Introduction to Mobile Email Management (MEM) for Multiple Deployments Administration Guide

Overview

Keeping in mind the complexity of deploying Mobile Email Management (MEM) at different organization groups and the related security concerns of large device fleet, AirWatch introduces the **Multi-MEM Deployment** model. This deployment model provides a simple and efficient solution to very complex business scenarios. Consider the following scenarios:

- You have AirWatch Secure Email Gateway (SEG) deployed with Exchange 2003. Now, you want to upgrade to the latest version of Exchange and migrate to AirWatch PowerShell integration.
- You have multiple email environments across different branches.You want to deploy MEM to manage all these and also provide email access to multiple environments for specific executives.

With single MEM deployment, the solution for the above scenarios is; create a parallel organization group, un-enroll all the managed devices, migrate to the new setup, and then enroll the devices again. Considering the large number of devices that are involved, this is time consuming and tedious. But with AirWatch's new capability of having multiple MEM deployments at a single organization group, this process becomes much simpler and faster. You can easily migrate devices and users seamlessly without being tied to a Active Directory or an Organization Group.

AirWatch version 7.1 onwards, you have the ability to configure multiple MEM deployments at a parent organization group.This way, you can manage emails of devices from the same organization group or child organization group irrespective of the user group or smart group to which the device belongs. AirWatch automatically associates the devices to a MEM deployment based on the EAS profile that have been provisioned to these devices. Not only that, you can also provide email access to multiple email servers at the same time.

Benefits

- You can manage email without limitations of user/smart/organization groups.
- You can migrate devices across email environments with a single administrative action on the email dashboard without the end-user interaction.
- You can view and manage devices connecting to multiple email infrastructure from a single parent organization group.

In This Section

- Before You Begin - This section covers the basic requirements and other topics that would help you to get started with the solution.
- Configuring Multiple MEM Deployment - This section explains the steps that you can follow to configure multiple MEM deployments using the AirWatch MEM Configuration wizard.
- Enrolling in Multi MEM Environment - This section explains how existing and new devices connect to the configured MEM.

- Managing and securing emails through Multi MEM Integration - This section covers how to manage and secure the connected devices with the features available in AirWatch.

Before You Begin

Overview

Before you deploy Mobile Email Management, consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team for a smooth user experience.

In this Section

- Supported Browser - This section provides a comprehensive list of browsers supported by AirWatch.
- Getting Started - This section provides some recommendations and tips from the AirWatch team to streamline the deployment.
- Recommended Reading - This section provides helpful background and supporting information available from other AirWatch guides.

Recommended Reading

- **Mobile Device Management** - A comprehensive guide of the AirWatch's device management functionality.
- **Mobile Email Management** - A comprehensive guide of the AirWatch's email management functionality.
- **Secure Email Gateway Integration Administration Guide** - Learn how the AirWatch's SEG model of email deployment works.
- **Google Apps for Business Integration Administration Guide** - Learn how the AirWatch's MEM model of email integration with Google Apps for Business works.
- **PowerShell Integration Administration Guide** - Learn how the AirWatch's MEM model of email integration with PowerShell works.

Getting Started

You can easily setup any of the MEM deployment model from the AirWatch Admin console.

1. Navigate to **Email ▶Settings**.
2. Choose your required email infrastructure from the available list.
3. Follow the instructions as specified.

For more information on setting up the different deployment model, please refer the **Configuring Multiple MEM at an Organization Group** section of this guide.

