



WHITEPAPER

42Gears Mobile Email Management

By 42Gears Team

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of 42Gears Mobility Systems Pvt. Ltd

Table of Contents

Overview	2
Mobile Email Management.....	2
Mobile Email Deployment.	3
Microsoft Exchange Server 2010/2013/2016	3
MEM Deployment Workflow - Using PowerShell Integration	3
MEM Infrastructure	4
Mobile Email Management Configuration.....	8
Configuring MEM Deployment	8
Office 365.....	8
On-Premise or Hybrid	9
Mobile Email Management Device Profiles	10
A. Configure Exchange Email Profiles on Android	10
B. Configure Exchange Email profiles on iOS devices	12
C. Configure Exchange Email profiles on Windows	13
Exchange ActiveSync.....	13
Email Data Loss Prevention.....	14
Android devices.....	14
iOS devices	15
Windows devices	17
Conclusion	18

Overview

Mobile Email Management

Emails are an integral part of every business. Although other modes of communication, such as instant messaging, text messaging and social media, have emerged and are fast gaining popularity, emails continue to be the primary means of official communication. According to an [Email Statistics Report](#) 2017-2021 by Radicati Group, the number of email users worldwide will exceed 4.1 billion by the end of 2021. In 2017, the number of business and consumer emails sent and received per day was expected to reach 269 billion.

The ability to view corporate emails on personal/corporate devices does offer convenience and improve productivity, but it also raises security and deployment concerns. Mobile Email Management (MEM) can help combat such challenges..

Today, businesses can no longer do without Mobile Email Management (MEM). MEM allows IT pros to control mobile devices accessing emails, prevent data loss, enforce strict compliance policies and encrypt sensitive corporate data. 42Gears Mobile Email Management (MEM) solution offers comprehensive features to safeguard corporate email infrastructures against threats.

Challenges of Mobile Emails

Mobile emails undoubtedly help the workforce become more productive. However, they also pose many challenges, such as securing email access across heterogeneous devices, OSs and email clients; protecting sensitive corporate data from malicious apps; preventing unauthorized, lost or stolen devices from accessing corporate emails; and restricting and securing email access over unsecured networks. Transferring corporate emails to personal accounts or other emails by employees can also pose a serious threat.

42Gears MEM - Key Features

- Containerization of corporate emails to keep personal apps separate and ensure data encryption
- Enforced SSL to protect emails from unsecured networks
- Email access on managed and compliant devices only
- Device lockdown and data wipe on stolen or lost devices
- Over-the -air email configuration
- Data loss prevention through various measures, such as disabling copy/paste, screenshots and printing of emails
- Certificate management for CBA (Certificate Based Authentication)

Mobile Email Deployment

42Gears UEM can deeply integrate with Mobile Email Infrastructure to effectively manage and control mobile devices accessing corporate emails. Compliance policies can be enforced and sensitive data can be encrypted on mobile devices that access emails. 42Gears UEM supports the following types of Mobile Email Infrastructures.

