



## API Installation Manual





# Table of Contents

## Chapter 1: Installation

Flex API Installation .....	1-1
Pre-Requisites .....	1-1
Server Requirements .....	1-1
Mobile Device Requirements .....	1-1
Installation .....	1-3

## Chapter 2: Setting Up Flex

Setting Up the Flex API .....	2-1
SSL Certificates .....	2-1
Importing a Certificate .....	2-3
Self-Signed Certificates .....	2-4
Site Bindings .....	2-5
Adding a New HTTPS (SSL) Binding .....	2-5
Adding a New HTTP Binding .....	2-6
Creating an API Client Key .....	2-7

## Chapter 2: Connecting Mobile Devices

Connecting to the Mobile Device .....	3-1
---------------------------------------	-----

This Page Intentionally Left Blank

# Installation

# 1

## ***In This Chapter***

- ✓ Flex API Installation
- ✓ Configuring Flex API

Flex API is a clean and easy-to-use open platform for developing third-party interfaces to Open Options' DNA Fusion access control software. The Flex API will allow for the development of applications utilizing the following features:

- Add, delete, modify Personnel records and the credentials assigned to them
- Assign, remove and modify Access Levels as well as Personnel and Access Level Groups
- Control hardware devices and receive their state and status
- Receive Events and Alarms with Alarm management
- Generating commonly used personnel and hardware reports
- Capability to view and control integrated DVR cameras
- Auditing of any actions implemented through the API Key

The Flex API installation process is very straightforward. While the installation can be performed without any knowledge of the software, configuring the application requires some knowledge of software development.

## **Flex API Installation**

The Flex API application must be installed on the computer that hosts the DNA Fusion driver. Contact Open Options Technical Support for the API installation file.

### ***Pre-Requisites***

#### ***Server Requirements***

- DNAFusion version 6.0 or above is required.
- .NET 4.0 Framework
- Must be installed on the DNAFusion server.
- Windows 7 Professional or higher
- XML-RPC



*The setup procedure must be performed with an administrator logon.*

#### ***Mobile Device Requirements***

- iPhone app is available for iOS 6 and higher. DNA Fusion can be downloaded from the App Store.
- Android (mobile devices and tablets) app is available for ICS 4.0 and up. DNA Fusion can be loaded from Google Play.

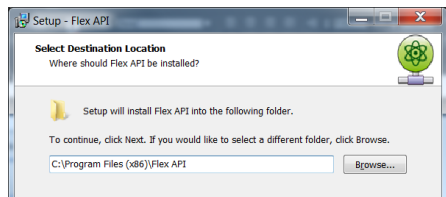
This Page Intentionally Left Blank

## Installation

The Flex API must be installed on the DNAFusion server running the DNAdrvr32 service.

1. **Double click** the Flex API Install icon to begin the installation.  
The Welcome screen will appear.
2. **Click** the Next button to continue.  
The Select Destination window appears.
3. **Click** Next to accept the default Destination Location or **click** the Browse button to **select** a different location.

The default location for a 32-bit environment is C:\Program Files\Flex API and C:\Program Files (x86)\Flex API for 64-bit environments.



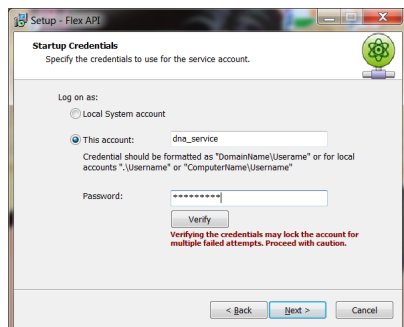
The Startup Credentials screen appears.

4. If needed, **select** This account, **enter** the Service Account information in the fields and **click** Next.  
Or

If the DNAdrvr32 service is already running under a named account, the information will be prepopulated.

The Flex API requires a service account to run the application; this account will need to be a local machine Administrative in order to operate.

Open Options recommends using the same account the DNA Fusion driver utilizes. The Flex API uses the same COM objects, database connections and file permissions as the DNA Fusion driver (dnadrvr32).

