



vFire Officer App
Server Installation Guide
Version 1.3

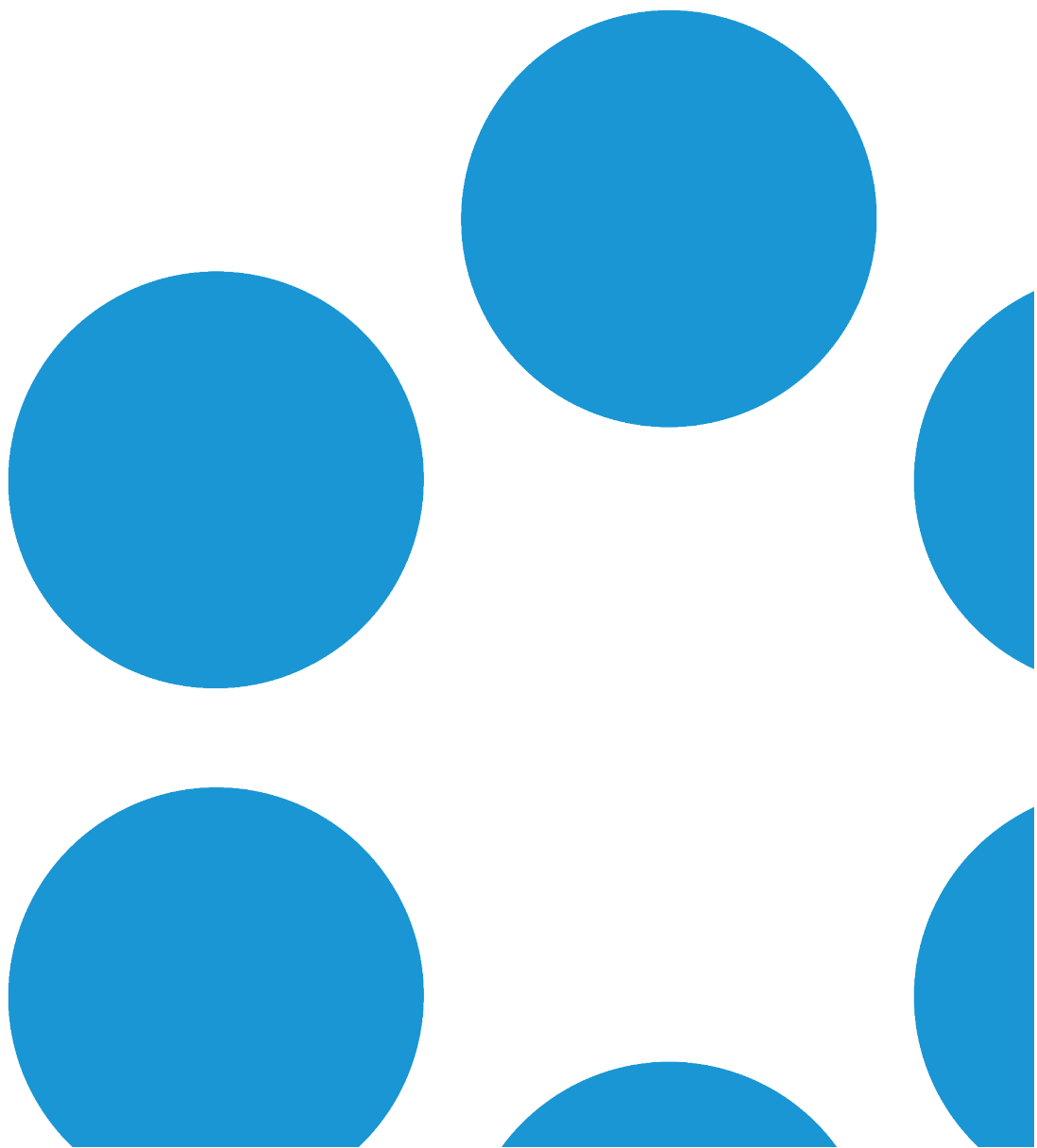




Table of Contents

Version Details	3
Online Support	3
Copyright	3
About this Document	5
Intended Audience	5
Standards and Conventions	5
vFire Officer App Prerequisites	6
Configuring your System for the vFire Officer App	7
Finding the App	7
Supported Platforms	7
Security and Authentication for the vFire Officer App	8
Scenario 1: DMZ with an Application Server	9
Scenario 2: DMZ with Reverse Proxy Server. Windows Auth Disabled	10
Scenario 3: DMZ with Reverse Proxy Server. Windows Auth Enabled	12
Disabling SSL for the vFire Officer App	14
Enabling the Logout Timer for the vFire Officer App	15
Getting Support	17



Version Details

This document supports the version of the product listed. The table below contains version details for the guide.

Version No.	Date	Details
1.0	1 April 2015	This guide documents the configuration of the vFire Officer mobile application.
1.1	17 July 2015	This version documents the changes introduced with the release of vFire Core 9.2.2. With this release, you are no longer required to use the 9.2.1 hotfix.
1.2	15 August 2016	This version documents the latest requirements and updates for the app, following release.
1.3	17 May 2017	This version of the documentation is released to coincide with the 9.8 software release.

Online Support

For information about Alemba products, or licensing and services, visit:

www.alemba.com.

For software updates, documentation, release notes and support using the system, visit:

www.alemba.help/help



You may need to register to access some of these details.

Copyright

Copyright © Alemba Limited (or its licensors, including ©2010 - 2017 VMware, Inc). All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at: <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. VMware Service



Manager™ is also trademark of VMware, Inc. Alemba™, vFire™ and vFireCore™ are trademarks of Alemba Limited (vFire Core™ is developed by Alemba Limited from VMware, Inc's product "VMware Service Manager", under licence from VMware, Inc). All other marks and names mentioned herein may be trademarks of their respective companies.



About this Document




This guide documents the steps which need to be carried out in order to configure the system before installing the vFire Officer mobile application.

Intended Audience