Microsoft Exchange Server 2010/2013/2016

Office 365

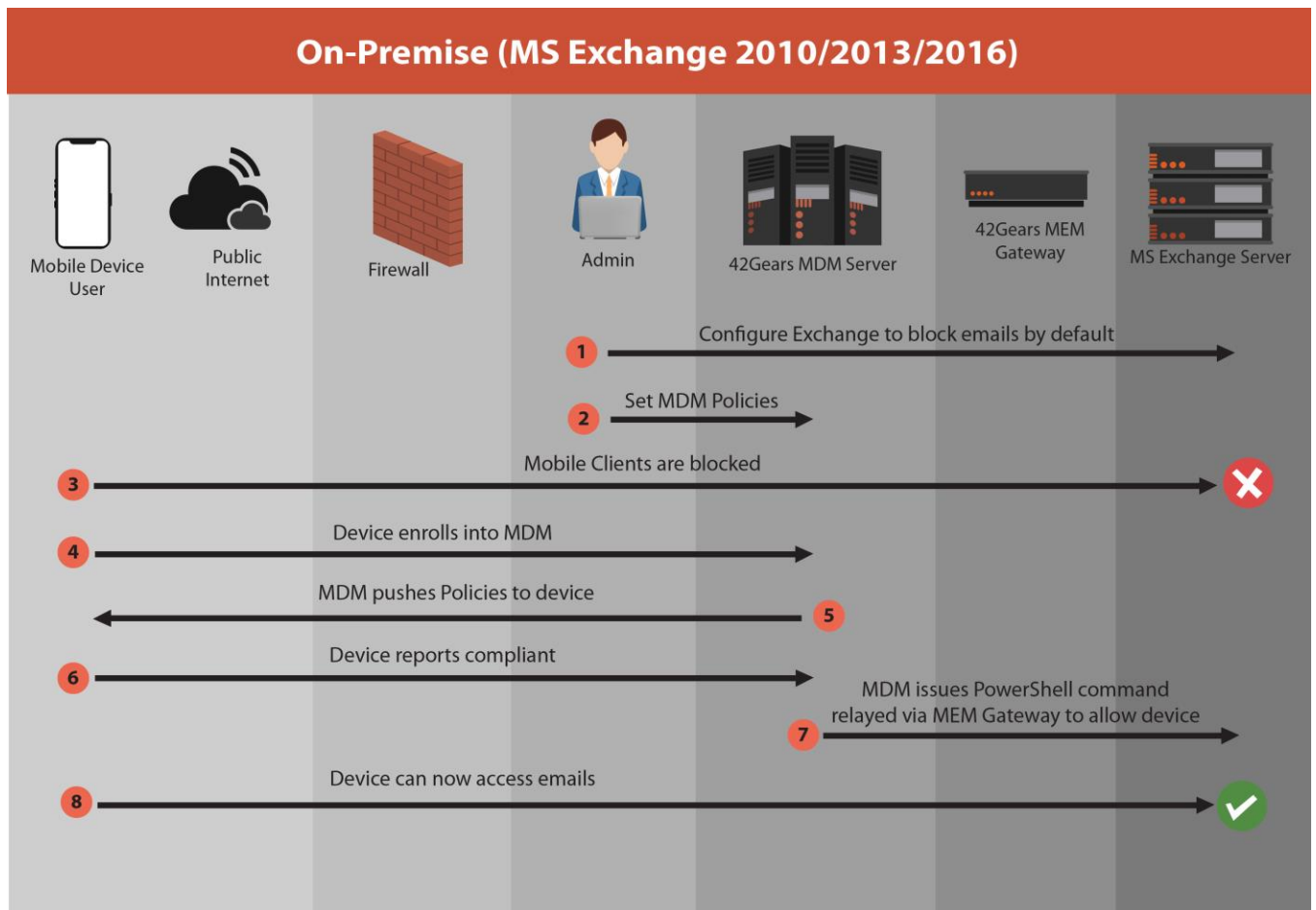
42Gears offers MEM services for MS Exchange-based infrastructure using PowerShell integration. 42Gears UEM acts as a PowerShell admin in this model and issues commands to the Exchange ActiveSync (EAS) infrastructure based on policies defined in the 42Gears Console to allow or deny email access.

