Introduction to Mobile Email Management (MEM)

Overview

To the users of most organizations, one of the most valued benefits of a managed device is the ability to access corporate mail on the go. Having the ability to immediately view corporate mail, contacts, and calendar from your device provides a level of convenience and access that can lead to productivity boosts and improve response time within your organization. Although there are many benefits of deploying mobile mail to your users, there are also many challenges of security and deployment that may make mobile mail seem daunting to IT:

- Different device types, Operating Systems, and email clients all require mail.
- Employees access mail over unsecured networks.
- Sensitive information can easily transfer into third party mail and apps.
- Unauthorized, lost or stolen devices can still access email.
- Email attachments are easily lost and disseminated through third party reader apps as soon as they are viewed.

With AirWatch, connect your employees to corporate email and ensure those connections are secured and managed. AirWatch's **Mobile Email Management (MEM)** solution delivers comprehensive security for your corporate email infrastructure. Address these challenges with an easy to use **MEM** solution that provides all of the key factors of a successful and secure mobile email deployment:

- Enforce SSL security.
- Configure email over-the-air.
- Discover existing un-managed devices.
- Protect email from data loss.
- Block un-managed devices from accessing email.
- Restrict email access to only company-approved devices using the customizable compliance policies.
- Use certificate integration and revocation.

In This Guide

This guide provides the basic functionality of the AirWatch's Mobile Email Management (MEM) solution.This guide has been divided into the following sections:

- Before You Begin - Covers the basic requirements and other topics that would help you to get started with the solution.
- Email Infrastructure - Covers the types of email deployments available as part of the MEM solution.
- Migrating Email - Explains the steps to migrate from your existing email infrastructure to the any of the MEM deployment models.
- Configuring MEM - Explains how to deploy the MEM solution and secure it using the many AirWatch features.
- Creating Email Profiles - Explains how to create, secure , and deploy email profile onto the device for the supported email clients.
- Enforcing Email Access Control - Explains how to create an email policy and the functionality of each of compliance policy.
- Managing Mobile Email - Explains how once deployed, you can manage the devices efficiently from the AirWatch Admin Console.

Before You Begin

Overview

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

In This Section

- Supported Browser - Provides a comprehensive list of browsers supported by AirWatch.
- Recommended Reading - Provides helpful background and supporting information available from other AirWatch guidesSupported Browsers

The AirWatch Admin Console supports the following web browsers:

- Internet Explorer 8+
- Google Chrome 11+
- Firefox 3.x+
- Safari 5.x

Comprehensive platform testing has been performed to ensure functionality using these web browsers. The AirWatch Admin Console may still function in non-certified browsers with minor issues.

Recommended Reading

- **Mobile Device Management (MDM) Guide** - Learn about the AirWatch's device management functionality.
- **Secure Email Gateway (SEG) 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 for Google Apps for Business works.
- **PowerShell Integration Administration Guide** - Learn how the AirWatch's MEM model of email integration for PowerShell works.

Protecting Your Email Infrastructure

Overview

In order to take advantage of AirWatch's Mobile Email Management (MEM) features and ultimately protect your mail infrastructure, you must first configure one of AirWatch's MEM models:

- SEG Proxy Model
- Direct PowerShell Model
- Direct Google Model

These models provide a very similar set of MEM capabilities and are, for the most part, selected solely based on what type of email infrastructure you are utilizing. For more information on which MEM capabilities are available per model, see Appendix A: Email Management Functionality.

AirWatch recommends that you use the following models based on your email infrastructure.

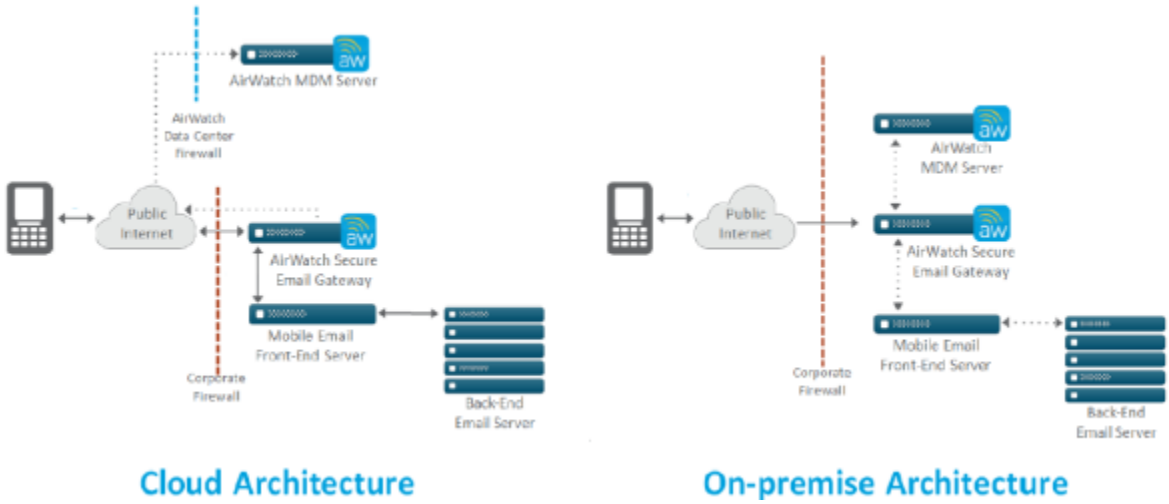
Deployment Model	Configuration Mode	Mail Infrastructure
Proxy Model	Secure Email Gateway Model (Proxy)	Microsoft Exchange 2003/2007/2010/2013 Lotus Domino w/ Lotus Notes Novell GroupWise (with EAS) Google Apps for business
Direct Model	Powershell Model	Microsoft Exchange 2010/2013 Microsoft Office 365
	Google Model	Google Apps for Business

In This Section

- SEG Proxy Model- Explains the Secure Email Gateway email infrastructure model and its architectural setup in AirWatch.
- Direct Powershell Model - Explains the PowerShell email infrastructure model and its architectural setup in AirWatch.
- Direct Google Model - Explains the Google Apps for business email infrastructure model and its architectural setup in AirWatch.

SEG Proxy Model

The SEG Proxy server is a separate server installed in-line with your existing email server to proxy all email traffic going to mobile devices. Based on the settings you define in the AirWatch Admin Console, the SEG Proxy server takes allow/block decisions for every mobile device it manages. The SEG Proxy server relays traffic from approved devices and thus protects corporate email server by not allowing any devices to directly communicate with email server. Instead, the SEG Proxy server filters all communication requests to the corporate email server.

