

# Managing and Protecting Mobile Email with AirWatch

© 2013 AirWatch, LLC. All Rights Reserved.

This document, as well as the software described in it, is furnished under license. The information in this manual may only be used in accordance with the terms of the license. This document should not be reproduced, stored or transmitted in any form, except as permitted by the license or by the express permission of AirWatch, LLC.

Other product and company names referenced in this document are trademarks and/or registered trademarks of their respective companies.

## Contents

<b>Introduction</b>	<b>2</b>
Mobility: A New Standard for Email Security	2
Unsecured Email Access: Mail Infrastructure Features	3
AirWatch MDM Email Security	4
Enforced Security Settings	4
Automatic Configuration	4
Customizable Restrictions	4
Certificates and AirWatch	5
AirWatch Mobile Email Management: The Secure Email Gateway	6
SEG Access Control	7
SEG Management Visibility	8
<b>Providing the Right Email Client</b>	<b>9</b>
AirWatch Email Container for Android	9
TouchDown for iOS and Android	9
<b>Choosing and Configuring the Right Email Solution</b>	<b>11</b>
Proxy Deployment	12
EAS SEG Configuration for AirWatch On-Premise Deployments	12
EAS SEG Configuration for AirWatch SaaS Deployments	12
AirWatch Advanced Email Security with PowerShell Infrastructures	13
PowerShell and System Requirements	13
Cloud Deployments	13
On-Premise Deployments	14
Securing PowerShell Email with EIS	14
AirWatch Advanced Email Management with Google Apps for Business	15
Google and System Requirements	16
<b>Additional SEG Security Features</b>	<b>17</b>
High Availability	17
Deployment Options for Maximum Security	17
Authentication Extensibility	17

## Introduction

The convenience of mobile email access has changed the face of corporate communication, but as soon as email is enabled on a device, all of the information exchanged over email becomes subject to new levels of exposure, putting the organization at unnecessary risk for data threats and security breaches.

### Mobility: A New Standard for Email Security

Email mobility introduces a number of new security concerns that are not addressed by standard email security infrastructures. Business and/or IT organizational leaders may believe that the basic vulnerability checking performed through the mail client is an adequate layer of security, but this is a dangerous misconception. By focusing on insufficient [basic Email security policies](#) and failing to implement additional security layers and access control to account for mobile email security, businesses are missing the mark in terms of targeting security resources where they are needed. When the basic security measures fail, this not only produces unwanted data exposure, but also results in wasted corporate resources given that the infrastructure in place did not suffice.

Consider the following facts regarding mobile email security:

- **Equal access does not mean equal security:**
  - Mail providers advertise seamless mobile access as an included component of their overall email client package, but it is important to realize that this access is not secured.
  - Even if the desktop client email infrastructure is under tight network restrictions, many of these security layers are no longer relevant or sufficient in a mobile environment.
- **Mobility introduces new levels of threats:**
  - Employees are accessing email from various locations over unsecured wireless and data networks.
  - Lost or stolen devices increase the potential for data exposure.
  - Mobile users have access to a vast market of unauthorized third-party mail client applications.
- **Device ownership issues** raise security concerns:
  - Recent studies have revealed that 40% of workers are using their personal devices to access business resources such as corporate email.
  - At least 50% of Enterprise email users will rely primarily on a browser, tablet, or mobile client instead of a desktop client by 2016 (According to research conducted by Gartner).
  - An increasing number of corporations are introducing Bring Your Own Device (BYOD) models, where employees bring their devices into the workplace and leave with them when they leave the company.
- Potential leakage of sensitive information exchanged or stored over email is a **legal liability**.
  - Gartner projects that more than 50% of global 1000 companies will have stored customer sensitive data in the public cloud by year-end 2016.
  - Industry-specific regulations, such as HIPAA compliance and privacy requirements, put organizations at risk for fines and other punitive measures if client information is not adequately protected from unauthorized access.

Additionally, the standard risks that permeate corporate email, such as copying corporate Email into other mail clients, extend to the less-policed realm of mobile devices. There is a clear need for a more advanced mobile Email solution. AirWatch offers an Email solution that sufficiently addresses the issues above an additional layer of access control and visibility that is not provided by the native mail infrastructure. AirWatch offers an Email Management solution that provides all of the key factors of a successful and secure mobile email deployment, including:

- Customizable access control and compliance policies.
- Monitoring capabilities.
- Tight integration with flexible configuration.

### Unsecured Email Access: Mail Infrastructure Features

Even as they create strict email security policies for locally-accessed email, many corporations do not implement the required level of mobile email security. Instead, they mistake the bare minimum of features (that require manually-configured intervention by the IT administrator) as adequate protection for mobile email. In most cases, the default mobile email access is completely unprotected; however, even the most advanced email infrastructures can only provide very limited security features such as the following:

- Encryption requirements
- Remote Wipe capability
- Password requirements
- Sync settings configuration

While these features are useful (when available from the provider), they are not sufficient for fully securing a corporate mobile email deployment due to a lack of IT management visibility and a failure to address many of the security holes introduced by mobile email. In general, the Email provider focuses on mobile **access** to email rather than providing dedicated mobile email **security**.