This document is written for system administrators who are responsible for the configuration of the server to support Officers using the vFire Officer mobile app.

Standards and Conventions

The following standards and conventions are used throughout the document:

	Prerequisites, including security rights and access you may need prior to completing the task. Prerequisites are also highlighted in a shaded box.
	Information related to the current topic that may be of interest/significance to certain users. Notes are also highlighted in a shaded box.
	Warnings. These are also highlighted in a shaded box.
Field name	Fields are highlighted in bold text.



We have used **System1** as our example in screenshots, etc. Where it appears in the instructions, we have indicated it in **blue font**.



vFire Officer App Prerequisites

Ensure that your system meets the following prerequisites before configuring your environment for the vFire Officer app.

- You need to be using vFire Core 9.2.2 or above (server version)
- Your mobile device must be able to navigate to the vFire HTML pages delivered via IIS web services. This may require you to configure your firewall.
- You must have a valid vFire login account, and be flagged as an Analyst.
 - If Directory authentication is used, you may need to configure a second basic authentication system.
 - Microsoft Active Directory or Novell eDirectory authentication are excluded from V1.0.0 of this mobile app.
- You must know your system name and URL to configure the settings when you first use the app. Your system administrator will provide these.

Specific Versions

The app is supported on the following iOS and Android mobile operating systems:

- Windows Phone 8.1
- iOS versions 7 or higher
- Android versions 4.3 or higher

It has been tested on the following devices. (Other devices are also supported.)

- iPhone 5
- iPhone 6
- Samsung Galaxy S3
- Sony Xperia Z3
- HTC One



Configuring your System for the vFire Officer App

Before analysts can install the vFire Officer app on their mobile devices, there are some preparatory steps which need to be carried out in order to configure the system.

Once these steps have been carried out, analysts can install and use the app as outlined in the **vFire Officer Mobile App User Guide**.

You need to carry out the following steps. Select the appropriate links for full instruction.