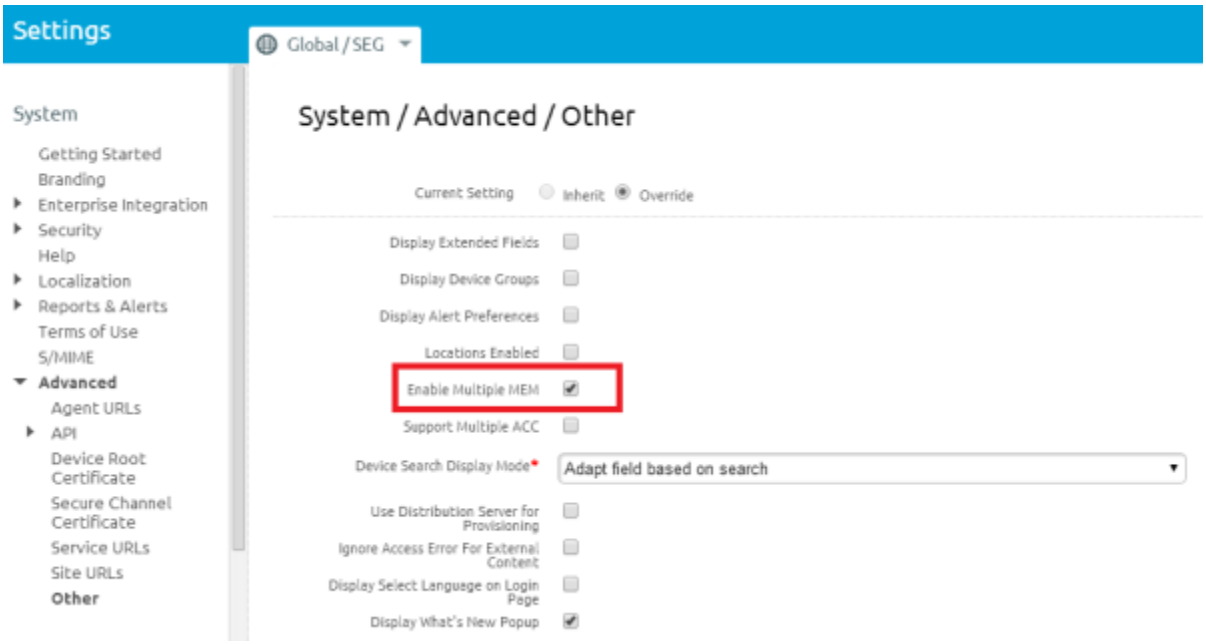
Configuring Multiple MEM at an Organization Group

Overview

AirWatch provides the flexibility of configuring multiple MEM through few simple steps. Once the email infrastructure configuration with AirWatch is complete, you can deploy the devices into the AirWatch Admin console. This section guides you on how to configure multiple MEM at an organization group.

Step 1: Enable Setting

To begin the configuration, navigate to **Groups & Settings ▶All Settings ▶System ▶Advanced ▶Other** and then select the **Enable Multiple-MEM** check box. Only the admins with role System Administrator and AirWatch Administrator can access this option.

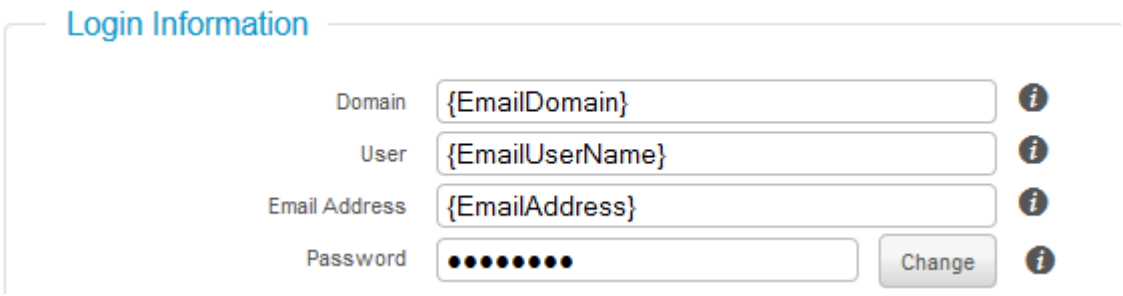


Step 2: Create EAS Profiles

Profile Configuration

1. Navigate to **Devices ▶Profiles ▶List View**.
2. Click **Add** and select the platform for the device that will receive the profile.
3. Enter the **General** settings for the profile.
4. Select **Exchange Active Sync** as the profile payload and then click **Configure**.
5. Select the type of **Mail Client**.
6. Enter your **Account Name**.