If your corporation is serious about email security, consider using one of the more robust solutions offered by AirWatch.



## AirWatch MDM Email Security

AirWatch MDM provides email security for mobile devices managed by AirWatch, and this solution is a good way to protect your corporate email infrastructure. AirWatch MDM offers all the basic security features provided by the email provider, as well as additional management options through over the air email profile provisioning.

### Enforced Security Settings

Take advantage of the latest modern email security features using AirWatch's advanced email tools:

- Use digital signatures through S/MIME capability.
- Protect sensitive data through forced encryption.
- Add an extra layer of security with SSL.
- Require Passcode for inbox access.

### Automatic Configuration

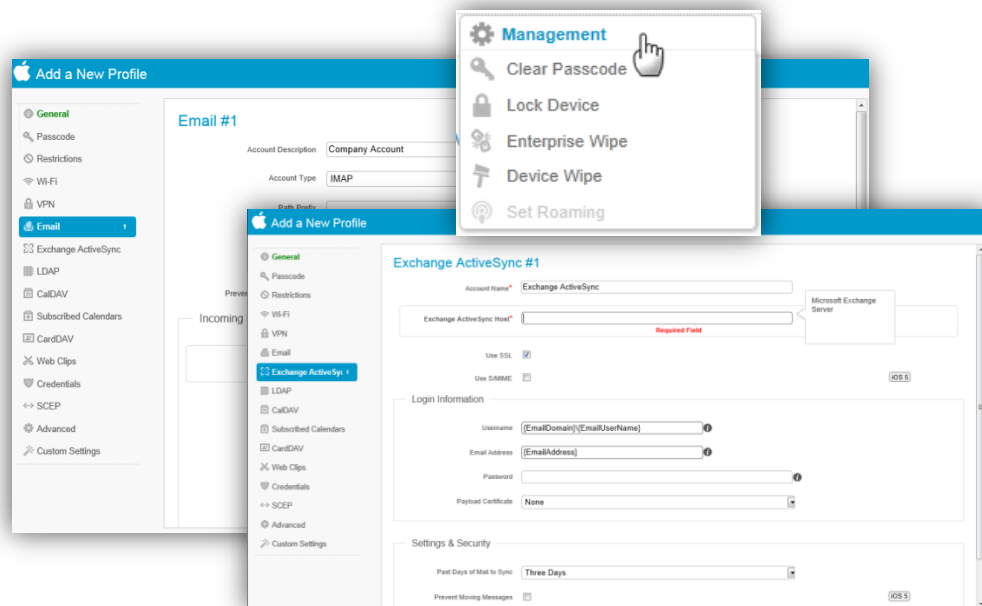
AirWatch's over-the-air provisioning capabilities allow the IT administrator to configure any necessary settings or authentication on behalf of the end-user so that employees have instant and secure access to corporate email:

- Certificate Management.
  - Install, remove, and manage certificates using the AirWatch certificate dashboard.
- Immediate and automatic security profile deployment.
- Set authentication type.

### Customizable Restrictions

Your corporation can customize email restrictions to prevent opening potential security holes and restrict data sharing according to corporate security needs and policies:

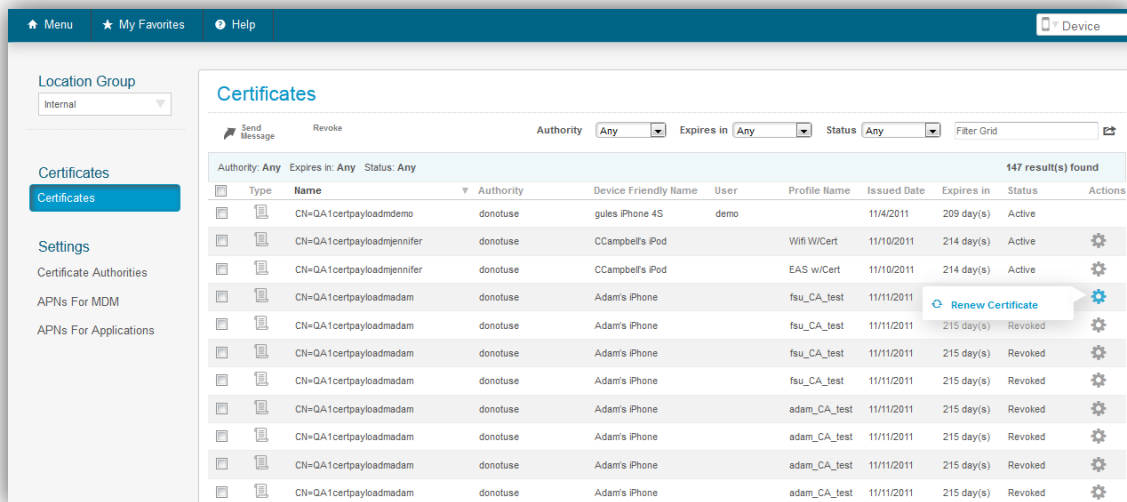
- Allow/disallow widgets.
- Allow/disallow the copy and paste feature to restrict data sharing.
- Prevent opening Email in third party applications.