1. Ensure that your system meets the **prerequisites**.
2. **Configure the environment** for a DMZ, if Windows Authentication is enabled in vFire Core.
3. **Disable SSL** if you do not have SSL running on your system.
4. **Enable the logout timer** if you want it to differ from the standard application logout timer.
5. **Download the app**.

Finding the App

The app is available from the following stores:

- **itunes** - <https://itunes.apple.com/gb/app/vfire-officer/id966173033?mt=8>
- **google play** - <https://play.google.com/store/apps/details?id=com.alemba.vfireapp>
- **microsoft** - <https://www.microsoft.com/en-us/store/p/vfire/9nblggh4wkvs>

Supported Platforms

vFire Core 9.2.2 and above



Security and Authentication for the vFire Officer App

The vFire Officer app provides connectivity from a mobile device, usually located on a public network, to a vFire Core system inside the corporate network.

Depending on organizational security requirements, the recommended environment and security configurations may differ. The most common security recommendation is to create a demilitarized zone (DMZ) containing a reverse proxy server buffered by firewalls.

Three scenarios involving a DMZ are outlined in this topic and provide recommended configurations based on whether or not Windows Authentication is enabled on the vFire Core system within the secure network.



The app is not compatible with Windows Authentication, and must be configured to use a virtual directory with Anonymous Authentication enabled.

The three scenarios are:

- DMZ contains an Application Server with vFire Core installed. The vFire Core system within the secure network may / may not have Windows Auth enabled.
- DMZ contains a reverse proxy server. The vFire Core system within the secure network has Windows Authentication disabled.
- DMZ contains a reverse proxy server. The vFire Core system within the secure network has Windows Authentication enabled.

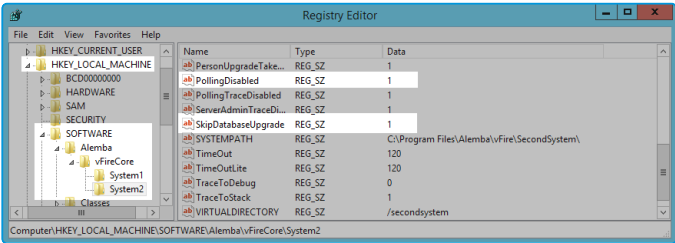
Work with your Network Administration teams to create a DMZ to safely expose connections to your vFire system.

