Mobile Email Management

VMware Workspace ONE UEM 1902

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction to Mobile Email Management

1

Use Workspace ONE UEM to manage your mobile email deployment.

The ability to view corporate data on your device provides convenience and improves productivity, but at the same time also presents security and deployment challenges. To overcome such challenges, VMware AirWatch® Mobile Email Management® (MEM) solution delivers comprehensive security for your corporate email infrastructure.

Challenges

Mobile email provides benefits and at the same time presents bigger challenges, such as the following:

- Provisioning email across different device types, operating systems, and email clients.
- Securing email access over unsecured networks.
- Protecting sensitive information from third-party apps.
- Restricting email access from unauthorized, lost, or stolen devices.
- Preventing email attachments from being lost and disseminated through the third-party reader apps when they are viewed.

Advantages of Mobile Email Management (MEM)

VMware AirWatch® MEM provides all the key factors that are required for a successful and secure mobile email deployment. The following are some of the advantages of using MEM:

- Enforce SSL security
- Configure email over-the-air
- Discover existing unmanaged devices
- Protect email from data loss
- Block unmanaged devices from accessing email
- Restrict email access to only company-approved devices
- Use certificate integration and revocation

MEM Requirements

Verify the browser requirements as given in this section before you proceed with the VMware AirWatch$^{®}$ Mobile Email Management$^{®}$ (MEM) solution.

Disclaimer

Integration with the third-party product is not guaranteed and dependent upon the proper functioning of those third-party solutions.

Supported Browsers

The Workspace ONE UEM console supports the latest stable builds of the following web browsers:

- Chrome

- Firefox

- Safari

- Internet Explorer 11

- Microsoft Edge

Note   If you are using using IE to access the UEM console, navigate to **Control Panel > Settings > Internet Options > Security** and ensure you have a security level or custom security level that includes the **Font Download** option being set to **Enabled**.

If you are using a browser older than those listed above, upgrade your browser to guarantee the performance of the Workspace ONE UEM console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The UEM console may experience minor issues if you choose to run it in a non-certified browser.

Email Infrastructure Management

<div style="text-align:right">2</div>

Workspace ONE UEM offers two types of deployment models to protect and manage your email infrastructure, the proxy model and the SEG Proxy deployment model.

You can use one of these email deployment models along with the email policies that you define in the UEM console, to effectively manage your mobile devices.

- In the proxy model, a separate server called the SEG proxy server is placed between the Workspace ONE server and the corporate email server. This proxy server filters all the requests from the devices to the email server and relays the traffic only from the approved devices. This way the corporate email server is protected as it does not directly communicate with the mobile devices.

- The SEG Proxy deployment model can be configured on two platforms: Classic or V2. Though the functionality of both the platforms are the same, the V2 platform assures improved performance over the Classic platform. This is a direct model approach where there is no proxy server involved and Workspace ONE UEM communicates directly with the email servers. The absence of proxy server simplifies the installation and configuration steps in this model.

Deployment Model	Configuration Mode	Mail Infrastructure
Proxy Model	Secure Email Gateway - Classic Platform	Microsoft Exchange 2003/2007/2010/2013/2016 Exchange Office 365 IBM Domino w/ Lotus Notes Novell GroupWise (with EAS) Gmail
Secure Email Gateway - V2 Platform	Microsoft Exchange 2010/2013/2016 Exchange Office 365	Microsoft Exchange 2010/2013/2016 Exchange Office 365
Direct Model	PowerShell Model	Microsoft Exchange 2010/2013/2016 Microsoft Office 365
Gmail Model	Gmail	

Note   Workspace ONE UEMWorkspace ONE UEM only supports the versions of third-party email servers currently supported by the email server provider. When the provider deprecates a server version, Workspace ONE UEM will no longer support integration with the deprecated version.

This chapter includes the following topics:

Secure Email Gateway Proxy Model

The Secure Email Gateway (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 UEM console, the SEG Proxy server allows or block decisions for every mobile device it manages.

The SEG Proxy server filters all communication requests to the corporate email server and relays traffic only from approved devices. This relay protects the corporate email server by not allowing any devices to communicate with it.

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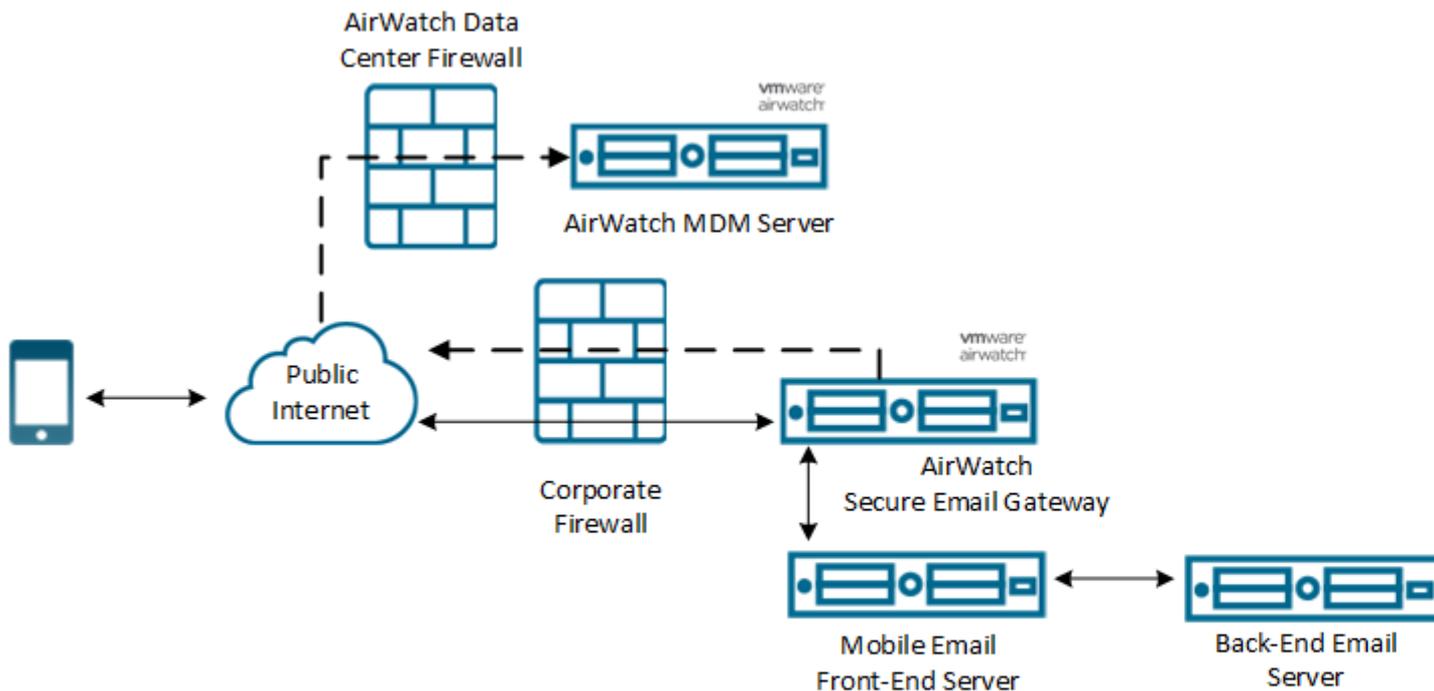
Cloud Architecture