## Certificates and AirWatch

AirWatch offers advanced certificate integration and management tools that make it easy for Administrators to deploy certificates to devices for email security and authentication. Certificates provide deeper levels of security and flexibility for corporate email authentication and access control. If your corporation needs the most advanced (and recommended) level of email security, as described in the next section, AirWatch recommends coupling their advanced certificate integration with their integrated Email Security solution, the Secure Email Gateway. In addition to the convenient security that certificates provide, AirWatch MDM makes it easy to manage certificates simultaneously with the smart device fleet:

- **Certificate dashboard** for convenient certificate management through the certificate management lifecycle. Issue, manage, renew, and revoke all digital certificates deployed to your device fleet.




The screenshot shows the AirWatch Certificates dashboard. On the left, there is a navigation menu with options like 'Location Group' (set to 'Internal'), 'Certificates', 'Settings', 'Certificate Authorities', 'APNs For MDM', and 'APNs For Applications'. The main area displays a table of certificates with 147 results found. The table has columns for Type, Name, Authority, Device Friendly Name, User, Profile Name, Issued Date, Expires in, Status, and Actions. A 'Renew Certificate' button is visible over one of the rows.

Type	Name	Authority	Device Friendly Name	User	Profile Name	Issued Date	Expires in	Status	Actions
	CN=QA1certpayloaddemo	donotuse	gules iPhone 4S	demo		11/4/2011	209 day(s)	Active	
	CN=QA1certpayloadjennifer	donotuse	CCampbell's iPod		Wifi W/Cert	11/10/2011	214 day(s)	Active	
	CN=QA1certpayloadjennifer	donotuse	CCampbell's iPod		EAS w/Cert	11/10/2011	214 day(s)	Active	
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		fsu_CA_test	11/11/2011	215 day(s)	Revoked	Renew Certificate
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		fsu_CA_test	11/11/2011	215 day(s)	Revoked	
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		fsu_CA_test	11/11/2011	215 day(s)	Revoked	
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		adam_CA_test	11/11/2011	215 day(s)	Revoked	
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		adam_CA_test	11/11/2011	215 day(s)	Revoked	
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		adam_CA_test	11/11/2011	215 day(s)	Revoked	
	CN=QA1certpayloadmadam	donotuse	Adam's iPhone		adam_CA_test	11/11/2011	215 day(s)	Revoked	

- **Deployment integration** to send certificates to devices according to the Location Group.
- **Network integration** to enable your existing email infrastructure to work seamlessly with the SEG and AirWatch to provide maximum feature and security extensibility.
  - Due to mail provider limitations, Certificate integration is not compatible with cloud-based Email infrastructures such as Office 365 and Google Apps for Business.
- **Varying levels of certificate deployment options** to assign a certificate to a group versus more advanced identity associations (such as with the SEG proxy) assigned to an individual.
- **Advanced options** to integrate with a number of Certificate Authorities and services, such as VeriSign, Symantec, ADCS, and MSCEP.

Depending on how your corporate certificate and email infrastructures are configured, you can add various levels of functionality and security in order to customize your Email management and security to your IT needs. By using AirWatch's email management tools in conjunction with the advanced capabilities leveraged through certificates, you can achieve the highest levels of email management and access control.

 **Note:** For more detailed information on setting up certificate authorities and certificate integration in AirWatch, contact [support@air-watch.com](mailto:support@air-watch.com).

## AirWatch Mobile Email Management: The Secure Email Gateway

The AirWatch Secure Email Gateway is a comprehensive and flexible email management and security solution that provides your corporation with the necessary tools for a successful mobile Email deployment: advanced access control, administrative visibility and management, and seamless integration with the existing mail infrastructure.

- **Advanced access control** - Robust Email compliance capabilities provide an advanced level of access control that is crucial to corporate Email security. Furthermore, the SEG tightly integrates with the existing AirWatch compliance engine, allowing administrators to develop and leverage custom responses to non-compliant actions or devices.
- **Administrative visibility and management** - Administrators can also take advantage of enhanced management visibility through interactive email activity dashboards. The IT administrator has full control over all mobile Email traffic to ensure that any non-compliant Email actions are detected, isolated, and managed according to corporate policies.
- **Easy and Integrated Deployment** - In addition to providing management visibility and access control, the SEG can be deployed to satisfy your email and network security needs regardless of your email infrastructure.
- **Certificate integration for advanced protection and management** - Couple the benefits of the AirWatch SEG with digital certificates to offer certificate-based email authentication, and S/MIME email encryption and signatures. Our flexible Secure Email Gateway solution can integrate with a number of PKI types to deliver and leverage certificates in a multitude of architecture models.

