50 QUESTIONS TO FAMOC

FREQUENTLY ASKED QUESTIONS ABOUT FAMOC MANAGE

Prepared by:
Famoc Software Ltd.

FAMOC manage gives you the opportunity to configure security policies, enforce passwords, geolocate devices or even the remote deletion of data stored on a mobile device.

BARTOSZ LEOSZEWSKI
CEO, Famoc

#ObsessedWithSecurity

FAMOC manage simplifies deploying, configuring and managing all smartphones and tablets in your organization. It's one place where you control everything: you can create profiles, enforce restrictions, set PIN and password policies and many more.

From ten devices to ten thousand, corporate-owned or BYOD, enrolling devices is quick, easy and seamless. FAMOC manage allows actions to be carried out on a single handset as well as performing bulk operations on OS-differentiated groups of devices.

What is FAMOC manage?

1. Does FAMOC manage support more than Android devices?

Yes, FAMOC manage supports all of the operating systems - Android, iOS, Windows, macOS*.

2. What are the possibilities of device enrollment in FAMOC manage?

You can enroll devices in FAMOC manage manually or automatically. The easiest way of manual enrollment is to scan a QR code (you can open a QR Reader by tapping a welcome screen on a wiped/ new device 6 times).

You can also enroll a device by using NFC (it requires an additional device already registered in FAMOC and with an active NFC communication) or an activation link that has been send to a user via e-mail or SMS).

This process can be automated thanks to the autoenrollment services, that remotely install and configure an MDM agent after a first run of the device and its connection to the internet. **More information about device enrollment you can find here.**

** Do you want to receive a set of functionalities for specific versions of the system? Contact us and get our functionality matrix!*

3. What device data are showed in FAMOC manage system?

Basic information, e.g.: name, model, manufacturer of the device, its serial number, ID numbers (phone number, IMEI, IMSI (ICCID) or number printed out on a SIM card (ID) that's assigned to a user. We can also monitor the memory usage, Wi-Fi connection, roaming data and unknown sources other that Google Play Store.

4. How many devices can be added to FAMOC manage?

The system allows for a full management of a number of devices stated in purchased license. Each record on the device list is one license that is valid for a specified period of time.

5. Can multiple users have access to FAMOC manage system?

Yes - multiple users can have access to FAMOC manage system. Users can have different, defined roles depending on permissions we want to give them to chosen functionalities and options.

6. What user roles are available in FAMOC? Is it possible to define your own?

In FAMOC, there are several predefined roles available: FAMOC system Administrator, FAMOC Web Services, FAMOC Group Manager, Device or User Groups Management, FAMOC Security Manager, FAMOC Resource Manager. In addition you can also create your own roles.

7. What kind of implementation of FAMOC manage is possible?

We offer an implementation in an internal environment, as well as a hosted solution.

We provide hosting on OVH servers. This implementation is chosen more often by small companies (with fewer devices) that don't have large IT departments, or in cases where the customer needs FAMOC quickly. The minimum cloud license period is 12 months and there's no minimum number of devices,

FAMOC manage system can also be installed on the client's own, physical server, located at the client's premises or based on the client's VMWare environment.
In both cases, implementation, integration and configuration support is provided. This installation option is chosen more often by larger companies, managing a large number of mobile devices, having large IT departments that want a full control over the managed fleet of mobile devices. The on-site license is perpetual.

Optionally, the customer can have a dedicated hosting - in the cloud, but on a separate server.

8. Does FAMOC manage have a remote access feature? Is it included in a standard license?

Remote access feature is available for all FAMOC manage users. It is included in a standard FAMOC manage license so there's no need to purchase it additionaly. **More information you can find here.**

9. What's the difference between FAMOC manage standard and FAMOC manage enterprise versions?

Both versions are based on the same FAMOC manage system. FAMOC manage enterprise version, however, has extended functionalities including API, management of devices with Windows 8 (and newer) and Mac operating system, dedicated VPN solution (FAMOC manage tunnel) and others. You can find a complete comparison of the two versions at **support.famoc.com**.

