cBRAIN

F2

Standard Server Infrastructure and Operations handbook

F2 Version 8

Updated: 13.11.2020

Table of Contents

Table of Contents 2

Introduction 4

Reference documentation 4

F2 Architecture 5

General 5

Architecture 5

Configuration 5

Sites 5

Architecture on premise 6

Server descriptions 6

cBrain cloud server installation 7

If the installation resides on cloud servers 8

F2 server descriptions and requirements 9

Important requirements 9

Database server 9

Integration server 9

Application server 11

Mobile server 13

Server surveillance 15

The surveillance level 15

F2 surveillance services 16

Integration server 16

Application server 16

Mobile server 16

Monitoring the F2 system 18

The Cockpit tool 18
Performance log 18
Service logs 19
Client log 19
IIS log and Windows logs 19
F2 server maintenance 21
cBrain patch policy, Windows updates etc. 21
Backup procedures 21
Database server maintenance 21
Starting up the F2 environment 22
Shutting down the F2 environment 22

Introduction

This document describes the most common tasks when operating F2 and is intended for technicians who have the required skillset needed to operate servers.

Reference documentation

The following documents are referred to and add valuable knowledge for the reader:

- F2 Pre-installation Documentation
- F2 Pre-configuration Documentation
- Standard F2 Hardware Requirements
- Standard F2 Software Requirements
- Standard F2 User Manuals

F2 Architecture

General

Architecture

F2 runs on a Microsoft SQL database, and several Microsoft Windows servers e.g application server, Integration server, Mobile server.

The application services, besides the database, are based on:

- Microsoft IIS websites
- Windows services
- Server scheduled tasks.

The F2 system can be integrated with several other services.

For F2 to work properly these integrations must first be in place via F2 Standard Integrations:

- Microsoft's Active Directory (for user authentication and authorisation)
- For communication via F2 an e-mail system (for receiving and sending emails)

Configuration

All configuration changes to the F2 installation are stored in the F2 database (except if the self-service modules are used). The F2 configurator creates the config-files in different folders in the F2 installation.

Only administrator or technicians, who are authorized by cBrain, can change these settings.

Sites

Under the website there are several IIS sites on the application server and the mobile server.

The F2 Desktop clients use sites on the application server to communicate with the backend of F2, and to authenticate the users.

F2 Touch and F2 Manager use sites on the mobile server to communicate with the backend of F2.

Only technicians, who are authorized by cBrain, can change the site application pools.

Architecture on premise

This section describes the standard architecture of a F2 installation.

An organisation's F2 installation can be integrated with other services (e.g. other third-party vendors) unique to their installation that are not in the illustration.

The AD service can reside in another domain.

The below figure provides an overview (the self service module and the IdentityHub is not included in the overview)