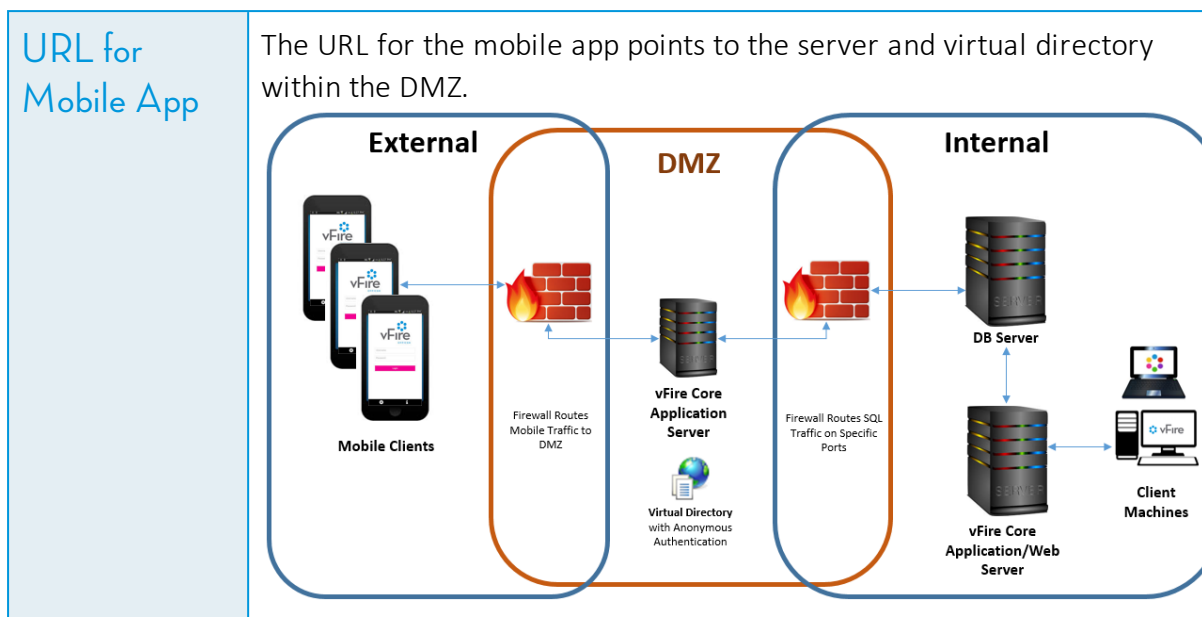
Ports for the vFire Mobile App

	HTTP	HTTPS	SQL
Ports	80	443	1433, 1434



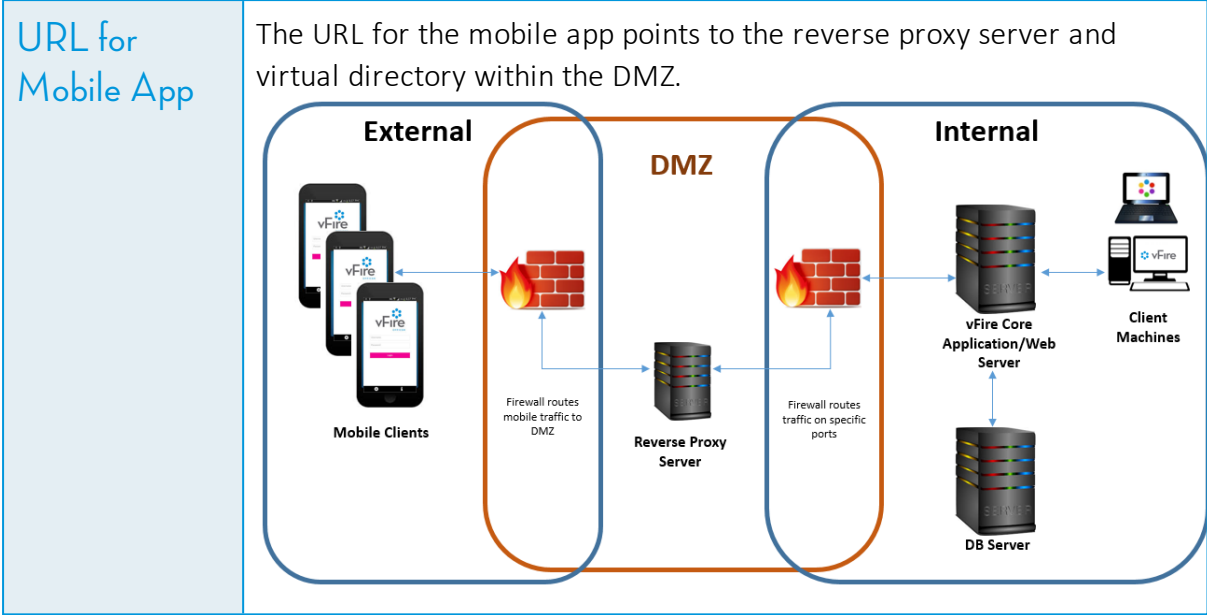
Scenario 1: DMZ with an Application Server

Internal network	The internal server's vFire Core system may or may not have Windows Authentication enabled; it has no effect on this configuration.
DMZ	<p>A second application server is configured within the DMZ to act as a reverse proxy server.</p> <p>On this server in the DMZ:</p> <ul style="list-style-type: none"> • A vFire Core system is created that points to the same database as the internal vFire Core system. <div data-bbox="549 748 1391 860" style="background-color: #e0f0f0; padding: 10px; border: 1px solid #ccc;"> <ul style="list-style-type: none"> • During system creation, when prompted to update the database, select No </div> <ul style="list-style-type: none"> • In the virtual directory for this system, Windows Authentication is disabled and Anonymous Authentication is enabled. • All vFire Core services are stopped and their "Start Up" property is set to Manual. • In the registry key for the new system, polling of services is disabled via registry string <code>PollingDisabled = 1</code> • In the registry key for the new system, database upgrade is disabled via registry string <code>SkipDatabaseUpgrade = 1</code> 