Direct Deployment - PowerShell Model

In the PowerShell model, Workspace ONE UEM 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 UEM console. PowerShell deployments do not require a separate email proxy server and the installation process is simpler.

PowerShell deployments are for organizations using Microsoft Exchange 2010,2013,2016, or Office 365.

In the setup where Office 365 the cloud email server is used, the Workspace ONE server sets up the PowerShell session directly with the email server.
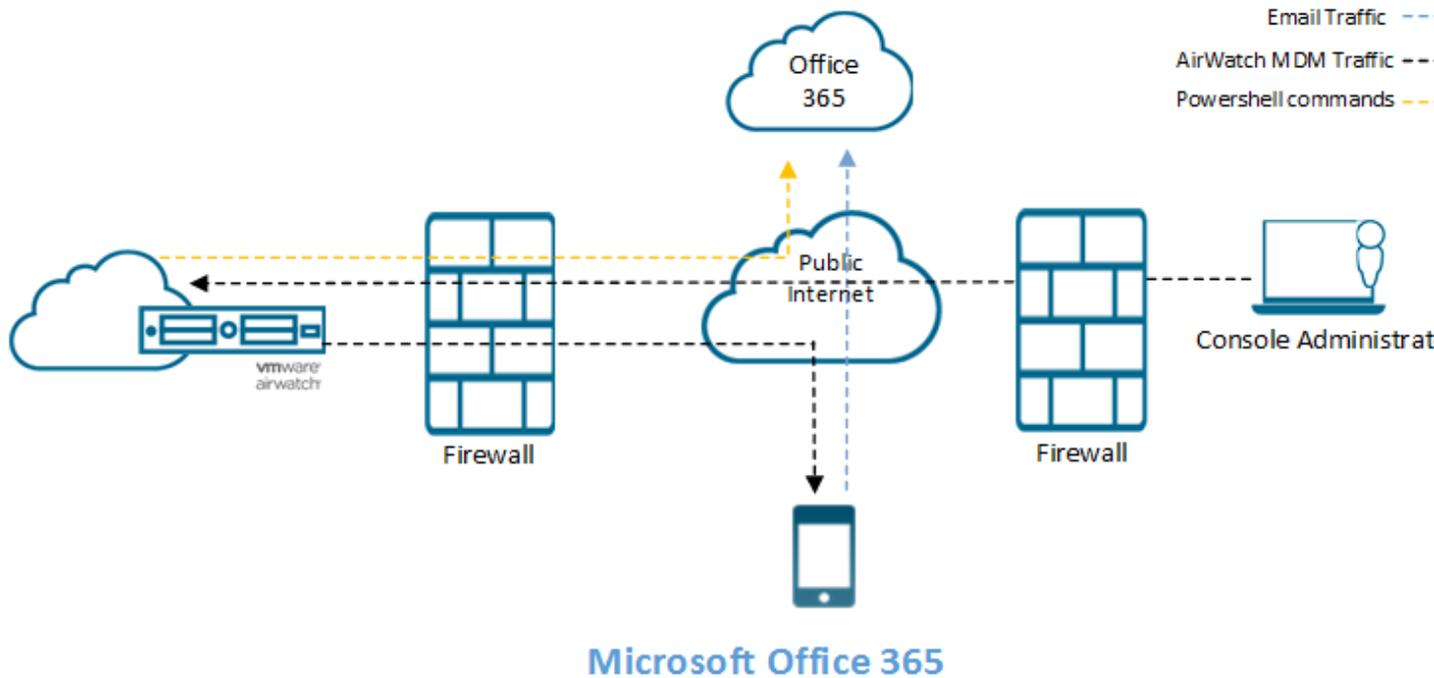
There are two ways in which the PowerShell commands are issued depending on where the Workspace ONE UEM server and Exchange server are located :

- Workspace ONE server is on the cloud and the Exchange server is on premise - Workspace ONE UEM server issues the PowerShell commands. The VMware Enterprise Systems Connector sets up the PowerShell session with the email server.

- Workspace ONE UEM server and the email server are on premise - Workspace ONE UEM server sets up the PowerShell session directly with the email server. Here, there is no VMware Enterprise Systems Connector server required unless the Workspace ONE UEM server cannot communicate with the email server directly.
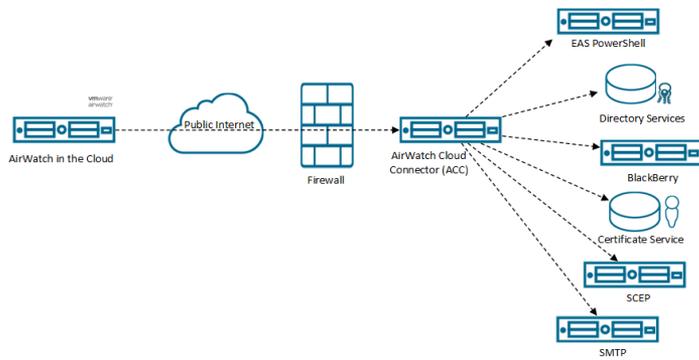
Microsoft Exchange 2010 with AirWatch Cloud
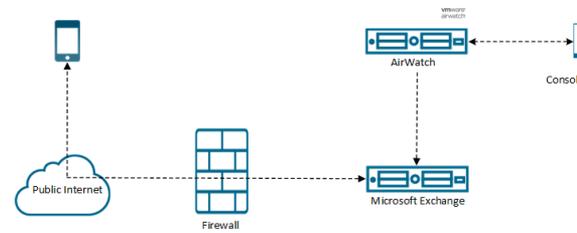
Microsoft Exchange 2010 with AirWatch On-Prem

For assistance in choosing between the Secure Email Gateway and PowerShell deployment models, see the Workspace ONE UEM Recommendations section .

