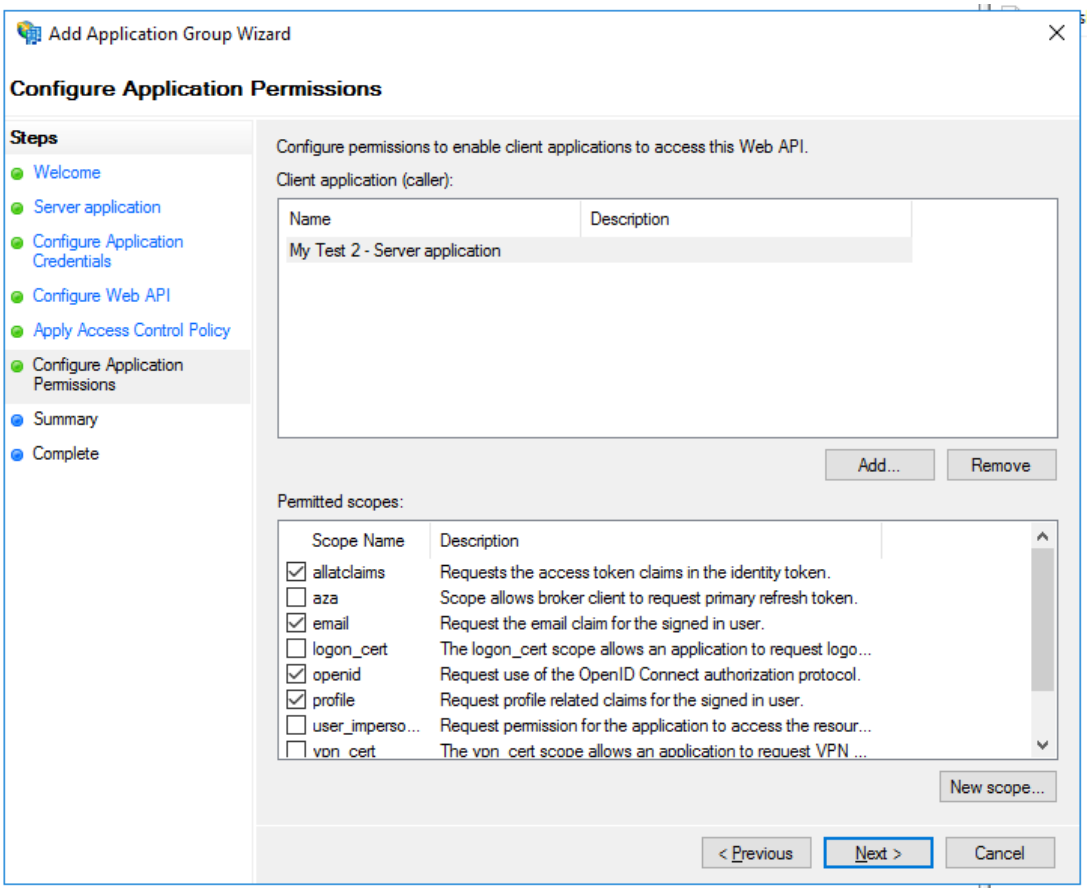
configuration item in FintechOS.




5. Configure the shared secret. The shared secret must be set also in the openid-client-secret configuration item in FintechOS.


Add Application Group Wizard
Configure Application Credentials
Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.
Register a key used to sign JSON Web Tokens for authentication
Configure...
Windows Integrated Authentication
Select the AD Account:
Example: CONTOSO\expensevc
Select...
Generate a shared secret
Secret:
[redacted]EnRB
Copy to clipboard
Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.
< Previous
Next >
Cancel

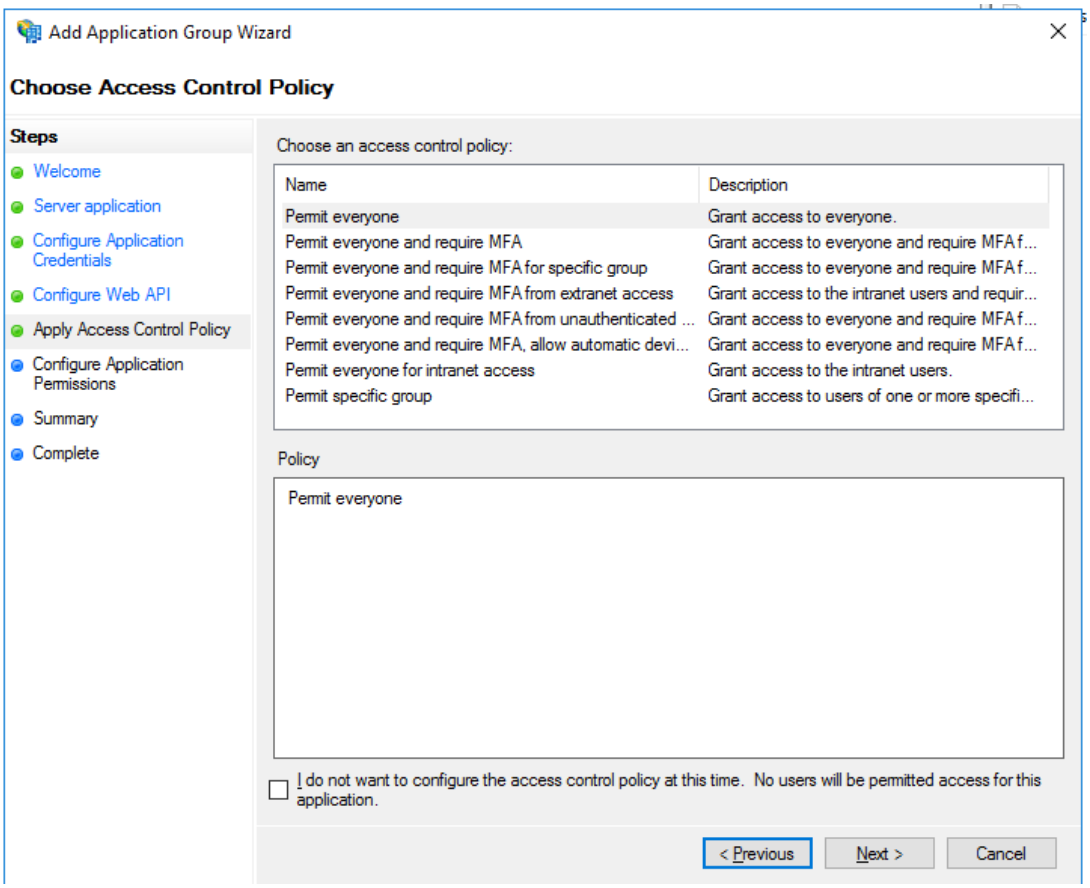
6. Configure the Web API identifier




**IMPORTANT!**

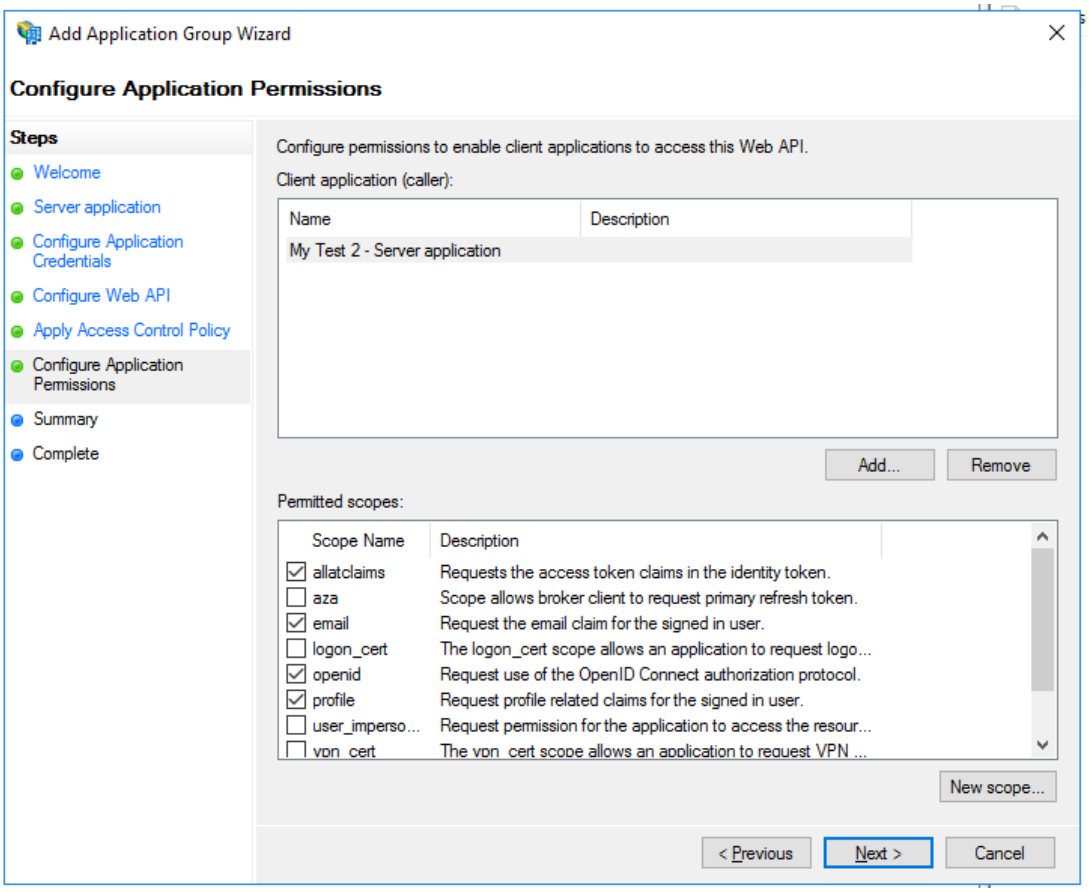
The Web API identifier must be THE SAME identifier as the one used for the CLIENT IDENTIFIER in the first step.