MEM Deployment Workflow - Using PowerShell Integration

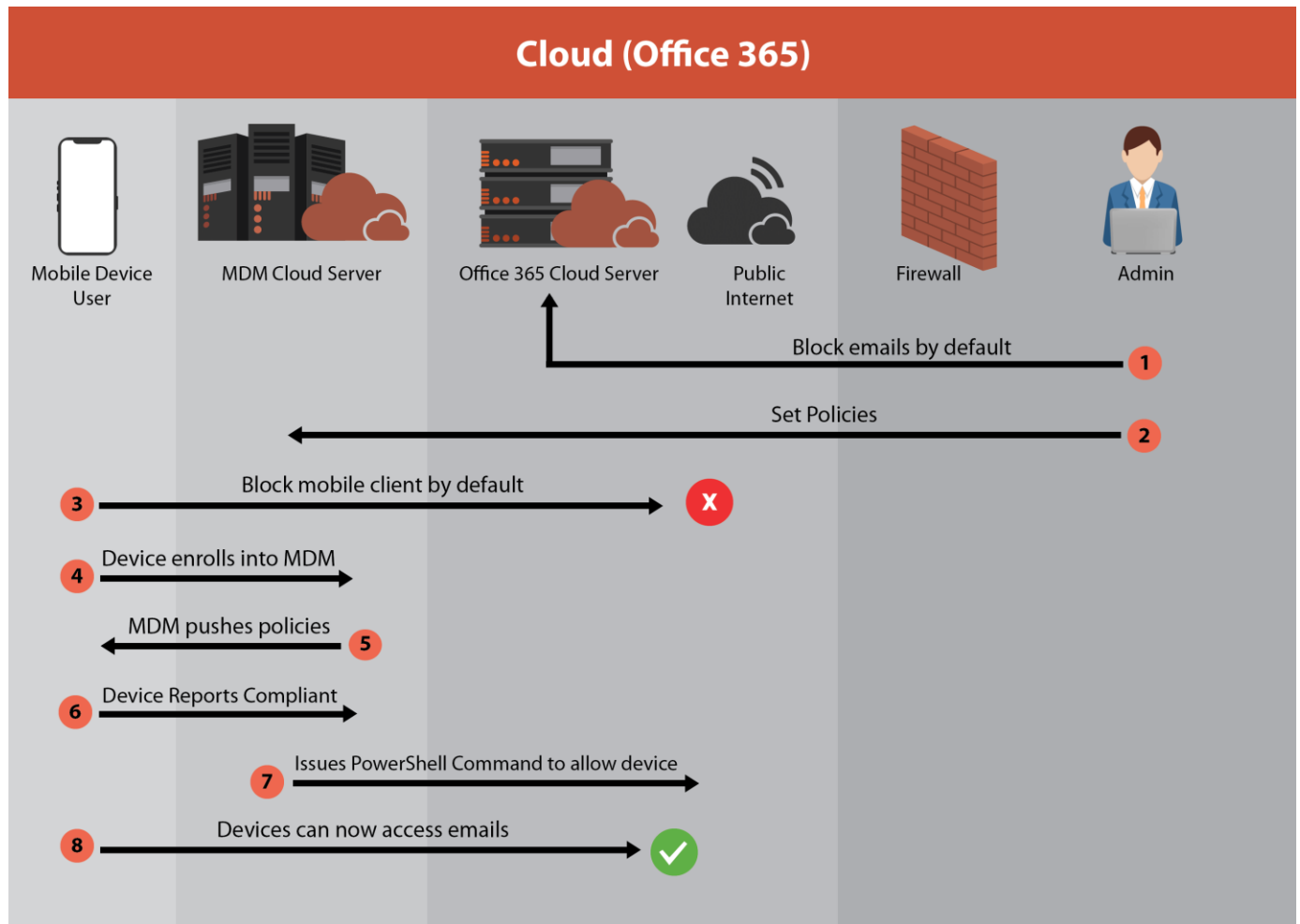
1. MDM admin configures MS Exchange to block all mobile email clients by default.
2. The admin sets policies on SureMDM.
3. Mobile devices are blocked by MS Exchange server by default as per policies set by the admin.
4. Users enroll devices into SureMDM.
5. MDM pushes security and compliance policies to all the devices.
6. Device reports to be compliant.
7. SureMDM issues the PowerShell command to MS Exchange (relayed via 42Gears MEM Gateway) to grant email access to compliant devices.
8. Devices can start accessing emails.