Direct Gmail Model

Integrate Workspace ONE server with Google.

Organizations using the Gmail infrastructure might be familiar with the challenge of securing email endpoints for Gmail and preventing mail from circumventing the secure endpoint. Workspace ONE UEM addresses these challenges by providing a flexible and safe method to integrate your email infrastructure.

In the direct Gmail deployment model, the Workspace ONE server communicates directly with Google.

Depending on the security needs, you can choose one of the following password configuration models:

- Store the Google password in the Workspace ONE database - When the device is non-compliant, Workspace ONE UEM resets the password on Google preventing the user from logging into other device. When the device is back to compliant status, Workspace ONE UEM resets the old password on the Google server and the user can log in using the old password.

- Do not store the Google password from the Workspace ONE database - When the device is non-compliant, the email profile is removed from the user's device preventing the user from receiving emails. When the device is back to compliant status, Workspace ONE UEM triggers a new password, sends it to Google and the device through the email profile.
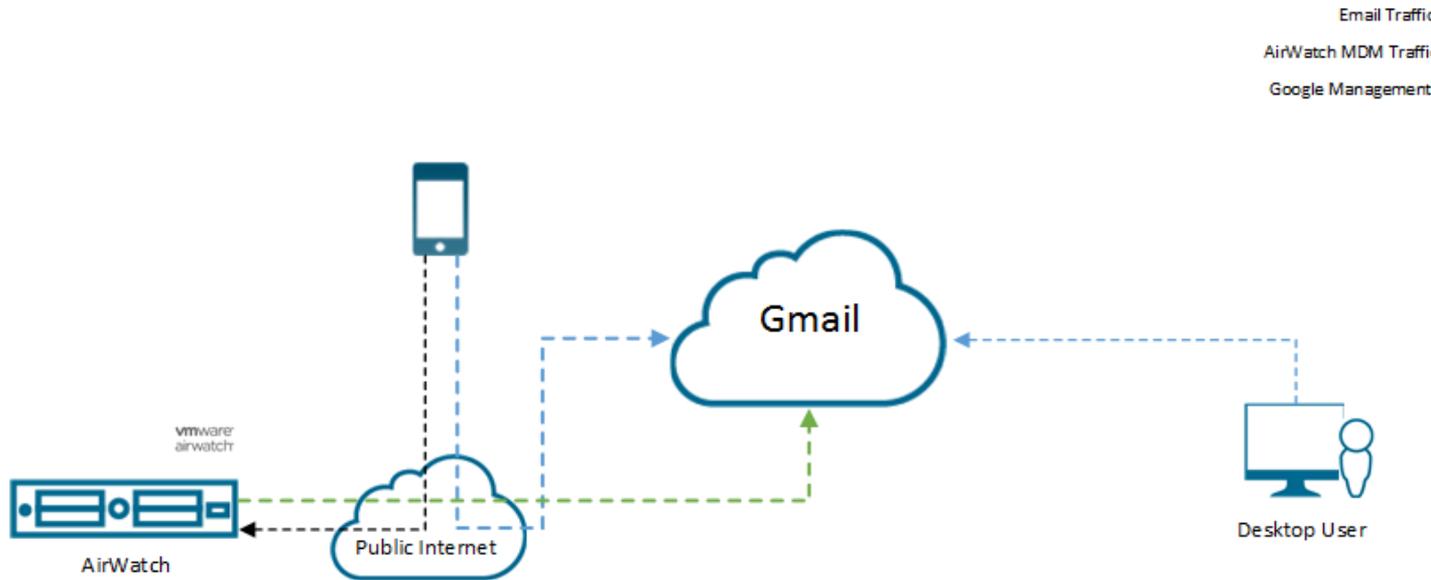
MEM Deployment Model Matrix

Use the feature matrix below to compare the features available in the different MEM deployment models.

Office 365 requires more configuration for the SEG Proxy model. Workspace ONE UEM recommends the Direct model of integration for Cloud-based email servers. See the Workspace ONE UEM Recommendations section for details.

✓	Supported	□	Not supported by Workspace ONE UEM
X	Feature not available	N/A	Not Applicable

Table 2-1. Deployment Matrix

	SEG Proxy Model			Direct Model		
	Exchange 2010/2013/2016	Lotus Traveler	Novell GroupWise	Office 365(PowerShell)	Exchange 2010/2013/2016 (PowerShell)	Gmail
Email Security Tools						
Enforced Security Settings						
Use digital signatures through S/MIME capability	✓	□	□	✓	✓	N/A
Protect sensitive data through forced encryption	✓	✓	✓	✓	✓	✓

Table 2-1. Deployment Matrix (Continued)

	SEG Proxy Model			Direct Model		
	Exchange 2010/2013/2016	Lotus Traveler	Novell GroupWise	Office 365(PowerShell)	Exchange 2010/2013/2016 (PowerShell)	Gmail
Enforce SSL Security	✓	✓	✓	✓	✓	✓
Email Attachment & Hyperlinks Security						
Enforce attachments and hyperlinks to open in VMware Content Locker or VMware Browser only	✓	✓	✓	x	x	x
Automatic Email Configuration						
Configure the email over-the-air on device	✓	✓	✓	✓	✓	✓
Email Access Control						
Block unmanaged devices from accessing email	✓	✓	✓	✓	✓	✓
Discover existing unmanaged devices	✓	✓	✓	✓	✓	N/A
Email access with customizable compliance policies	✓	✓	✓	✓	✓	✓
Require device encryption for email access	✓	✓	✓	✓	✓	✓
Prevent compromised devices from email access	✓	✓	✓	✓	✓	✓
Allow / block email - Mail client	✓	✓	✓	✓	✓	x
Email Access Control						
Allow / block email - User	✓	✓	✓	✓	✓	x
Allow / block email - Device model	✓	✓	✓	✓	✓	✓
Allow / block email - Device OS	✓	✓	✓	✓	✓	✓
Allow / block email - EAS Device type	✓	✓	✓	✓	✓	x
Management Visibility						
Email traffic statistics	✓	✓	✓	x	x	x

Table 2-1. Deployment Matrix (Continued)