7. Configure Access Control Policy.




8. Configure claims to be sent with the openid token.

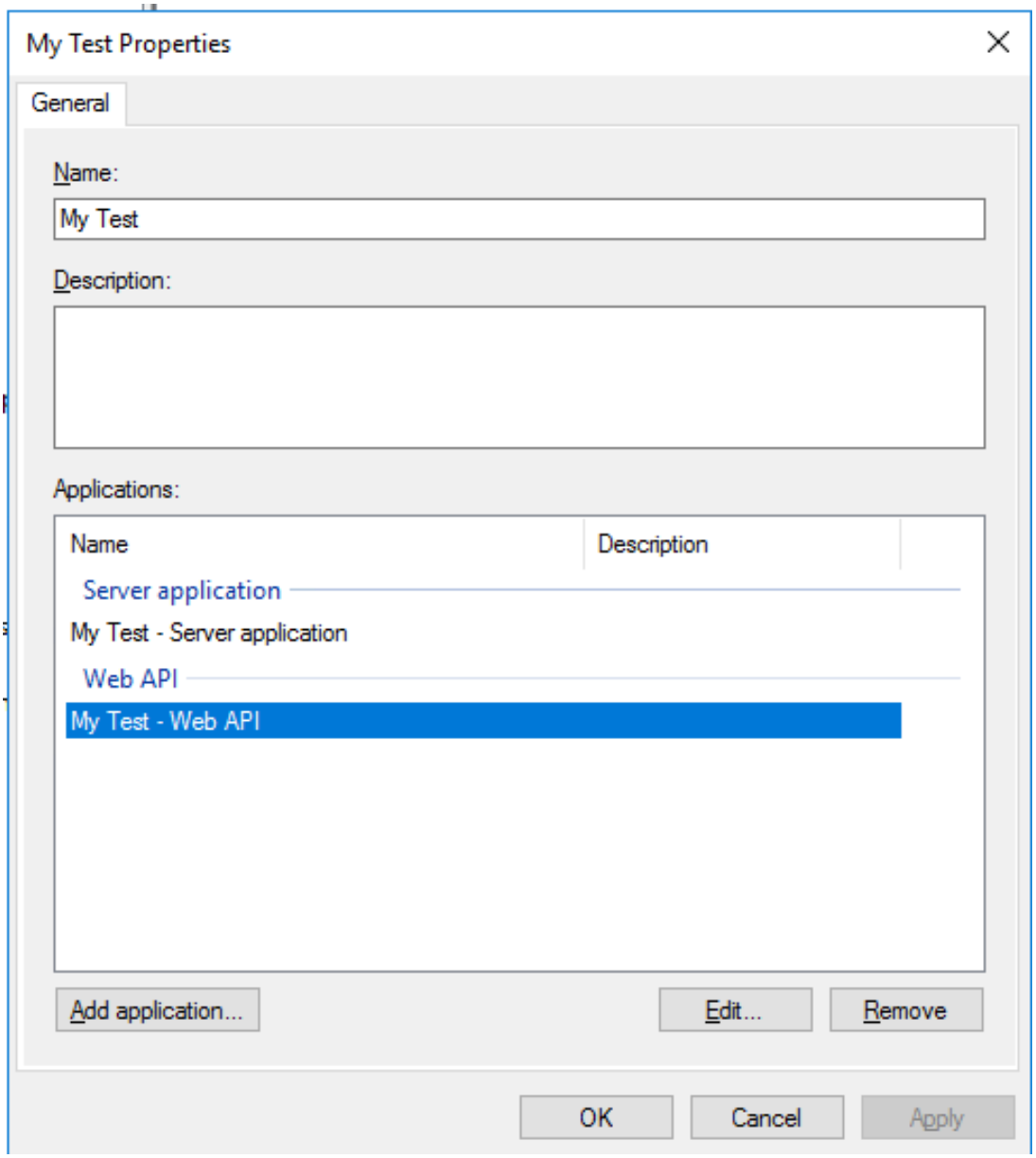
9. Following claims must be included: allatclaims, email, openid, profile.



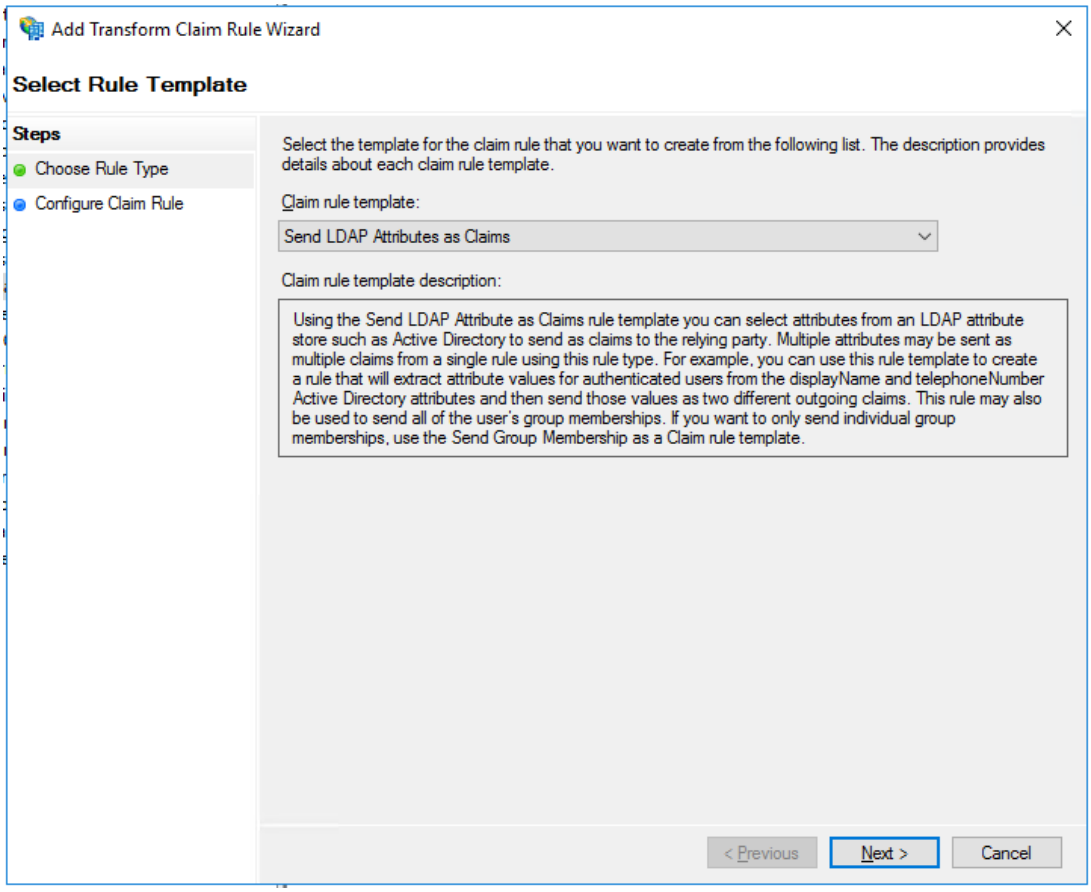

10. Review the configuration in the Summary step and go to Complete step.

> **IMPORTANT!**
>
> In the following steps we need to expose the GROUP INFORMATION, EMAIL, GIVEN NAME and SURNAME information from AD directory to be included in the claims. This will permit the correct mapping of the users to FintechOS.