10. What is FAMOC lock solution?

FAMOC lock solution is based on FAMOC manage system. Its element is an application pre-installed on the device that cannot be removed. The aim is to protect and control devices that were purchased on credit and the end-user pays in installments. In case of overdue fees, the app displays a notification about the lack of payment, which for a specified period of time (e.g. several minutes) cannot be minimized or closed. If the user is still late with payment, the device can be locked remotely.

11. What is FAMOC defend solution?

FAMOC defend solution is also based on FAMOC manage. Because this solution is targeted mainly at the public and government sectors, the priority in this case is the complex requirements related to data protection. Thanks to FAMOC defend, state institutions receive support on the first day for all operating systems, they can control the method of encrypting communication and manage network access from remote devices. It is a tailor-made solution according to the needs of a specific organization.

12. Does FAMOC manage integrate with SSO authentication systems?

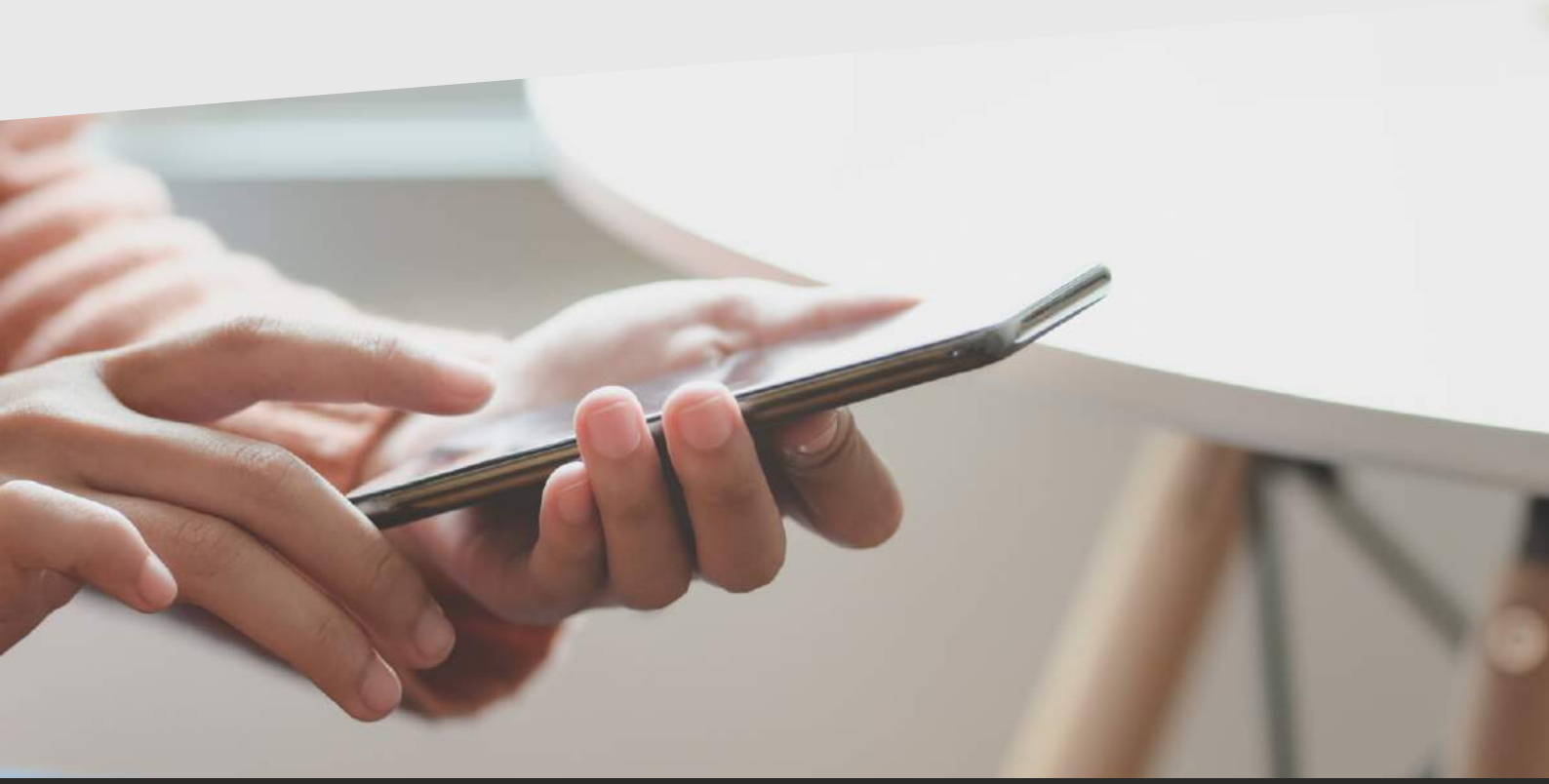
Of course, FAMOC manage has the ability to integrate with authentication and authorization system SSO - Microsoft Active Directory and with solutions based on a SAML protocole - Azure Active Directory, Swivel Secure and Okta.