	SEG Proxy Model			Direct Model		
	Exchange 2010/2013/2016	Lotus Traveler	Novell GroupWise	Office 365(PowerShell)	Exchange 2010/2013/2016 (PowerShell)	Gmail
Email clients statistics	✓	✓	✓	x	x	x
Certificate Management						
CA Integration / revocation	✓	□	□	✓	✓	N/A
Architecture						
Inline gateway (Proxy)	✓	✓	✓	N/A	N/A	✓
Exchange PowerShell	N/A	N/A	N/A	✓	✓	N/A
Password management for Gmail	N/A	N/A	N/A	N/A	N/A	✓
Directory API Integration for Gmail	N/A	N/A	N/A	N/A	N/A	✓
Supported						
VMware Boxer for iOS and Android [^]	✓	□	□	✓	✓	□
AirWatch Inbox for iOS	✓	✓	□	✓	✓	□
AirWatch Inbox for Android	✓	✓	□	✓	✓	✓
AirWatch Inbox for Windows Desktop	✓	□	□	✓	✓	N/A
iOS Native Email Client	✓	✓	✓	✓	✓	✓
Android Native Email Client**	✓	✓	✓	✓	✓	✓
Windows Mobile Native Email Client	✓	✓	✓	✓	✓	x
Windows Phone	✓	✓	✓	✓	✓	✓
Blackberry 10***	✓	✓	✓	✓	✓	N/A
iOS Touchdown*	✓	✓	✓	✓	✓	✓
Android Touchdown	✓	✓	✓	✓	✓	✓
Android Lotus Notes Client*	N/A	✓	N/A	N/A	N/A	N/A

*Email Attachments & Hyperlinks security is not supported on the Android Lotus Notes client and iOS Touchdown client

**Android native email client supports SAFE, HTC Pro2, LG Optimus Pro, and Intuition devices only

***EAS profile is not supported

+ Exchange 2003 is not supported

^ Exchange 2003, Require ActiveSync Profile, and Multi MEM are not supported for VMware Boxer.

Workspace ONE UEM Recommendations

The features supported by Workspace ONE UEM and the suitable deployment sizes are listed in this section. Use the decision matrix to choose the deployment that best suits your need.

Attachment Encryption

With enforced attachment encryption on your mobile devices, Workspace ONE UEM can help keep your email attachments secure without hindering the end users' experience.

	Native	AirWatch Inbox	Touchdown	Traveler	VMware Boxer
iOS	✓	✓			✓
Android	✓	✓	✓		✓
Windows Phone*	✓				

*If your deployment includes Windows Phone 8/8.1/RT devices, use attachment encryption.

SEG supports attachment encryption and hyperlink transformation on Boxer, only if these features are enabled for the Boxer app configuration on the UEM console.

SEG supports attachment encryption with Exchange 2010/2013/2016 and Office 365.

Email Management

The list gives you the greatest level of security with the easiest deployment and management.

	G mail	PowerShell	Secure Email Gateway (SEG)
Cloud Mail Infrastructure			
Office 365		✓	✓
Gmail	✓		✓
On-premises Email Infrastructure			
Exchange 2010		✓	✓
Exchange 2013		✓	✓
Exchange 2016		✓	✓
Lotus Notes			✓
Novel GroupWise			✓

^Use the Secure Email GatewaySecure Email Gateway (SEG) for all on-premises email infrastructures with deployments of more than 100,000 devices. For deployments of less than 100,000 devices, using PowerShell is another option for your email management. Refer to the Secure Email Gateway vs. PowerShell Decision Matrix.

**The threshold for PowerShell implementations is based on the most recent set of completed performance tests, and can change on a release by release basis. Deployments up to 50,000 devices can expect reasonably quick sync and run compliance time frames (less than three hours). As the deployment size expands closer to 100,000 devices, then administrators can expect the sync and run compliance processes to continue to increase in the 3–7 hour time frame.

Secure Email Gateway vs PowerShell Decision Matrix

The matrix informs you about the deployment features of SEG and PowerShell to help you choose which deployment suits your need.

	Pros	Cons
SEG	▪ Real-Time Compliance ▪ Attachment encryption ▪ Hyperlink transformation	▪ Additional server (s) required ▪ ADFS must be configured to prevent end users from connecting directly to Office 365 (around SEG)
PowerShell	▪ No additional on-premises server required for email management ▪ Mail traffic is not routed to an on-premises server before being routed to Office 365, so ADFS is not required	▪ No real-time compliance sync ▪ Not for large deployments (more than 100000) ▪ AirWatch Inbox must be used to containerize attachments and hyperlinks in VMware Content Locker and VMware Browser respectively

Microsoft suggests using Active Directory Federated Services (ADFS) for preventing direct access to Office 365 email accounts.

Connecting IBM Notes Traveler Server through AirWatch Inbox

If you are using a Workspace ONE UEM Exchange ActiveSync profile to connect to an IBM Notes Traveler server through the Android AirWatch Inbox, you might receive an 'HTTP 449' response. This response is seen when an Android device attempts to connect to the Traveler server. This 'HTTP 449' error occurs if the ActiveSync policy headers sent from the client (and enforced through Workspace ONE UEM console) do not match the policy headers supported by the Traveler server.

To resolve such issues, follow these steps:

1 Add the following flag to the **notes.ini** file on the Traveler server.

```
NTS_AS_PROVISION_EXEMPT_USER_AGENT_REGEX =(AirWatch*) | (Apple*; AWInbox*)
```

1 Next, restart the Traveler server.

Adding this flag disables Traveler from enforcing any policies to the AirWatch Inbox. You must use Workspace ONE UEM for applying the required policies to the app.

Devices that use policies provisioned directly by Traveler (that is, not configured through Workspace ONE UEM), are not affected.

Note If you are using IBM Notes Traveler with SEG 7.3+, then the IBM Notes Traveler requires the Microsoft-Server-ActiveSync website support.

Email Migration to Workspace ONE UEM

3

You can migrate your email to a Mobile Email Management (MEM) model using Workspace ONE UEM

By migrating to one of the following MEM models, you can enforce email access control policies ensuring email access is provided only to the approved users and devices:

- Secure Email Gateway (SEG)

- PowerShell

- Gmail

This chapter includes the following topics:

- Migrate to Secure Email Gateway (SEG)

- Migrate to PowerShell

- Integrate Gmail With Workspace ONE UEM

- Migrate Devices

Migrate to Secure Email Gateway (SEG)

Email migration to Secure Email Gateway (SEG) enables users to access emails only through the SEG proxy.

Using SEG enforces email access control policies, giving access only to approved users and devices. Attachment encryption policies ensure data security.