With the AirWatch Secure Email Gateway, you can provide the IT administrator with the highest level of security, management, and flexibility in managing the organization's mobile Email.

## SEG Access Control

The SEG allows the organization's IT administrator to create tailored email access policies in order to both account for non-compliant email actions and make any necessary exceptions to the established policies.

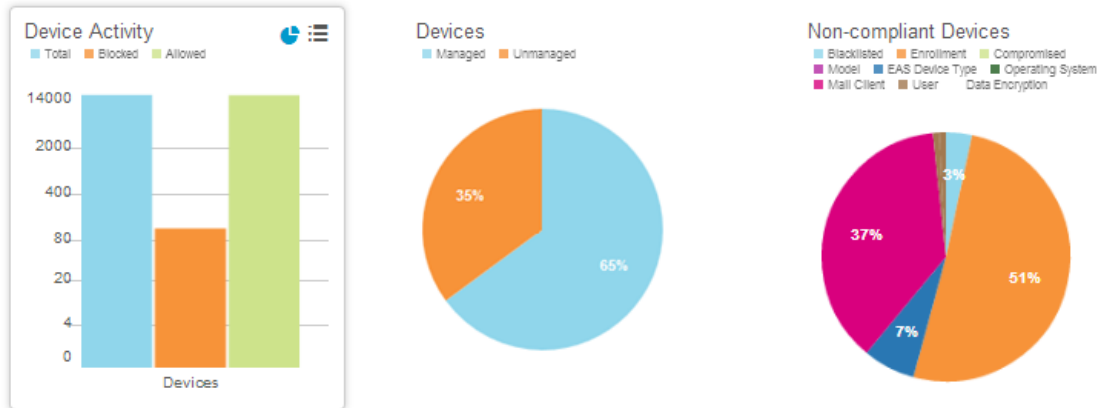
- General access configurations
  - Block unmanaged, non-compliant, or compromised devices.
  - Create Whitelist and Blacklist policies to only allow approved devices or to only block specific devices.
- Establish system requirements
  - Block outdated or problematic Operating System versions that stress the email server.
- Device-level compliance policies and exceptions. For example, consider the following scenarios:
  - An employee leaves your company and his or her personal device should no longer be permitted to connect to the corporate email server.
  - An authorized device is lost or stolen; In addition to performing a remote-wipe of the device, the device should be blocked from the corporate email server.
  - A company executive has a device that would normally be prevented from accessing the email server, and the IT administrator must ensure that the executive's device can connect to mobile email.

Email Policies			
Disable Compliance		Current Setting <input type="radio"/> Inherit <input checked="" type="radio"/> Override	
General Email Policies			
Active	Policy	Current Compliance Policies	Actions
<input checked="" type="radio"/>	Sync Settings	Sync Settings Disable	
<input checked="" type="radio"/>	Managed Device	Allow unmanaged devices	
<input type="radio"/>	Mail Client	Allow unlisted clients, Allow Discovered Clients	
<input type="radio"/>	User	Allow unlisted users, Allow Discovered Users	
<input type="radio"/>	EAS Device Type	Allow other device types	
Managed Device Policies			
Active	Policy	Current Compliance Policies	Actions
<input checked="" type="radio"/>	Inactivity	Allow Inactive Devices	
<input checked="" type="radio"/>	Device Compromised	Allow compromised devices	
<input checked="" type="radio"/>	Encryption	Allow unencrypted devices	
<input type="radio"/>	Model	Allow new models	
<input type="radio"/>	Operating System	Allow new OS	



## SEG Management Visibility

Administrators can regain insight and visibility over Mobile Email activity through the interactive SEG dashboard. The dashboard presents both real-time and historic data, which allows administrators and company executives to instantly react to real-time data and to perform long-term data analysis on corporate mobile activity.



The detailed list of real-time server requests allows administrators to quickly pinpoint actions that need to be allowed or blocked, and add them to the policy override list. AirWatch collects information every time a device makes a request to the mobile email server through the AirWatch Secure Email Gateway and compiles it on a dashboard in the AirWatch MDM console to help you assess the health of your mobile email deployment. The following is a sample of the type of data collected:

- ActiveSync command (sync, provision, etc.).
- Date and time of sync attempt.
- Mobile user's Email username.
- Amount of data traffic to and from the device.

AirWatch's Secure Email Gateway allows control of both known devices under management by AirWatch MDM console, as well as unknown, unmanaged devices. Managed device data can be correlated to the device's existing record to show how devices are interacting with the corporate email server. Unmanaged device data is also presented, as it is useful for tracking rogue devices and providing a more complete picture of the corporate mobile email deployment.