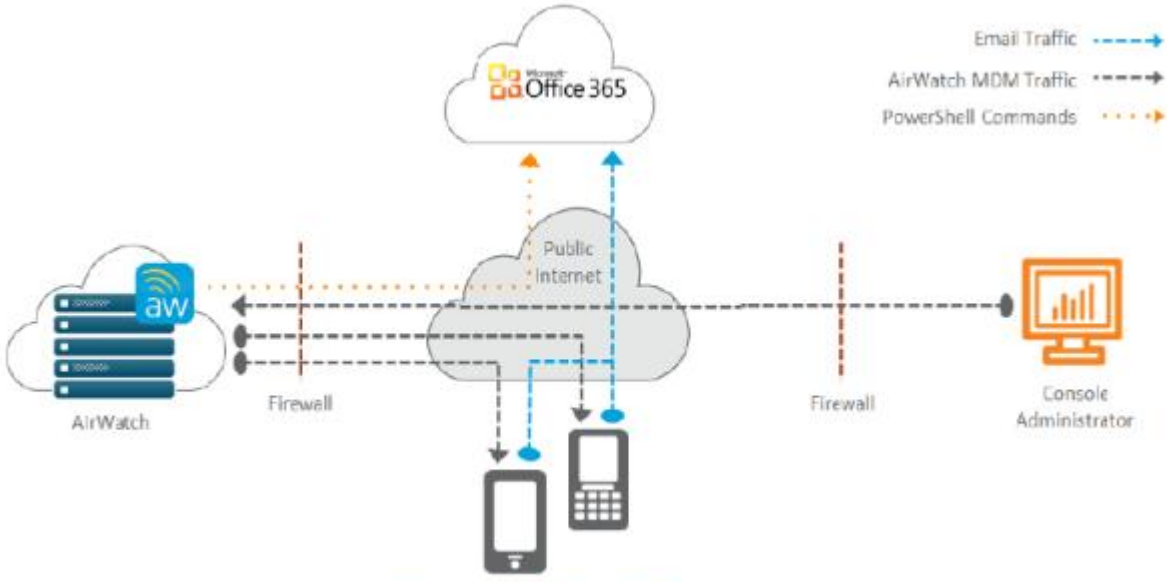


Install the SEG server in your network so that it is in-line with the corporation's email traffic. You can also install it in a Demilitarized Zone (DMZ) or behind a reverse proxy. You must host the SEG server in the customer data center, regardless of whether your AirWatch MDM server is in the cloud or on-premise.

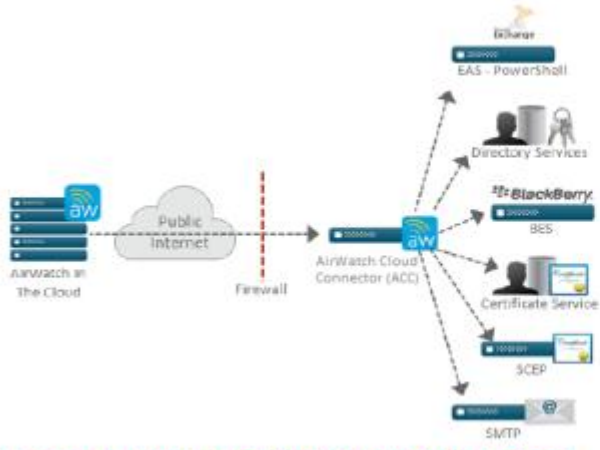
Note: For more information on how to configure the SEG Proxy Model, see the **AirWatch Secure Email Gateway (SEG) Administration Guide**.

Direct PowerShell Model

In the PowerShell model, AirWatch adopts a PowerShell administrator role and issues commands to the Exchange ActiveSync (EAS) infrastructure to permit or deny email access based on the policies defined in the AirWatch Admin Console. PowerShell deployments do not require a separate email proxy server and the installation process comprises of few simple steps.



Microsoft Office 365



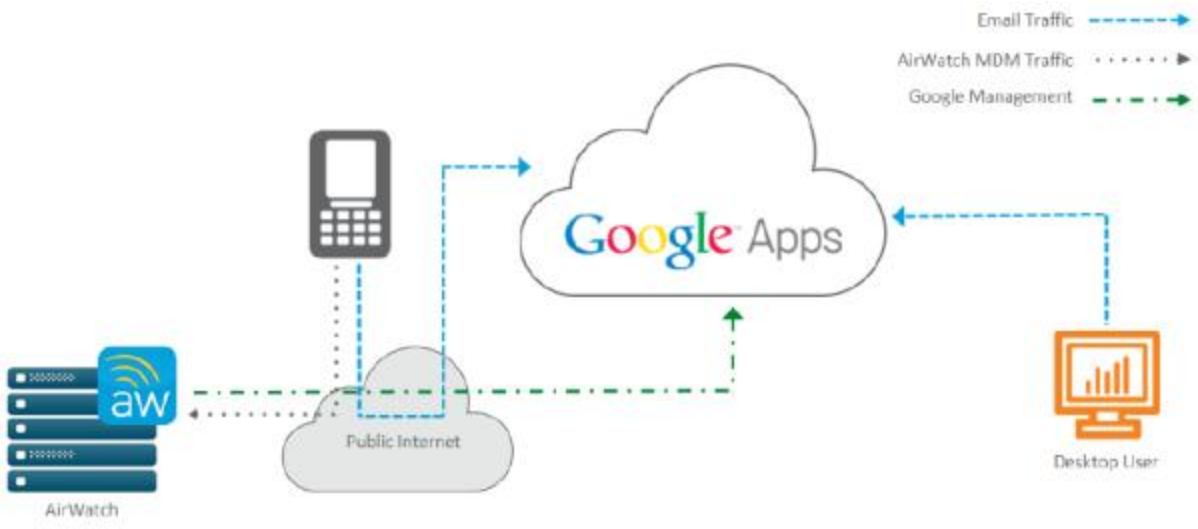
Microsoft Exchange 2010 with AirWatch Cloud

Microsoft Exchange 2010 with AirWatch On-Prem

Note: For more information on how to configure the PowerShell Model, see the AirWatch **Powershell Integration Administration Guide**.

Direct Google Model

Organizations using the Google Apps for Business email infrastructure may be familiar with the challenge of securing email endpoints for Gmail and preventing mail from circumventing the secure endpoint. AirWatch addresses these challenges by providing a flexible and safe method to integrate and secure you email infrastructure.



Note: For more information on how to configure the Google Model, see the AirWatch **Google Apps for Business Integration Administration Guide**.

Migrating Corporate Email to AirWatch

Overview

With AirWatch,migrating devices from your existing email infrastructure to one of the MEM deployment models that includes Secure Email Gateway, PowerShell, or Google Apps for Business is a simple process. You can also easily migrate devices between each deployment models using the steps mentioned in this section.

In This Section

- Migrating to SEG - Explains the steps required to migrate from your existing email infrastructure to Secure Email Gateway deployment model.
- Migrating to PowerShell - Explains the steps required to migrate from your existing email infrastructure to PowerShell deployment model.
- Migrating to Google Apps- Explains the steps required to migrate from your existing email infrastructure to Google Apps deployment model.

Migrating to SEG

Benefits of migration

- Enables users access to email only through the secure SEG proxy.
- Enforce email access control policies, thus giving access to approved users and devices.
- Enforce attachment encryption policies for data security.