7. Enter the **Exchange ActiveSync Host** server name.
8. Under **Login Information**, use Lookup Values to populate the end-user's account information, including {EmailPassword} for the password field.



Note: In case you have migrated from a single MEM configuration to Multi MEM configuration, you may also use the existing EAS profiles that are relevant to the new configurations.

Step 3: Configure MEM Using the Wizard

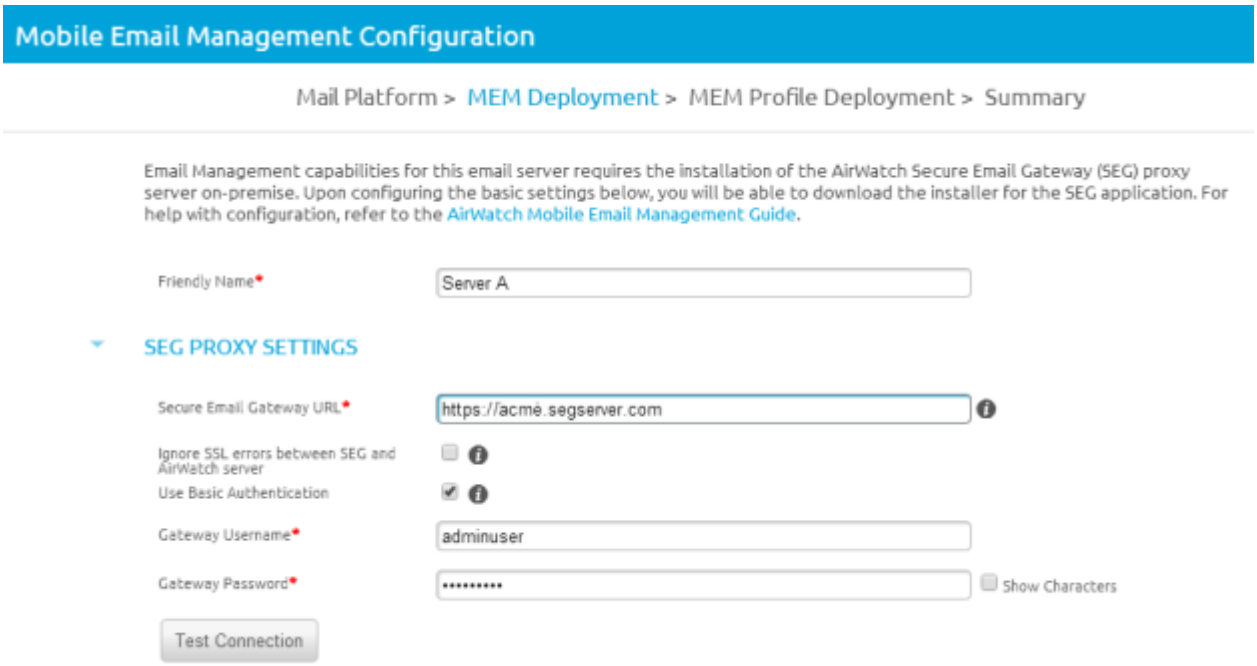
1. Navigate to **Email ▶Settings** and then click **Configure**.
2. Select your email server type and the exchange version. If you select the exchange version as Exchange 2010/2013/Office 365, you need to select your preferred deployment method. Click **Next**.

For more information on the deployment methods, please see **Mobile Email Management Administration Guide**.