## Providing the Right Email Client

### AirWatch Email Container for Android

AirWatch's Email Container for Android, a secured email client provides the comfort of the native android user experience with additional usability features without the hassle of buying a third-party email app. With AirWatch, you can silently configure and update email profiles over-the-air. The Email container ensures that all your emails are tightly secured and provides additional features that include:

- **Security**
  - Enforce container simple or alphanumeric pin, or active directory password
  - Enforce pin/password timeout settings and max failed attempts
  - AES 256-bit encryption of email and attachments
  - Prevent copy/paste
  - Prevent contacts sync with native contacts app
  - Prevent attachments
  - Set maximum attachment size
  - Force viewing of attachments through whitelisted apps (i.e. Secure Content Locker)
  - Restrict forwarding of email to only whitelisted domains
  - Block forwarding of email to blacklisted domains
- **Support and Configuration**
  - Support for Android 4.0 devices and above
  - Over-the-air configuration of EAS, sync and general settings through profiles
  - Native Android email user experience
  - Support for certificate-based authentication
  - Integration with AirWatch's Secure Email Gateway and PowerShell solution

### TouchDown for iOS and Android

AirWatch integration with NitroDesk TouchDown enables a separate container for email on iOS and Android devices. With AirWatch, you can set sync settings, passcode requirements, and security restrictions via Profiles. You can configure and push these profiles silently over-the-air on multiple devices. Administrators can also enforce device and SD card encryption for ultimate security. Touchdown integrated with AirWatch provides you with the following benefits:

- Easy and secured end-user configuration
- Policy enforcement
- Data loss prevention
- Compliance monitoring

For **iOS**, NitroDesk TouchDown integration requires use of AirWatch MDM Agent v4.4 and an updated version of the NitroDesk TouchDown application. TouchDown Integration through AirWatch SDK offers you the following features:

- Remotely configure and manage email using NitroDesk TouchDown mail client/container.
- TouchDown app automatically detects when a device is enrolled in AirWatch and then automatically configures to receive updated settings using the AirWatch Agent.
- Frequent communication with the AirWatch server to process any policy updates or configuration changes.
- Additional passcode security to access the TouchDown mail client.
- Enforce email security policies on TouchDown mail client.
- Keep attachments within the TouchDown container or block attachments entirely.
- Automatically remove access and wipe email data when a device is non-compliant (using the compliance engine) or enterprise wiped.

## Choosing and Configuring the Right Email Solution

One of the major benefits of the Secure Email Gateway is that it is compatible with many email infrastructures and can be tight integrated into the existing email and network system. The SEG has several different deployment models, and the design of each model is tailored to the corresponding compatible email infrastructures.

Equally important to the SEG's compatibility is the customization capability. Each SEG deployment is configured in a way that meets the security needs and preferences of the organization. For example, the proxy model can be configured in front of or behind the existing firewall, or in the DMZ. If your organization is not sure of the best configuration, AirWatch will make an expert recommendation based on an analysis of your existing infrastructure.

Mail Infrastructure	SEG Configuration Model
Exchange 2007 and lower Lotus Domino w/ Lotus Traveler Novell GroupWise 8.0 (with EAS) Beehive Any other EAS infrastructure	<a href="#">Proxy model</a>
Exchange 2010 Office 365 / BPOS Any other PowerShell infrastructure	<a href="#">PowerShell model</a>
Google Apps for Business	<a href="#">Google model</a>

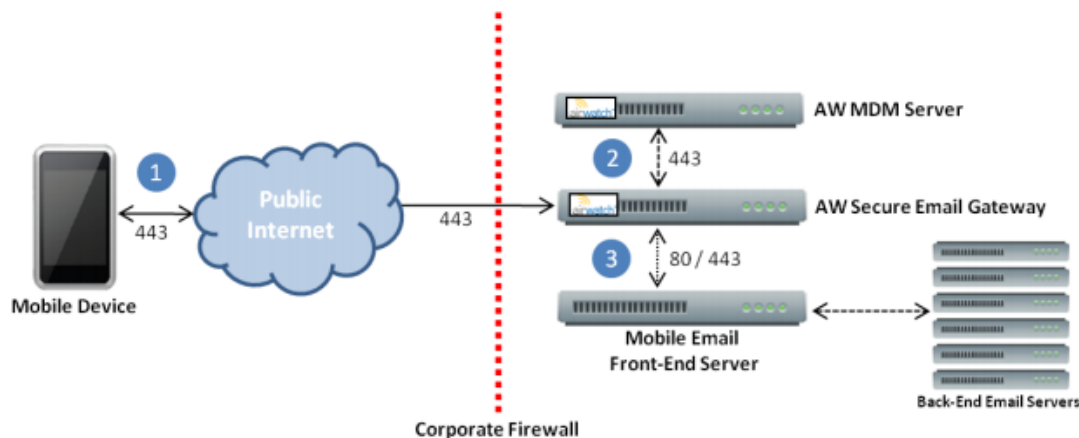
## Proxy Deployment

For those organizations using an email infrastructure that supports the proxy model, a separate email server containing the Secure Email Gateway is installed locally. The SEG server sits in front of your existing email server and makes allow/deny decisions for every mobile device that connects to it based on settings you've defined in the AirWatch MDM console. The SEG only relays traffic from approved devices, and further protects your corporate email server by never allowing any devices to directly communicate with it. Instead, devices interact with the SEG server and all requests to the mail server are filtered through the SEG. The specific placement of the SEG server varies depending on your existing network and security requirements. However, the SEG server is typically installed locally.