Steps to migrate

1. Configure SEG at your required organization group below Global in the AirWatch Admin Console.
2. Download and Install SEG as mentioned in the **AirWatch Secure Email Gateway Administration Guide**.
3. Test the SEG functionality using the email compliance policy.
4. Disable all the compliance policies temporarily.
5. Ask all the users to enroll their devices into AirWatch.
6. Provision a new email profile (with the SEG server URL as the hostname) to all these devices.
7. Periodically, inform the users with unmanaged devices to enroll into AirWatch.

8. Modify firewall (or TMG) rules to block EAS access to the mail server ,on a specific date. This ensures mobile devices are blocked from accessing the mail server directly.

Note: All the existing Webmail, Outlook Web Access (OWA) and other email clients continues to access the mail server.

9. Enable Email policies on the SEG server to begin enforcing access control and data security on devices attempting to access corporate email.

Migrating to PowerShell

Benefits of migration

- Sync devices with Exchange or Office365 for email.
- Discover managed and unmanaged devices.
- Enforce email access control policies, thus giving access to approved users and devices.

Steps to migrate

1. Configure PowerShell integration at your required organization group below Global in the AirWatch Admin Console.
2. Configure the integration with User Groups (either custom or pre-defined) .
3. Test the PowerShell functionality with a subset of users (for example, test users) to ensure the following features work:
    - Syncing with email server to discover devices.
    - Ensuring access control is performed in real-time.
4. Disable all compliance policies temporarily.
5. Provision a new email profile to all devices that have enrolled into AirWatch with the email server hostname.

Note: The above step is highly recommended since this allows you to remove the email profile from the device using Device Compliance policies.

6. Sync with email server to discover all devices (managed and unmanaged) that are syncing for email.
7. Inform the users periodically with unmanaged devices to enroll into AirWatch.
8. Activate and enforce compliance rules to block all non-compliant devices from email access, including unmanaged devices, on a specific date.
9. Set up the email server to block all devices by default.
10. Sync with the email server to retrieve a list of allowed and blocked devices (as a result of the above policy change) and **Run Compliance** against these devices. Once done, you observe:
    - Unmanaged devices report as blocked.
    - Managed devices are immediately allowed for email.

Migrating to Google Apps

Benefits of migration

- Sync devices with Google Apps for Business.
- Integrate with or without a SEG proxy server.
- Enforce email access control policies, thus giving access to approved users and devices.

Steps to migrate

1. Prepare Google Apps for Business for AirWatch integration.
2. Enable SSO (Single Sign On) option on Google Apps.
3. Configure the Google Apps for Business integration from the AirWatch console using the MEM configuration wizard.
4. Provision EAS profiles to users with the new randomized password. Devices that do not receive this profile are automatically blocked from accessing Google Apps.

Configuring Mobile Email

Overview

Once the email infrastructure configuration with AirWatch is complete, you can deploy the devices into the AirWatch Admin console. This section explains how to configure Mobile Email Management (MEM) solution, smoothly deploy your devices into the AirWatch Admin Console, and then push the email security features onto the enrolled devices.

In This Section

- Configuring the Wizard - Learn how to configure the MEM deployment models using the MEM deployment wizard.

Configuring Mobile Email Management (MEM) Deployments

You can integrate your email infrastructure in a few simple steps using the MEM configuration wizard. To configure:

1. Navigate to **Email ▶Settings** and then select **Configure**.
2. Select your email server type and the Exchange version and if prompted, the preferred deployment type and then choose **Next**.

Note: For more information on the deployment methods, please see Protecting Your Email Infrastructure section.

3. Choose the deployment type and enter the details.

- If you choose the deployment type as SEG, then:
  - Enter a **Friendly Name** for this deployment.
  - Enter the SEG proxy server details.
- If you choose the deployment type as PowerShell, then:
  - Enter a **Friendly Name** for this deployment.
  - Enter the PowerShell server, authentication, and sync settings.
- If you choose the 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.

4. Create a template EAS profile for devices that you will manage using this MEM deployment. This template profile is 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**.
5. The **Summary** page displays the configuration details. **Save** the settings.

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

- Select the **Advanced** icon  corresponding to your deployment.
- Configure the available settings for the user mailboxes as per requirement in the **Mobile Email Advanced Configuration** screen.
    - **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 and others.
    - **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.

7. Select **Save**.

Note: For more information on the Basic and Advanced settings of the MEM configuration, please refer the **Administration Guide** of each deployment typethat includes SEG, PowerShell, and Google Apps for.

Mobile Email Profiles

Overview

Once the email infrastructure configuration with AirWatch is complete, you can deploy the Exchange Active Sync (EAS) payload onto the enrolled devices. For businesses requiring greater levels of device-level security and configuration, AirWatch provides several options to deploy containerized email through third-party email clients such as AirWatch Inbox and NitroDesk Touchdown and also deploy certificate-based email to your devices. Leverage AirWatch to seamlessly deploy, manage, renew, and revoke your email certificates. The following are few of the benefits of using certificates over standard username/password credentials:

- **Stronger Authentication** – Prevent unauthorized access through conventional cracking methods.
- **Seamless Access** – Prevent the need for end user to enter in a password or renew one every month.
- **Email Encryption and Signatures** – Encrypt sensitive mail between recipients through S/MIME or prove your identity through a message signature.

The below sections explain how to create and deploy the EAS payloads with or without certificates onto devices belonging to different platforms and with different email clients.

Note: For information about configuring EAS profiles for other platforms, please see the respective Platform Guides.

In This Section

- Configuring General Profile Settings – See how to set up a profile's general settings.
- Deploying EAS Mail via Native Mail Client for Android- Covers how to create and deploy Exchange Active Sync payload for native client on Android devices.
- Deploying EAS Mail via AirWatch Inbox for Android Devices - Covers how to create and deploy Exchange Active Sync payload for AirWatch Inbox client on Android devices.
- Deploying EAS Mail via NitroDesk's TouchDown Client for Android Devices- Covers how to create and deploy Exchange Active Sync payload for Nitrodesk Touchdown client on Android devices.
- Deploying EAS Mail via Native Mail Client for iOS Devices - Covers how to create and deploy exchange active sync payload for native client on iOS devices.
- Deploying EAS Mail via AirWatch Inbox for iOS Devices - Covers how to create and deploy Exchange Active Sync payload for AirWatch Inbox client on iOS devices.
- Deploying EAS Mail via NitroDesk's TouchDown Client for iOS Devices - Covers how to create and deploy Exchange Active Sync payload for Nitrodesk Touchdown client on iOS devices.
- Enabling Certificate-Based Email - Covers the steps to better secure your email using the certificates.