11. Double click the newly created Application Group.

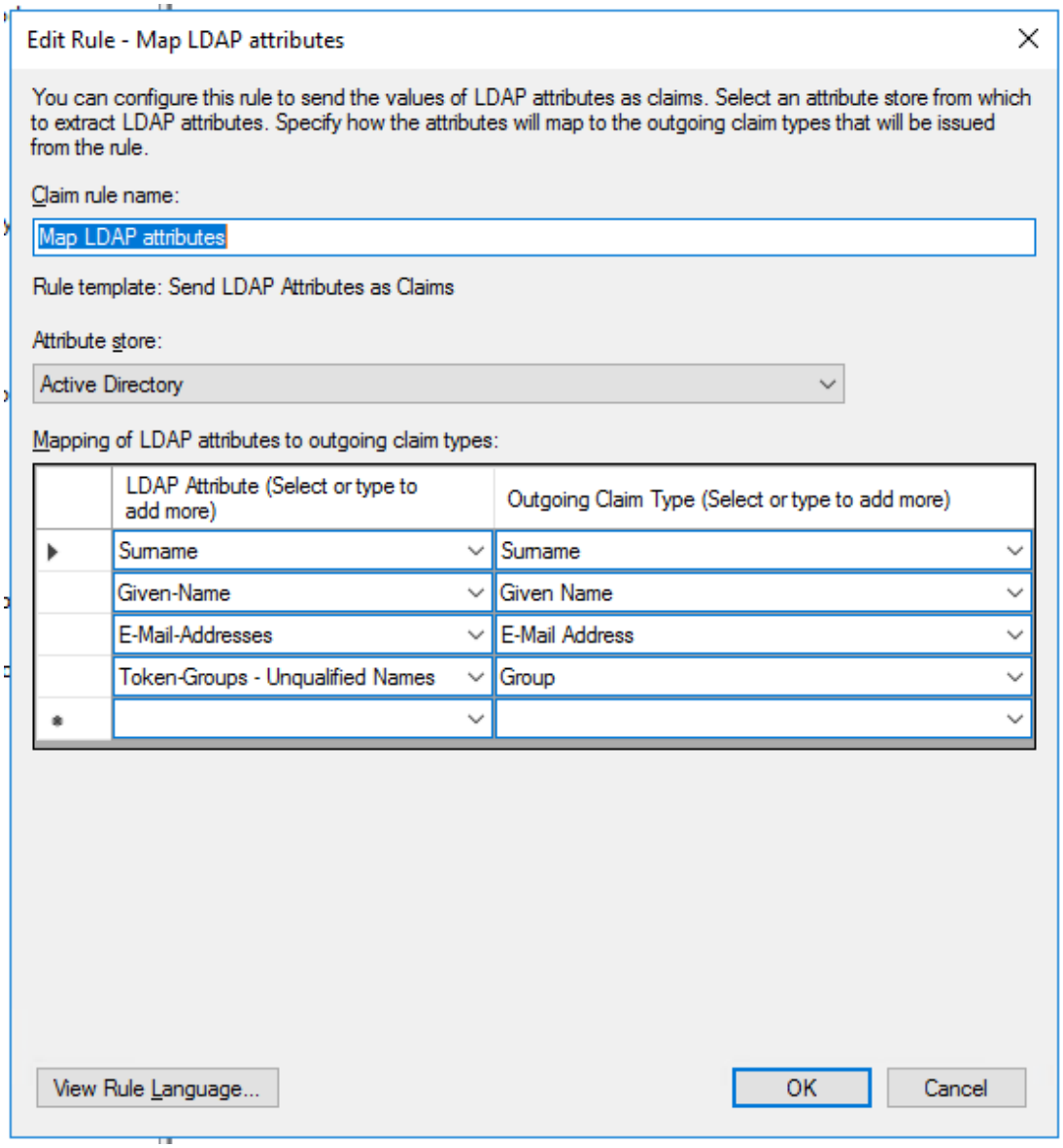


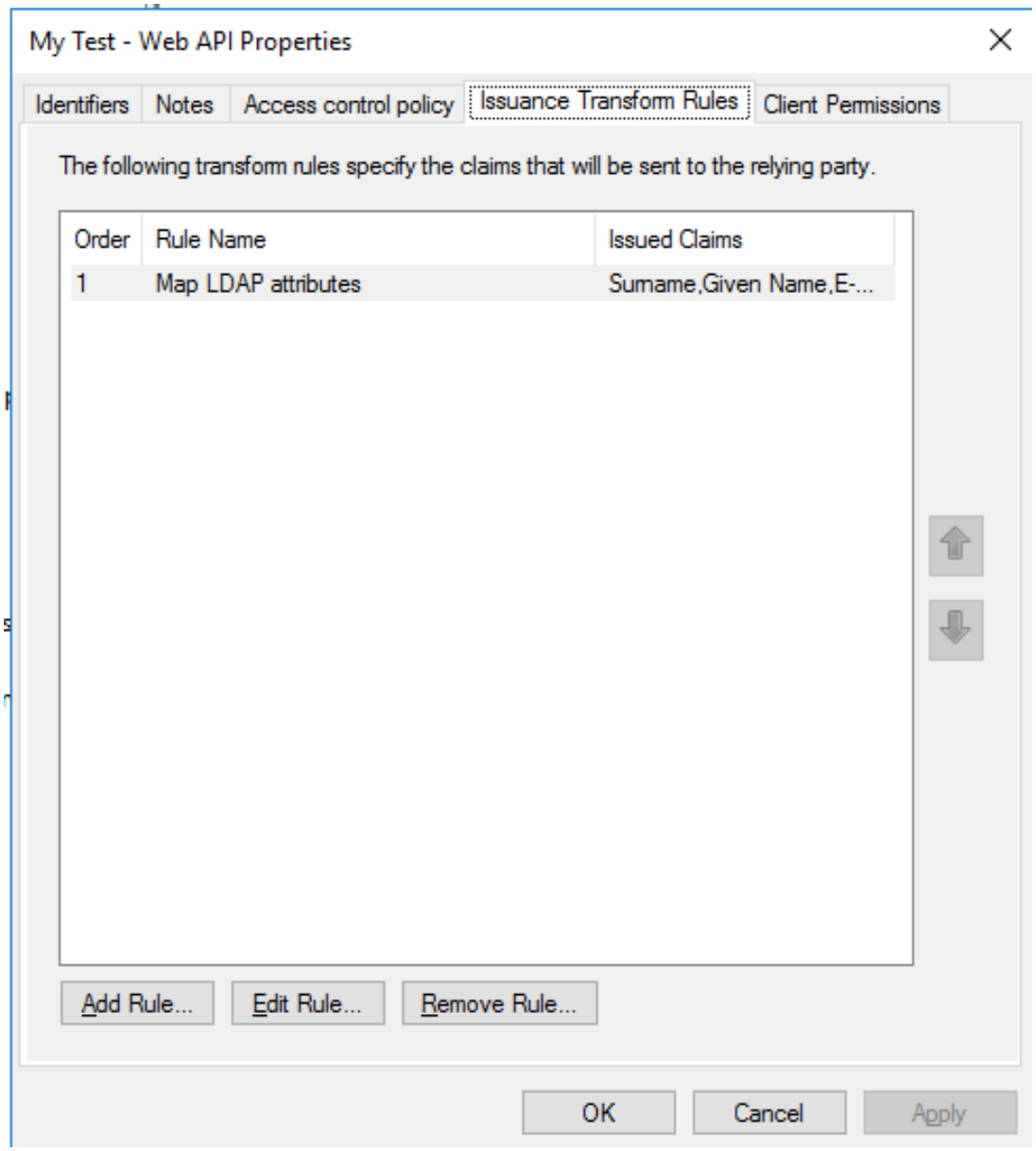
12. Select the Web API element and click the Edit... button.




13. Go to tab Issuance Transform Rules and add a new rule of type Send LDAP Attribues in Claims

14. Map the AD attributes as in the image below:






## Group mapping in FintechOS

Once the system user has been created in the FintechOS Studio, it is possible to have default roles for this user, organization, business unit and user type configured in web.config.

To configure the mappings, an XML file named OpenIdUserConfiguration.xml must be placed in the root of the web application. When the ADFS configuration was performed as in the section above, the ADFS token for an user authentication will include a group claim with the names of the Groups where the user is member from AD.

## Authentication with AWS Cognito

This service provided by Amazon Web Services manages the user sign-in information for members of a platform. If your organization is using AWS Cognito for identity and access management of your users, it is possible to map the users already existing in AWS Cognito to FintechOS Security Roles. Through Azure AWS OpenId provider, users to log in to FintechOS using their existing AWS Cognito credentials.

### Add keys to the web.config file

In the web.config file of your environment add the following keys.

```
 <add key="EBSDefaultAuthentication" value="AWSCognito" />

    <!-- BEGIN AWS COGNITO IDOPEN ID CONFIGURATION -->

    <add key="openid-client-id" value="AWS Cognito client id xxxxx"
/>
    <add key="openid-client-secret" value="AWS Cognito client
secret yyyyyy" />

    <add key="openid-callback-
url" value="http://${portalRoot}/Account/LogonCallback" />

    <add key="openid-discovery-endpoint" value="https://cognito-
idp.xxx/.well-known/openid-configuration" />

    <!-- USER MAPPING SETTINGS -->

    <add key="openid-auto-user-
roles" value="Guest,Developer,Registered Users" />
    <add key="openid-auto-user-organization" value="ebs" />
    <add key="openid-auto-user-businessunit" value="root" />
    <add key="openid-auto-user-type" value="Back Office" />

    <add key="openid-auto-user-remote-roles-add" value="0"/>
```

```
    <add key="openid-auto-user-remote-roles-sync" value="0"/>

    <!-- END AWS COGNITO ID CONFIGURATION -->
```

**Configuration Keys:**

| Key | Value |
|---|---|
| openid-auto-user-roles | Platform role names, separated by colon. These roles will be added automatically when the AWS Cognito user is mapped to a platfrom user |
| openid-auto-user-organization | Platform organization name. The mapped user will be added in this organization |
| openid-auto-user-businessunit | Platform business unit name. The mapped user will be added in this business unit |
| openid-auto-user-remote-roles-add | not supported yet |
| openid-auto-user-remote-roles-sync | not supported yet |

**Parameters:**

| Parameter | Value |
|---|---|
| ${portalRoot} | root url for FintechOS portal |

## Group mapping for users

For each user in FintechOS, default roles can be created in the web.config file for this user, organization, business unit and user type.

1. An XML file named **OpenIdUserConfiguration.xml** must be placed in the root of the web application of FintechOS.

> **IMPORTANT!**
>
> Any changes to OpenIdUserConfiguration.xml require a manual Application Domain restart.

2. The ADFS token for an user authentication will include a group claim with the names of the Groups where the user is member from AD.

## Example:

```
<root>
    <SecurityGroup>
        <Name>GROUP1</Name>

<DefaultBusinessUnitName>root</DefaultBusinessUnitName>
        <SecurityRoleName>Registered
Users,Developers</SecurityRoleName>
    </SecurityGroup>
    ...

    <SecurityGroup>
        <Name>GROUP2</Name>

<DefaultBusinessUnitName>root</DefaultBusinessUnitName>
        <SecurityRoleName>GROUP2</SecurityRoleName>
    </SecurityGroup>
</root>
```

## Random Character Password Authentication

This method of authentication does not require the full password, only random characters are typed in by the user. This is done in order to mitigate potential "person in the middle" type of cyber attacks. The number of asked random characters is 3. For example, if the password is "MyPassword" the user might be asked to provide the chars on positions 1,3,6 ('M','P','s'). The positions (indexes) asked are different on

each attempt. The number of failed log-ins that block the user is 5. To support this, a new column was added to `EbsMetadata.SystemUser`, called `PartialPass`.This is populated by a json with the details necessary to validate the random character login.

Add the following setting in the web.config, under `<appSettings>` to enable the feature:

- ebsauth-partial-password to true (default this is false),
- within the keys that have the following structure:

```
<appSettings>
...
<add key="core-setting-ebsauth-partial-password" value="true"/>
...
</appSettings>
```

### Architecture

**1 Capture the Username**

In order to determine the password identity (such as the password length), the username is captured firstly. Once the identity is set, random characters can be extracted from the password.