MEM Infrastructure

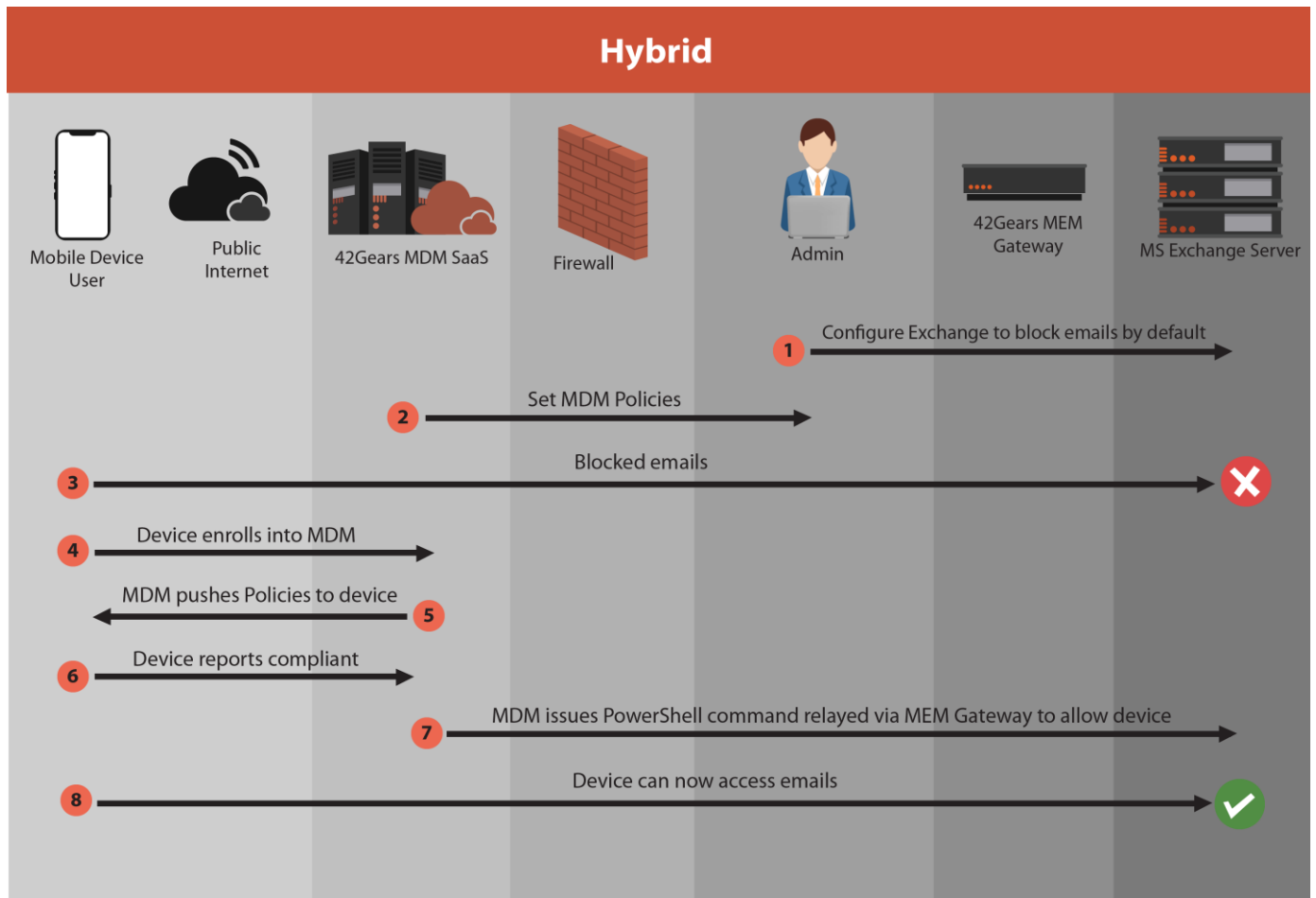
A. On-Premise



B. Cloud



C. Hybrid (42Gears UEM on cloud and on-premise MS exchange server)



Features Matrix

	Office 365	OnPremise Exchange 2010/2013/2016
Security and Policies		
S/MIME	Yes	Yes
Over the air configuration	Yes	Yes
Allow email access only over SSL	Yes	Yes
Allow email access only to encrypted devices	Yes	Yes
Allow email access only for managed devices	Yes	Yes
Allow email access only for compliant devices	Yes	Yes
Block email access for compromised (lost/stolen) devices	Yes	Yes
Certificate based authentication for email access	Yes	Yes
Infrastructure Integrations		
Certificate Authority	Yes	Yes
Exchange PowerShell	Yes	Yes
Supported Email Clients		
iOS Native Email Client	Yes	Yes
Android Native Email Client (GMAIL)	Yes	Yes
Windows 10 Native Mail Client	Yes	Yes

Mobile Email Management Configuration

Configuring MEM Deployment

Office 365

MEM configuration for Office 365 does not require any MEM connector. Below are the steps to configure MEM for Office 365-based accounts:

1. Go to **42Gears UEM Console**.
2. Navigate to **Account Settings**.
3. Click **Mobile Email Management**.
4. Check **Enable Exchange Activesync**.
5. Select **Office 365**.
6. Enter the **Powershell Gateway URL**, **Powershell Admin Username** and **Password**.
7. Click **Done** to save the changes.

The screenshot shows the SureMDM 42Gears Mobility Systems console. The top navigation bar includes links to Home, Dashboard, Inbox, Jobs, Profiles, App Store, File Store, and Reports. The left sidebar lists various settings categories, with 'Mobile Email Management' highlighted. The main content area is titled 'Account Settings' and contains the following configuration options:

- Enable Exchange ActiveSync**: Checked (indicated by a green checkmark).
- Powershell Integration**: Enabled.
- Select Server**: A dropdown menu set to 'Office 365'.
- Powershell Gateway Url**: A text field containing 'https://adfs.office365.com/adfs/ls/' with a hint '(e.g. : https://adfs.42gears.com/adfs/ls/)'.
- Administrator Integration Username**: A text field containing 'serviceaccount@org42.onmicrosoft.com'.
- Administrator Integration Password**: A password field with masked characters and a visibility toggle.

A note at the bottom states: **Note** : These changes might take upto 30 minutes to reflect on the device. A green 'Done' button is located at the bottom right of the configuration area.

On-Premise or Hybrid

MEM setup based on On-Premise Exchange server requires installation and configuration of 42Gears UEM connector. This connector needs to be installed on premise such that it has direct connectivity with On-premise Exchange server. Below is the configuration for such a setup.

UEM console setup:

1. Login to **42Gears UEM Console**.
2. Navigate to **Account Settings**.
3. Click **Mobile Email Management**.
4. Check **Enable Exchange Activesync**.
5. Select **Exchange Activesync**.
6. Enter the **Powershell Gateway URL**.
7. Click **Done** to save the changes.