Configuring General Profile Settings

The process for creating a profile consists of two parts. First, you must specify the **General** settings for the profile. The **General** settings determine how the profile is deployed and who receives it as well as other overall settings. Next, you must specify the payload for the profile. The payload is the type of restriction or setting applied to the device when the profile is installed. The general settings listed below apply to any profile:

1. Navigate to **Devices ▶Profiles ▶List View** and select **Add**.
2. Select the appropriate platform for the profile you wish to deploy.
3. Configure **General** settings on the applicable tab. These include:
    - **Name** – Name of the profile to be displayed in the AirWatch Admin Console.
    - **Description** – A brief description of the profile that indicates its purpose.
    - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
        - **Managed** – The profile is removed.
        - **Manual** – The profile remains installed until removed by the end user.
    - **Assignment Type** – Determines how the profile is deployed to devices:
        - **Auto** – The profile is deployed to all devices automatically.
        - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.
        - **Interactive** – This is a unique assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device.
        - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
    - **Minimum Operating System** – The minimum operating system required to receive the profile.
    - **Model** – The type of device to receive the profile.
    - **Ownership** – Determines which ownership category receives the profile:
    - **Allow Removal** – Determines if the profile can be removed by the device's end user:
        - **Always** – The end user can manually remove the profile at any time.
        - **With Authorization** – The end user can remove the profile with the authorization of the administrator.
        - **Never** – The end user cannot remove the profile from the device.
    - **Managed By** – The Organization Group with administrative access to the profile.
    - **Assigned Organization Groups** – The Organization Groups that receive the profile.
    - **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
        - **Publish only to users in selected User Groups** – Specify one or more User Groups to receive the profile.

- **Enable Geofencing and install only on devices inside selected areas** – Specify a configured geofence in which devices receive the profile only within the specified geographic limits. See Geofences for more information.

  Note: Geofencing is available for Android and iOS only.

- **Enable Scheduling and install only during selected time periods** – Specify a configured time schedule in which devices receive the profile only within that time-frame. See Time Schedules for more information.

4. Configure a payload for the device platform.

   Note: For step-by-step instructions on configuring a specific payload for a particular platform, please refer to the applicable **Platform Guide**.

5. Select **Save & Publish**.

Deploying EAS Mail via Native Mail Client for Android Devices

1. Navigate to **Devices ▶Profiles ▶List View ▶Add.** Select **Android**.
2. Select **Device** to deploy your profile to a device.

   Alternatively, select **Container** to deploy your profile to a container within a Samsung KNOX device.

   Note: For more information on Samsung KNOX containerization, please see the Containerization with Samsung KNOX section.

3. Configure General profile settings as appropriate.
4. Select the **Exchange ActiveSync** payload.
5. Select **Native Mail Client** for the **Mail Client**. Fill in the **Account Name** field with a description of this mail account. Fill in the **Exchange ActiveSync Host** with the external URL of your company's ActiveSync server.

   Note: The ActiveSync server can be any mail server that implements the ActiveSync protocol, such as Lotus Notes Traveler, Novell Data Synchronizer, and Microsoft Exchange. In the case of Secure Email Gateway (SEG) deployments, use the SEG URL and not the email server URL.

6. Enable **Ignore SSL Errors**, if desired.
7. Fill in the **Domain, User**, and **Email Address** using look-up values. Look-up values pull directly from the user account record. To use the {EmailUserName} and {EmailDomain} look-up values, ensure your AirWatch user accounts have an email address and email username defined.
8. Leave the **Password** field empty to prompt the user to enter a password.
9. Select the desired **Identity Certificate** from the drop-down menu to provide credentials for cert-based authentication after the certificate is added to the **Credentials** payload.
10. Set the following optional **Settings**, as necessary:
    - Set the **Past Days of Mail/Calendar to Sync** that should sync and display.
    - Enable **Sync Calendar**, **Sync Contacts** and **Allow Sync Tasks**, if desired.

- Provide a **Maximum Email Truncation Size**.
- Add an **Email Signature**.

11. Provide the following **Restrictions**, if desired:
    - Enable **Allow Attachments** and provide a **Maximum Attachment Size**.
    - Disable **Allow Email Forwarding** to prevent data loss.
    - Enable **Allow HTML Format** to display in a plain text format.
    - Enable**Disable Screenshots**to prevent the device user from taking screenshots on the device.
12. Configure the **Peak Days for Sync Schedule** to set the syncing schedule.
    - Schedule the peak week days for syncing and the **Start Time** and **End Time** for sync on selected days.
    - Set the frequency of **Sync Schedule Peak** and **Sync Schedule Off Peak**.
        - Choosing **Automatic** syncs email whenever updates occur.
        - Choosing **Manual** only syncs email when selected.
        - Choosing a time value syncs the email on a set schedule.
    - Enable **Use SSL**, **Use TLS** and **Default Account**, if desired.
13. Select **Use S/MIME**and provide a**Migration Host** if you are using S/MIME certificates for encryption. From here you can select an S/MIME certificate you associate as a **User Certificate** on the **Credentials**payload.
14. Select**Save**to save the settings or**Save & Publish**to save and push the profile settings to the required device.

Deploying EAS Mail via AirWatch Inbox

Use the following steps to create a configuration profile for the AirWatch Inbox:

1. Navigate to **Device ▶Profiles ▶List View.**
2. Click **Add** and select **Android** as the platform.
3. Configure General profile settings as appropriate.
4. Select the **Exchange ActiveSync** payload and then select the **AirWatch Mail Client** from the **Mail Client** drop-down.
5. Enter the **Exchange ActiveSync Host**, which is the information from your EAS server. For example, **webmail.corpmdm.com**.
6. Enter **Login Information**, which is the information used to authenticate user connections to your EAS Host. The profile supports lookup fields for inserting enrollment user's information and login information. See Username and Password for more information.

   You can also select an Identity Certificate that you have defined in the AirWatch Admin Console.
7. Configure general email **Settings**, such as:
    - Past Days of Mail to Sync
    - Sync Interval

- Past Days of Calendar to Sync
- Email Signature

8. Set which **Contacts and Calendar** data to use within the AirWatch Inbox:
   - **Native Contacts/Calendars** – Syncs the native calendar and contact app with AirWatch Inbox.
   - **AirWatch Contacts/Calendars** – AirWatch has now introduced its own **Contacts** and **Calendar** applications as an add-on to the AirWatch Inbox. These applications are downloaded together as a single app from the Play Store. Unlike Native Contacts/Calendars application, AirWatch Contacts/Calendars application encrypts the contacts and calendar data.
     - Additionally, AirWatch Inbox allows you to export individual contacts or in bulk from the corporate contact to the AirWatch Contacts app.
   - **Do Not Sync** – You can disable the sync of contacts and calendars within the AirWatch Inbox profile.
9. Configure a **Passcode** for AirWatch Inbox. You can require an end user to enter a passcode when the AirWatch Inbox is opened. This is not the email account password, but the passcode the user enters to access the application. The following passcode settings are available:
   - Authentication Type

     To allow Android users to log in using their Active Directory credentials, select **Active Directory Password** as the **Authentication Type** under the **Passcode** section.
   - Passcode Complexity.
   - Minimum Passcode Length.
   - Minimum Number of Complex Characters.
   - Maximum Passcode Age (days).
   - Passcode History.
   - Auto-Lock Timeout (min).
   - Auto-Lock When Device Locks.
   - Maximum Number of Failed Attempts.
10. Configure additional restrictions and security settings. The following restrictions are available:
    - Allow Copy and Paste:
      - Disable user's ability to long press email text and copy it to the clipboard.
      - Disable user's ability to copy text from outside of the email client and paste it into a mail message.
    - Allow Attachments.
    - Restrict attachments to set which applications can open attachments.
    - Restrict taking screenshots in the app.
    - Restrict domains by creating either a blacklist or whitelist of domain names.
    - Allow opening of links only through the AirWatch Browser.
11. Select **Save & Publish** when you are done.