**2 Generate the random characters**

When the user is asked to input random characters, they are from the entire range of the password, and not just the minimum required length.

## Multi-Factor Authentication

Multi-Factor Authentication (MFA) adds an extra layer of security on top of the basic authentication methods. It requires users to provide multiple proof of their claimed identity prior being granted access to resources based on business need to know according to their security role and granted permissions.

User access can be granted on two-factors:

- Something the user knows (login credentials): username and password.
- Something the user has (pass code received via an SMS/E-mail or mobile soft token).

When users access the app, they will be prompted to provide the login credentials associated with their FintechOS account. To make sure account access is protected, after the login credentials are provided, a one-time security pass code is sent to the user's phone (the phone number set in the user account profile) or email. Once the user enters the code received via the SMS/e-mail, access into the system is granted.

## SMS-based Two-Factor Authentication

SMS-based two-factor authentication is the most popular choice when it comes to multi-factor authentication as most users have their own mobile phones and have them handy when logging into apps.

#### How it works?

Users will be granted access to the FintechOS app following these two steps:

- Users will navigate to the FintechOS web app and they will provide their account credentials (username and password). Based on the app configuration, the credentials can be either local or from external providers. To make sure account access is protected, after the login credentials are provided, a one-time security pass code is sent to the user's phone (the phone number set in the user account profile).
- In the web app, they provide the pass code received via SMS. Access into the system is granted.

#### How to set up the SMS-based MFA?

Setting up the SMS-based multi-factor authentication is a two-step process:

##### 1 Enable Multi-Factor Authentication

On the server where the FintechOS installation package resides, go to the **web.config** file and add the following settings:

- To the **<configSections>** tag, add the **multifactorAuthentication** section:

```
<configuration>
    <configSections>
        ...
         <section name="multiFactorAuthentication" type=
"EBS.Core.Authentication.Common.MultiFactorAuthentication.Co
nfig.MultiFactorAuthenticationSection,
EBS.Core.Authentication.Common" />
    </configSections>
<configuration>
```

- Add the **<multiFactorAuthentication>** tag:

```
<configuration>
...
    <multiFactorAuthentication
xmlns
=
"http://fintechos.com/ebs/schemas/multiFactorAuthentication"
 enabled="true">
        <providers>
            <provider
name="SMS" enabled="true" default="true">
                <type fullName=
"EBS.Core.Web.MVC.Security.SmsMultiFactorAuthenticationProvi
der, EBS.Core.Web.MVC" />
                <properties>
                    <property
name="ChannelProvider" value="GatewaySmsOTP" />
                    <property
name="CommunicationChannel" value="Sms" />
                    <property
name="MaxNumberOfAuthenticationRetries" value="3" />
                    <property
name="MaxNumberOfSmsSendings" value="3" /> </properties>
            </provider>
        </providers>
        <runtime>
            <providers>
                <provider name="SMS">
                    <roles>
                        <role name="*" /> </roles>
                </provider>
            </providers>
        </runtime>
```

```
    </multiFactorAuthentication>
</configuration>
```

Where:

- `multiFactorAuthentication/@enabled` - controls if MFA is enabled or not. Default value: false;
- `multiFactorAuthentication/providers/provider/@enabled` - controls if a specific MFA provider is enabled or not. Default value: true;
- `multiFactorAuthentication/providers/provider/@default`
  - When MFA is enabled, there can be at most one provider marked with default="true".
  - The provider marked with default="true" will be selected for MFA when there are multiple providers available for user's roles and the user hasn't selected any preferred communication channel or his preferred communication channel is not present into the configured providers list.
  - Default value: false.
- on `multiFactorAuthentication/providers/provider/properties`:
  - `ChannelProvider` - the channel provider used by the SMS MFA provider to send text messages. Its value must be the Name of one of the records from **EbsMetadata.FTOS_DPA_ChannelProvider** table;
  - `CommunicationChannel` - the communication channel used by the SMS provider to send text messages. Its value must be the Name of one of the records from **EbsMetadata.FTOS_DPA_CommunicationChannel** table;
  - `MaxNumberOfAuthenticationRetries` - the user has up to MaxNumberOfAuthenticationRetries chances to enter the correct code. If this threshold is reached the user will be redirected to the login page. Default value: **3**;

- `MaxNumberOfSmsSendings` - if needed the user may request a resending of the code for up to MaxNumberOfSmsSendings times. If this threshold is reached the user will be redirected to the login page. Default value: **3**;

- `multiFactorAuthentication/runtime/providers/provider[@name='SMS']/roles` will include a <role name=""/> child for each role that contains users that have to be authenticated through this provider. Note that a `<role name="*"/>` means that all roles will be taken into account;

If the multi-factor authentication is activated, at the next profile change, users will have to provide their phone number (in the Edit System User, My Account page, the Phone Number field is mandatory).

Once you've activated the SMS-based authentication, you need to configure the Job Server for Multi-Factor Authentication.

#### 2 Configure the Job Server for MFA

> **IMPORTANT!**
> The MessageBus (OCS) plugin for the FintechOS Job Server already includes the configurations required for multi-factor authentication (see the *FintechOS Installation Guide* for details about MessageBus (OCS) installation).
>
> - If you have the MessageBus (OCS) plugin installed, skip this step.
> - If you are using the standard Job Server configuration, follow the instructions below to configure the multi-factor authentication settings.

1. On the server where the FintechOS installation package resides, go to the **schedule.config** file and add the following section:

```
<triggers>
...
    <trigger>
        <name>FTOS.OCB.OTP</name>
        <startTime>02.11.2017 11:00</startTime>
        <endTime>03.11.2080 11:02</endTime>
```

```
        <repeatCount>-1</repeatCount>
        <rescheduleAfterRun>false</rescheduleAfterRun>
        <async>false</async>
        <expression>0/10 * * * * ?</expression>
        <services>

<service>FTOS.OCB.SendMessagesServiceSmsOTP</service>

<service>FTOS.OCB.UpdateStatusServiceSmsOTP</service>

<service>FTOS.OCB.UpdateExpiredMessageServiceSmsOTP</service>
        </services>
    </trigger>
</triggers>
```

2. On the server where the FintechOS installation package resides, go to the **services.config** file and add the following sections:

```
<serviceList>
...
    <!--OTP-->
    <service>
        <name>FTOS.OCB.SendMessagesServiceSmsOTP</name>
        <type>class</type>
        <method></method>

<
class
>
FTOS.MessageBus.ScheduledServices.SendMessagesService</class>

<assembly>FTOS.MessageBus.ScheduledServices</assembly>-->

<execParams>
provider=gateway;providerSetting=gatewaySmsOTP</execParams>
    </service>
    <service>
        <name>FTOS.OCB.UpdateStatusServiceSmsOTP</name>
        <type>class</type>
        <method></method>
        <class>
FTOS.MessageBus.ScheduledServices.UpdateStatusMessagesService
</class>

<assembly>FTOS.MessageBus.ScheduledServices</assembly>-->
```

```
<execParams>
provider=gateway;providerSetting=gatewaySmsOTP</execParams>
    </service>
    <service>

<name>FTOS.OCB.UpdateExpiredMessageServiceSmsOTP</name>
        <type>class</type>
        <method></method>
        <class>
FTOS.MessageBus.ScheduledServices.UpdateExpiredMessageService
</class>

<assembly>FTOS.MessageBus.ScheduledServices</assembly>-->

<execParams>
provider=gateway;providerSetting=gatewaySmsOTP</execParams>
    </service>
</serviceList>
```

**Configure Multi Factor Authentication to use an SMS Service provider**

In the web.config file, set the ChannelProvider property of the MFA provider with value “FTOSApiSms“.

# Example

```
<multiFactorAuthentication xmlns
="http://fintechos.com/ebs/schemas/multiFactorAuthenticatio
n" enabled="true">
        <providers>
            <provider name="SMS" enabled="true">
                <type fullName
="EBS.Core.Web.MVC.Security.SmsMultiFactorAuthenticationProv
ider, EBS.Core.Web.MVC" />
                <properties>
                    <property
name="ChannelProvider" value="FTOSApiSms" />
                    <property
name="MaxNumberOfAuthenticationRetries" value="3" />
                    <property
name="MaxNumberOfSmsSendings" value="3" />
                    <property
name="MessageTemplate" value="myMessageTemplate_SmsApi" />
                </properties>
```

```
            </provider>
        </providers>
        ...
</multiFactorAuthentication>
```

## Password reset SMS for the log-in credentials

To set up password reset confirmation:

Add section

```
<configSections>
...
  <section name="passwordReset"
type="EBS.Core.Web.MVC.PasswordResetConfig, EBS.Core.Web.MVC"/>
</configSections>
```

Add configuration element

```
<configuration>
...
  <passwordReset xmlns="urn:EBS.Core.Web.MVC">
    <confirmation channelProvider="" messageTemplate=""
enabled="true"/>
  </passwordReset>
...
</configuration>
```

where:

- enabled - if true, after the completion of the password reset flow a message will be sent to user's phone number. Default value: false;
- channelProvider - the provider that will be used to send the message. Must be one of "GatewaySmsOTP" or "FtosApiSms";

- messageTemplate - the template that will be used to create the message. Must be a record from FTOS_CMB_ActionTemplate entity.

If the configuration element is missing the message will not be sent.

## Email-based Two-Factor Authentication

Email-based two-factor authentication is a popular choice when it comes to multi-factor authentication.

#### How it works?

Users will be granted access to the FintechOS app following these two steps:

- Users will navigate to the FintechOS web app and they will provide their account credentials (username and password). Based on the app configuration, the credentials can be either local or from external providers. To make sure account access is protected, after the login credentials are provided, a one-time security pass code is sent to the user's email address.
- In the web app, they provide the pass code received via email. Access into the system is granted.