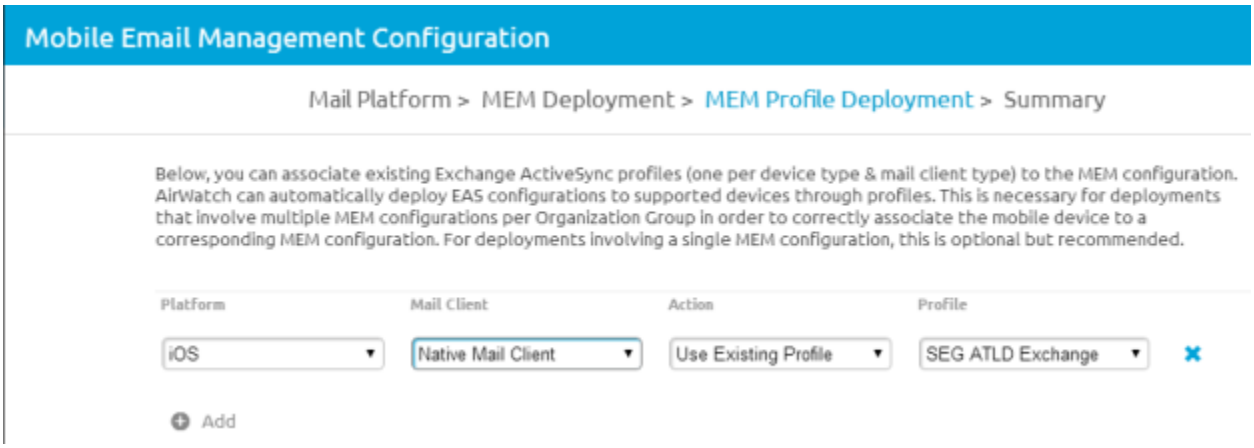
Note: For more information on how to implement multiple MEM at an organization group, please contact your AirWatch representative.

3. Deployment types that are available:

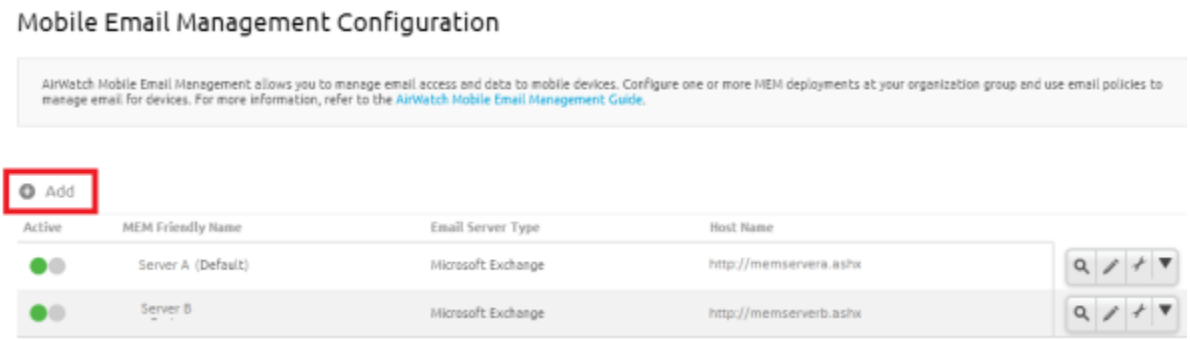
- If you choose deployment type as SEG, then:
  - Enter a Friendly name for this deployment.
  - Enter the SEG proxy server details.
- If you choose deployment type as PowerShell, then:
  - Enter the PowerShell server, authentication, and sync settings.
- If you choose deployment type as SEG for Google Apps for Business then:
  - Enter a Friendly name for this deployment.
  - Enter the Google App, authentication, and SEG proxy settings.



5. Create a template EAS profile for devices that you will manage using this MEM deployment. This template profile are not published to devices automatically. This needs to be done from the **Profiles** page. Alternatively, you can also choose to associate an existing profile to this deployment. This is mandatory if more than one MEM deployment is to be configured at a single organization group. Select **Next**.



6. The **Summary** page displays the configuration details. **Save** the settings.
7. Click **Add**(available on the Email Configuration main page) to configure multiple MEM deployments.
8. In a SEG deployment, you may assign a particular configuration as the default using the option **Set as default** available under ▼.



Note: One MEM configuration can be associated with a single or multiple EAS profiles.

9. Once saved, you can add the advanced settings to this deployment.

- Click the advanced icon corresponding to your deployment.
- In the Mobile Email Advanced Configuration screen, configure the available settings for the user mailboxes as per requirement.