Procedure

1   Configure SEG at your required organization group under Global in the Workspace ONE UEM console. .

2   Download and install SEG..

3   Test the SEG functionality using the email compliance policy.

    a   Disable all compliance policies temporarily.

    b   Ask all users to enroll their devices into Workspace ONE UEM.

    c   Provision a new email profile (with the SEG server URL as the hostname) to all the enrolled devices.

d   Periodically, remind users with unmanaged devices to enroll into Workspace ONE UEM.

e   To block EAS access to the mail server on a specific date, modify firewall (or Threat Management Gateway) rules. It ensures that mobile devices are blocked from accessing the mail server directly.

Existing Webmail, Outlook Web Access (OWA), and other email clients can continue to access the mail server.

Migrate to PowerShell

You can secure your devices and sync the devices with Exchange or Office 365 for emails by migrating to PowerShell.

PowerShell discovers managed and unmanaged devices and with the help of email access control policies gives access to only approved users and devices.

Prerequisites

Procedure

1   Configure PowerShell integration at your required organization group under Global in the Workspace ONE UEM 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

   a   Syncing with the email server to discover devices.

   b   Access control in real time.

4   Disable all compliance policies temporarily.

5   Provision a new email profile for all devices that have enrolled into Workspace ONE UEM, with the email server hostname.

6   Sync with the email server to discover all devices (managed and unmanaged) that are syncing for email.

7   Periodically remind users with unmanaged devices to enroll into Workspace ONE UEM.

8   Activate and enforce compliance rules to block email access from all non-compliant devices on a specific date including the unmanaged devices.

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 previous policy change) and **Run Compliance** against these devices.

   The Email Dashboard displays the list of unmanaged devices as blocked and managed devices that are allowed for email.

What to do next

Workaround for Boxer Flexible Deployment:

The Flexible Deployment feature of Boxer enables you to create different assignments for smart groups in your Organization Group.

If PowerShell is being used for Email Management, then when migrating between Exchange environments or to Office 365, email access might be blocked for Boxer. To avoid blocking email access, create a Device Access Rule in Exchange to allow Workspace ONE UEM managed Workspace ONE Boxer configurations.

You can follow the steps below to configure a device access rule for Office 365 to allow email access to devices installed with Boxer:

1 Log in to the Exchange Control Panel.

2 Select **Mobile**.

3 To add a rule, select the '+' icon under **Device Access Rules**.

4 From the Device family, select **browse**, and then select **BoxerManagediPhone**, **BoxerManaged iPad**, or **BoxerManagedAndroid**. Select **OK**. Repeat this step for other Boxer Managed devices.

5 From **Only this model**, select **All models**.

6 Select **Allow access** for the rule.

To prevent the compliance restriction during MEM migration, follow the preceding instructions on other Exchange versions.

Integrate Gmail With Workspace ONE UEM

By migrating to Gmail, you can sync your devices with the Gmail server. You can integrate your Gmail with or without aSecure Email Gateway (SEG) or directly with the Directory APIs.

Procedure

1 Enable the Single Sign On (SSO) option on Gmail or create the Service Account certificate.

2 Configure the Gmail integration from the Workspace ONE UEM console using the MEMMEM configuration wizard.

3 Provision EAS profiles to users with the new randomized password. Devices that do not receive this profile are automatically blocked from accessing Gmail.

Migrate Devices

You can migrate devices across organization groups and MEM deployments using Workspace ONE UEM.

Procedure

1 In the Workspace ONE UEM console, navigate to **Email Dashboard**.

2   Filter the managed devices that are under your present MEM deployment.

3   In the **List View** page, select all the devices and select **Administration > Migrate Devices** from the drop-down menu.

4   On the **Migrate Devices Confirmation** page, enter the given key code to confirm the migration and select the configuration to which you want to deploy the devices.

5   Click **Continue**.

After completing the above steps, Workspace ONE UEM automatically removes the earlier Exchange ActiveSync (EAS) profile and pushes the new EAS profile with the target deployment group. The device then connects to its new deployment group. The updated *memconfigID* for the device is displayed on the Email Dashboard.

Configure Mobile Email Management Deployment

4

Integrate your email infrastructure in a few simple steps using the Mobile Email Management (MEM) configuration wizard.

MEM can only be configured at a parent organization group and cannot be overridden at a child organization group. One MEM configuration can be associated with a single or multiple Exchange ActiveSync (EAS) profiles.

To configure the MEM deployment:

1   Navigate to **Email** > **Settings**, and then select **Configure**.

2   Select the deployment model and then select the email type. Select **Next**.

3   ▪   If Proxy is the deployment model, select the Gateway Platform:

   ▪   For Classic platform, the email types that can be selected are :

      ▪   Exchange

      ▪   Google Apps using Password Provisioning

      ▪   Novell Groupwise

      ▪   IBM Notes.

   ▪   For V2 platform, the email type available is Exchange.

   ▪   If Direct is the deployment model, then the email types that can be selected are:

      ▪   Exchange

      ▪   Google App with Direct API

      ▪   Google App using Password Provisioning - Select With Password Retention or Without Password Retention as the Gmail Deployment Type.

For more information on the deployment methods, see the Email Deployment Types section.

1   Enter the details for the chosen deployment type:

2   ▪   For SEG deployments:

   ▪   Enter a friendly name for this deployment.

   ▪   Enter the SEG proxy server details.

3 ▪ For PowerShell deployments:

  ▪ Enter a friendly name for this deployment.

  ▪ Enter the details of the PowerShell server, authentication, and sync settings.

4 ▪ For Gmail :

  ▪ Enter a friendly name for this deployment.

  ▪ Enter the details of the Gmail settings, authentication, Gmail Directory APIs Integration, and SEG proxy settings.

5 Associate a template EAS profile with the MEM deployment and select **Next**.

6 ▪ Create a template EAS profile for this deployment. New template profiles are not published to devices automatically. You can publish profiles to your devices from the Profiles page.

  ▪ 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.

7 The **MEM Config Summary** page displays the configuration details. **Save** the settings.

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

9 ▪
  Select the **Advanced** icon corresponding to your deployment.

  ▪ Configure the available settings for the user mailboxes as per requirement in the **Mobile Email Management Advanced Configuration** page.

  ▪ Select **Save**.

10 To configure multiple MEM deployments, select **Add** (available on the **Mobile Email Management Configuration** main page) and perform steps 2–7. In a SEG deployment, you may assign a particular configuration as the default using the option **Set as default** available under .