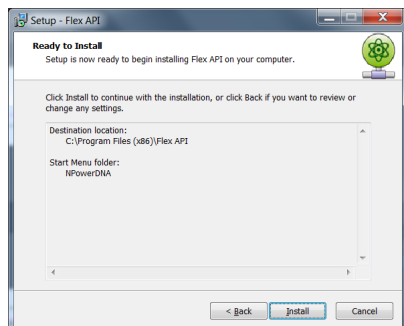


The Start Menu Folder screen appears.

5. **Click** Next to accept the default Start Menu location or **click** the Browse button to **select** a different folder.

The installation will attempt to place the Flex API in the same location as the DNAFusion shortcut.

The Ready to Install screen appears.

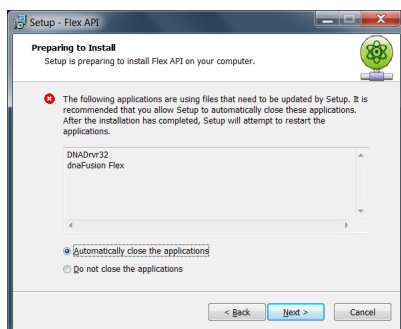


6. **Click** the Install button to start the installation process.

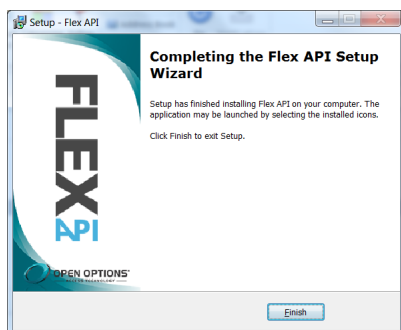
Installation will begin.

If the DNADrvr32 service is running, it will be stopped and a dialog will appear. **Click** the Next button to continue.

7. When installation is complete a dialog box will appear, **press** Finish to complete the set up.



8. The Flex API installation is complete.





# Setting Up Flex 2

## ***In This Chapter***

- ✓ Setting up the Flex API
- ✓ Configuring Certificates
- ✓ Editing Site Bindings
- ✓ Creating API Client Keys

The Flex API configuration depends on a number of variables. In this chapter we will cover the various setup components.

## **Setting Up the Flex API**

After installing the Flex API application, there are a number of settings that need to be configured in order for the application to successfully communicate with the Flex API.

These settings include certificates and bindings as well as API client keys if the application will be used for third party integrations.

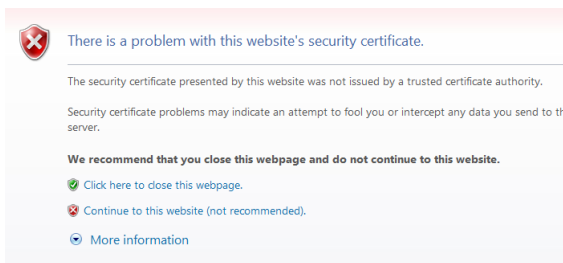
- Certificates are used to secure the data between the Flex API application and the mobile devices.
- Bindings allow communication through the use of ports.
- An API client key is only required for third party applications to access the service.

### ***SSL Certificates***

Secure Sockets Layer (SSL) certificates are not required however Open Options highly recommends the use of SSL certificates. By default, mobile devices are configured to use SSL certificates. Certificates can be purchased from a number of online providers.

There are 2 types of security certificates: Signed Certificate by a certificate authority and Self-Signed Certificate.

- Signed Certificate: A certificate authority (CA) confirms that the server's information has been verified by a trusted source. Depending upon which CA is used, the domain is verified and a certificate is issued.
- Self Signed: If the connection is self-signed, this will be flagged as potentially risky and an error message will be displayed alerting the user to not trust the site. The user must select the Continue to Website option to continue.