13. Is it possible to integrate FAMOC manage with mail server Microsoft Exchange?

Yes, FAMOC manage is integrated with mail server Microsoft Exchange and also supports authentication to the Microsoft Exchange server using a private key certificate.

14. My company needs to make reports about managed devices. Is it possible to generate such reports in FAMOC manage?

Sure, In FAMOC manage you can create periodic data reports about managed devices. Reports may contain, among others, information such as: device type and model, version of the operating system installed on the device, list of installed applications along with their version, amount of used and free memory, SIM card serial number etc.



15. Which languages are supported in FAMOC manage?

Languages available in FAMOC manage console are Polish, English and Spanish. In addition, thanks to an extensive partner network, we can support also languages like Russian and German in FAMOC manage system.

16. Where can I find documentation of FAMOC manage?

FAMOC manage documentation, both in Polish and English, is available on **support.famoc.com** - it contains descriptions and instructions intended for users as well as for system administrators. Examples of instructions:

FAMOC Admin Guide
Policy Templates Guide
Adding a new device
Android Enterprise

17. Is the licence assigned per device or per user?

The license is generated for a specified number of devices and time (or perpetual license). After deleting any device, you can re-use a license to register a new device.

18. Can we freely set a registered devices list view as we want?

Yes, the view of the registered devices list in admin console can be modified e.g. in terms of: device model, IMEI number of the device, name and surname of the user, operating system etc.