Mobile Email Management Configuration

Note   a. You should create mutually exclusive user groups when connecting multiple PowerShell environments to the same Exchange server.b. Use different domains in the configuration when connecting multiple Gmail environments.d. Consider connecting SEG and PowerShell integration to the same email environment only during migration of MEM deployments with appropriate settings. Workspace ONE Support can help you with this implementation.

Device Assignment to Mobile Email Management MEM

<div style="text-align: right">5</div>

Device enrollments, assignment of email profiles to devices, and change in the device compliance status impacts. MEM configurations are assigned to devices based on the EAS profiles present on the devices. The Managed and Require ActiveSync Profile compliance policies ensures that unmanaged and manual configurations remain unpermitted.

Devices with Exchange Active Sync (EAS) profile

When a device with an EAS profile associates to a particular MEM configuration, Workspace ONE UEM sends policy updates to that MEM configuration. This feature facilitates migrations and multiple MEM configurations where one or more email environments are managed.

Regardless of the email client, all Google MEM models require an EAS profile. For new installs, associating an EAS profile to a MEM configuration is mandatory. For upgrades, an admin has to associate an EAS profile to the MEM configuration upon completion of the upgrade process.

SEG Proxy Integrated

Workspace ONE UEM sends a broadcast message to all the MEM configurations of the organization group to which the device has enrolled. This message states the compliance status of the device. When compliance changes, an updated message is sent. When the device connects to a particular SEG server, the SEG recognizes the device from the broadcast message sent earlier. The SEG Proxy then reports the device as discovered to VMware AirWatch. Workspace ONE UEM then associates the device with the MEM Configuration for SEG and displays it on the Email Dashboard.

If multiple SEG servers are load balanced, single policy broadcast messages apply to only one SEG. This includes the messages sent from the Workspace ONE UEM console to SEG upon enrollment, compliance violation, or correction. Use Delta Sync with a refresh interval of ten minutes to facilitate newly enrolled or compliant devices. These devices experience a waiting period of maximum ten minutes before email begins to sync.

Benefits:

- Updated policies from the same API source for all SEG servers.

- Smaller performance impact on API server.

- Reduced implementation or maintenance complexity compared to the SEG clustering model.

- Fewer failure points as each SEG is responsible for its own policy sets.

- Improved user experience.

PowerShell Integrated

PowerShell MEM configurations behave the same as SEG in terms of policy updates. For migrations to PowerShell, it is important that new profiles are associated to the PowerShell MEM configuration. Associating a new profile reduces unnecessary communication with the previous MEM configuration.

Gmail Integrated

Profiles are required for this type of deployment except when integrating with Google Directory APIs. Unless the devices are provisioned with the profiles, the configured Gmail deployment does not identify or manage the device.

Synchronize Devices

Use MEM to synchronize devices associated with an organization group.

Once you configure a Mobile Email Management (MEM) deployment, the devices of the associated organization group syncs up with MEM. You can view the status of the devices and other details on the **Email Dashboard** page of the Workspace ONE UEM console.

The devices appear on the dashboard depending on the deployment models the devices are assigned to.

- SEG Proxy - Devices managed with the SEG Proxy appear on the dashboard when the SEG Proxy reports the device as connected and managed.

- PowerShell - Devices managed with PowerShell appear on the dashboard when Workspace ONE UEM sends a PowerShell cmdlet, allowing the device to connect to email.

- Gmail - Devices managed with Gmail appear on the Dashboard when the Workspace ONE UEM EAS profile is queued up for the device.

The Email Dashboard shows one of the following statuses:

- **Managed Assigned** - Enrolled devices with identified *memconfigID*.

- **Managed Unassigned** - Enrolled devices for which the *memConfigID* has not yet been identified through profile assignment or auto discovery.

- **Unmanaged Discovered** - Devices that are not yet enrolled in Workspace ONE UEM and a specific MEM configuration at the organization group that has discovered them.

Email Profiles

6

MEM Email Profiles

EAS Profiles

Deploy EAS Mail using Native Mail Client (Android (Legacy))

Use the following steps to create a configuration profile for the Native Mail Client:

1   Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android (Legacy)**.

2   Select **Device** to deploy your profile to a device.

3   Configure the profile's **General** settings.

4   Select the **Exchange ActiveSync** payload.

5   Configure Exchange ActiveSync settings:

Setting	Description
Mail Client	Select **Native Mail Client** as the account type.
Account Name	Enter a description for the mail account.
Exchange ActiveSync Host	Enter the external URL of your company's ActiveSync server. The ActiveSync server can be any mail server that implements the ActiveSync protocol, such as IBM 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.
Ignore SSL Errors	Enable to allow devices to ignore SSL errors for Workspace ONE Intelligent Hub processes.
Login Information	
Domain	Enter the end-user's domain. You can use the Lookup Values instead of creating individual profiles for each end user.
User	Enter the end-user's username. You can use the Lookup Values instead of creating individual profiles for each end user.
Email Address	Enter the end-user's email address. You can use the Lookup Values instead of creating individual profiles for each end user.
Password	Enter the password for the end user. You can use the Lookup Values instead of creating individual profiles for each end user.

Setting	Description
Identity Certificate	Select (if desired) an Identity Certificate from the drop-down if you require the end user to pass a certificate in order to connect to the Exchange ActiveSync, otherwise select **None** (default).
Settings	
Past Days of Mail to Sync	Select the number of days worth of past mail to sync with device.
Past Days of Calendar to Sync	Select the number of past days to sync on the device calendar.
Sync Calendar	Enable to allow calendars to sync with device.
Sync Contacts	Enable to allow contacts to sync with device.
Allow Sync Tasks	Enable to allow tasks to sync with device.
Maximum Email Truncation Size	Specify the size beyond which e-mail messages are truncated when they are synced to the devices.
Email Signature	Enter the email signature to be displayed on outgoing emails.
Restrictions	
Allow Attachments	Enable to allow attachments with email.
Maximum Attachment Size	Specify the maximum attachment size in MB.
Allow Email Forwarding	Enable to allow email forwarding.
Allow HTML Format	Specify whether e-mail synchronized to the device can be in HTML format. If this setting is set to false, all e-mail is converted to plain text.
Disable screenshots	Enable to disallow screenshot to be taken on the device.
Sync Interval	Enter the number of minutes between syncs.
Peak Days for Sync 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.
S/MIME Settings	
	Select **Use S/MIME** From here you can select an S/MIME certificate you associate as a **User Certificate** on the **Credentials** payload.
	■ **S/MIME Certificate** – Select the certificate to be used.
	■ **Require Encrypted S/MIME Messages** – Enable to require encryption.
	■ **Require Signed S/MIME Messages** – Enable to require S/MIME signed messages.
	Provide a **Migration Host** if you are using S/MIME certificates for encryption.
	Select **Save** to save the settings or **Save & Publish** to save and push the profile settings to the required device.