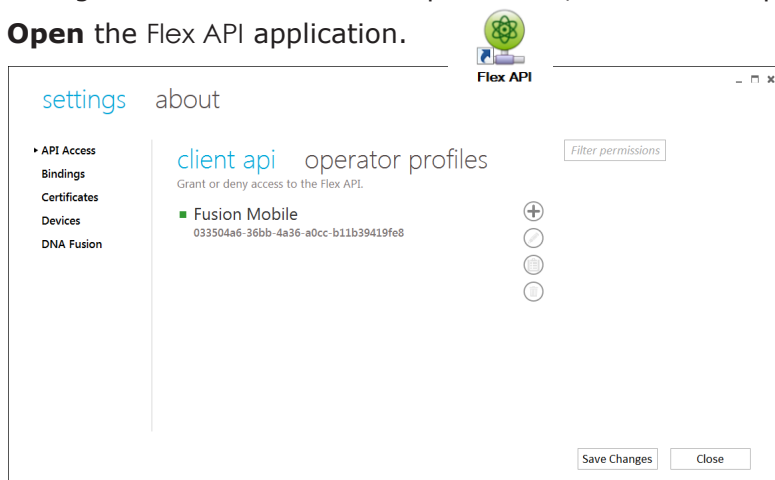
Both certificates will generate a site that cannot be read by third-parties. The data sent over an https connection or SSL, will be encrypted regardless of whether the certificate is signed or self-signed. In other words, both types of certificates will encrypt the data to create a secure website.

This Page Intentionally Left Blank

## Importing a Certificate

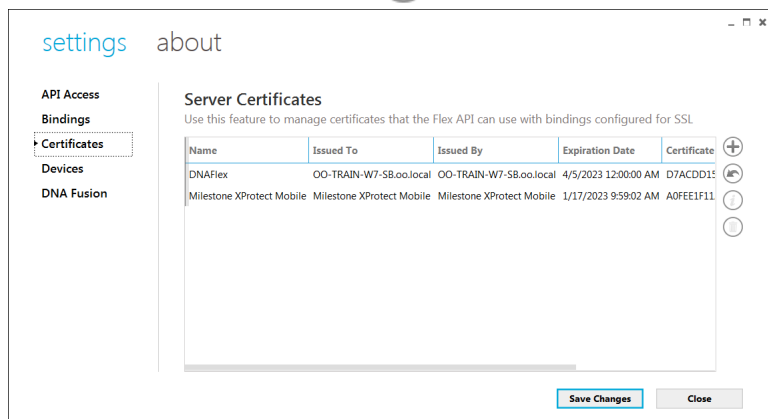
Once a Signed Certificate has been purchased, it must be imported into the Flex API before it can be used.

1. **Open** the Flex API application.



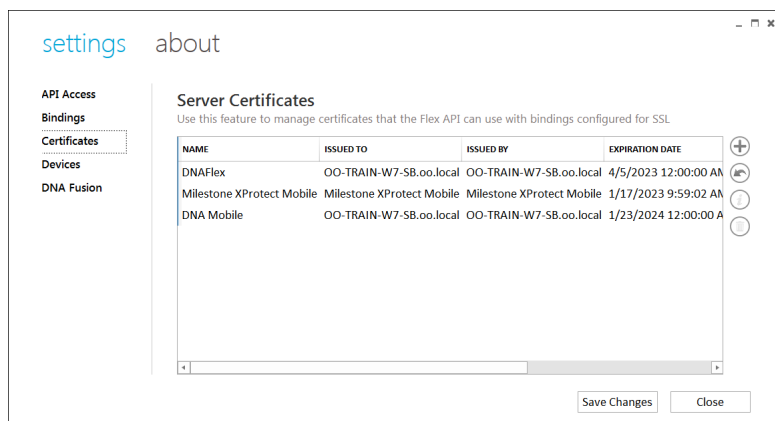
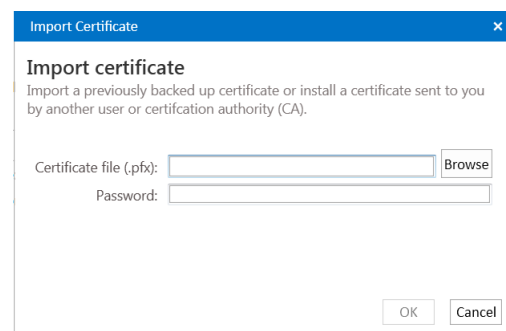
2. **Select** the Certificates option from the Main Menu on the left. The Server Certificates dialog appears.

3. **Click** the Import Certificate  button.



The Import Certificate dialog opens.

4. **Click** the Browse button and **locate** the .pfx certificate file. If required, enter the Password.
5. **Click** the OK button to save the file. The new SSL certificate will appear in the Certificates dialog.