  - **Enable Real-time Compliance Sync** - Select to enable API sever to remotely provision compliance policies to SEG server.
  - **Ignore SSL errors between SEG and email server** - Select to ignore any SSL errors for communication between SEG proxy and email infrastructure.
  - **Ignore SSL errors between SEG and AirWatch server** - Select to ignore any SSL errors for communication between SEG proxy and AirWatch.
  - **KCD authentication** - Enable or disable the Cross Domain KCD authentication using the settings available.
  - **Required transactions** - Enable or disable the required transactions such as Folder Sync, Settings etc.
  - **Optional transactions** - Enable or disable the optional transactions such as Get attachment, Search, Move Items etc.
  - **Diagnostic** -Set the number and frequency of transaction for a device.
  - **Sizing** - Set the frequency of SEG and API server interaction.
  - **S/MIME Options** - Enable the checkbox to disallow the encryption of attachments and hyperlinks through SEG.

3. Click **Save**.

For more information on configuring each deployment type, please refer the deployment specific **Administration Guide**.

Keep In Mind

- You should use mutually exclusive user groups when connecting multiple PowerShell environments to the same Exchange server.
- Use different domains in the configuration when connecting multiple Gmail environments.
- Consider connecting SEG and PowerShell integration to the same email environment only during migration of MEM deployments with appropriate settings. It is recommended that you implement this with assistance from your AirWatch representative.

Enrolling in Multi-MEM Environment

Overview

After the configuration is complete, the configured MEM starts managing their respective devices. This section explains how MEM identifies and connects to the devices associated with or without an EAS profile.

Devices with EAS profile

Once the configuration is complete, based on the EAS profile, the already enrolled devices are automatically assigned to the specific MEM deployment. The MEM server then starts managing the devices.When a new device enrolls with an EAS profile, then AirWatch sends a policy update to the configured MEM to start managing the device. AirWatch then displays the memconfigID for this device on the Email Dashboard.

Devices without EAS Profile

When a new device enrolls without having a profile associated to it, the assignment of MEM for this device happens based on the auto discovery process i.e. AirWatch attempts to discover a MEM for the device. For each integration type, this assignment varies.

Note: Irrespective of the email clients, all the Google models require an EAS profile. For new installs, associating an EAS profile is mandatory. For the upgrades, the admin has to manually associate an EAS profile to the MEM configuration upon completion of the upgrade process.

The below sections explain each integration type.

SEG Proxy Integrated

AirWatch sends a broadcast message stating that a device has enrolled to all the configured Secure Email Gateway Proxy servers of the organization group to which the device has enrolled. As soon as the device connects to a particular SEG server, the SEG recognizes the device as managed from the broadcast message sent earlier. The SEG Proxy then reports the device as discovered with its memConfigID to AirWatch. AirWatch then associates the enrolled device to that memConfigID and displays it on the Email Dashboard.

PowerShell Integrated

AirWatch sends an 'Allow' command to all the PowerShell integrated environments. For the environment that the command succeeds against, AirWatch automatically associates the device to the corresponding memConfigID.

Google Apps Integrated

Profiles are a must for this type of deployment. Unless the devices are provisioned with the profiles, the configured Google App deployment cannot identify and subsequently manage the device.

After Device Enrollment

Once the AirWatch MEM configured model and device starts syncing, their status and details gets listed on the **Email Dashboard**. The devices first appear on the dashboard when:

SEG Proxy	PowerShell	Google Apps
The SEG Proxy reports the device as connected and managed	AirWatch sends a PowerShell cmdlet i.e perform Sync mailboxes to allow the device to connect to email	AirWatch EAS profile is queued up for the device

Device status

On the Email Dashboard, you may notice the below status:

- **Managed Assigned** - Enrolled devices with identified memconfigID.
- **Managed Unassigned** - Enrolled devices for which the memConfigID has not yet been identified either through profile assignment or through auto discovery.
- **Unmanaged Discovered** - These devices are not yet enrolled in AirWatch and a specific MEM configuration at that organization group has discovered them.