19. Do you offer any administration or maintenance of FAMOC manage trainings?

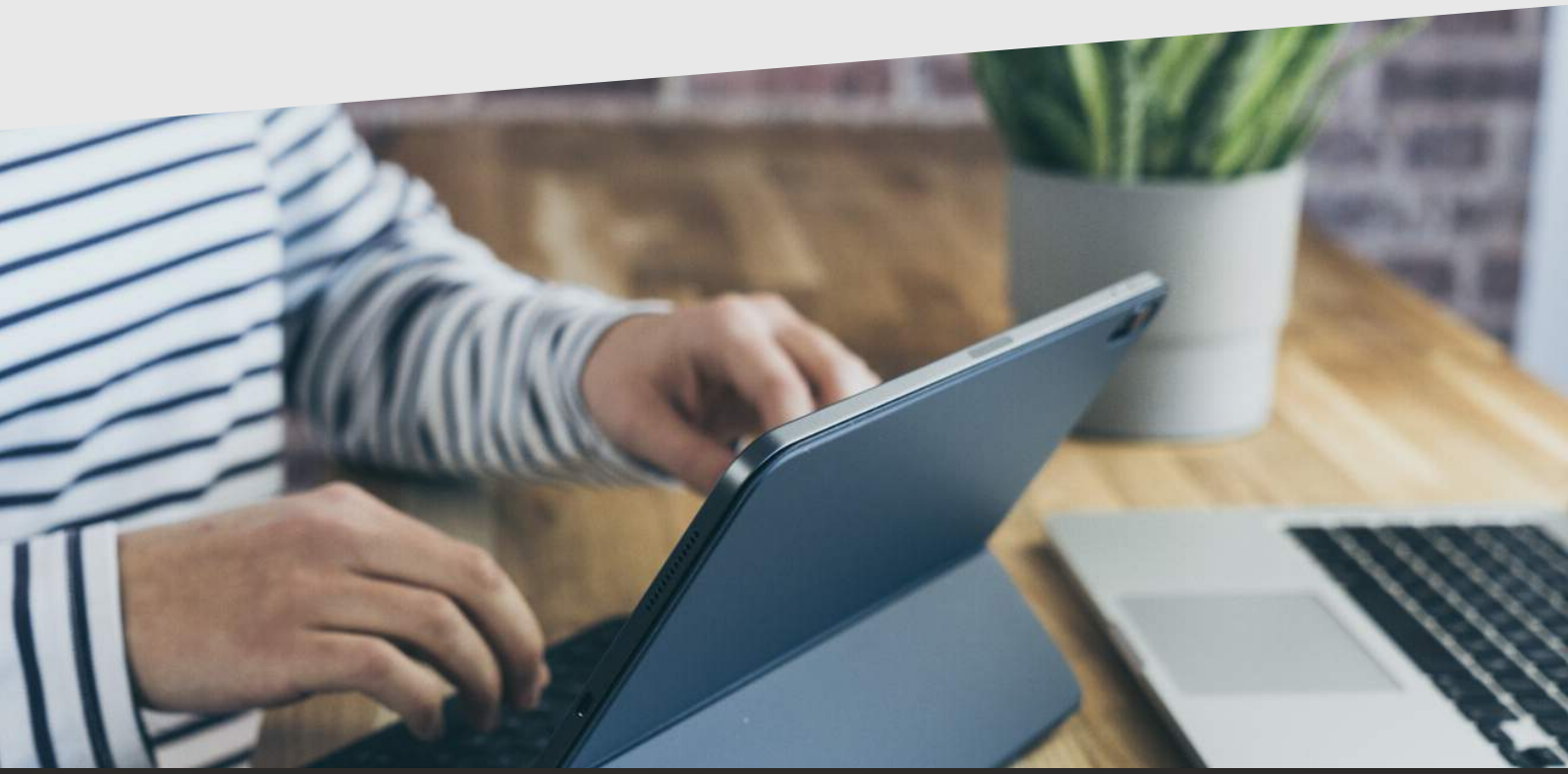
Yes, we offer trainings in various options, depending on the needs. We offer trainings for administrators where attendees learn how to manage and administrate FAMOC manage platform. We also train helpdesk providers, where participants from the technical support departments learn the mechanisms of FAMOC manage system and how to solve potential problems of end users using FAMOC manage. We also support maintenance departments - during these trainings (dedicated for on-site implementations) participants acquire basic knowledge about management and administration of FAMOC manage, but above all they learn how to efficiently navigate FAMOC manage server, database, logs and configuration tools.

20. Is FAMOC manage among Android Enterprise Recommended solutions?

Right now we meet the requirements of Advanced Management Set for both Work Profile and Full Device Management. The next step is of course Android Enterprise Recommended, on which we work very hard. Our current status you can check **here**.

21. What information about location monitoring is available in FAMOC manage system?

The Locations tab enables FAMOC user to monitor devices' or users' positions, which may be retrieved from a mobile device. The administrator can see on the map the last position of every mobile device, which retrieves location data. All listed devices can be sorted on the list by using the chosen column and clicking on the column name. For each device you can see last retrieved location and another 20 previous locations.



#Security

22. What security restrictions we can force on a user?

There are many possibilities for such configurations: forcing the appropriate device lock code (e.g. 6-digit PIN), restrictions related to the use of available WiFi networks, restrictions on availability and use of the applications and web browser, the ability to wipe or block the device in case of theft or loss. There's a lot of similar examples and ways to force security restrictions.

23. Can security restrictions be different for different users / user groups?

Yes. Depending on your needs, you can create multiple security policies / profiles for different user groups and device groups.