Scenario 2: DMZ with Reverse Proxy Server. Windows Auth Disabled

<p>Internal network</p>	<p>The internal server's vFire Core system does not have Windows Authentication enabled.</p>
<p>DMZ</p>	<p>A reverse proxy server is configured within the DMZ.</p> <p>On this server in the DMZ:</p> <ul style="list-style-type: none"> • IIS is installed • A virtual directory is created, with Windows Authentication disabled and Anonymous Authentication enabled. • IIS is configured to redirect traffic to the vFire Core application server and virtual directory within the internal secure network.






Scenario 3: DMZ with Reverse Proxy Server. Windows Auth Enabled


Internal network

The internal server's vFire Core system has Windows Authentication enabled.

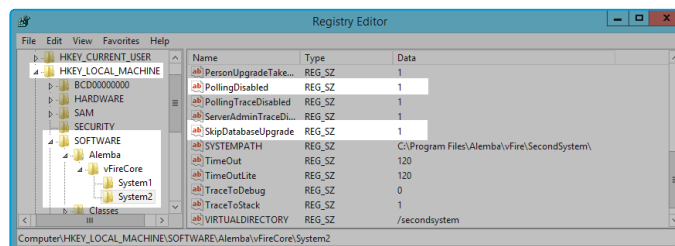
 vFire Officer Mobile App is not compatible with Windows Authentication and must use a virtual directory with Windows Auth disabled.

On the internal server:

- A second vFire Core system is created that points to the same database as the primary vFire Core system.

 During system creation, when prompted to update the database, select **No**

- In the virtual directory for the new system, Windows Authentication is disabled and Anonymous Authentication is enabled.
- In the registry key for the new system, polling of services is disabled via registry string `PollingDisabled = 1`
- In the registry key for the new system, database upgrade is disabled via registry string `SkipDatabaseUpgrade = 1`





<p>DMZ</p>	<p>A reverse proxy server is configured within the DMZ. On this server in the DMZ:</p> <ul style="list-style-type: none"> • IIS is installed • A virtual directory is created, with Windows Authentication disabled and Anonymous Authentication enabled. • IIS is configured to redirect traffic to the internal application server and the virtual directory that has Anonymous Auth enabled.
<p>URL for Mobile App</p>	<p>The URL for the mobile app points to the reverse proxy server and virtual directory within the DMZ.</p> <p>The diagram illustrates the network architecture. On the left, 'External' shows 'Mobile Clients' (smartphones) sending traffic through a 'Firewall' (brick wall icon) to the 'DMZ'. The 'DMZ' contains a 'Reverse Proxy Server'. A second 'Firewall' routes traffic from the Reverse Proxy Server to the 'Internal' network. Inside the 'Internal' network, there is a 'vFire Core Application/Web Server' connected to a 'DB Server'. Two 'Virtual Directory' components are shown: one with 'Anonymous Authentication' connected to the vFire Core server, and another with 'Windows Authentication' connected to 'Client Machines' (laptops and desktops).</p>



Disabling SSL for the vFire Officer App

If you do not have SSL running on your system, you must disable the SSL in the WEB Config file to enable Officers to use the vFire Officer app.