Securing and Managing Mobile Email in a Multi-MEM Environment

Overview

AirWatch provides various features to secure and manage the devices effectively. Below sections mention these features.

Securing with Email Policies

Creating compliance policies for a multi-MEM deployment is same as that of single MEM. The compliance policies created for an organization applies to all the MEM deployed at that organization group.

To Create an Email Policy

1. Navigate to **Email ▶Compliance Policies ▶Email Policies**
2. Edit any of the email policies.
   - **General Email Policies** – Enforces policies on all devices accessing email.
   - **Managed Device Policies** – Enforces policies on managed devices accessing email.
   - **Email Security Policies** – Enforces policies on attachments and hyperlinks.
3. Create your compliance rule and **Save**.
4. The policy is now active. Select the colored circles that appear under the **Active** column to disable or enable a policy.

The below table provides an overview of the email policies that are applicable for each deployment type.

✓ - Applicable, ☐ - Not Applicable

	SEG PowerShell		Google Apps		
General Email Policies			**Without SEG and without Password Purge**	**Without SEG and with Password Purge**	**With SEG Proxy**
Sync Settings	✓	☐	☐	☐	✓
Managed Device	✓	☐	☐	☐	✓
Mail Client	✓	☐	☐	☐	✓
User	✓	☐	☐	☐	✓
EAS Device Type	✓	☐	☐	☐	✓
Managed Device Policies					
Inactivity	✓	✓	✓	☐	✓
Device Compromised	✓	✓	✓	☐	✓
Encryption	✓	✓	✓	☐	✓
Model	✓	✓	✓	☐	✓
Operating System	✓	✓	✓	☐	✓
Email Security Policies					
Attachments (managed devices)	✓	☐	☐	☐	✓
Attachments (unmanaged devices)	✓	☐	☐	☐	✓
Hyperlink	✓	☐	☐	☐	✓

The explanation for each feature is given below:

General Email Policies

- **Sync Settings** – This policy prevents the device from syncing with specific EAS folders. Note that AirWatch prevent devices from syncing with the selected folders irrespective of other compliance policies. For the policy to take effect, it is necessary to republish the EAS profile to the devices (this forces devices to re-sync with the email server).
- **Managed Device** – This policy restricts email access only to managed devices.
- **Mail Client** – This policy restricts email access to a set of mail clients.
- **User** – This policy restricts email access to a set of users.
- **EAS Device Type** – This policy allows or blocks devices based on the EAS Device Type attribute reported by the end-user device.

Managed Device Policies

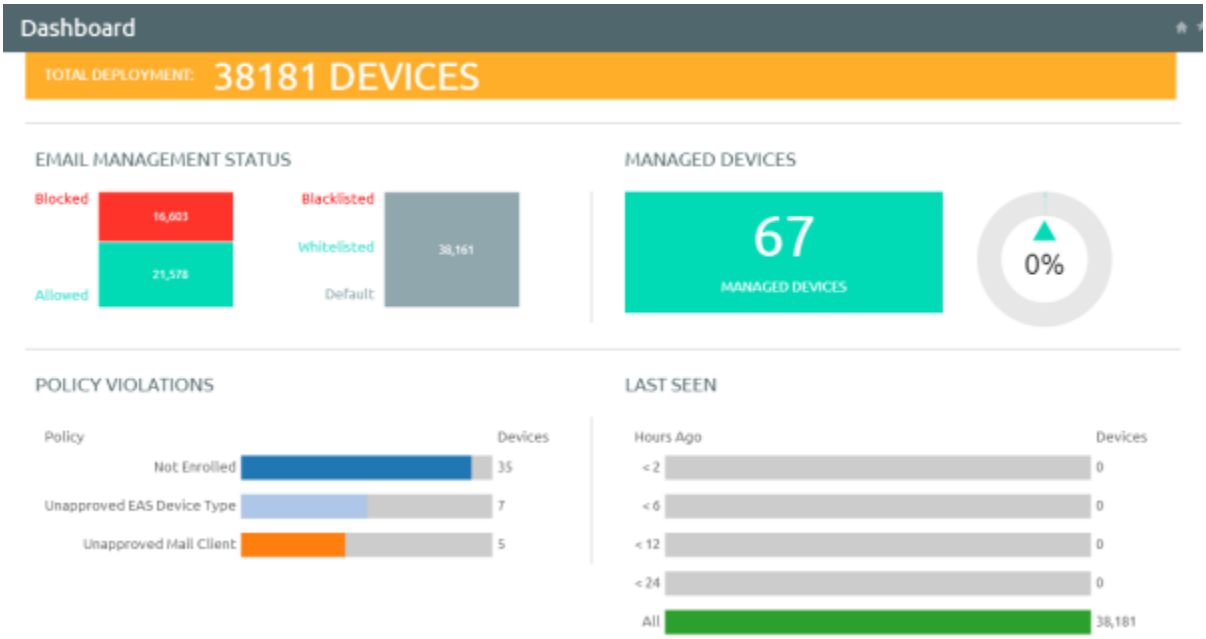
- **Inactivity** – This policy allows you to prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (i.e. does not check-in to AirWatch), before email access is cut off.