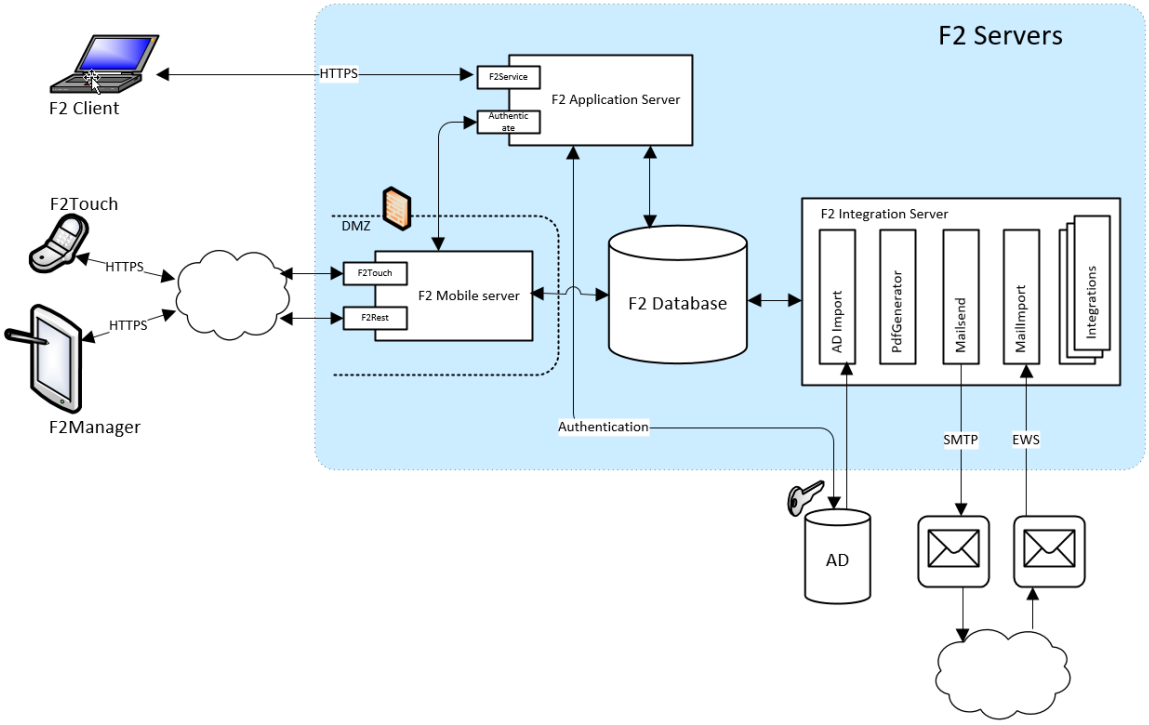

Figure 1: F2 default architecture

Server descriptions

Server/component	Description
Database	The SQL database contains all data, documents and configurations to the F2 system.
Application server	The Desktop client server interface. AD authentication and F2 internal web services.

Server/component	Description
Integration server	Integration to services (Exchange, SMTP, Scanner, AD etc.) Creation of PDF versions of documents.
Mobile server	F2 Touch and F2 Manager interface server. Provides self-service websites, if present. Integration with Internet based services (i.e. REST service)

Servers may be integrated with third-party servers depending on which F2 add-on modules are selected.

For technical documentation regarding required server port openings, domain users, IP addresses etc., please refer to the Pre-configuration and Pre-installation documents.

cBrain cloud server installation

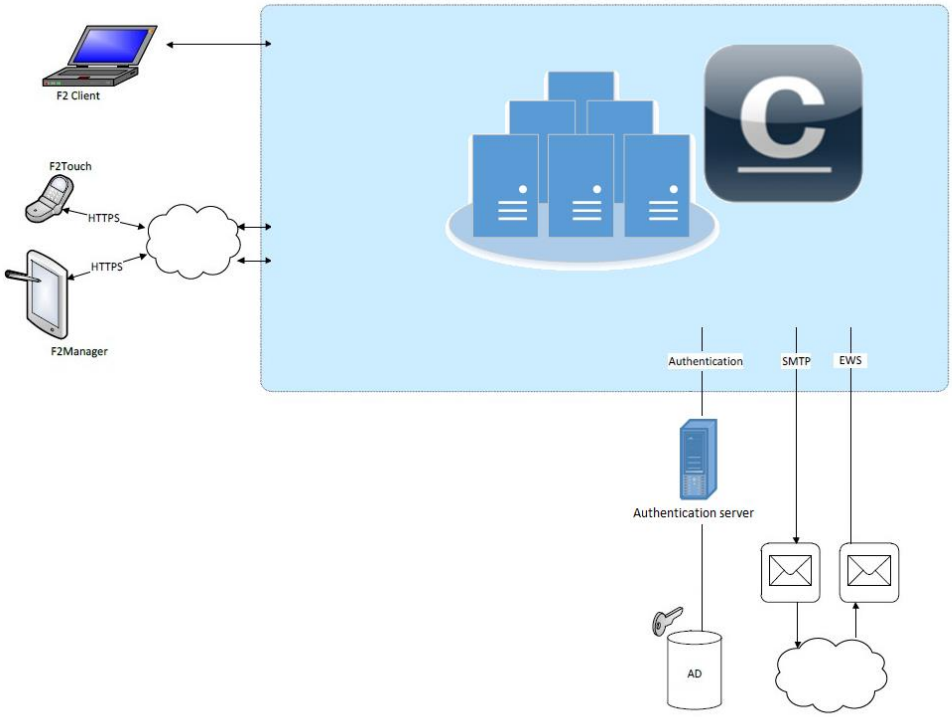

Figure 2: cBrain Cloud server installation

If the installation resides on cloud servers

There are two ways of authenticating users:

- Using an ADFS service.
- Using an authentication server.