1. Navigate to the folder containing your system, for example:

C:\Program Files\Alemba\vFire\System1

2. Open the **Web.config** file.
3. Locate the following code:

```
<webHttpBinding>
  <binding name="WebHttpBinding_IServiceManagerMobile">
    <!-- COMMENT THIS OUT TO DISABLE MOBILE SECURE ENDPOINT -->
    <security mode="Transport"></security>
    <!-- COMMENT THIS OUT TO DISABLE MOBILE SECURE ENDPOINT -->
  </binding>
</webHttpBinding>
```

4. Comment it out, as follows:

```
<webHttpBinding>
  <binding name="WebHttpBinding_IServiceManagerMobile">
    <!-- COMMENT THIS OUT TO DISABLE MOBILE SECURE ENDPOINT -->
    <!-- <security mode="Transport"></security> -->
    <!-- COMMENT THIS OUT TO DISABLE MOBILE SECURE ENDPOINT -->
  </binding>
</webHttpBinding>
```

5. Save and close the file.



Enabling the Logout Timer for the vFire Officer App

The vFire Officer mobile app does not have its own session logout time by default. It will use the same logout period as the vFire Core desktop application which is set in the Server Console. The default timeout setting is 120 minutes.

If you would like to enable a specific logout timer for the mobile app then you can do so via the Registry Settings.

1. Navigate to the system location in the Registry Editor. It may be in either of the following locations:

HKEY_LOCAL_MACHINE/SOFTWARE/WoW6432Node/Alemba/vFireCore/System1

HKEY_LOCAL_MACHINE/SOFTWARE/WoW6432Node/EMC/Ionix Service Manager/System1



Within vFireCore are files for each of your systems. If you have more than one system you can check which one it relates to by opening the file and checking the **DATABASE** name.

2. Add the following registry keys.

LogMobileActivityInformation

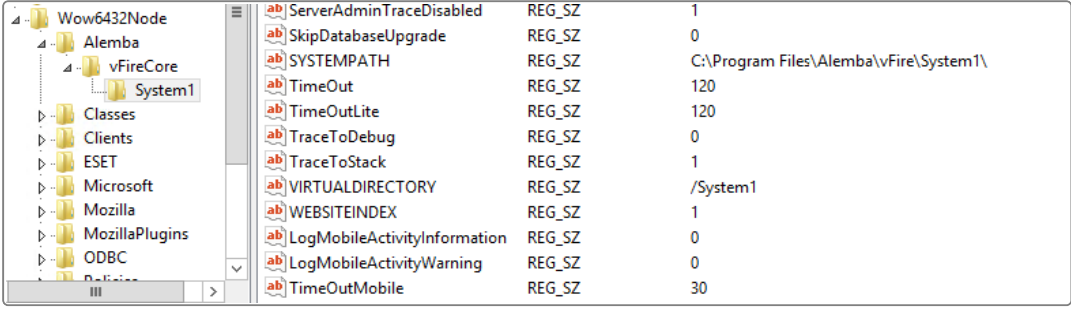
LogMobileActivityWarning

TimeOutMobile

3. Configure **TimeOutMobile** to the number of minutes until the system logs out. The time is taken from the last time an Analyst performs an action in the app such as saving a call or refreshing a list.



4. LogMobileActivityInformation and LogMobileActivityWarning should be set to 0 (zero) if you are not actively monitoring mobile app activity. If you do wish to monitor activity to appear in the Activity Log, select 1.



ServerAdminTraceDisabled	REG_SZ	1
SkipDatabaseUpgrade	REG_SZ	0
SYSTEMPATH	REG_SZ	C:\Program Files\Alemba\vFire\System1\
TimeOut	REG_SZ	120
TimeOutLite	REG_SZ	120
TraceToDebug	REG_SZ	0
TraceToStack	REG_SZ	1
VIRTUALDIRECTORY	REG_SZ	/System1
WEBSITEINDEX	REG_SZ	1
LogMobileActivityInformation	REG_SZ	0
LogMobileActivityWarning	REG_SZ	0
TimeOutMobile	REG_SZ	30

5. Close the file.
6. Perform an IIS reset to implement the changes.



Getting Support

For further support, use any of the following:

Support Numbers	
USA	+1 (855) 261- 1797
UK & Europe	+44 (0) 203 4797900
Australia	+61 (0)2 8520 3584
New Zealand	+64 (0)4 8318797
Support Mail	
servicedesk@alemba.com	
Log in to Support:	
http://www.alemba.help	