#### How to set up the Email-based MFA?

Setting up the email-based multi-factor authentication is a two-step process:

##### Step 1 Enable Multi-Factor Authentication

On the server where the FintechOS installation package resides, go to the **web.config** file and add the following settings:

- To the **<configSections>** tag, add the **multifactorAuthentication** section:

```
<configuration>
    <configSections>
        ...
        <section name="multiFactorAuthentication" type=
"EBS.Core.Authentication.Common.MultiFactorAuthentication.Co
nfig.MultiFactorAuthenticationSection,
EBS.Core.Authentication.Common" /> </configSections>
    <configuration>
```

- Add the **<multiFactorAuthentication>** tag:

```
<configuration>
    ...
    <multiFactorAuthentication
xmlns
=
"http://fintechos.com/ebs/schemas/multiFactorAuthentication"
 enabled="true">
        <providers>
            <provider
name="Email" enabled="true" default="true">
                <type fullName=
"EBS.Core.Web.MVC.Security.EmailMultiFactorAuthenticationPro
vider, EBS.Core.Web.MVC" />
                <properties>
                    <property
name="ChannelProvider" value="GatewayEmailOTP" />
                    <property
name="CommunicationChannel" value="Email" />
                    <property
name="MaxNumberOfAuthenticationRetries" value="3" />
                    <property
name="MaxNumberOfEmailSendings" value="3" /> </properties>
            </provider>
        </providers>
        <runtime>
            <providers>
                <provider name="Email">
                    <roles>
                        <role name="*" /> </roles>
                </provider>
            </providers>
        </runtime>
    </multiFactorAuthentication>
```

```
</configuration>
```

Where:

- `multiFactorAuthentication/@enabled` - controls if MFA is enabled or not. Default value: false;
- `multiFactorAuthentication/providers/provider/@enabled` - controls if a specific MFA provider is enabled or not. Default value: true;
- `multiFactorAuthentication/providers/provider/@default`
    - When MFA is enabled, there can be at most one provider marked with default="true".
    - The provider marked with default="true" will be selected for MFA when there are multiple providers available for user's roles and the user hasn't selected any preferred communication channel or his preferred communication channel is not present into the configured providers list.
    - Default value: false.
- on `multiFactorAuthentication/providers/provider/properties`:
    - `ChannelProvider` - the channel provider used by the Email MFA provider to send email messages. Its value must be the Name of one of the records from **EbsMetadata.FTOS_DPA_ChannelProvider** table;
    - `CommunicationChannel` - the communication channel used by the Email provider to send email messages. Its value must be the Name of one of the records from **EbsMetadata.FTOS_DPA_CommunicationChannel** table;
    - `MaxNumberOfAuthenticationRetries` - the user has up to MaxNumberOfAuthenticationRetries chances to enter the correct code. If this threshold is reached the user will be redirected to the login page. Default value: **3**;

    - `MaxNumberOfEmailSendings` - if needed the user may request a resending of the code for up to MaxNumberOfSmsSendings times. If this threshold is reached the user will be redirected to the login page. Default value: **3**;

- `multiFactorAuthentication/runtime/providers/provider [@name='Email']/roles` will include a <role name=""/> child for each role that contains users that have to be authenticated through this provider. Note that a `<role name="*"/>` means that all roles will be taken into account;

Once you've activated the Email-based authentication, you need to configure the Job Server for Multi-Factor Authentication.

#### Step 2. Configure the Job Server for MFA

> **IMPORTANT!**
> The MessageBus (OCS) plugin for the FintechOS Job Server already includes the configurations required for multi-factor authentication (see the *FintechOS Installation Guide* for details about MessageBus (OCS) installation).
>
> - If you have the MessageBus (OCS) plugin installed, skip this step.
> - If you are using the standard Job Server configuration, follow the instructions below to configure the multi-factor authentication settings.

1. On the server where the FintechOS installation package resides, go to the **schedule.config** file and add the following section:
2. 
```
<triggers>
    ...
    <trigger>
        <name>FTOS.OCB.OTP</name>
        <startTime>02.11.2017 11:00</startTime>
        <endTime>03.11.2080 11:02</endTime>
        <repeatCount>-1</repeatCount>
        <rescheduleAfterRun>false</rescheduleAfterRun>
        <async>false</async>
        <expression>0/10 * * * * ?</expression>
```

```
        <services>

<service>FTOS.OCB.SendMessagesServiceEmailOTP</service>

<service>FTOS.OCB.UpdateStatusServiceEmailOTP</service>

<service>
FTOS.OCB.UpdateExpiredMessageServiceEmailOTP</service>
        </services>
    </trigger>
</triggers>
```

3. On the server where the FintechOS installation package resides, go to the **services.config** file and add the following sections:

```
<serviceList>
    ...
    <!--OTP-->
    <service>
        <name>FTOS.OCB.SendMessagesServiceEmailOTP</name>
        <type>class</type>
        <method></method>

<
class
>
FTOS.MessageBus.ScheduledServices.SendMessagesService</class>

<assembly>FTOS.MessageBus.ScheduledServices</assembly>-->

<execParams>
provider=gateway;providerSetting=GatewayEmailOTP</execParams>
    </service>
    <service>
        <name>FTOS.OCB.UpdateStatusServiceEmailOTP</name>
        <type>class</type>
        <method></method>
        <class>
FTOS.MessageBus.ScheduledServices.UpdateStatusMessagesService
</class>

<assembly>FTOS.MessageBus.ScheduledServices</assembly>-->
```

4.

```
<execParams>
provider=gateway;providerSetting=GatewayEmailOTP</execParams>
    </service>
    <service>

<name>FTOS.OCB.UpdateExpiredMessageServiceSmsOTP</name>
        <type>class</type>
        <method></method>
        <class>
FTOS.MessageBus.ScheduledServices.UpdateExpiredMessageService
</class>

<assembly>FTOS.MessageBus.ScheduledServices</assembly>-->

<execParams>
provider=gateway;providerSetting=GatewayEmailOTP</execParams>
    </service>
</serviceList>
```

# Register TLS Client Certificates

Client certificates allow you to access web services that require client authentication via the TLS/SSL protocol. Once a certificate is registered, you can refer it in your server side scripts and include it in API calls.

To register a TLS Client Certificate add the following key to the `<appSettings>` node in the FintechOS Studio *web.config* file:

```
<appSettings>
    ...
    <add key="automation-client-certificate-clientCert1" value="{
'storeName': 'My', 'storeLocation': 'LocalMachine', 'thumbPrint':
'd77621fa50114404a6e5820c6d066b019c13fdd8', 'description':'Client
certificate for Api1' }">
    or
    <add key="automation-client-certificate-clientCert1" value="{
&apos;storeName&apos;: &apos;My&apos;, &apos;storeLocation&apos;:
&apos;LocalMachine&apos;, &apos;thumbPrint&apos;:
&apos;d77621fa50114404a6e5820c6d066b019c13fdd8&apos;,  &apos;descri
ption&apos;:&apos;Client certificate for Api1 a&apos; }">
```

```
    ...
</appSettings>
```

You must provide a programmatic **name**, preceded by the `automation-client-certificate-` prefix. For instance, in the example above, the name of the client certificate is going to be *clientCert1*.

The **value** is provided in JSON format and must be XML escaped. For simpler scenarios you can use single quotes instead of double quotes. The JSON value has the following structure:

```
{
    "storeName": "My",
    "storeLocation": "LocalMachine",
    "thumbPrint": "d77621fa50114404a6e5820c6d066b019c13fdd8",
    "description": "Client certificate for Api1",
    "checkValidity": true
}
```

| Property | Description |
|---|---|
| storeName | You can populate the storeName property with one of the following values:<br>• AddressBook - X.509 certificate store for other users.<br>• AuthRoot - X.509 certificate store for third-party certificate authorities.<br>• CertificateAuthority - X.509 certificate store for intermediate certificate authorities.<br>• Disallowed - X.509 certificate store for revoked certificates.<br>• My - X.509 certificate store for personal certificates.<br>• Root - X.509 certificate store for trusted root certificate authorities.<br>• TrustedPeople - X.509 certificate store for directly trusted people and resources.<br>• TrustedPublisher - X.509 certificate store for directly trusted publishers. |
| storeLocation | You can populate the storeLocation property with one of the following values:<br>• CurrentUser - X.509 certificate store used by the current user.<br>• LocalMachine - X.509 certificate store assigned to the local machine. |
| thumbPrint | This is the thumbprint of the client certificate. |
| description | A user-friendly description of the certificate. This information will be displayed in the code editor's intelligent code completion suggestions. |

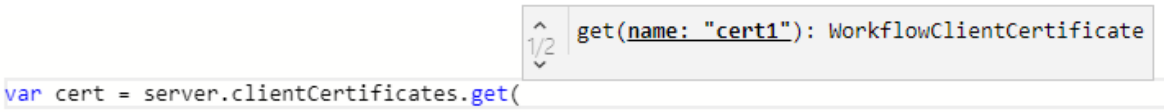
| Property | Description |
| --- | --- |
| checkValidity | • true - Even if the thumbprint is found, the API returns the certificate only if the root issuer in the certificate build chain is part of the trusted root certification authorities.<br>• false - For development or testing purposes. |

## Usage in server-side scripts

The automation API supports referencing client certificates and passing them in the httpGet/httpPost functions. For more information, see the Server SDK Reference Guide documentation.

```
var cert = server.clientCertificates.get('clientCert1');
var getResult = httpGet('https://server.com/route1', {}, {
    clientCertificate: cert
});
var postResult = httpPost('https://server.com/route2', myPostData,
{
    clientCertificate: cert
});
```

In the code editor, the `server.clientCertificates.get` function provides automatic code completion suggestions for the registered client certificates.




# Authorization

In FintechOS, access to specific resources (authorization) is done via security role-based access which enables you to

- Protect information from being mishandled by users.
- Ensure that users have access to information based on business need to know.

This section covers platforms' critical aspects of segregation of duties and data ownership.