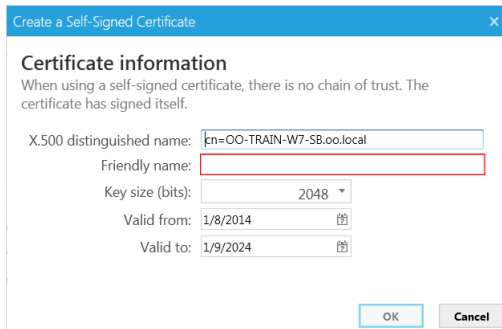
## Self-Signed Certificates

Self-signed certificates can be used for testing or when a verified certificate is not required.

To create a self-signed certificate:

1. **Click** the Create Self-Signed Certificate  button from the menu.

The Create a Self-Signed Certificate dialog will open.



**Create a Self-Signed Certificate**

**Certificate information**  
When using a self-signed certificate, there is no chain of trust. The certificate has signed itself.

X.509 distinguished name:

Friendly name:

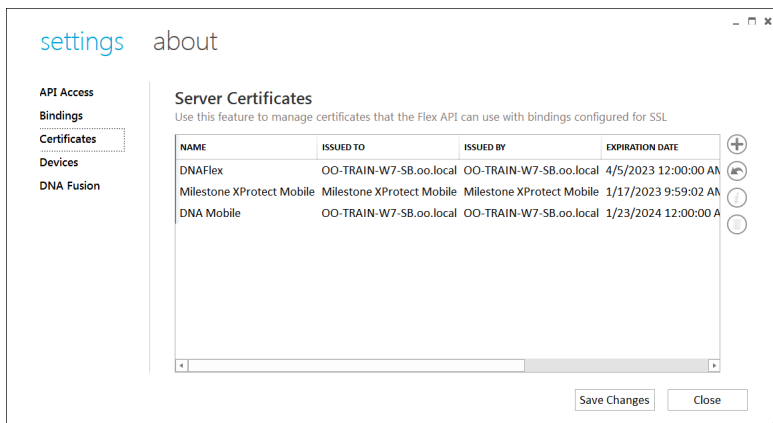
Key size (bits):

Valid from:

Valid to:

Open Options recommends that the default settings be used.

2. **Enter** a Friendly name for the certificate.  
This name will be used to identify the certificate later.
3. **Click** the OK button to save the self-signed certificate.  
The certificate will appear in the Certificates dialog.



**settings** **about**

**API Access**  
**Bindings**  
**Certificates**  
**Devices**  
**DNA Fusion**

**Server Certificates**  
Use this feature to manage certificates that the Flex API can use with bindings configured for SSL

NAME	ISSUED TO	ISSUED BY	EXPIRATION DATE
DNAFlex	OO-TRAIN-W7-SB.oo.local	OO-TRAIN-W7-SB.oo.local	4/5/2023 12:00:00 AM
Milestone XProtect Mobile	Milestone XProtect Mobile	Milestone XProtect Mobile	1/17/2023 9:59:02 AM
DNA Mobile	OO-TRAIN-W7-SB.oo.local	OO-TRAIN-W7-SB.oo.local	1/23/2024 12:00:00 AM

4. **Click** the Save Changes button in the Server Certificate dialog.

## Site Bindings

Bindings define which ports the Flex API application will accept communication on.

The following ports are used by default.

- Listening Port - 8888
- Web Page Port - 80
- SSL Communication Port - 443.

If any changes are made to the binding ports, the dnaFusion Flex service will need to be restarted for the changes to go in effect.

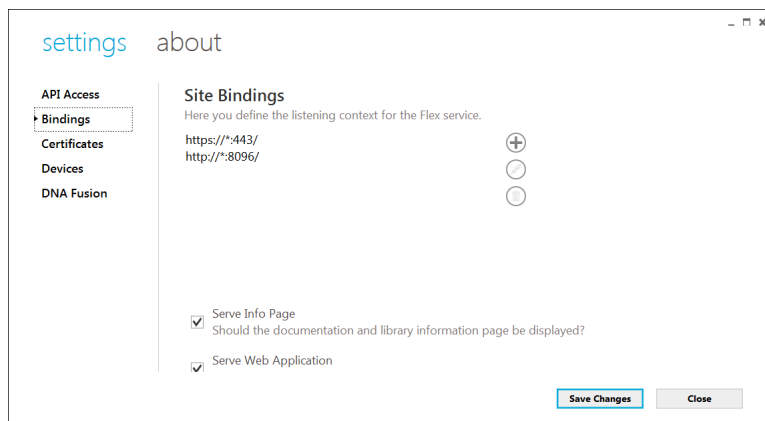
There are two types of bindings:

- HTTPS (SSL) Bindings - Uses an encrypted protocol to access secure webpages and requires an SSL certificate.
- HTTP Bindings - Basic unencrypted protocol.