### EAS SEG Configuration for AirWatch On-Premise Deployments

In this case, the Airwatch SEG and MDM server are both locally hosted.

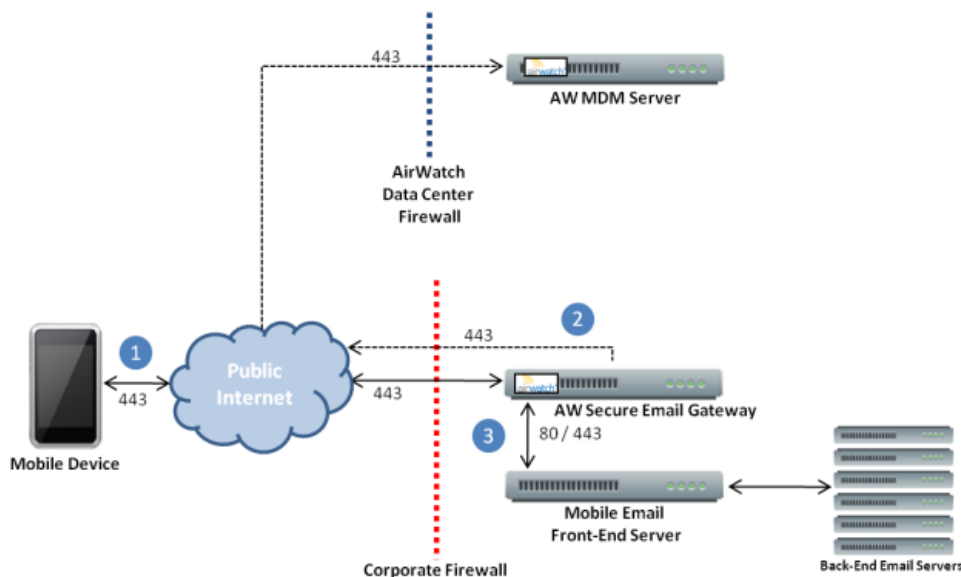
- This solution is commonly used for on-premise deployments with local email infrastructure.
  - The AirWatch SEG can also be deployed in front of your firewall or in the DMZ.



### EAS SEG Configuration for AirWatch SaaS Deployments

In this deployment, the AirWatch SEG is hosted locally and AirWatch MDM is SaaS-hosted.

- This solution is commonly used for SaaS deployments with local email infrastructure.



## AirWatch Advanced Email Security with PowerShell Infrastructures

In this model, the AirWatch SEG adopts a PowerShell administrator role and issues cmdlets to the EAS infrastructure to permit or deny email access based on the settings defined in the AirWatch web console. PowerShell deployment does not require any physical server installation and involves three steps:

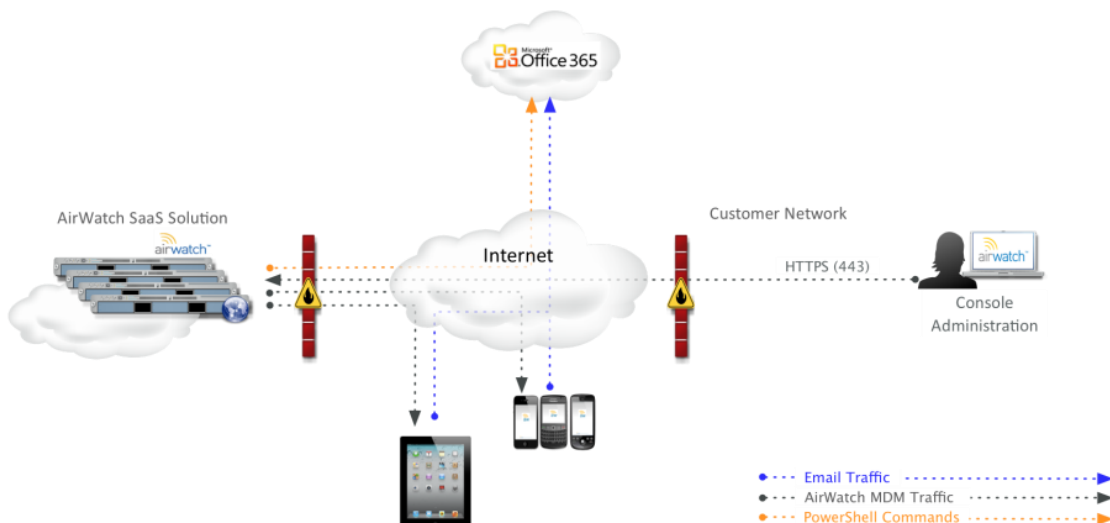
- AirWatch sends a command to the EAS server to authenticate AirWatch as an administrator.
- EAS establishes a trust relationship with AirWatch.
- AirWatch sends cmdlets to PowerShell in accordance with the established email policies, and PowerShell executes the actions.