6   Select **Save** to save the settings or **Save & Publish** to save and push the profile settings to the required device.

This chapter includes the following topics:

- Deploy EAS Mail using AirWatch Inbox for Android

- Configure an EAS Mail Profile using Native Mail Client (iOS)

- Configure an EAS Mail Profile using Workspace ONE UEM Inbox (iOS)

- Exchange ActiveSync Profile (Windows Desktop)

Deploy EAS Mail using AirWatch Inbox for Android

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

1   Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Android**.

2   Configure the profile's **General** settings.

3   Select the **Exchange ActiveSync** payload and select **AirWatch Inbox** from the **Mail Client** drop-down.

4   Configure the payload settings:

Table 6-1. Payload Settings

Setting	Description
Account Name	Enter the name of the Exchange ActiveSync account.
Exchange ActiveSync Host	Enter the public host name for the server.
Ignore SSL Errors	Enable to allow the device to ignore Secure Socket Layer certificate errors for Hub processes.
Use SSL	Send all communications through Secure Socket Layer.
Use S/MIME	Store user's S/MIME certificate to be used with S/MIME enabled profiles.
Login Information	
Domain	Use look-up values which pull directly from the user account record.
	The profile supports lookup fields for inserting enrollment user's information and login information. See the Username and Password section at the bottom of this page for more information.
User	Use look-up values which pull directly from the user account record.
Email Address	Use look-up values which pull directly from the user account record.
Password	Enter the password that will be provided to users to log in to the email account.Leave this field empty to prompt the user to create their own password.
Identity Certificate	Select from the drop-down menu to provide credentials for cert-based authentication after the certificate is added to the Credentials payload.
Email Settings	
Past Days of Mail	Specify the number of past days of mail to sync.
Sync Interval	Determine how often data is synced to devices.

Table 6-1. Payload Settings (Continued)

Setting	Description
Past Days of Calendar to Sync	Specify the number of past days of calender items to sync.
Email Signature	Predetermine the email signature information.
Contacts and Calendars	
Contacts Application	Syncs the native calendar and contact applications with AirWatch Inbox.
	VMware AirWatch **Contacts** and **Calendar** applications are add-ons to the AirWatch Inbox. These applications are downloaded as a single app from the play store. Unlike Native Contacts/Calendars application, VMware 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 by enabling the **Allow Single Contact Export** and **Allow Bulk Contacts Export** options.
Allow Single Contact Export	Allows the export of individual contacts.
Allow Bulk Contacts Export	Allows the export of bulk contacts.
Calendar Application	Specify to use the AirWatch Calendar or the Native calendar to the device.
Passcode	
Require Passcode	Enable so that an end-user has 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.
Allow SSO to Override Passcode	Enable the SSO passcode over the application passcode set in this profile.
Authentication Type	Select the authentication type to be used with the enterprise applications.
	Select **Active Directory Password** to use active directory credentials to login or select passcode.
Passcode Complexity	Determine whether the password is simple or complex.
Minimum Passcode Length	Set the minimum number of characters allowed for the passcode.
Maximum Passcode Age	Limit the number of days allowed before passcode has to be reset.
Passcode History	Determine the history of passcodes used to prevent the user from reusing passcodes.
Auto-Lock	Set the number of minutes before the device automatically locks.
Auto Lock When Device Locks	Lock the application immediately when the device is locked.
Maximum Number of Failed Attempts	Determine the number of passcode entry attempts allowed before the data is erased.
Restrictions	
Restrict Copy and Paste	Allows users to only copy and paste items the selected within the inbox.
Allow Attachments	Prevents users from adding attachments to email and also prevents viewing incoming attachments in the email.
Maximum Attachment Size (MB)	Specify the maximum attachment size.

Table 6-1. Payload Settings (Continued)

Setting	Description
Restricts which application attachments can be opened into	Whitelist applications that will be allowed to open attachments.
	AirWatch recommends using this setting instead of the SEG policy to encrypt attachments where the use case allows for increased SEG performance.
Disable Screenshots	Restrict users from taking screenshots in the app.
Restrict Domains	Restrict domains by creating either a blacklist or whitelist of domain names.
Open all links in VMware Browser	Allow opening of links only through the VMware Browser.
	AirWatch recommends using this setting instead of the SEG policy to transform hyperlinks where the use case allows for increased SEG performance.

5   Select **Save & Publish**.

Username and Password

You can define the user name that is assigned for users to log in to the Workspace ONE UEM Inbox. The user name can be their actual email address or an email user name that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the Workspace ONE UEM **Inbox** profile settings, there is a **User** text box under **Login Information** that you can set to a predefined lookup value.

If you have email user names that are different than user email addresses, you can use the **{EmailUserName}** text box, which corresponds to the email user names imported during directory service integration. Even if your user user names are the same as their email addresses, use the **{EmailUserName}** text box, because it uses email addresses imported through the directory service integration.

Configure an EAS Mail Profile using Native Mail Client (iOS)

Use the following steps to create an email configuration profile for the native mail client on iOS devices.

1   Navigate to **Devices > Profiles & Resources > Profiles > Add.** Select **Apple iOS**.

2   Configure the profile's **General** settings.

3   Select the **Exchange ActiveSync** payload.

4   Select **Native Mail Client** for the **Mail Client**. Fill in the **Account Name** text box with a description of this mail account. Fill in the **Exchange ActiveSync Host** with the external URL of your company's ActiveSync server.

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   Select the **Use SSL** check box to enable Secure Socket Layer use for incoming email traffic.

6   Select the **S/MIME** check box to use more encryption certificates. Prior to enabling this option, ensure you have uploaded necessary certificates under **Credentials** profile settings.

- Select the **S/MIME Certificate** to sign email messages.

- Select the **S/MIME Encryption Certificate** to both sign and encrypt email messages.

- Select the **Per Message Switch** check box to allow end users to choose which individual email messages to sign and encrypt using the native iOS mail client (iOS 8+ supervised only).