## Security Roles

Users with elevated privileges (admin users) can control data access by setting up the organizational structure to protect sensitive data and configuring various organization layers to allow communication, collaboration or reporting.

To set up the organizational structure, they need to create the business units, security roles, and assign users the appropriate security roles to map the job-related responsibilities with the required level of access privileges within the platform.

You can grant even more granular access privileges in FintechOS, by associating security roles to digital journeys, digital journey steps, business workflows, dashboards, endpoints and DB tasks. The data is automatically filtered based on the privileges and level of access defined within the security role via the security items.

The lowest level of access privileges you can grant to users in FintechOS is on attribute level. You can choose if a specific attribute (field) is to be mandatory, recommended or optional, by selecting the desired option from the Required Level drop-down:

- None – The field is optional. No error message will be displayed if the field is empty.
- Recommended – A blue dot will be displayed on the upper-left corner of the field in the user interface to indicate that it might be useful to fill in the field.
- Required - A red dot will be displayed on the upper-left corner of the field in the user interface to indicate that it is a mandatory field. The end user will not be able to add a new record if the field will be left blank.

**NOTE**

- You can only add required attributes to entities which have no records (empty entities), so if you try adding a required attribute to an entity for which you already have required attributes stored within the database, you'll receive an error message.
- You can add required attributes without creating constraints in the database, from entity form/digital journey configuration page, Advanced tab > After Events tab, by providing a code in the JavaScript field and the capabilities of field options.

For information on how create security roles and how to provide granular access to entities, digital journeys and dashboards, see the *FintechOS Studio User Guide*.

## Data Ownership

In FintechOS, data ownership is given by the security roles, which allows you to manage complex scenarios of access privileges and the level of access.

Admin users are the ones who can define the organizational structure, create users and assign the security roles according to the business need-to-know, inline with their job responsibilities.

The information presented in the user menu and the actions a user is able to perform are aligned with the security roles assigned.

For information on how create the organizational structure, add users and assign security roles, see the *FintechOS Studio User Guide*, section Security.

# Password Security

By default, FintechOS can log into the FintechOS Studio by using FintechOS credentials: username and password. After successfully logging in, users can access the FintechOS resources based on the privileges granted by the security role assigned.

FintechOS has various options in place to ensure password security:

- prevent users to log in using a wrong password
- set the password to expire
- allow users to recover their password
- set password complexity
- forbid users setting their password matching previous passwords
- forbid users logging in with expired passwords
- lock users who have been inactive for a specific number of days

In order to comply with any password policies that might be enforced within your organization, you can customize the FintechOS password complexity either from the **web.config** file (see section Global Password Complexity Settings) or by using server scripting (see section Customize Password Complexity Rules using Server Scripting).

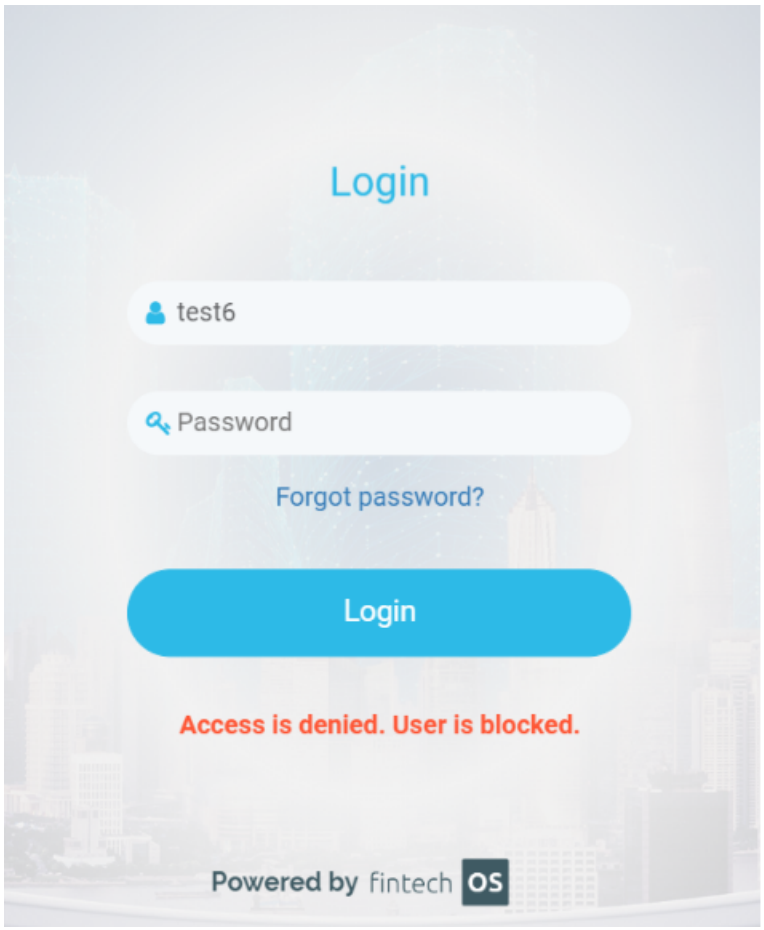
When users will choose to reset their password, an email is sent to the email address associated with their FintechOS account. FintechOS offers a default email template that is used for password reset. It's easy to customize the default email template, or by using server scripting .

If the Forgot Password feature has been activated, users will be able to reset their password from the login page by providing either their emails address or their username.

In addition to the forgot password security, you can also forbid access for users who have been idle for a specific period of time.

## Locked account

If users enter a wrong password multiple times, reaching the maximum number of retries (that is, 5), their account will be locked.




To unlock their account they should contact their FintechOS admin to unlock their account. After the account is unlocked, they will be able to log in using the last password (if they remember it) or recover the password if they forgot it.

## Password expired

If the password is expired, a message displays on the login page notifying the user that the password. It also provides the user with the option to reset the password.

> **NOTE** This feature is available only for EBS Authentication Provider.

## Activate Forgot Password Feature

In FintechOS, the Forgot Password feature allows users to reset their password and enables FintechOS developers to set the password complexity and to customize the password reset email template.

> **NOTE** The forgot password feature is disabled by default and the validity of the password reset token is by default 15 minutes.

To activate the forgot password feature, on the server where the FintechOS installation package resides, go to the **web.config** file and set the following setting:

```
<appSettings>
    <add key="feature.reset-password" value="1" />
    ...
</appSettings>
```

In order to send email instructions to users who have requested password reset from the login page, also make sure to include the following settings in the **web.config** file:

```
<add key="SMTP:Port" value="" />
<add key="SMTP:Host" value="" />
<add key="SMTP:EnableSSL" value="" />
<add key="SMTP:User" value="" />
<add key="SMTP:Password" value="" />
<add key="DefaultFromEmail" value="" />
```

In the **web.config** file, set the validity of the password reset token by configuring the following key: **PasswordResetExpiration**. The default value of this key is 15 minutes.

Token expiration after 5 minutes:

```
<appSettings>
    <add key="PasswordResetExpiration" value="00:05:00"/>
```

```
    ...
</appSettings>
```

# Configure Password Change

FintechOS provides you with various options to configure password change:

- set the period of time (in hours) to pass until users are able to change their password.
- set the period of time (in days) allowed before a password must be changed.
- configure password change based on the password history.

## Setting password minimum age

The minimum password age setting determines the period of time (in hours) that a password can be used before the users can change their password.

To set the password minimum age, on the server where the FintechOS installation package resides, go to the **web.config** file and add the following setting:

```
<add key="core-setting-ebsauth-password-min-age" value="24"/>
```

Where **value** is the number of hours until users can change their password.

If **value** is empty or a negative value or the key is missing from **web.config** the **minimum password age** is set to 0 hours allowing immediate password changes, which is not recommended.

When using the minimum password age, we recommend you to configure the password history as well. This way you prevent users to changing their password with the same password.

## Setting password expiry

The maximum password age setting determines the period of time (in days) that a password can be used before the system requires the user to change it

To enable password expiry feature (Maximum password age), on the server where the FintechOS installation package resides, go to the **web.config** file and add the following setting:

```
<add key="core-setting-ebsauth-password-max-age" value="30"/>
```

Where **value** is the number of days allowed before a password expires and should be changed. The maximum number of days is limited to 999. If value is empty, 0 or a negative value or the key is missing from **web.config** the password expiration feature is disabled, that is, the password never expires, which is not recommended.

If the user tries to authenticate with an expired password the login page will provide the user with the option to reset the password only if the reset password feature is enabled.

## Configuring password change based on password history

FintechOS provides you with the password history features which allows you to set whether a new password is checked against passwords stored in the user's password history. This prevents the user from re-using a recently used password.

To configure the password change to take into consideration user's password history, on the server where the FintechOS installation package resides, go to the **web.config** file and add the following setting:

```
<add key="core-setting-ebsauth-password-history-depth" value="5"/>
```

Where **value** is the number of historical passwords that will be checked when a user tries changing the password. If the user tries to set one of the old passwords then the system will forbid user to use that password. If **value** is empty, 0 or a negative value or the key is missing from the **web.config** file, the password history feature is not enabled (i.e. the user can change the password with the same password).

## Setting password about to expire notifications

You might want to remind users that they should change their passwords within x days before their password expired. FintechOS allows you to set such a notification to be shown on a web page and also customize the notification message.

To set the password expiry notification, on the server where the FintechOS installation package resides, go to the **web.config** file and add the following setting:

```
<add key="core-setting-ebsauth-password-about-to-expire-days-until-
expiration" value="30"/>
```

If the number of days until the password will expire is less than the **value** specified, a page with the remaining days will be shown.

The notification message is localizable, so in order to be properly interpreted by the system, make sure that the text is a json array.

To customize the notification message , in the **web.config** file, add the following setting:

```
<add key="core-setting-ebsauth-password-about-to-expire-
message" value="[{'en-GB':'Password will expire in {10} days.'},
{'ro-RO': 'Parola va expira in {10} zile.'}]"/>
```

When the language is set to Romanian the message will be : "Parola va expira in {10} zile.", where {10} is the number of days until the password will expire.