The screenshot displays the 42Gears UEM console interface. The top navigation bar is blue with the 'SureMDM' logo and the text '42Gears Mobility Systems'. It includes links for Home, Dashboard, Inbox, Jobs, Profiles, App Store, File Store, and Reports. A left sidebar lists various settings categories, with 'Mobile Email Management' highlighted in a dark grey bar. The main content area is titled 'Account Settings' and contains the following elements:

- A toggle for 'Enable Exchange ActiveSync Powershell Integration' which is checked, indicated by a green checkmark.
- A 'Select Server' dropdown menu currently showing 'Exchange active sync'.
- A red note stating: 'Note : These changes might take upto 30 minutes to reflect on the device'.
- A green 'Done' button at the bottom right.

UEM Connector setup:

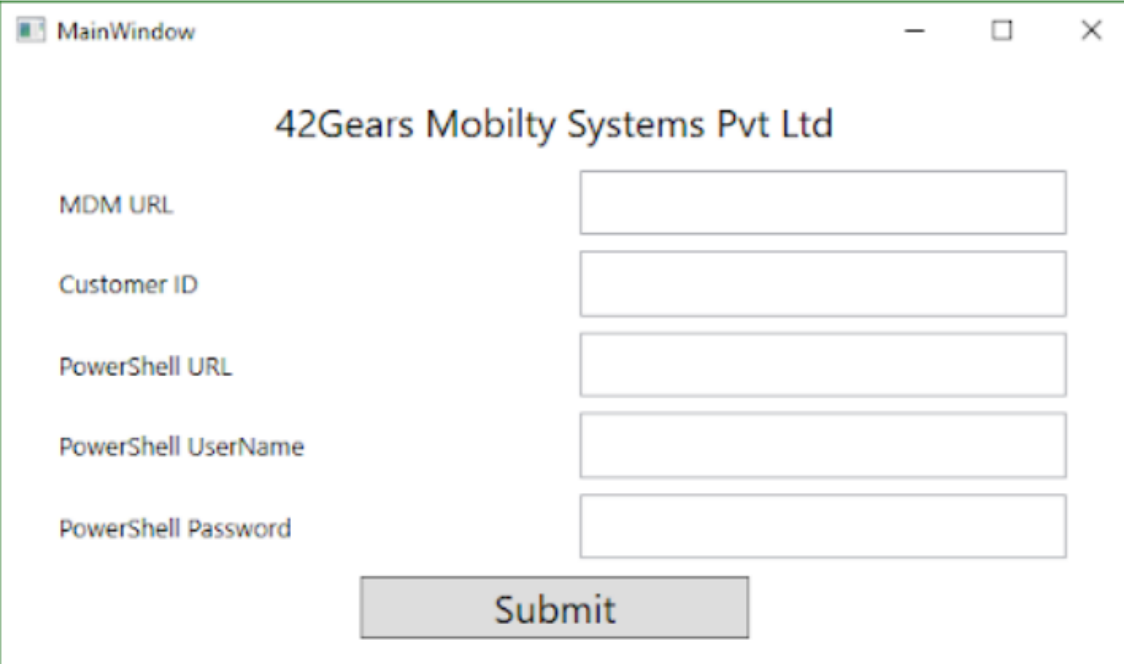
White Paper: 42Gears Mobile Email Management

Install and launch UEM connector on On-Premise network and enter the following details and click **Submit** to save the details:

- **MDM URL** - Server path of **SureMDM Console** - Example - wasteconnections.suremdm.io (**Note:** URL should be entered without https.)
- **Customer ID** - Unique ID of **SureMDM Console** - Example - 121800891
- **Powershell URL** - Example: https://<FQDN>/Powershell
- **Powershell Username** - Username of Exchange ActiveSync's service account
- **Powershell Password** - Password of Exchange ActiveSync's service account

Note: It might take 5-10 minutes for the device to get whitelisted and configure email account on the device.

Below given a screenshot for more clarity:



Mobile Email Management Device Profiles

A. Configure Exchange Email Profiles on Android

Configuring exchange email profiles is important before they get deployed on Android devices. This is how it can be configured:

1. Login to **42Gears UEM Console** and go to **Profiles**.
2. Select **Android** and click **Add** to create new profiles or edit an existing profile.
3. Next, select **Mail Configuration** and click **Using Gmail App**.
4. On the **Mail Configuration** screen, enter the following details:

White Paper: 42Gears Mobile Email Management

Email Address- \$emailaddress\$

The above-mentioned wildcard is used to dynamically replace the actual user email address at the time of pushing the profile.