Username and Password

You can define the username that is used for users to log in to the AirWatch Inbox. This could be their actual email address or an email username that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the AirWatch **Inbox** profile settings, there is a **User** field under **Login Information** that you can set to a predefined lookup value.

If you have email usernames that are different than users' email addresses, you can use the {EmailUserName} field, which corresponds to the email usernames imported during directory service integration. If your users' email usernames are same as their email addresses, you would still use the {EmailUserName} field, which would use their email addresses as they were imported during directory service integration.

Deploying EAS Mail via NitroDesk's TouchDown Client for Android Devices

Once each user has an email address and email username you can create an EAS profile with the following steps:

1. Navigate to **Devices ▶Profiles ▶List View ▶Add.** Select **Android**.
2. Select **Device** to deploy your profile to a device.

   Alternatively, select **Container** to deploy your profile to a container within a Samsung KNOX device.

   Note: For more information on Samsung KNOX containerization, please see the Containerization with Samsung KNOX section.

3. Configure General profile settings as appropriate.
4. Select the **Exchange ActiveSync** profile payload.
5. Choose the **NitroDesk TouchDown Mail Client** when deploying mail to Android devices. Assign an **Account Name**, enter the name or address of the **Exchange ActiveSync Host** server, and indicate if AirWatch should **Ignore SSL Errors** by selecting the applicable check box.

   Optionally, select **Use S/MIME** if you are using S/MIME certificates for encryption. From here you can select an S/MIME certificate you associate as a **User Certificate** on the **Credentials** payload.
6. Leverage user account info to simplify authentication in **Login Information**. Fill in the **Domain**, **User** and **Email Address** using look-up values to pull directly from the user account record. To use the **{EmailUserName}** and **{EmailDomain}** look-up values ensure your AirWatch user accounts have an email address and email username defined.
7. Leave the **Password** field empty to prompt the user to enter a password.
8. Select the desired **Identity Certificate** from the drop-down menu to provide credentials for certification-based authentication after the certificate is added to the **Credentials** payload.
9. Set the following optional **Settings**, as necessary:
   - Set the **Past Days of Mail/Calendar to Sync** that should sync and display.
   - Provide a **Maximum Email Truncation Size**.
   - Add an **Email Signature**, and **Enable Signature Editing**, if desired.
10. Configure **Passcode Settings**.
    - Enable **Require Passcode** to necessitate the input of a Passcode to access EAS mail.
    - Enable **Suppress Application PIN**, if desired.
11. **Enable Security Restrictions** to enable or disable functionality that TouchDown may natively restrict. The following list details some of the key settings you can apply to your EAS profile to allow certain functionality:
    - Enable **Allow Copy-paste** the copying and pasting of data from the TouchDown client.
    - Enable **Copy to Phonebook** to cause TouchDown to copy contacts to the device phonebook.
    - Select **Allow SD Card**.

- Enable **Allow Attachments** to permit users to download email attachments.
- Set the **Maximum Attachment Size** (in MB) that emails can receive.
- Require Device Encryption.
- Require SD Card Encryption.
- Select **Allow Widgets** to enable or disable widget functionality including: **Email Widget**, **Calendar Widget**, **Task Widget**, **Universal Widget** and **Show Data On Lock Screen Widgets**.
- Enable **Show Email/Calendar/Task Info on Notification Bar** TouchDown to show information (for example, the first few lines of an email) as a notification when email/calendar/task information is received.
- Enable **Data/Settings Backup** to allow end users to backup data and settings to an SD card.

12. Provide an enterprise **License Key** under **TouchDown License** for a seamless end-user experience. After deploying Touchdown as a recommended app, all profile configurations are applied to the app automatically.
13. Select **Save & Publish**.

Deploying EAS Mail via Native Mail Client for iOS Devices

1. Navigate to **Devices ▶Profiles ▶List View ▶Add.** Select **Apple iOS**.
2. Configure General profile settings as appropriate.
3. Select the **Exchange ActiveSync** payload.
4. Select **Native Mail Client** for the **Mail Client**. Fill in the **Account Name** field with a description of this mail account. Fill in the **Exchange ActiveSync Host** with the external URL of your company's ActiveSync server.

   Note: The ActiveSync server can be any mail server that implements the ActiveSync protocol, such as Lotus Notes Traveler, Novell Data Synchronizer and Microsoft Exchange. In the case of Secure Email Gateway (SEG) deployments, use the SEG URL and not the email server URL.

5. Fill in the **Username, Email Address** and **Email Domain Name** using look-up values. Look-up values pull directly from the user account record. To use the {EmailUserName} and {EmailDomain} look-up values, ensure your AirWatch user accounts have an email address and email username defined.
6. Leave the **Password** field empty to prompt the user to enter a password.
7. Set the following optional settings, as necessary:
   - **Payload Certificate** – Define a certificate for cert-based authentication after the certificate is added to the **Credentials** payload.
   - **Past Days of Mail to Sync** – Downloads the defined amount of mail. Note that longer time periods will result in larger data consumption while the device downloads mail.
   - **Prevent Moving Messages** – Disallows moving mail from an Exchange mailbox to another mailbox on the device.
   - **Prevent Use in 3rd Party Apps** – Disallows other apps from using the Exchange mailbox to send messages.
   - **Disable recent contact sync** – Prevent the automatic sync of recent contacts to devices.
8. Select **Save and Publish** to push the profile to available devices.

Deploying EAS Mail via AirWatch Inbox for iOS Devices

Use the following steps to create a configuration profile for the AirWatch Inbox. For more information about AirWatch Inbox, please see the **AirWatch Inbox Guide**.

1. Navigate to **Device ▶Profiles ▶List View.**
2. Click **Add** and select **iOS** as the platform.
3. Configure General profile settings as appropriate.
4. Select the **Exchange ActiveSync** payload and then select the **AirWatch Inbox** from the **Mail Client** drop-down.
5. Enter the **Exchange ActiveSync Host,** which is the information of your EAS server. For example: **webmail.airwatchmdm.com**.
   - Enable **Ignore SSL Errors** to allow the devices to ignore Secure Socket Layer errors from agent processes.
   - Enable **Use S/MIME** to select the certificate/smart card for signing and encrypting email messages. Prior to enabling this option, ensure you have uploaded necessary certificates under **Credentials** profile settings.