The Server SDK function `usersAboutToExpirePasswords(int passwordExpireDaysMax)` enables you to get the list of users for which the password will expire in '**passwordExpireDaysMax**' days or less.

## Skipping the password expiry rule for specific security roles

> **NOTE** To ensure higher security, we recommend you to use this feature only in rare specific cases, e.g., for admin accounts.

To set password never expire for users who have specific security roles, in the **web.config** field, add the following setting:

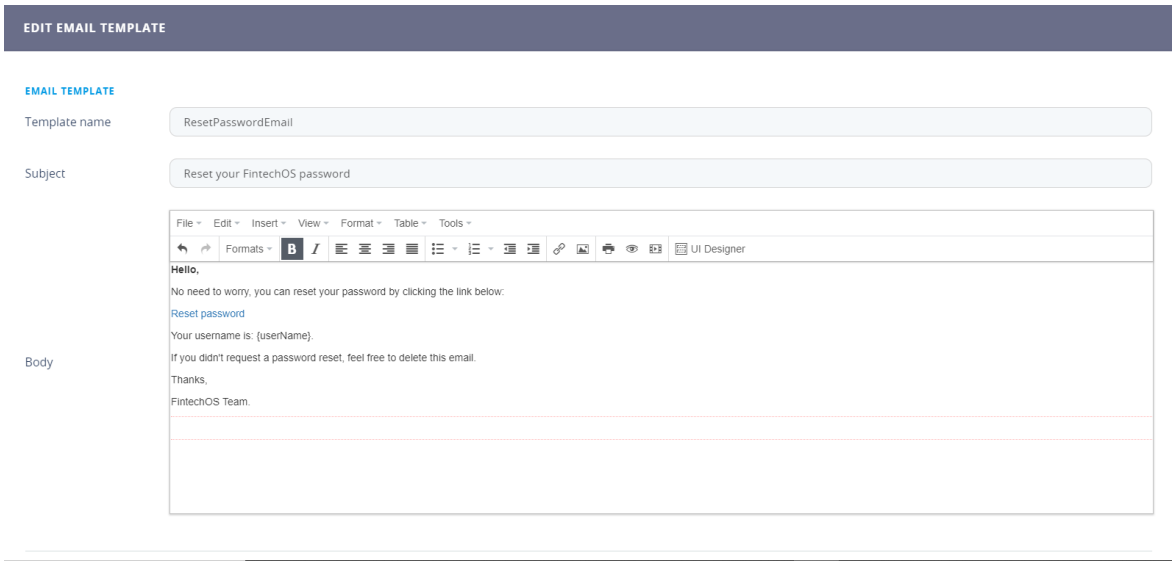
```
<add key="core-setting-ebsauth-password-expired-excepted-
role" value="securityRole"/>
```

The users with the security role specified in the value will never have to reset the password due to the password expiry rule.

# Reset Password Global Email Template

The default email template for password reset is named: “ResetPasswordEmail” and it is included in the installation script.

To see the content of the default email template, from the Admin menu, click Email Templates. The Email Templates List page appears. Double-click on the “ResetPasswordEmail” record. The Edit Email Template page will be displayed.




> **NOTE** You can change the content of the default email template based on your preferences, but make sure to include in the template the following tokens: **username** and **generatedToken**, otherwise, the email sent to users will contain incomplete information.

You can also customize the email template by using server scripting. For information on how to do it, see Customize Reset Password Email Template using Server Scripting

# Customize Reset Password Email Template

You can customize the reset password email template using server scripting (automation scripts) by following two steps:

## Step 1. Add a specific key to the web.config file

On the server where the FintechOS installation package resides, go to the web.config file and provide the name of the automation script name which customizes the email template, by adding the following key:

```
<appSettings>
        <add
key="ResetPasswordEmailTemplateWorkflowName" value="WorkflowName"/>
        ...
</appSettings>
```

If you do not provide the name of the automation script for email template customization, the system will search for an on-demand automation server script named “FTOS_ResetPasswordEmail”. For backwards compatibility, the system also searches for ‘ResetPasswordEmail’.

> **NOTE** The FTOS_ResetPasswordEmail” on-demand automation server script does not exist by default; you have to create it.

## Step 2. Create FTOS_ResetPasswordEmail on-demand automation script

The automation script offers customization based on associated user and roles.

The new password reset email template must be returned as the “emailTemplate” key of the Values property:

```
var user = context.Values["user"];
for(var i=0;i<user.Roles.length;i++)
        {
            let role = user.Roles[i];
            if (role.Name == "special")
                {
                context.Values["emailTemplate"] =
"SpecialEmailTemplate";
                break;
                }
        }
```

The user value has the following format:

```
{
    "UserName" : "user1",
    "BusinessUnitId" : "guid",
    "DisplayName" : "user display name",
    "Email" : "user email",
    "ExternalId" : "guid",
    "OrganizationId" : "guid"
    "Roles" :
        [
            {
                "SecurityRoleId" : "guid",
                "Name" : "role name 1"
            },
            {
                "SecurityRoleId" : "guid",
                "Name" : "role name 2"
            },
        ]
}
```

For information on how to create an on-demand server automation scripts, see the *FintechOS Studio User Guide*, section *Creating On-demand Server Automation Scripts*.

## Global Password Complexity Settings

For the default Membership provider, the complexity of the password is controlled by the following settings in the **web.config** file:

- minimum required password length
- minimum required non alpha numeric characters
- password strength regular expression

web.config settings for password complexity:

```
<membership defaultProvider="SqlProvider"
    userIsOnlineTimeWindow = "20>
    <providers>
        <add name="CustomMembership"
        type="EBS.Core.Authentication.Providers.CustomMembership"
        connectionStringName="EbsSqlServer"
        ...
```

```
        minRequiredNonalphanumericCharacters="1"
        minRequiredPasswordLength="7"
        passwordStrengthRegularExpression="(?=.*[A-Z].*[A-Z])(?=.*
[#@$*!&amp;])(?=.*[0-9].*[0-9])(?=.*[a-z].*[a-z].*[a-z])"
        />
    </providers>
</membership>
```

You can also customize the password complexity by using server scripting. For more information, see Customize Password Complexity Rules using Server Scripting.

# Customize Password Complexity Rules

You can customize the password complexity using server scripting (automation scripts) by following two steps:

## Step 1. Add a specific key to the web.config file

On the server where the FintechOS installation package resides, go to the web.config file and provide the name of the automation script name which configures the password complexity, by adding the following key:

```
<appSettings>
        <add
key="ResetPasswordRulesWorkflowName" value="WorkflowName"/>
        ...
</appSettings>
```

If you do not provide the name of the automation script for password complexity customization, the system will search for an on-demand automation server script named “FTOS_ResetPasswordRules”.

> **NOTE** The “FTOS_ResetPasswordRules” on-demand automation server script does not exist by default; you have to create it.

#### Step 2. Create FTOS_ResetPasswordRules on-demand automation script

The server automation script offers customization based on password content and associated user and roles.

For information on how create an on-demand server automation script. For information on how to create an on-demand server automation scripts, see the *FintechOS Studio User Guide*, section *Creating On-demand Server Automation Scripts*.

Do not permit passwords containing letter ‘z’

```
var password = context.Values["password"];
if (password.match(/z/))
        throwException("Password contains letter z");
```

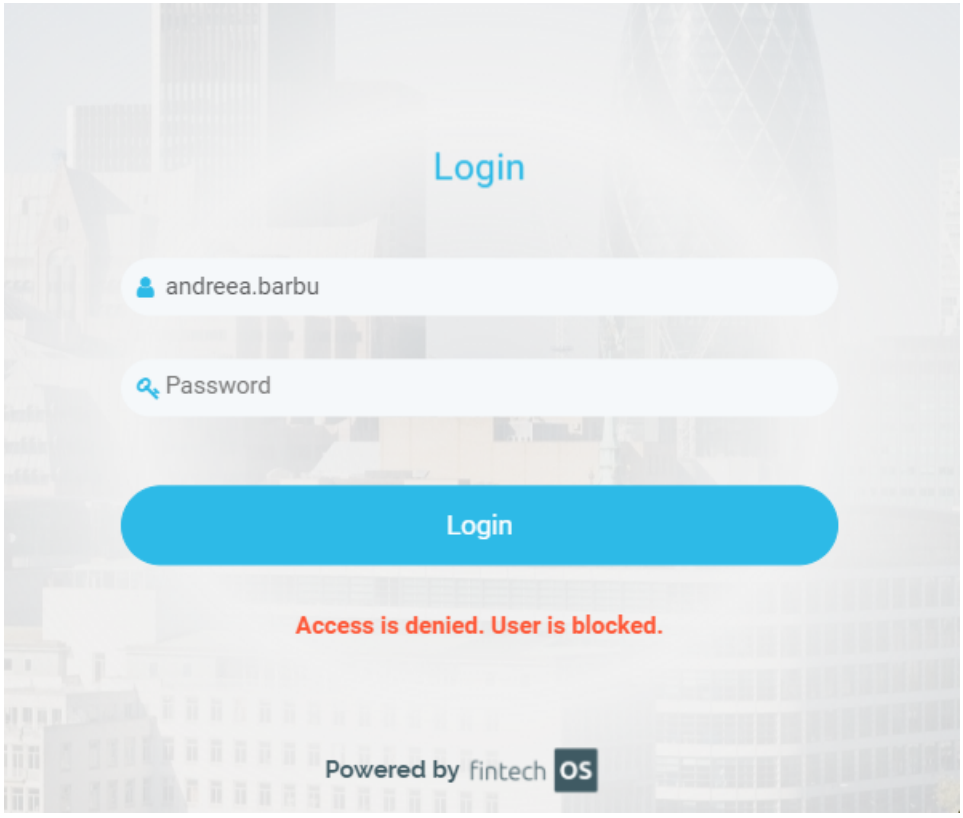
Context contains two keys in the **Values** property:

- password
- user, which contains a json similar to:

```
{
    "UserName" : "user1",
    "BusinessUnitId" : "guid",
    "DisplayName" : "user display name",
    "Email" : "user email",
    "ExternalId" : "guid",
    "OrganizationId" : "guid"
    "Roles" :
        [
            {
                "SecurityRoleId" : "guid",
                "Name" : "role name 1"
            },
            {
                "SecurityRoleId" : "guid",
                "Name" : "role name 2"
            },
        ]
}
```

## Temporary Blocked User

A temporary blocked user is the account that has opened the FintechOS Portal, inserted the wrong password for that said account for a maximum of five times or for a maximum that was set previously and cannot access the Portal anymore.