If the ADUserImport option is selected, the XML-list is created by a scheduled task on the authentication server.

cBrain will monitor and operate all servers except the authentication server.

The authentication server operations are the responsibility of the customer's operations provider. Authentication server is not relevant if you use the ADFS as authentication.

The authentication server is a standard IIS server and requires that all standard Windows services and functions are working.

Any restrictions placed on the server must be agreed upon and verified by cBrain to ensure continued stable operations.

The customer's normal procedures regarding surveillance, antivirus, patch etc., as well as the cBrain requirements also apply to the authentication server.

The customer is responsible for maintaining the authentication server's certificates.

F2 server descriptions and requirements

Important requirements

Installation and configuration of F2 may only be carried out by cBrain authorized technicians.

The customer is required to answer questions related to the installation when necessary. cBrain must be able to get full knowledge on server and hosts servers in order to trouble shoot or in order to guide operations for normal performance.

Read the documents newest version of *F2 Software Requirements* and *F2 Hardware Requirements* for more information about the supported software versions like SQL versions, office versions etc and the required hardware specifications for each server. Please note the correct versions and appropriate update of the documentation.

Database server

All data, documents including configurations is stored in the Microsoft SQL server database.

The customer must create a service account - either a SQL server account, or a Windows account used by integrated security. The account must have F2 database owner rights to the database.

This account is used to initiate all activity from the F2 services to the database.

Integration server

The F2 installationsscript via the Octopus Deploy will ensure that the correct service is initiated. These are IIS website, IIS applications, IIS app pools and scheduled tasks.

Before the installation can be performed the user accounts needs to be setup. These are not setup automatically.

The F2 installation will have an integration server that includes the following Windows services.

Service	Description
Email import service	Imports e-mail from a queue that is created by the e-mail import scheduled task.
PDFGenerator	Creates PDF versions of all supported files in F2. Microsoft Office needs to be installed. Requires access to the database and shall be executed under a separate service account, with the necessary rights to execute Microsoft Office.
Queuehandlerservice	Handles queues of internal messages in F2.

There can be more services depending on the installed F2 add-on modules.

The Scheduled tasks will be created for the integration server.

Scheduled task	Description
Email import	Checks the user's mailboxes for e-mails to import to F2.
Email send	Sends e-mails from the e-mail send queue.
AdXmlimport	Imports users from XML-file to F2 (if installed).

There can be other scheduled tasks depending on the installed F2 add-on modules.

The following service accounts will be created for the integration server.

Service account	Description
PDF user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service Logon as a batch job **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders.

Service account	Description
F2 service user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service Logon as a batch job **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders.
F2 email user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service Logon as a batch job **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders.

Application server

The application server is a webserver containing the following sites:

Site	Description
F2service	Handles client communication. Requires access to the database and the F2 authentication service.
F2autenticationservice	Handles user authentication. Requires access to the database and the Active Directory.
Installer	The site used to download and install the F2 client.
DocumentSite	Handles documents in F2. Requires access to the database.

Several app pools are created and named with the following naming standard:

App pools	Description
	<customer>.<Environment>.<POOLName> Example: *cBrain.Prod.App*

There can be more sites depending on the installed F2 add-on modules.

Depending on the installed F2 add-on modules, some scheduled tasks will be installed:

Scheduled task	Description
F2Indexer	Maintains the query index for cSearch (if installed).
AdXmlExtractor	Imports users from XML-file to F2 (if installed). Runs every night and imports users from the AD.

There can be other scheduled tasks depending on the installed F2 add-on modules.

The following table shows an overview over service accounts for the application server.

Service account	Description
IIS application pool user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders.

Service account	Description
F2 service user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service Logon as a batch job **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders. Read/Write to cSearch index folder.
F2 AD user	**Group membership** Performance Log Users Performance Monitor Users **Domain Security Policy (Active Directory)** Read access to F2 security groups, with F2 users as members. **Local Security Policy** Logon as a batch job **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders.

Mobile server

The mobile server is a webserver containing the following sites:

Site	Description
F2Rest	F2-REST serves a general REST API towards F2. General access requires appropriate license
F2Touch	Handles communication with F2 Touch (mobile devices) and F2 Manager (iPad). Requires access to the database and the F2 authentication service on the application service.