     Note: You do not need to upload any certificates if a smart card is selected as the credential source in the **Credentials** profile settings.

   - Select the certificate/smart card to sign only email messages in the **S/MIME Certificate** field.
   - Select the certificate/smart card to both sign and encrypt email messages in the **S/MIME Encryption Certificate** field.
   - If the smart card is selected, default information populates the **Smart Card Reader Type** and **Smart Card Type**.
   - Choose the **Smart Card Timeout** interval.
6. Enter **Login Information**, which is the information used to authenticate user connections to your EAS Host. The profile supports lookup fields for inserting enrollment user's information and login information. See Username and Password for more information.
7. Configure Settings, such as:
   - Enable Email
   - Enable Calendar
   - Enable Contacts
   - Sync Interval – The frequency with which the AirWatch Inbox app syncs with the email server.
   - Email Notifications – Configure how end users can be notified of new emails. **Disabled** means they will not receive a notification. You can also trigger the device to play an alert sound, or allow the device to display specific email message details such as the sender, subject, and message preview.
   - Past Days of Mail to Sync
   - Past Days of Calendar to Sync
   - Email Size (default is unlimited)
   - Email Signature

- Enable Signature Editing

8. Configure a Passcode for AirWatch Inbox. You can require an end user to enter a passcode when the AirWatch Inbox is opened. This is not the email account password, but the passcode the user will have to enter to access the application. The following passcode settings are available:

   - Authentication Type

     To allow iOS users to log in using their AirWatch credentials, select **Username and Password** as the **Authentication Type** under the **Passcode** section.

   - Complexity, including whether to allow simple passcodes (e.g. 1111).
   - Minimum Length
   - Minimum Number of Complex Characters, if your **Complexity** is set to **Alphanumeric**.
   - Maximum Passcode Age (days)
   - Passcode History
   - Auto-Lock Timeout (min)
   - Maximum Number of Failed Attempts

9. Configure additional restrictions and security settings. The following restrictions are available:

   - Allow/Disable Copy and Paste:
     - Disable user's ability to long press email text and copy it to the clipboard.
     - Disable user's ability to copy text from outside of the email client and paste it into a mail message.
   - Restrict all links to open in the AirWatch Browser app only.
   - Restrict attachments to open only in the Secure Content Locker, or in other apps of your choosing.
   - Set a Maximum Attachment Size (MB).
   - Allow Printing.

10. Select **Save & Publish** when you are done.

Username and Password

You can define the username that is used for users to log in to the AirWatch Inbox. This could be their actual email address or an email username that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the AirWatch **Inbox** profile settings, there is a **User** field under **Login Information** that you can set to a predefined lookup value.

If you have email usernames that are different than users' email addresses, you can use the {EmailUserName} field, which corresponds to the email usernames imported during directory service integration. If your users' email usernames are same as their email addresses, you would still use the {EmailUserName} field, which would use their email addresses as they were imported during directory service integration.

Removing Profile or Enterprise Wiping

If the profile is removed via the remove profile command, compliance policies, or through an enterprise wipe, all email data gets deleted, including:

- User account/login information.
- Email message data.
- Contacts and calendar information.
- Attachments that were saved to the internal application storage.

Note: Attachments saved outside of AirWatch Inbox will **not** be deleted.

Deploying EAS Mail via NitroDesk's TouchDown Client for iOS Devices

The NitroDesk TouchDown mail application provides additional email security flexibility for iOS devices. It is a paid application available from the App Store. NitroDesk TouchDown integration with iOS devices requires the AirWatch Agent v4.4 or higher and the TouchDown mail client v1.8.1 or higher. You can create an EAS profile to leverage NitroDesk TouchDown with the following steps:

1. Navigate to **Devices ▶Profiles ▶List View ▶Add.** Select **Apple iOS.**
2. Configure General profile settings as appropriate.
3. Select the **Exchange ActiveSync** payload.
4. Select **NitroDesk TouchDown** for the **Mail Client**. Fill in the **Exchange ActiveSync Host** with the external URL of your company's EAS server.

   Note: The EAS server can be any mail server that implements the EAS protocol, such as Lotus Notes Traveler, Novell Data Synchronizer and Microsoft Exchange.

5. Fill in the **Username** and **Email Address** using look-up values. Look-up values pull directly from the user account record. To use the {EmailUserName} and {EmailDomain} look-up values, ensure your AirWatch user accounts have an email address and email username defined.
6. Leave the **Password** field empty to prompt the user to enter a password.
7. Set the additional NitroDesk TouchDown settings, such as sync settings, passcode requirements and security restrictions. Key settings include:
   - **Past Days of Mail/Calendar to Sync** – Set the amount of past days of Mail/Calendar TouchDown should sync and display.
   - **Require Manual Sync While Roaming** – Suppress automatic data sync when a device is on a roaming network. This can help reduce roaming charges.
   - **Enable HTML Email** – Enable to display all emails in HTML format.
   - **Maximum Email Truncation Size** – Set the maximum allowed email size (in KB) that can be received.
   - **Email Signature** – Specify an email signature to be used on the application.

- **Enable Email Signature Editing** – Allow users to change the email signature.
- **Passcode** – Enable this setting and configure various passcode complexity parameters.
- **Enable Security Restrictions** – Enable this setting to enable or allow functionality that TouchDown may natively restrict. The following list details some of the key settings you can apply to your EAS profile to allow certain functionality:
    - **Allow Copy-paste** – Allow the copying and pasting of data from the TouchDown client.
    - **Enable Copy to Phonebook** – Enable this setting to cause TouchDown to copy contacts to the device phonebook.
    - **Allow Attachments** – Allow users to download email attachments.
    - **Maximum Attachment Size** – Sets the maximum attachment size (in MB) that can be received.
    - **Allow Data Export** – Enable this setting to allow export of calendar/email to native apps.
    - **Show Email/Calendar/Task Info on Notification Bar** – Enable TouchDown to show information (for example, the first few lines of an email) as a notification when email/calendar/task information is received.
    - **Allow Printing** – Allows users to print email.
    - **Show Data On Lock Screen Widgets** – Enable this setting to allow lock screen widgets to display email/calendar/task data.

8. Select **Save & Publish**.

Note: For iOS devices, you do not enter License Key information in the EAS Profile for NitroDesk TouchDown. You can deploy it as a Volume Purchase Program (VPP) application from the AirWatch Admin Console. Alternatively, you may tell users to purchase and download it themselves.

After deploying TouchDown as a recommended app, all profile configurations are applied to the app automatically. When the user first opens the TouchDown application the AirWatch Agent will launch and prompt the user to authorize the TouchDown application. Once authorized, TouchDown will re-open and the settings will be automatically applied.