- **Device Compromised** – This policy allows you to prevent compromised devices from accessing email. Note that this policy does not block email access for devices that have not reported compromised status to AirWatch.
- **Encryption** – This policy allows you to prevent email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to AirWatch.
- **Model** – This policy allows you to restrict email access based on the Platform and Model of the device.
- **Operating System** – This policy allows you to restrict email access to a set of operating systems for specific platforms.
- **Hyperlink** – This policy allows device users to open hyperlinks contained within an email directly with a secure AirWatch application (e.g. AirWatch Browser) present on the device. Based on the application list sample, AirWatch dynamically modifies the hyperlink for the appropriate application on the device.

Managing through the Email Dashboard

Gain visibility into the email traffic and monitor the devices through the AirWatch**Email Dashboard**. This dashboard gives you a real-time summary of the status of the devices connected to the email traffic. You can access the Dashboard from **Email ▶Dashboard**. The email dashboard enables you to:

- Whitelist or blacklist a device to allow or deny access of email.
- View the devices which are managed, un-managed, compliant, non- compliant, blocked, or allowed.
- View the device details such as OS, Model, Platform, Phone Number, IMEI, IP address.



From the Dashboard, you can also use the available Graphs to filter your search. For example, if you want to view all the managed devices of that organization group, select the Managed Devices graph. This displays the results in the List View screen.

Performing Administrative Actions through the List View

View all the real-time updates of your end user devices that you are managing with AirWatch MEM. You can access the **List View** from **Email ▶List View**. You can view the device or user specific information by switching between the two tabs: **Device** and **User** available here. You can change the **Layout** to either view the summary or the detailed list of the information based on your requirement.

The List View screen provides detailed information that include:

- **Last Request** - In PowerShell integration, this column displays the last state change of the device either from AirWatch or from Exchange. In SEG integration this column shows the last time a device synced mail.
- **User** - The user account name.
- **Friendly Name** - The friendly name of the device.
- **MEM Config** - The configured MEM deployment that is managing the device.

- **Email Address** - The email address of the user account.
- **Identifier** - The unique alpha-numeric identification code associated with the device.
- **Mail Client** - The email client syncing the emails on the device.
- **Last Command** - The last state change of the device and populates the **Last Request** column.
- **Last Gateway Server** -The server to which the device connected.
- **Status** - The real time status of the device and whether email is blocked or allowed on it as per the defined policy.
- **Reason** - The reason code for allowing or blocking email on a device. Please note that the reason code displays 'Global' and 'Individual' only when the access state of the email is changed by an entity other than AirWatch (for example, an external administrator).
- **Platform, Model, OS, IMEI, EAS Device Type, IP Address** - All the device information displays in these fields.
- **Mailbox Identity** - The location of the user mailbox in the Active Directory.