Hostname or Host- Server Host name

Example- outlook.office365.com

Username- \$emailaddress\$

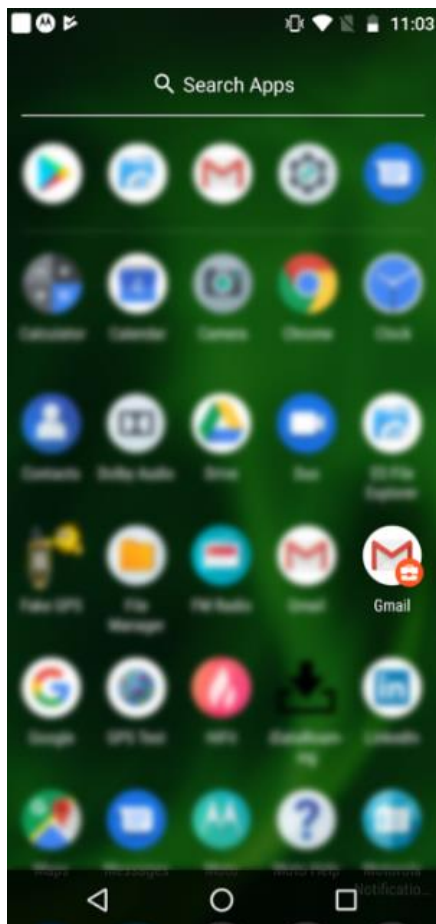
The above-mentioned wildcard is used to dynamically replace the actual user email address at the time of pushing the profile.

5. Enter Profile Name and click Save.

MEM configuration profile is now ready and can be deployed to any device.

6. Go to Home, select the device and apply MEM Configuration profile created above.

7. Once the device picks up this configuration, Gmail appears inside work container on device. This inbox is pre-configured with EAS account from MEM profile.



8. When the containerized **Gmail** application is launched, it asks for the account password. Once the password is entered, Exchange Mails start to sync.

B. Configure Exchange Email profiles on iOS devices

Deployment of MEM profiles on iOS devices requires configuring exchange email profiles on devices first and then pushing it to devices. This is how it can be configured:

1. Login to **42Gears UEM Console** and Go to **Profiles**.

2. Select **iOS > Add** to create new profile or edit an existing profile.

3. Select **Exchange ActiveSync** and click **Configure**.

4. Enter below details in the profile.

- **Account Name** - Exchange ActiveSync (you can enter any name)
- **Exchange ActiveSync Host** - Server Host name. Example: *outlook.office365.com*
- **User** - *%emailaddress%*. The above-mentioned wildcard is used to dynamically replace the actual user email address at the time of pushing the profile.
- **Email Address** - *%emailaddress%*. The above-mentioned wildcard is used to dynamically replace the actual user email address at the time of pushing the profile.

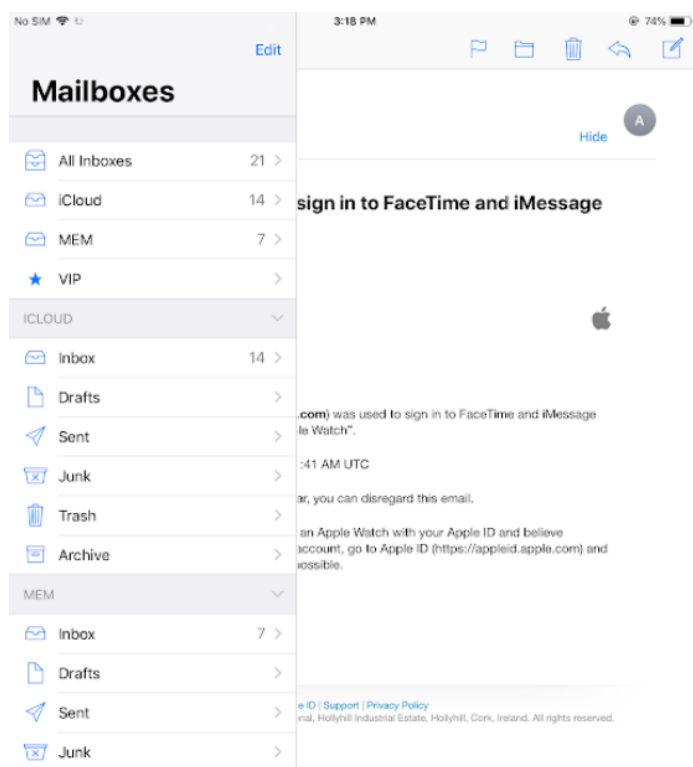
5. Enter **Profile Name** and click **Save**.

MEM configuration profile is now ready and can be deployed on any device.

6. Go to **Home**, select the device and apply **MEM Configuration** profile created above.

7. Once the device picks up this configuration, the iOS Mail client gets configured with EAS account from the MEM profile.