### Adding a New HTTPS (SSL) Binding

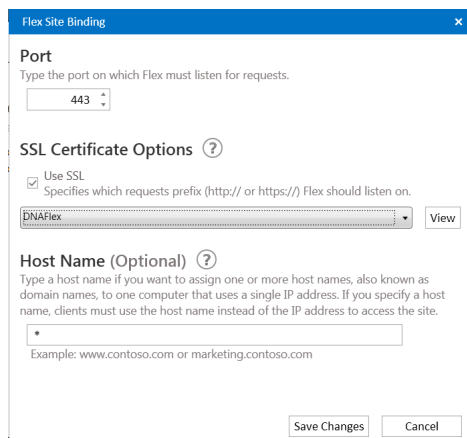
1. **Select** the Bindings option from the menu on the left hand side.

The Site Bindings dialog appears.



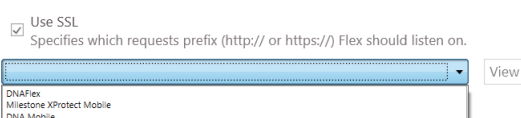
2. **Click** the Add (+) button to define the new binding.

The Flex Site Binding dialog opens.



3. Use the following parameters to configure the binding.

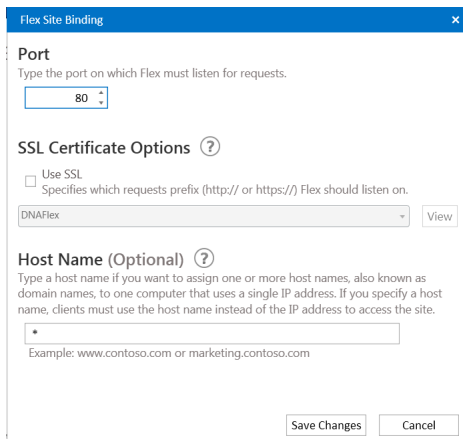
- Port: 443
- **Select** the Use SSL checkbox
- **Select** the imported SSL or self-signed certificate from the drop down



4. If desired, **enter** a Host Name.  
If a host name is specified, clients must enter the host name to connect to the site instead of the site's IP address.
5. **Click** the Save Changes button.  
The new binding is added to the Site Bindings dialog.
6. **Click** the Save Changes button in the Site Bindings dialog.

## Adding a New HTTP Binding

1. From the Bindings dialog, **click** the Add  button to define the new binding.  
The Site Bindings dialog appears.



2. Use the following parameters to configure the binding.
  - Port: 80
3. If desired, **enter** a Host Name.  
If a host name is specified, clients must enter the host name to connect to the site instead of the site's IP address.
4. **Click** the Save Changes button.  
The new binding is added to the Site Bindings dialog.
5. **Click** the Save Changes button in the Site Bindings dialog.



*Changes to the bindings will require a restart of the dnaFusion Flex service in order for the changes to take effect.*

## Creating an API Client Key

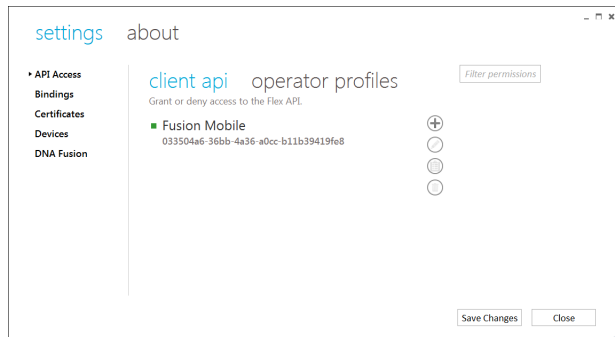
Flex API requires a unique API key to access the services for third party applications. The application programming interface (API) key is used to authenticate the application.