24. Can we enforce special restrictions on passwords on the device?

Definitely. We can for example define the requirement to enter the password when starting a device, define the complexity of the password (requirement of numbers, special characters), but also the time of inactivity after which a device gets automatically locked, forcing the password to be re-entered. You can also set the maximum number of attempts to enter a password, followed by the removal of data from the device.

25. What can we do in case of theft or loss of the device?

First of all, we can locate the device. Of course, we can also remotely delete data from the device in case of its loss. We can remotely block device and display a message to the "finder" in case of such a blockade.

26. What options to block the use of Wi-Fi are available in FAMOC manage system?

FAMOC manage provides the following Wi-Fi control options: lock of Wi-Fi interface, block of automatic connection to Wi-Fi access points, block of reporting of Wi-Fi access points and block of manual Wi-Fi configuration.

27. Can FAMOC manage be uninstalled from the device?

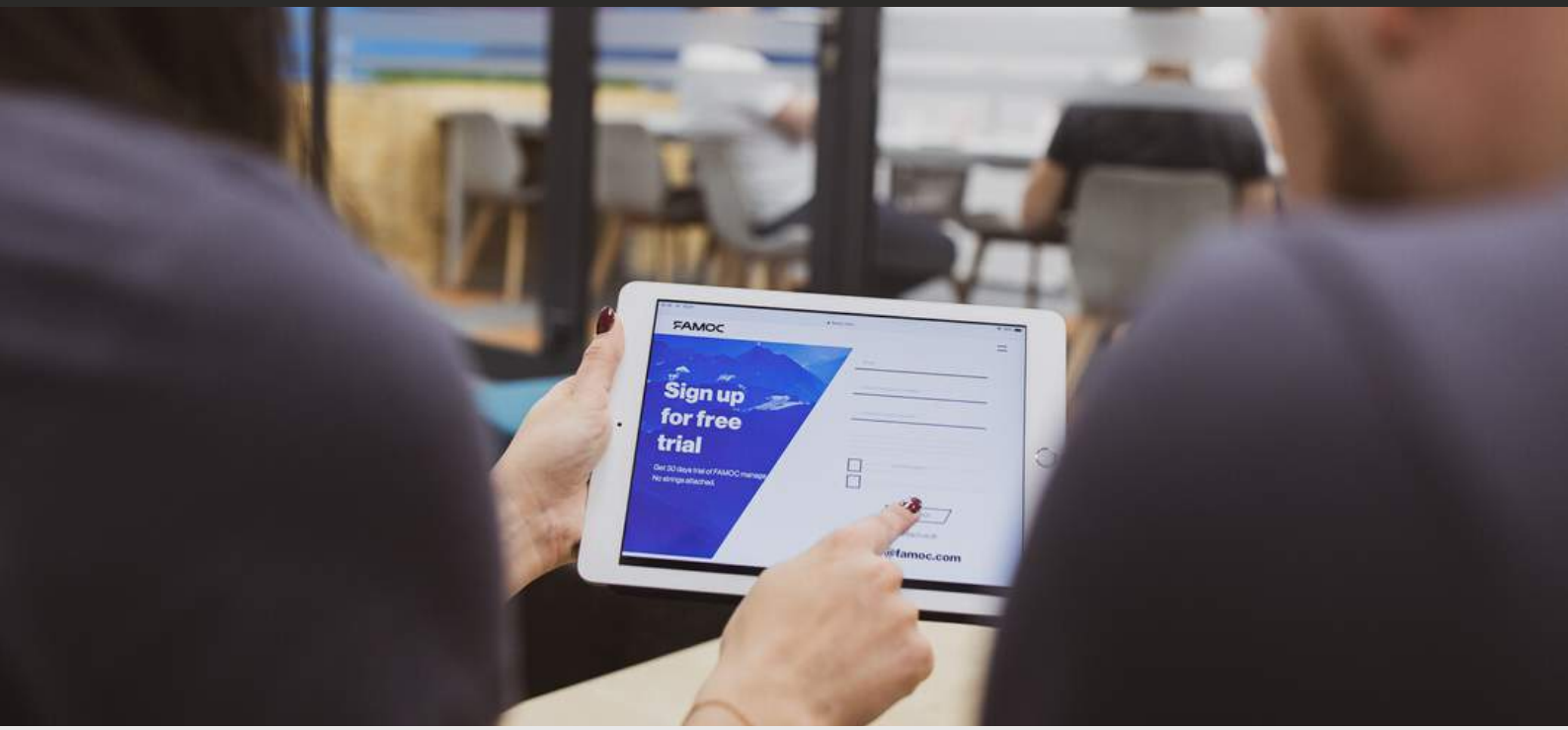
If the device is configured in Device Owner mode, it is not possible to remove FAMOC manage application (only the wipe option is possible). When the device is in a BYOD mode, it is possible to remove FAMOC manage manually.