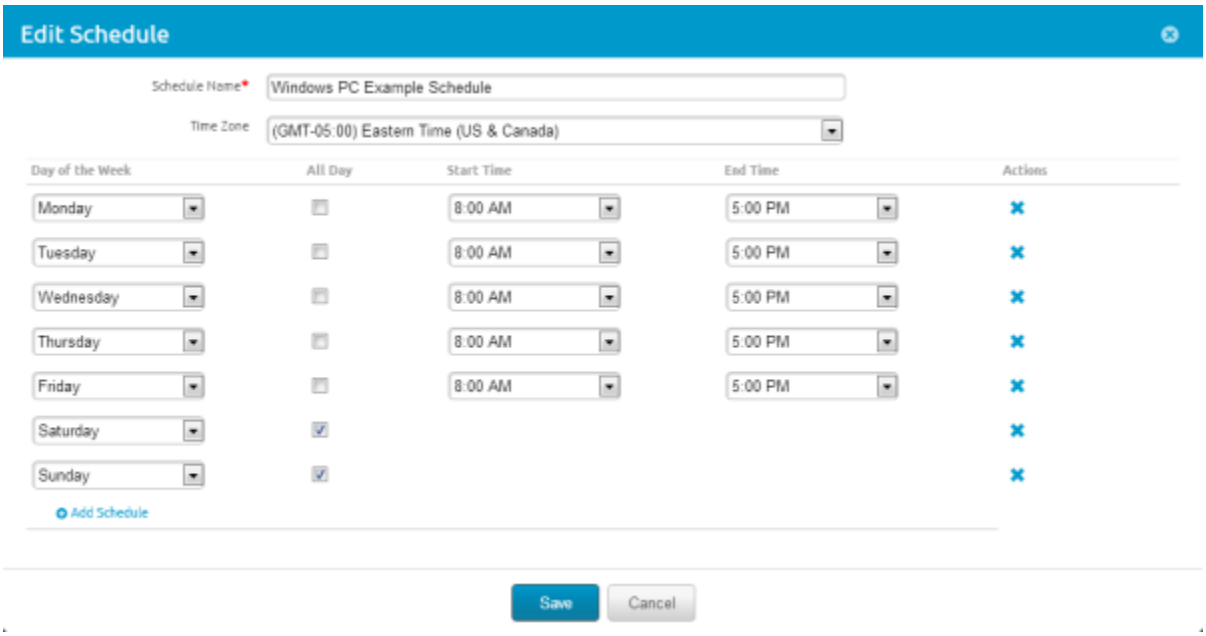
Enabling Certificate-Based Email

1. Navigate to **Devices ▶Profiles ▶List View**.
2. Select **Add** and then select the required platform.
3. Choose the **Credentials** profile setting and configure it.
    - **Credential Source**: Select any from the available list
        - **Upload** – Upload a certificate and enter a name for the certificate.
        - **Defined Certificate Authority** – Select the CA and the certificate template from the dropdown list for your organization group.

        Note: The certificate authorities and the templates are added for an organization group at **Devices ▶Certificates ▶Certificate Authorities**.
    - **User Certificate** – Select the type of S/MIME certificate.

Time Schedules

In addition to simply assigning applicable profiles, you have the ability to enhance device management further by controlling when each profile assigned to the device is active. Configure and apply time schedules to restrict when profiles are active on the device. Applying time schedules to profiles secures your corporate resources by only allowing employees access during the specific days and time frames. Conversely, applying time schedules can also limit personal content and access during work hours.



In This Section

- Defining Time Schedules – See how to create a time schedule, which allows or denies access to internal content and features based on the day and time.
- Applying a Time Schedule to a Profile – See how to apply a time schedule to a profile, which lets you control when and how a particular profile is activated.

Defining Time Schedules

To create a time schedule:

1. Navigate to **Devices ▶Profiles ▶Settings ▶Time Schedules**.
2. Select **Add Schedule** to launch the **Add Schedule** window.
3. Enter a name for the schedule in the **Schedule Name** field.
4. Select the applicable **Time Zone** using the drop-down menu.
5. Select the **Add Schedule** hyperlink.

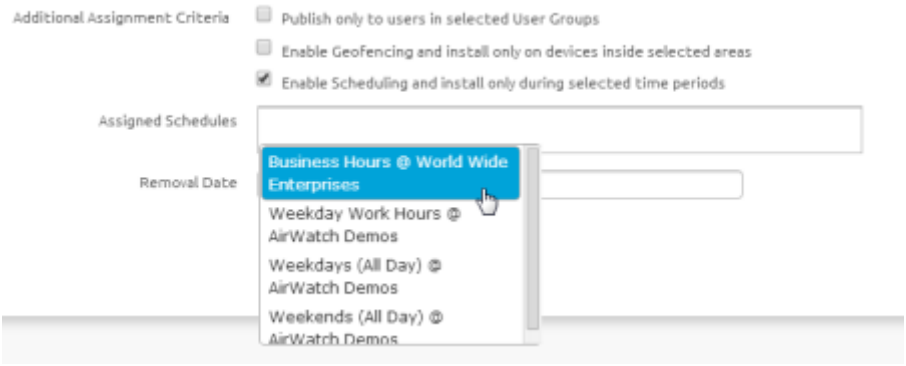
6. Select the **Day of the Week**, **Start Time** and **End Time** using the applicable drop-down menus. You can also select the **All Day** check box to disable start and end times for the schedule.
   To remove a day from the schedule, select the applicable **X** under **Actions**.
7. Repeat steps 5 and 6 as many times as is necessary to add additional days to the schedule.
8. Select **Save**.

Applying a Time Schedule to a Profile

Once you have defined a time schedule, you can apply it to a profile and combine it with other payloads to create more robust profiles. For example, you can define time schedules for the normal work hours of different organization groups and add a Restrictions payload that denies access to the Game Center, multiplayer gaming or YouTube content based on ratings and other settings.

Once activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

1. Navigate to **Devices ▶Profiles ▶List View ▶Add** and select your platform.
2. Select **Enable Scheduling and install only during selected time periods** on the **General** tab. An **Assigned Schedules** box displays.



3. Enter one or multiple Time Schedules to this profile.
4. Configure a payload, such as Passcode, Restrictions or Wi-Fi that you want to apply only while devices are inside the time frames.
5. Select **Save & Publish**.

Enforcing Email Access Control

Overview

Now that email has been deployed, you can further protect your mobile mail with access control to only allow secure, compliant devices to access your mail infrastructure. Mobile email access control can be used in many ways to restrict mails from:

- Inactive or un-managed devices
- Compromised or Non-encrypted
- Devices by Make/Model/OS

AirWatch provides the Email Compliance policies that include the General Email Policies, Managed Device Policy, and the Email Security Policy. The following sections explain the compliance policies available in the AirWatch Admin Console, their features and how to create a policy.

In This Section

- Creating an Email Policy - Explains the type of compliance polices available and how to create email compliance policies for the devices.

Creating an Email Policy

Email policy enables you to provide email access to only the required and approved devices.

Note: Some email policies may not be applicable to all the Mobile Email Management deployment models. Refer to the corresponding Administration Guide for additional info regarding email policies for a MEM deployment model.