The API key often acts as both a unique identifier and a secret token for authentication. Each Flex API has a set of access permissions/rights associated with it.

1. **Open** the Flex API interface.

Default location: Start / All Programs / NPowerDNA / Flex API

The Flex API opens.




2. From the API Access page, **click** the Add button  to add a new API Client.

The Flex Client API dialog opens.

3. **Enter** a Name for the API Client.

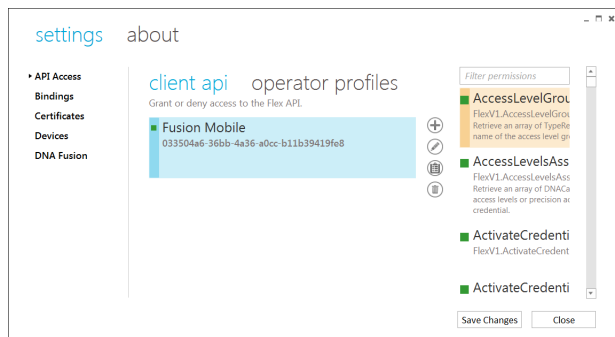
This name will be used for operator's audit entries.

4. If desired, **enter** a Description.

5. If needed, a new API Key can be generated by **clicking** the Refresh button .

6. **Click** the Save Changes button.

The Flex Client API key is added to the list and a list of permissions is displayed in a menu on the right. See page x-x for more information on operator permissions.



*To disable a Flex API Client without deleting it, uncheck the ALLOW ACCESS checkbox.*

This Page Intentionally Left Blank



# Connecting Mobile Devices

# 3

## In This Chapter

- ✓ Host Name Information
- ✓ Connecting to a Mobile Device

The DNAFlex API for mobile devices allow users to control the DNAFusion Access Control system through a management app on iPhone and Android devices.

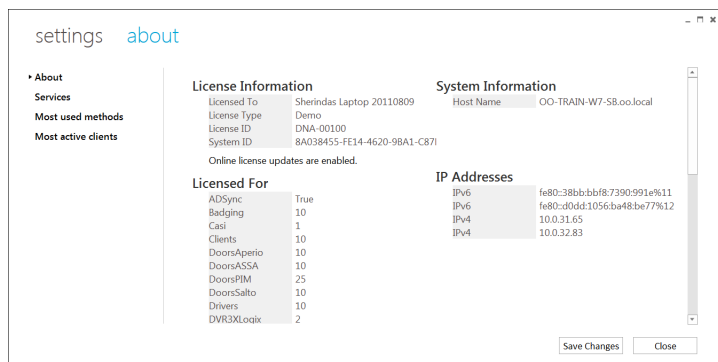
In order for a mobile device to connect to the Flex API, the device must be configured with the host name or the IP address of the workstation that is running the Flex API service.

This information can be obtained by checking the About dialog within the Flex API application. The About view displays the computer's host name along with the available IP addresses.

### To view the About dialog:

1. **Select** the About option from the menu at the top of the application.

The About screen is displayed.

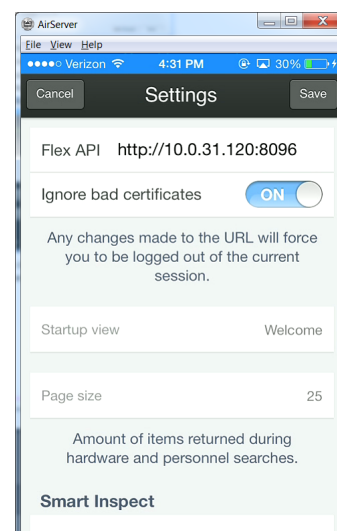


The License information is displayed along with the computers Host Name and all available IP addresses.

2. Note of the Host Name.

## Connecting to the Mobile Device

1. **Start** the DNA Fusion application on the mobile device.  
The DNA Fusion Mobile Main Screen is displayed.
2. **Click** the Settings button.  
The Settings screen appears.
3. **Enter** the Host Name in the Flex API field.  
If needed, **enter** the port number.
4. If using a self-signed certificate, **turn** the Ignore Bad Certificates OFF.  
If the site is using a valid SSL certificate, either setting can be selected.
5. **Click** the Save button.  
The DNA Fusion Mobile Main Screen appears.



This Page Intentionally Left Blank