28. Is it possible to configure the device so that it locks after inserting an unknown SIM card?

Yes, it is possible to lock the device if the SIM card is changed, with simultaneous notification to the administrator.

29. Why does FAMOC manage require an outdated and fairly flawed FLASH solution?

In the past, our remote access solution was based on flash technology (the Remote Access tab in Advanced UI). It has now been replaced by newer technology and modern HTML5 based solution.



30. Is it possible to block selected functions on the phone, e.g. a camera?

Yes, it is possible to block some functions of the phone (e.g. camera, web browser, bluetooth connection etc.). **More information you can find here.**

31. What accesses in a container can we block for user?

We can block access to the web browser, to configuration of the email account or to the settings options in the container. We can also e.g. block data sharing outside the container environment etc.

#Configurations

32. Can remote device configuration (including, for example, app installation) include only a specific group of devices?

Sure, all actions performed on devices (e.g. application installation, configuration, data backup) can be performed on a single device, on all devices at the same time or on a specific group (or multiple groups) of devices - you can do it from the console administrative system.

33. Is it possible to configure third-party applications as part of the e-mail configuration on smartphones?

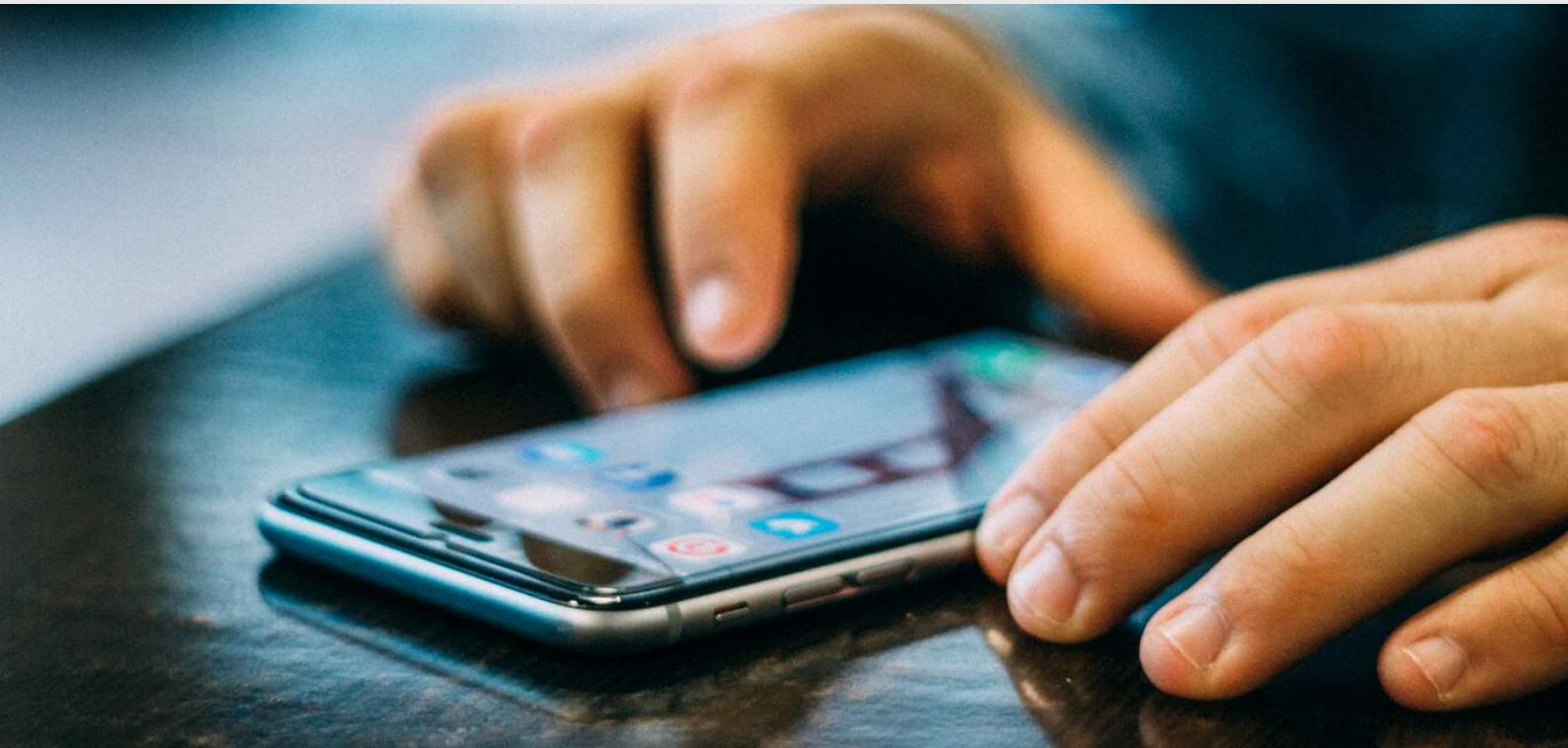
Yes, it is possible to install and configure third-party applications, as well as it's possible to configure the customer's internal applications through dedicated integration with client database systems.