1. Navigate to **Email ▶Compliance Policies ▶Email Policies**.
2. Edit any of the email policies. Use the edit policy icon under the **Actions** column to allow or block a policy.
    - **General Email Policies** – Enforce policies on all devices accessing email.
        - **Sync Settings** – Prevent the device from syncing with specific EAS folders. Note that AirWatch prevents devices from syncing with the selected folders irrespective of other compliance policies.

        Note: 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** – Restrict email access only to managed devices.
        - **Mail Client** – Restrict email access to a set of mail clients. You can allow or block mail clients based on the client type such as **Custom**, **Pre-defined**, and **Discovered**. You can also set default actions for mail client and newly discovered mail clients that do not display in the Mail Client dropdown field. For the custom client type, wild card (*) characters and auto-complete are supported.

Note: On choosing a User Group, the policy applies to all the users of that group.

- **User** – Restrict email access to a set of users. You can allow or block mail client based on the user type that includes Custom, Discovered,AirWatch User Account and AirWatch User Group. You can also set default actions for usernames and new or discovered mail clients that do not display in the Username/Group dropdown field. For the custom client type, wild card (*) characters and auto-complete are supported.
- **EAS Device Type** – Whitelist or blacklist devices based on the EAS Device Type attribute reported by the end user device. You can allow or block EAS device type based on the client type that includes Custom and Discovered mail client. You can also set default actions for EAS device types that do not display in the Device Type dropdown field.For the custom client type, wild card (*) characters and auto-complete are supported.

- **Managed Device Policies** – Enforce policies on managed devices accessing email.
  - **Inactivity** – 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 AirWatch prevents email access.
  - **Device Compromised** – Prevent compromised devices from accessing email.

Note: This policy does not block email access for devices that have not reported compromised status to AirWatch.

  - **Encryption** – Prevent email access for unencrypted devices.

Note: This policy is applicable only to devices that have reported data protection status to AirWatch.

  - **Model** – Restrict email access based on the Platform and Model of the device.
  - **Operating System** – Restrict email access to a set of operating systems for specific platforms.
  - **Email Security Policies** – Enforce policies on attachments and hyperlinks. **Attachments (managed devices)** – Encrypt email attachments of selected file types. These attachments are secured on the device and are only available for viewing on the AirWatch Secure Content Locker.

Note: Currently, this feature is only available in managed iOS, Android devices, and Windows Phone 8 with the Secure Content Locker application. For other managed devices, you can choose to either allow encrypted attachments, block attachments, or allow unencrypted attachments.

  - **Attachments (unmanaged devices)** – Encrypt and block attachments or allow unencrypted attachments for un-managed devices.
  - **Hyperlink** – Allow 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.

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.


Email Policies
Disable Compliance
Current Setting
Inherit
Override
General Email Policies
Active
Policy
Current Compliance Policies
Actions
Sync Settings
Sync Settings Disable
Managed Device
Allow unmanaged devices
Mail Client
Allow unlisted clients, Allow Discovered Clients
User
Block unlisted users, Block Discovered Users
EAS Device Type
Allow other device types
Managed Device Policies
Active
Policy
Current Compliance Policies
Actions
Inactivity
Allow Inactive Devices
Device Compromised
Allow compromised devices
Encryption
Allow unencrypted devices
Model
Allow new models
Operating System
Allow new OS
Email Security Policies
Active
Policy
Current Compliance Policies
Actions
Attachments (managed devices)
1 or more file types encrypted, 1 or more file types blocked
Attachments (unmanaged devices)
1 or more file types blocked

Managing Mobile Email

Overview

Once your email infrastructure is secure, manage email access and settings for all enrolled devices from the AirWatch Admin Console with the tools and features listed below.

In This Section

- Email Dashboard - Details how to manage the deployed devices from the Email Dashboard page.
- List View - Explains the List View screen and how it provides real time updates of the MEM managed devices.

Using 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**. From the Email Dashboard, you can access the **List View** that enables you to:

- Whitelist or blacklist a device to allow or deny access to email respectively.
- 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, and 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 an organization group, select the Managed Devices graph. This displays the results in the List View screen.

Note: AirWatch provides you with the option to block emails on non- compliant devices (example, device with blacklisted app). Emails are enabled once the devices become compliant. You can view the list of such devices on the Email Dashboard marked with reason tag as 'MDM Compliance'.

Using the Email 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**. View the device or user specific information by switching between the **Device** and **User** tabs. 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 includes:

- **Last Request** - The last state change of the device either from AirWatch or from Exchange in the PowerShell integration. 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.

Note: 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** - The device information displays in these fields.
- **Mailbox Identity** - The location of the user mailbox in the Active Directory.

Searching With Filters

Narrow the device search using the **Filter** option on the List View page. Use the following filter options:

- **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 Email Actions

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

Note: Please note that these actions once performed cannot be undone.

Override

Select the check box corresponding to a device to perform actions on it. Whitelist or blacklist a device irrespective of the compliance policy and revert back to the policy when needed.

- **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** - Queries the Exchange server for an updated list of devices that have attempted to sync email (Direct PowerShell Model). If you do not choose this option, the unmanaged device list does not change unless one of the unmanaged devices is enrolled into AirWatch or you manually whitelist or blacklist a device, thus initiating a state change command.

Note: AirWatch offers the 'Email Sync' option within the Self Service Portal (SSP) so that end users can sync their devices with the mail server 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. This command operates differently when using the PowerShell model versus the SEG model.
    - If SEG is configured, this command updates SEG with the latest compliance policies.
    - If the PowerShell model is configured, this command manually runs a compliance check on all devices and blocks or allows device access to email.

Note: When the Direct PowerShell Model is configured, AirWatch communicates directly to the CAS array via remote signed PowerShell sessions established from the console server or AirWatch Cloud Connector (ACC) (depending on the deployment architecture). Using remote signed sessions, PowerShell commands are sent to blacklist (block) and whitelist (allow) device ID's on a given users CAS mailbox in Exchange 2010/2013 based on the device's compliance status in AirWatch.

- **Enable Test Mode** - Tests email policies without applying them on devices of SEG integrated deployments.

Administration

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

- **Enrollment Email** - Sends an email to the user with all the details required for enrollment.

On discovering an un-managed device, send an enrollment email asking the user to enroll the device (PowerShell only).

- **Dx Mode On** - Runs the diagnostic for the selected user mailbox.
- **Dx Mode Off** - Turns off the diagnostic for the selected user mailbox.

  Disable or enable diagnostics to observe granular process information as devices access email (SEG only).
- **Update Encryption Key** - Resets the encryption and then re-syncs the emails for the selected devices.
- **Remote Wipe** - Resets the device to factory settings.

  Perform a device wipe (reset to factory settings) on a lost or stolen device containing sensitive information (PowerShell only).
- **Delete Unmanaged Devices** - Deletes the selected unmanaged device record from the dashboard.

Note: Please note that this record may reappear after the next sync.

- **Migrate Devices** - Migrates selected devices to other chosen MEM configurations by deleting the installed EAS profile and pushing the EAS profile of the chosen configuration on the device.