Filters for Quick Search

From here, using the **Filter** option,you can narrow-down your device search based on:

- **Last Seen**: All, less than 24 hours, 12 hours, 6 hours, 2 hours.
- **Managed**: All, Managed, Unmanaged.
- **Allowed**: All, Allowed, Blocked.
- **Policy Override**: All, Blacklisted, Whitelisted, Default.
- **Policy Violation**: Compromised, Device Inactive, Not data Protected/Enrolled/MDM Compliant, Unapproved EAS Device Type/Email Account/Mail Client/Model/OS.
- **MEM Config** - Filter devices based on the configured MEM deployments.

Performing Actions

The **Override**,**Actions**,and the **Administration** dropdown menu provides a single location to perform multiple actions on the device.

Override

Select the check box corresponding to a device to perform actions on it.

- **Whitelist** - Allows a device to receive emails.
- **Blacklist** - Blocks a device from receiving emails.
- **Default** - Allows or blocks a device based on whether the device is compliant or non compliant.

Actions

- **Sync Mailboxes** - Syncs mailboxes of PowerShell integrated deployments.Select the check box to specifically choose which devices you want to sync.

Note: AirWatch offers the **Email Sync** option on the Self Service Portal to sync their mailbox in Exchange and also run preconfigured compliance policies for all their devices. This process is typically much faster than the bulk sync performed on all the devices.

- **Run Compliance** - Triggers the compliance engine to run for the selected MEM configuration.
- **Test Mode** - Tests email policies without applying them on devices of SEG integrated deployments.

Administration

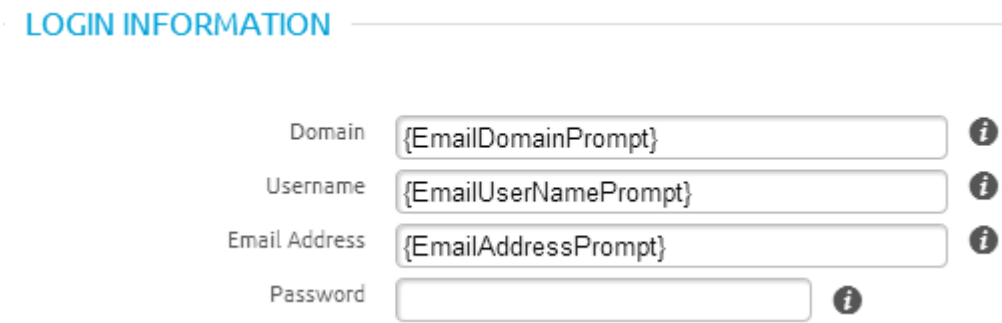
- **Enrollment Email** - Sends an email to the user with all the details required for enrollment.
- **Dx Mode On** - Runs the diagnostic for the selected user mailbox.
- **Dx Mode Off** - Turns off the diagnostic for the selected user mailbox.
- **Update Encryption Key** - Resets the encryption and then re-syncs the emails for the selected devices.
- **Remote Wipe** - Resets the device to factory settings.
- **Delete Unmanaged Devices** - Deletes the selected unmanaged device record from the dashboard. Please note that this record may reappear after the next sync.
- **Migrate Devices** - Migrates selected device to other chosen MEM configurations by deleting the installed EAS profile and pushing the EAS profile of the chosen configuration on the device. For example, if you have migrated from PowerShell to SEG, then EAS profile of PowerShell gets deleted from the device and EAS profile of SEG is pushed on the device.

Installing Email Profiles through SSP

Using the Self Service Portal, the device users can gain email access to multiple email servers at the same time.

Installing and enabling multiple email accounts on SSP involves the following steps:

1. For the required organization group, create an EAS profile with the assignment type as Optional and the Login information as shown below. On the SSP, this profile can be viewed from the **Profiles** tab.



2. The device user logs into SSP and selects the install icon next to the optional EAS profile.
3. The user is prompted to enter the required Email Address, Domain and Username.
4. On saving the details, the profile gets installed on the device.
5. On the device, the user is then prompted to enter a password to access the secondary email account.

Once done, you can view the configured email accounts for the user from the **Email Dashboard** page.