34. What are the possibilities of "moderation" of applications on devices?

FAMOC manage allows you to create white list (allowed) applications and blacklist (applications not allowed), as well as silent removal of unwanted applications from devices. We can also configure the internal store with "corporate appstore" applications.

35. In what mode is it possible to collect the location of a device?

It is possible to collect an information about location on demand, but also in continuous mode with a possibility to define intervals depending on change of the location, a specific distance or a change of the base station ID in which the device is located.



36. What restrictions on the work profile can the administrator configure?

Examples of these are: image capture lock (to prevent data sharing), camera lock, disable copy-paste, file transfer lock between profiles and many others.

37. What is a corporate store?

The Corporate store tab allows administrator to create a number of various corporate stores and assign a group of users to them. The corporate stores repository includes store name, creation date and assigned user groups. Administrator is also allowed to preview corporate store (list of applications and configurations divided into groups), preview corporate store settings, edit and remove a store.

38. Is it possible to configure the device to have only one specific function (e.g. work of only one application)?

Yes. This possibility is provided by so-called kiosk mode (running one application on a mobile device, without the ability to disable it). **More information you can find here.**

39. Can we preview the list of installed applications on the device and details of these apps?

Yes, we can view the list of installed applications on the device, as well as detailed information about these applications (including name and version of the app).

40. Can we force a periodic password change on the device from the administration console?

Yes, we can force a periodic password change on the device.

41. What is the integration of Yubikey keys with the FAMOC manage system for?

Powered by FAMOC, the IT admin can remotely configure VPN and use physical key for VPN connection and user authentication. The employee will authenticate with a simple tap over NFC and log in to a corporate network with a handy dongle.