When the temporary block time interval has passed and the user wishes to reset the password, click **Forgot password** and follow the steps to receive the email with reset password which implies opening the e-mail and follow the reset password link. The user is unblocked so that reset password flow can be followed.

## How to setup the number of retries Portal - Web.config setup

In order to create the setup, head over to installation files of the FintechOS environment where you wish to make the necessarily modifications, and in the web.config file add the following configurations.

To configure the the maximum amount of retries (the default value is zero):

<add key="core-setting-ebsauth-account-lockout-duration" value="5"/>

<add key="feature.reset-password" value="1" />

### When using the EbsAuth provider

For those who are using the EbsAuth provider, to web.config insert an up to date key ("core-setting-ebsauth-account-lockout-duration") to set the amount of minutes the user will not be able to access the account after having tapped in the false password. The key inserted earlier can be zero/ can be a negative value/ empty, then only the administrator has the power to unblock the account for the user.

> **IMPORTANT!**
> The userId present in TemporarilyLockedAccount is deleted when an admin unlocks an account.

The system entity "**TemporarilyLockedAccount**" tracks the modifications happening when an user's account is blocked after having inserted the wrong password.

The feature temporary blocked user has the key set to a positive value, the user wishes to open the FintechOS Portal and **EbsAuth provider** states that the account has been locked after failed attempt to log in, there are two situations:

Firstly, the user was previously temporarily locked out with the current date/ time bigger than the Lockeduntil value, the user will be automatically unlocked, the data from the system entity "**TemporarilyLockedAccount**" is eased and the user will be able to use the Portal. However, when the current date/ time is smaller than the Lockeduntil value, the system will not automatically unlock, but the block will be effective.

Secondly, when the user is not blocked, the LockedUntil value is equal to aspnet_ Membership.LastLockoutDate plus value of "account-lockout-duration". Then, when the current date/ time is bigger than the LockedUntil value, the user's account is automatically unblocked and the user will be able to use the Portal. Nevertheless, when the current date/ time is equal or smaller than the LockedUntil value, there is an entry in the TemporarilyLockedAccount and the user cannot log in the Portal.

# Unauthorize Inactive Users

The company's security policies might require that users who have been idle for a specific number of days are forbidden access to the company's resources.

FintechOS provides you with two SDK functions which enable you to identify any inactive FintechOS users and disable their access as an extra security measure for protecting your FintechOS resources against unauthorized access:

- `inactiveUsers(int daysOfInactivity)` - get the list of users who have not been active in FintechOS in the last number of days specified by the **daysOfInactivity** parameter.
- `unauthorizeUser(string userName)` - makes the user who has the username specified by the **userName** parameter not authorized.

# Session Expiration Time

Each session is timed to a specific interval during which if the user presents no inactivity, the Studio/Portal will expire. To set the session timing, the key core-setting-tokenExpiresIn is used and it functions with a specific time syntax. The availability time frame when working inside the Studio and Portal is set using the following syntax d/day/days m/min/minutes h/hour/hours s/sec/seconds. For example, it is possible to set:

- 3 d 5 h
- 3 days 5 hours 3 minutes 20 seconds
- 3 d/days 5 h 3 m/min 20 s/sec

The default value is 20 minutes.

The necessarily changes are made in the web.config. If core-setting-tokenExpiresIn is not found in the config, the legacy appSetting TokenExpiresIn is loaded.

## Example:

How to set the time for when the Portal/Studio should log out the user:

```
<add key="core-setting-tokenExpiresIn" value="2d 12h 3m
5s"/>
```

```
<add key="core-setting-tokenExpiresIn" value="600"/> <!--
seconds-->
<add key="TokenExpiresIn" value="1200" />
<add key="TokenExpiresIn" value="1h30min" />
```

# Data Audit

The forth pillar of FintechOS security, logging, provides you with comprehensive audit trail of what happened at any given time and who performed the action.

The logging configuration is specified within the **web.config** file. The platform uses the log.NET component for logging and it generates a **trace_roll.log** file and multiple **trace_roll.dd-mm-yyyy.n.log** files. The log files are saved in the web directory.

**NOTE** FintechOS API logs and FintechOS LOGS are kept in different audit tables.

## Entity Audit

FintechOS has an extensive audit functionality that can be enabled for any entity, allowing change tracking at entity level.

Using the FintechOS Studio, users can activate the auditing feature for a specific entity, by selecting the **Is Audited** checkbox.  When auditing is enabled, the platform creates and maintains a system entity named **{entityName}_ADT** where all changes to the initial entity are recorded including: the type of changes on the entity, when the changes have been made and by whom.

When the user navigates to the list view of an entity with audit enabled the **History** button will be available on the toolbar.

Clicking the **History** button will open the History List view which lists all the changes associated to the current entity instance (the associated ADT entity).

When navigating to the detail view for an audited entity, the **History** button will open a list with all the changes associated to the current entity instance.

To programmatically navigate to the audit logs use the commands below:

To get all audit logs for the specified entity (where, the ID is the entity ID):

```
'entity/{entityName}/history/viewAll/{id}'
```

To get audit logs for the specified operation:

```
'entity/{entityName}/history/{operation}'
```

To get audit logs for two specific operations:

```
'entity/{entityName}/history/{opOne}/{opTwo}'
'entity/{entityName}/businessTransactions/{id}'
```

The data audit is independent of entity records (when the **Audit enabled** checkbox is selected on entity). An unique identifier (UID) is automatically added by the system to records. When users delete records, based on the UID, the action is logged into the audit trail.

The History List view which lists all the changes associated to the current entity instance (the associated ADT entity) has a new column, Unique Identifier (UID).

If the user deletes an income of a customer. the action is logged into **{entityName}_ADT**. The user can consult anytime the History List page on that customer entity and see that the income has been has been deleted, when and by whom.

# FintechOS Logging

FintechOS logs all CRUD operations executed in the platform, by default, in a separate database schema named EbsLogs.UniversalLog.

Database administrators can restrict read access for this schema and grant insert rights only for the SQL login used by the FintechOS platform.

### How to Configure the Logging of CRUD Operations

To configure this feature, go to the **web.config** file and set the feature-universal-logging setting, as desired. By default, it is set to **0**, that is, the feature is enabled.:

```
<configuration>
      <appSettings>
                  ...
                  <add key="feature-universal-
logging" value="0|1|true|false"/>
      </appSettings>
</configuration>
```

## FintechOS API Logging

FintechOS logs the calls over the FintechOS API (REST AND WCF) and DataService CRUD operations.

The logs are saved by default in a separate database schema named EbsLogs. Database administrators can restrict read access for this schema and grant insert only rights for the SQL login used by the FintechOS platform.

Source names:

- OpenApi (REST endpoint)
- ApiService (WCF endpoint)
- DataService (MVC endpoint)

### EbsLogs.ApiLog Schema

| Field | Type | Description |
|---|---|---|
| Id | bigint | identity, primary key |
| LogId | uniqueidentifier | alternate unique key |
| Tenant | nvarchar(150) | tenant name, default value: ebs_default |
| UserName | nvarchar(200) | authenticated user name |
| Source | nvarchar(150) | controller name : OpenApi, ApiService or DataService |
| Method | nvarchar(150) | action name |

| Field | Type | Description |
|---|---|---|
| Request | nvarchar(max) | request parameter as JSON |
| Response | nvarchar(max) | response as JSON |
| Message | nvarchar(max) | response message |
| Exception | nvarchar(max) | response error |
| Success | bit | success/error |
| CreatedAtUtc | datetime | call moment UTC |
| Duration | bigint | call duration milliseconds |
| CorrelationId | nvarchar(100) | correlation id |
| RequestId | nvarchar(100) | request id |
| ApiInfo | nvarchar(max) | call authentication information |

## How to Configure the FintechOSAPI Logging

To configure this feature, go to the **web.config** file and use a custom configuration section, as provided below:

```
<configuration>
     <configSections>
                <section name="ftosApiLogging"

type
="EBS.Core.Utils.ApiLoggingConfiguration.ApiLoggingConfigSection,
EBS.Core.Utils"/>
     </configSections>
     <ftosApiLogging enabled="true|false">
                <sources>
                    <source
name="OpenApi|ApiService|DataService" exclude="true|false">
                        <methods>
                            <method name="*">
                                <input exclude="true|false">
                                </input>
                            </method>

<method name="GetById" exclude="true|false">
                                <input exclude="true/false">
                                    <properties>
                                        <property
name="A" exclude="true|false"/>
                                    </properties>
                                </input>
                                <output exclude="true|false">
                                    <properties>
```

```
                                        <property
name="B" exclude="true|false"/>
                                    </properties>
                                </output>
                            </method>
                        </methods>
                    </source>
                </sources>
        </ftosApiLogging>
 </configuration>
```

The configuration allows filtering the out from logging elements at different levels of granularity: source, method (action), input (request), output (result), input property, output property.

The user can configure all other methods of a source by specifying "*" for method name. Any explicitly defined method will override all settings from "*".

**NOTE** When a property is excluded, it will not be serialized in the log.