### PowerShell and System Requirements

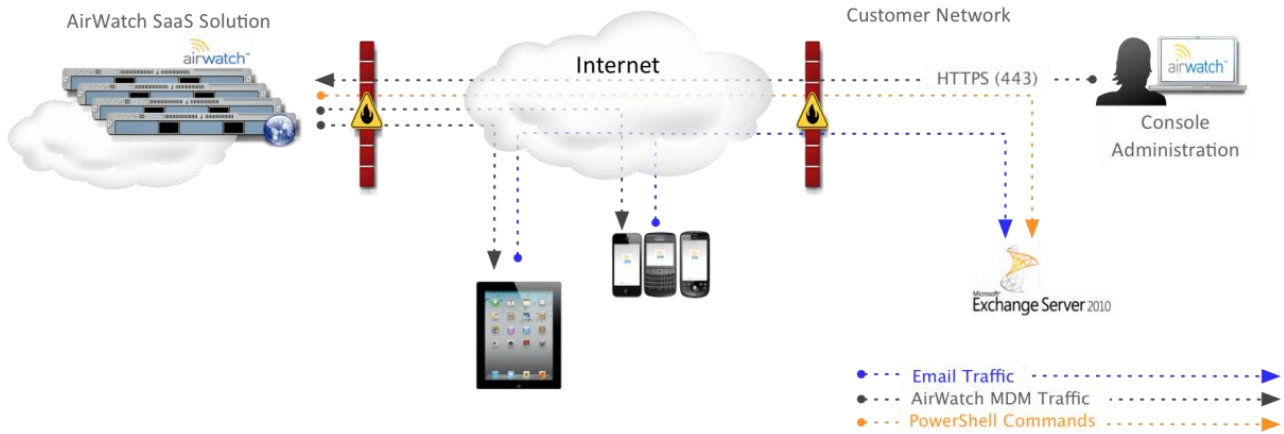
- The following PowerShell roles must be enabled:
  - Organization Management
  - Server Management
  - Recipient Management
- Access to the server-side session is required in order to execute Exchange commands.
- Port 443 is the communication channel.

This model does not require the Secure Email Gateway to be a proxy to mail traffic. Therefore, it can be deployed from AirWatch SaaS or On-Premise solutions provided that the Secure Email Gateway server can communicate with the respective email infrastructure.

### Cloud Deployments

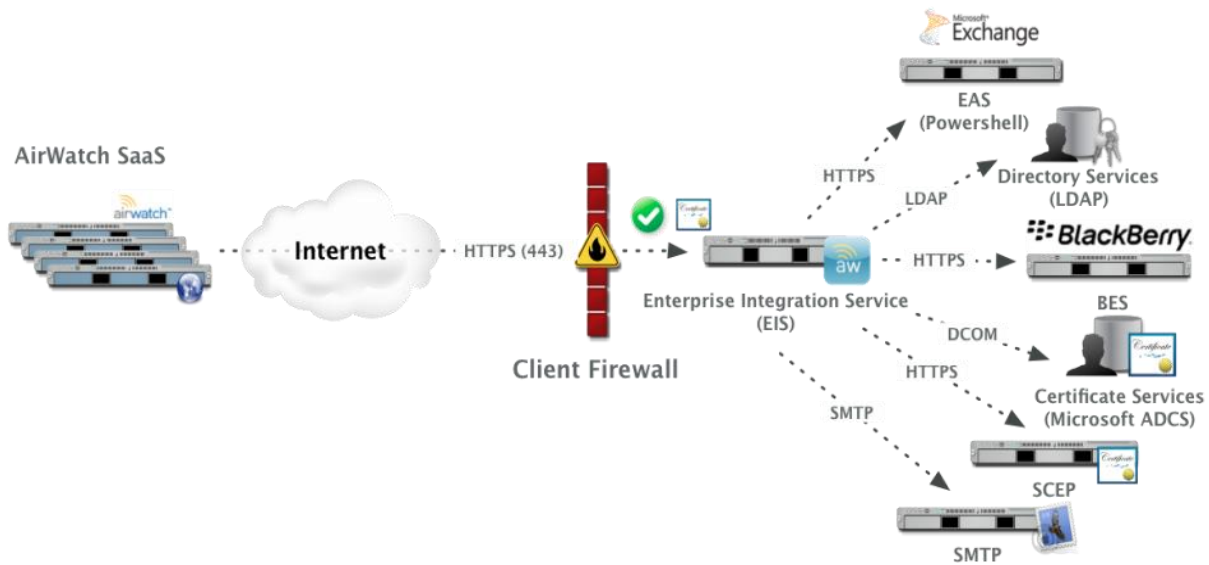


## On-Premise Deployments



## Securing PowerShell Email with EIS

The PowerShell deployment model also leverages the AirWatch Enterprise Integration Service in order to deliver PowerShell commands to your mail server. By utilizing this module, administrators are able to securely and easily communicate with email infrastructure whether you are utilizing AirWatch SaaS or On-Premise solutions.