More sites can be added, depending on the configuration and the installed F2 add-on modules. Sites for self-service solutions are often placed on the mobile server.

For the installation, separate app pools for F2 Touch and for self-service sites are required (if installed).

The following Windows services are installed:

Service	Description
SubmissionService	Handles messages from the SelfServiceWebsite queue, and sends them to F2 using F2 Rest (only if self-service is installed).
PushService	Sends notifications to mobile devices (mobile phones and iPads).
F2WebPushService	Sends notifications to non F2 services (only if installed).

The following service accounts shall be created for the mobile server:

Service account	Description
IIS application pool user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log og Upload folders.
F2 service user	**Group membership** Performance Log Users Performance Monitor Users **Local Security Policy** Logon as a service Logon as a batch job **File/Folder rights:** Read/Write to Windows\temp folder Read/Write to ApplicationFiles folder Read/Write to Data, Data Temp, Log and Upload folders.

Server surveillance

As a standard cBrain requires that server surveillance be implemented on all F2 servers. It is recommended that the minimum level of surveillance should be set to the same level as surveillance level on the cBrain cloud servers.

The surveillance level

The table below describes cBrain's standard for the surveillance level regarding servers in the F2 environment.

Area	Description
Alive	Monitors that the servers are online and raise an alert in case of inaccessibility. Be aware that pinging an IP address in a virtual environment can result in false feedback where the network adapter will reply even when the server is not running. For example, "Alive" can be implemented by reading the contents of a file.
Storage surveillance	Monitors storage surveillance on all drives with alerts: 35% storage left (budget warning) 20% storage left (incident reaction level) 10% storage left (major incident reaction level)
CPU usage	The utilization of CPU shall be recorded over time for analytical purposes. An alert shall be raised, if: the average CPU is more than 75%. the integration server CPU is more than 90%.
Memory usage	The utilization of memory shall be recorded over time for analytical purposes. An alert shall be raised, if: the application servers' utilization of memory over time exceeds 90%.
Windows services	Monitors that all auto started services are running.

F2 surveillance services

If the F2 services listed below are not running an alert shall be raised.

> **Note**: There are more services and scheduled tasks depending on the installed F2 add-on modules.

Integration server

Windows services:

- MailImportservice
- PdfGeneratorservice
- Queuehandlerservice
- Outputmangerservice
- Digitalmailservice (if used).

These task scheduler jobs must be monitored to ensure they have run successfully:

- Mailimport
- Mailsend
- Folderimport
- AdXmlImporter (if exported from different domain)
- AdImport (synchronise user information in F2 with the AD, if installed)
- Cockpit (database queue monitoring tool).

Application server

Checks that the webserver is running, and that the following sites are available:

- F2Service
- F2authenticationservice.

> **Note**: More sites can be monitored, if needed depending on the installed F2 add-on modules.

Mobile server

Windows services:

- Submissionservice

Checks that the webserver is running and that the following sites are available:

- F2Rest
- F2Touch

> **Note**: More sites can be monitored, if needed. Additional sites are typically created when setting up self-service solutions.

Monitoring the F2 system

The Cockpit tool

cBrain uses a tool called F2 Server Cockpit tool to monitor queues in the database. From F2 version 8 the Server Cockpit tool is standard and is installed as part of the cBrain automatic installation tools.

The Server Cockpit runs as a scheduled task and performs several counts towards tables in the database.

Cockpit raises an alert if:

- the amount of waiting tasks in a queue rises beyond a defined value.
- the number of failed messages changes.

As a minimum, Cockpit monitors:

- the number of messages that have an error (have failed).
- the number of documents waiting for the PDF generator.
- the number of e-mails that have failed when importing to F2.

The configuration and setup of the cockpit tool may only be carried out by cBrain authorized consultants.

By default, all alerts are sent as mail via as SMTP to administrator account for support.

Performance log

F2 collects data about transactions in a table called Performance log.

Each entry contains information about:

- Logtime
- StaffID (user number)
- Login (user initials)
- Elapsedtime (time to perform operation)
- Message (F2 action)
- Client host address (IP from client)
- LogType (method that was performed)

As a standard, alerts shall not be raised based on the performance log.