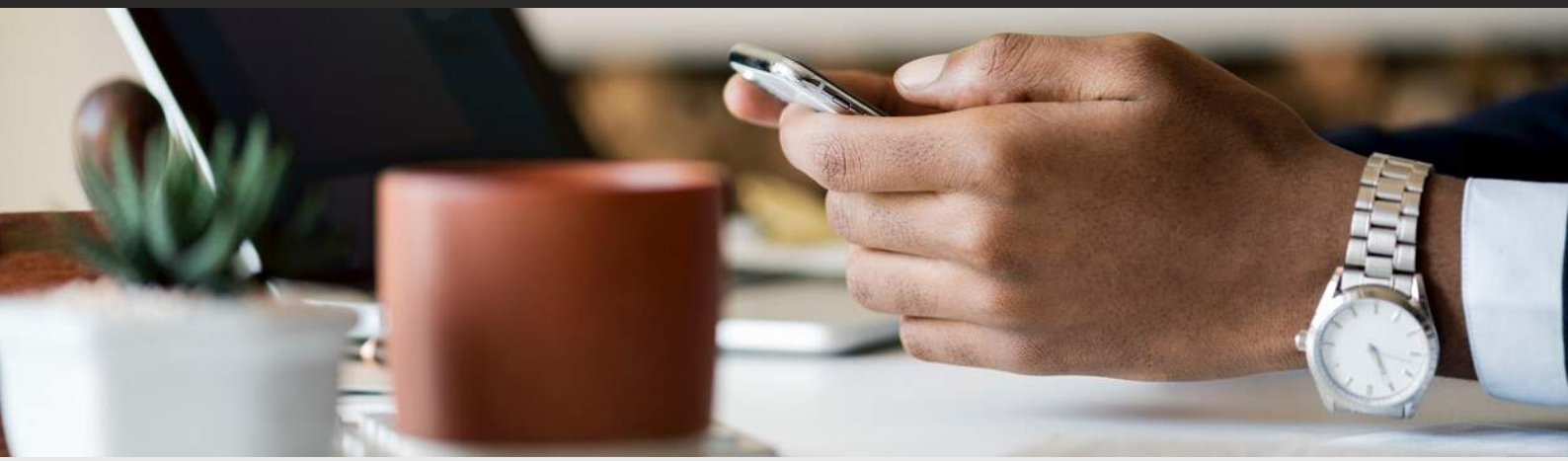
42. Can I configure the VPN client on managed devices with FAMOC manage? If so, from which supplier?

FAMOC manage element is a built-in VPN gateway that can easily be forced remotely on managed devices. Additionally, from the FAMOC manage level, there's a possibility of remote configuration of VPN clients from leading providers such as Cisco Anyconnect, F5, Pulse Secure, Palo Alto, Fortinet and many others.

43. In my company we need a centrally managed business book. Does FAMOC manage offer such functionality?

Yes, in FAMOC manage it is possible to enable synchronization of user contacts. This allows you to create a business book dedicated to each employee. Then the employee will receive contacts to all employees or just to selected ones - depending on in which department he works.

#Privacy



44. Does the device user have to agree to the screen capture and access to the device?

Yes, the device user must agree to remote access, i.e. authorize the connection.

45. Will the administrator have access to the user's private data (photos, messages etc.)?

Our system meets the requirements of the General Data Protection Regulation and we believe that the privacy of users is crucial. We support data containerization - even if employees use their private devices for private purposes (*BYOD - Bring Your Own Device*), business data management only takes place within the designated container. In this case, the Administrator does not have access to the user's private data outside the official part.

46. Can the user install any application on the work phone?

It depends on the mobile device management model and permissions granted by the IT administrator in a specific organization. In FAMOC manage system, you can configure white and blacklist of applications that will apply to the entire device or only to the corporate part.

47. Can I use the same application in separate profiles (private / work)?

Yes, in this case you need to install the same application separately on both profiles.

48. In case of a loss or theft of the device, can we wipe the data on the device except the user's private data?

On devices that have a separate work space managed by the IT admin, it is possible to interfere only with the data on this part of the device.

49. How do you know that - if you use your private devices for business purposes (BYOD) - your business data will be properly secured?

The corporate container can be encrypted and protected by an additional password. We can, for example, block the sending / copying of content from work space to private space to prevent its forwarding.

50. Can we temporarily disable the work profile?

Yes, it can be done by the device user. The work profile can be turned off (e.g. during the weekend or holiday) - then no notifications come to the user, but to get it activate again, you must enter the lock password.

DO YOU HAVE MORE QUESTIONS? CONTACT US:

presales@famoc.com