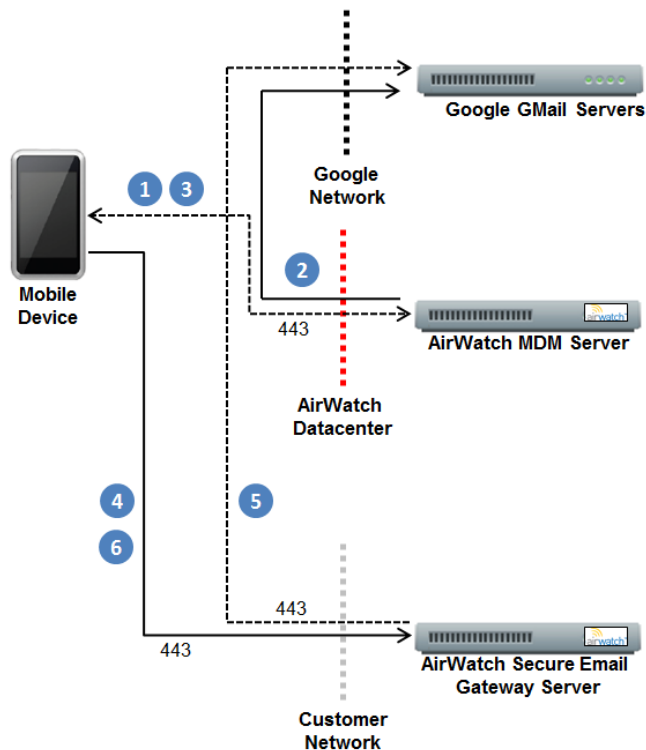


Additionally, EIS sets the stage for administrators to easily integrate with other back-end systems such as internal certificate authorities, directory services, SMTP, BES, and other servers.

## AirWatch Advanced Email Management with Google Apps for Business

Organizations using the Google apps for business email infrastructure may be familiar with the challenge of securing email end points for Gmail and preventing mail from circumventing the secure end point. IT administrators are primarily concerned with the potential for security breaches due to the inability to enforce IP or Layer 1 network control to force email sent through Google apps through a specific secure route. AirWatch resolves this issue and fully secures corporate email sent through Gmail by implementing password obfuscation security control.

All Gmail platforms use a specific configuration model unique to the Gmail infrastructure. The SEG integrates with and protects Gmail through password authentication. AirWatch conceals randomly generated Google account passwords and re-routes email authentication through the SEG. Only AirWatch-authenticated devices are allowed to access Gmail. By never giving out the Google account passwords, the IT administrator can customize mobile access to Gmail according to the settings specified in the AirWatch web console.



- When a device enrolls in AirWatch MDM, AirWatch configures the Google account password for the user associated with the enrolling device to a random string known only to AirWatch (Steps 1 & 2 in diagram).
- AirWatch then deploys an email profile to the device containing the separate password (or authentication certificate) known only to AirWatch which allows the device to authenticate with the SEG (Steps 3 & 4 in diagram).
- The SEG then re-routes mobile email traffic to Gmail and relays the Gmail response back to the device. The true Google account password is never shared with the user or device, and users cannot manually deploy the Gmail settings to another device since only AirWatch knows the true password (Steps 5 & 6 in diagram).



## Google and System Requirements

- Web-based access to Google services is authenticated via a Single-Sign-On server.
- Active Directory passwords are not synced to the respective Google accounts.
- Password management is configured in one of two ways:
  - AirWatch manages all Google account passwords. Passwords are randomly generated long strings and unknown to the user.
  - AirWatch integrates with a corporate IDM system of choice which manages Google account passwords.

## Additional SEG Security Features

### High Availability

The Secure Email Gateway is fault tolerant and secure; in other words, the SEG will never interfere with your organization's ability to receive mobile email.

- Load balancing for High Availability (HA)
  - AirWatch data centers use multiple, high-power load balancers configured in HA mode.
  - If for any reason the load balancer fails, email is re-routed directly to the server and there is no impact on email availability for the end-user.

### Deployment Options for Maximum Security

- Flexible integration options to ensure optimal security
  - The SEG can be deployed in front of your Firewall or in the DMZ.

### Authentication Extensibility

The SEG supports many different authentication types, including:

- Basic username and password authentication
- Certificates
- Token-based authentication

The sole intent of this document is to provide AirWatch customers with initial guidance to technical issues. The suggestions given herein are provided as a courtesy and are not intended to replace specific personalized advice provided by the reader's network administrators, computer security personnel, or other technical experts and consultants. References in this document whitepaper to any specific service provider, manufacturer, company, product, service, or software do not constitute an endorsement or recommendation by AirWatch. Under no circumstances shall AirWatch be liable to you or any other person for any damages, including without limitation, any direct, indirect, incidental, special or consequential damages, expenses, costs, profits, lost savings or earnings, lost or corrupted data, or other liability arising out of or related in any way to information, guidance, or suggestions provided in this document.