Based on the data, incidents can be investigated, and trends can be analysed. Since the table contains a lot of data, job reading from the table during normal operation shall not be run. As consulting services, cBrain can set up a special Log4Net-appender

to distribute the data to the customers administrator account limiting the effect o the performance of the online system.

Service logs

Each service (including web services) has its own log. The logs are located under the module's name.

F2 uses Log4Net as the logging component. The logging level can be changed in the configuration file.

Logs are by default placed in a Log folder under the F2 installation path but can be placed on a separate drive or in a different location.

The logs contain information about each of the operations the service has performed.

The service and cockpit surveillance will catch failed messages and the service logs are meant to support the incident management process when failures occur.

The logs are created as txt-files with a default size of 1 MB. Based on the configuration the logs are overwritten after a period of time (by default 100 files).

The customer must implement a log archive tool, that compresses and stores the logs in a specified folder. This prevents the logs from being overwritten. On consultancy basis cBrain can help implement tool for compressing log files.

Client log

The F2 client (PC), has a log that collects information about each action performed in the F2 client.

The client log is by default placed in:
\%Users%\<user>\AppData\Roaming\cBrain\cF2\Logfiles

For F2 system administrators the log can provide information about the causes of the incidents in F2 (e.g. timeout, insufficient rights etc.).

When an incident is reported to cBrain's, cBrain must have access to the log file for trouble shooting.

IIS log and Windows logs

F2 is a Windows application, that depends on Windows .Net framework, and Windows IIS server. Therefore, a lot of events are logged in the Windows event log, and Windows IIS log.

System administrators should also check these logs, in case of incidents in the F2 services.

> **Note**: cBrain recommends contacting cBrain F2 Support in case of any doubts regarding F2 incidents.

F2 server maintenance

cBrain patch policy, Windows updates etc.

cBrain recommends that customers follow normal patch procedures on the F2 servers. In some cases, a specific patch level can be required for the F2 system to maintain normal operations. In this case the required patch level will be stated in our software and hardware requirements documents.

Note: cBrain installs a Windows update patch on our systems immediately after they are released. If any problems occur, a recommendation regarding the patch will be released to our customers.

Backup procedures

It is the responsibility of the organisation's IT department to assess an appropriate level of backup strategy and security for the backup strategy. On consultancy basis cBrain can provide input to the customers back-up strategy.

It is the responsibility of the organisation's IT department to make the customers F2 administrator ware of the backup strategy and ensure that the organisation performs a recover exercise at least 2-3 times a year. Considerations regarding the highest acceptable level of data loss in a disaster scenario should be considered.

It is the responsibility of the organisation's IT department to maintain a disaster recovery plan that must be shared with the appropriate system owner and administrators. If cBrain has a part in the disaster recovery plan appropriate agreements must be made with cBrain beforehand.Anti-virus

The customer's normal antivirus procedures shall be followed on F2 servers. However, for F2 specific folders the following rules must apply:

- Microsoft's best practice procedures are followed on SQL servers e.g All data and logfiles for databases are excluded from any virus scanning etc.
- Log files on servers and PCs are excluded from "on access" scans.
- <F2 home>\ .. See hardware and software requirements for detailed information on which folders to avoid.

Database server maintenance

Regular maintenance shall be carried out regarding:

- Consistency check.
- Index defragmentation.

Backup and other database maintenances shall be carried out according to best practice for Microsoft SQL server.

The database server shall be patched on a regular basis. In case of any doubt regarding SQL server maintenance, please contact cBrain for support.

Starting up the F2 environment

Starting up a F2 environment requires an accessible Active Directory where the users are defined.

The servers shall be started in the following order:

1. The database server
2. The authentication server if present (if users' AD is in another domain)
3. The application server
4. The mobile server
5. The integration server (depends on the database).

Please ensure that each server is running and fully operational, before moving on to the next server.

Shutting down the F2 environment

To shut down the F2 system correctly, the servers should be shut down in the following order:

1. The mobile server (if one exists)
2. The application server
3. The integration server
4. The database server

Note: The integration server and the services on the server can be restarted without affecting the user's connections, and normally users will not notice it.

The shutdown/restart of the application server will affect the user's connection to the F2 services, and there is a risk of data loss.

The shutdown/restart of the mobile server causes F2 Touch and F2 Manager to be disconnected. If the customer has any self-services, they will also be affected.