White Paper: 42Gears Mobile Email Management



8. On launching containerized **iOS Mail** application, it asks for password for the mail account. Once password is entered, **Exchange Mails** start to sync.

C. Configure Exchange Email profiles on Windows

Exchange ActiveSync

When an email account is configured in **Exchange ActiveSync**, device users can sync their Mails, Contacts, Calendars, Reminders and Notes remotely on enrolled devices.

To configure **Exchange ActiveSync** remotely on an enrolled device, follow these steps:

1. Login to the **42Gears UEM Console**.
2. On the **SureMDM Web Console**, click **Profiles**.
3. On the **Profiles** screen, click **Windows > Add**.
4. On the **Windows Profile** screen, select **Exchange ActiveSync > Configure**.
5. Enter **Profile Name**.
6. Click **Add** and enter the following details:

White Paper: 42Gears Mobile Email Management

- **Account Name**- Exchange ActiveSync (you can enter any name) Exchange ActiveSync Host- Server Host name. Example: outlook.office365.com
- **Username**- *\$username\$*. The above-mentioned wildcard is used to dynamically replace the actual user email address at the time of pushing the profile.
- **Email Address**- *\$emailaddress\$*. The above-mentioned wildcard is used to dynamically replace actual user email address at the time of pushing the profile.
- **Password**
- **Sync Schedule**
- **Days to Sync**

7. Click **Add > Save**.

The newly created profile gets listed in the **Profiles** section.

8. Go back to the **Home** tab and select the device(s) or group.

9. Click **Apply** to launch the **Apply Job To Device** prompt.

10. On the **Apply Job To Device** prompt, select the created profile and click **Apply** to complete.

Email Data Loss Prevention

42Gears Data Loss Prevention (DLP)

42Gears MEM prevents data loss through emails. It supports platforms like Android, iOS and Windows.

Android devices

42Gears MEM offers following DLP features for Android devices:

White Paper: 42Gears Mobile Email Management

1. Prevent moving corporate emails to personal email - Corporate emails can comprise sensitive data or info that should not be shared with those outside the organization. In case an employee shares such data through their personal mail to someone outside the organization, it can put the data in wrong hands, without any trace. 42Gears MEM will prevent employees from forwarding corporate emails from their personal email ids.

2. Prevent opening corporate email attachments from personal apps- Opening corporate email attachments from personal apps can jeopardise corporate data. Most consumer apps present on personal devices offer options like sharing data over social networks. MEM deployment ensures, attachments in corporate emails cannot be opened from unauthorized personal mails. They can only be opened from authorized containerized viewer apps.

3. Disable screen capture- Capturing screen of emails with sensitive information and pasting it in a personal app can put company data at risk. Screen-capture for MEM client and other work apps can be disabled via MEM. This is available under

- *Profiles -> Android -> System Settings -> Disable screen capture*

Disable Screen Capture ⓘ



4. Disable cross profile copy-paste - Copying and pasting any document from work apps (including work email client) should be disabled on personal apps as it may lead to data loss. This is available under

- *Profiles -> Android -> System Settings -> Disable Cross Profile Copy Paste*

Disable Cross Profile Copy Paste ⓘ

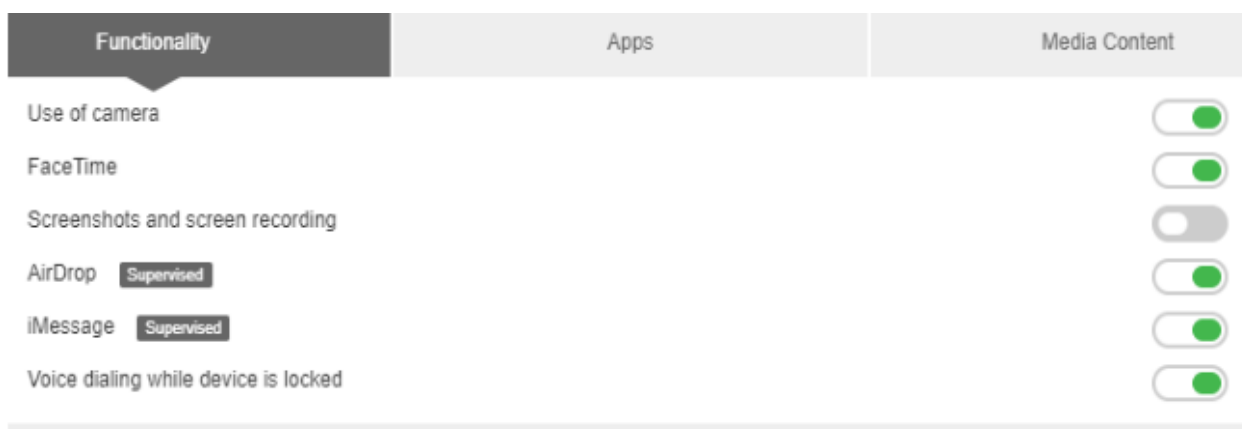


iOS devices

42Gears MEM offers following DLP features for iOS devices:

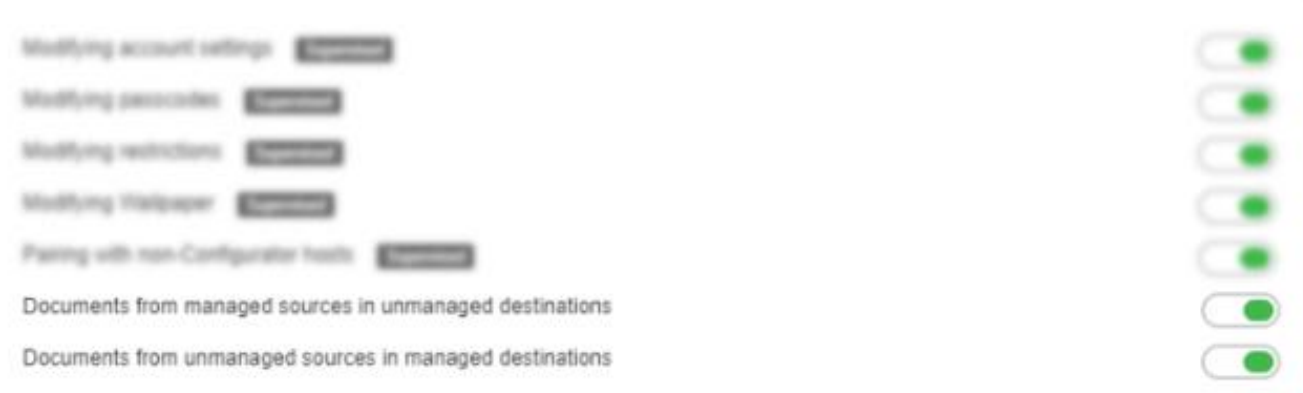
1. Screenshot and screen recording - Screenshots and screen recording feature may put corporate data at risk, so MEM offers the capability to turn it off/disable it on iOS devices. This is available under

- *Profiles -> iOS -> Restrictions Profile -> Screenshot and screen recording*



2. Turn off Documents from managed sources in unmanaged destinations and Documents from managed sources in managed destinations - Opening corporate email attachments from personal apps can jeopardize corporate data. Most consumer apps present on personal devices offer options like sharing data over social networks. MEM deployment ensures, attachments in corporate emails cannot be opened from unauthorized personal apps. They can only be opened from authorized containerized apps. This is available under:

- *Profiles -> iOS -> Restrictions Profile -> Documents from managed sources in unmanaged destinations*
- *Profiles -> iOS -> Restrictions Profile -> Documents from managed sources in managed destinations*



3. Turn on Treat Airdrop as unmanaged destination - Through the Airdrop feature, employees can share corporate email contents and resources with other unmanaged or non-corporate devices which may lead to data loss. By default, this feature is enabled on SureMDM. In order to make data secure, we need to define Airdrop as an unmanaged destination. This is available under

- *Profiles -> iOS -> Restrictions Profile -> Treat Airdrop as unmanaged destination*

White Paper: 42Gears Mobile Email Management



Windows devices

42Gears MEM offers following DLP features for Windows devices:

1. Prevent screen-capture - This is available under:

- *Profile -> Windows -> Restriction Policy -> Allow screen capture*

2. Prevent copy-paste

This is available under:

- *Profile -> Windows -> Restriction Policy -> Allow copy paste*

Experience

- ☒ Allow Cortana ⓘ
- ☒ Allow device discovery ⓘ
- ☒ Allow manual MDM unenrollment ⓘ
- ☐ Allow copy and paste ⓘ
- ☐ Allow screen capture ⓘ
- ☒ Display dialog prompt when no SIM card is detected ⓘ
- ☒ Allow task switching on the device ⓘ
- ☒ Allow voice recording ⓘ

Conclusion

Mobile Email Management (MEM) will no longer be a matter of choice for organizations, but will become mandatory to secure sensitive data. 42Gears MEM solution offers seamless support for all platforms including Android, iOS and Windows. The solution help companies secure their sensitive data while in-transit or at rest. Also, 42Gears MEM ensures smooth communication between stakeholders without compromising sensitive data.

To explore more on 42Gears UEM solution, [click here](#).