7   Fill in the **Login Information** including **Domain Name, Username and Email Address** using look-up values. Look-up values pull directly from the user account record. To use the {EmailDomain}, {EmailUserName} {EmailAddress} look-up values, ensure your Workspace ONE UEM user accounts have an email address and email user name defined.

8   Leave the **Password** field empty to prompt the user to enter a password.

9   Select the **Payload Certificate** to define a certificate for cert-based authentication after the certificate is added to the **Credentials** payload.

10   Configure the following **Settings and Security** optional settings, as necessary:

- **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 message.

- **Prevent Recent Address Syncing** – Disables suggestions for contacts when sending mail in Exchange.

- **Prevent Mail Drop** – Disables use of Apple's Mail Drop feature.

11   Assign a **Default Audio Call App** that your Native EAS account will use to make calls when you select a phone number in an email message.

12   Select **Save and Publish** to push the profile to available devices.

Configure an EAS Mail Profile using Workspace ONE UEM Inbox (iOS)

Use the following steps to create a configuration profile for the Workspace ONE UEM Inbox.

1   Navigate to **Devices > Profiles & Resources > Profiles.**

2   Select **Add** and select **iOS** as the platform.

3   Configure the profile's **General** settings.

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.Workspace ONE UEMmdm.com`.

     ■   Enable **Ignore SSL Errors** to allow the devices to ignore Secure Socket Layer errors from Hub
         processes.

     ■   Enable **Use S/MIME** to select the certificate/smart card for signing and encrypting email
         messages. Before enabling this option, ensure that you have uploaded necessary certificates
         under **the Credentials** profile settings.

         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** text box.

     ■   Select the certificate/smart card to both sign and encrypt email messages in the **S/MIME
         Encryption Certificate** text box.

     ■   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** to authenticate user connections to your EAS Host. The profile supports
     lookup values for inserting enrollment user's information and login information.

7   Configure additional settings:

     ■   **Enable Calendar**

     ■   **Enable Contacts**

     ■   **Caller ID**

     ■   **Sync Interval** – The frequency with which the Workspace ONE UEM Inbox app syncs with the
         email server.

     ■   **Email Notifications** – Configure how end users can be notified of new emails. **Disabled** means
         they do 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**

     ■   **Enable HTML Email**

     ■   **Email Signature**

     ■   **Enable Signature Editing**

8   Configure a Passcode. You can require an end user to enter a passcode when the 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 iOS users to log in using their Workspace ONE UEM credentials, select **Username and Password** as the **Authentication Type** under the **Passcode** section.

- **Passcode Complexity** – Determine whether the password is simple or complex.

- **Minimum Length** – Set the minimum number of characters allowed for the passcode.

- **Minimum Number of Complex Characters**, if the **Complexity** is set to **Alphanumeric**.

- **Maximum Passcode Age (days)** – Limit the number of days allowed before passcode has to be reset.

- **Passcode History** – Determine the history of passcodes used to prevent the user from reusing passcodes.

- **Auto-Lock Timeout (min)** – Set the number of minutes before the device automatically locks.

- **Maximum Number of Failed Attempts** – Determine the number of passcode entry attempts allowed before the data in Workspace ONE UEM Inbox are erased.

9   Configure more 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 VMware Browser app only.

   Consider using this setting instead of the SEG policy to transform hyperlinks where the use case allows for increased SEG performance.

- Restrict attachments to open only in the VMware Content Locker.

   Consider using this setting instead of the SEG policy to encrypt attachments where the use case allows for increased SEG performance.

- **Set a Maximum Attachment Size (MB)**

- **Allow Printing**

10   Select **Save & Publish**.

Username and Password

You can define the user name that is assigned for users to log in to the Workspace ONE UEM Inbox. The user name can be their actual email address or an email user name that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the Workspace ONE UEM Inbox profile settings, there is a **User** text box under **Login Information** that you can set to a predefined lookup value.

If you have email user names that are different than user email addresses, you can use the **{EmailUserName}** text box, which corresponds to the email user names imported during directory service integration. Even if your user user names are the same as their email addresses, use the **{EmailUserName}** text box, because it uses email addresses imported through the directory service integration.

Removing Profile or Enterprise Wiping

Exchange ActiveSync Profile (Windows Desktop)

The Exchange ActiveSync profiles enable you to configure your Windows Desktop devices to access your Exchange ActiveSync server for email and calendar use.

Use certificates signed by a trusted third-party certificate authority (CA). Mistakes in your certificates expose your otherwise secure connections to potential man-in-the-middle attacks. Such attacks degrade the confidentiality and integrity of data transmitted between product components, and might allow attackers to intercept or alter data in transit.

The Exchange ActiveSync profile supports the native mail client and AirWatch Inbox for Windows Desktop. The configuration changes based on which mail client you use.

Important   Native Mail Client support is only available for Windows 10 devices.

Removing Profile or Enterprise Wiping

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

- User account/login information.

- Email message data.

- Contacts and calendar information.

- Attachments that were saved to the internal application storage.

Username and Password

You can define the user name that is assigned for users to log in to the Workspace ONE UEM Inbox. The user name can be their actual email address or an email user name that is different from their actual email address. When configuring the **Exchange ActiveSync (EAS)** payload in the Workspace ONE UEM **Inbox** profile settings, there is a **User** text box under **Login Information** that you can set to a predefined lookup value.

If you have email user names that are different than user email addresses, you can use the **{EmailUserName}** text box, which corresponds to the email user names imported during directory service integration. Even if your user user names are the same as their email addresses, use the **{EmailUserName}** text box, because it uses email addresses imported through the directory service integration.

Configure an EAS Profile for AirWatch Inbox (Windows Desktop)

Create an Exchange ActiveSync profile.

Create an Exchange ActiveSync profile to give Windows Desktop devices access to your Exchange ActiveSync server for email and calendar use. The settings change when you use the AirWatch Inbox as your Windows Desktop email client.

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

1   Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2   Select **Windows** and choose **Windows Desktop** as the platform.

3   Select **User Profile**.

4   Configure the profile **General** settings.

5   Select the **Exchange ActiveSync** payload. By default, **AirWatch Inbox** is selected in the **Mail Client** drop-down menu.

6   Enter the **Exchange ActiveSync Host**, which is the information of your EAS server. For example: `webmail.airwatchmdm.com`.

Settings	Descriptions
Use SSL	Enable to send all communications through the Secure Socket Layer.
Use S/MIME	Enable to store end-user S/MIME certificates. This option is necessary for S/MIME-enabled profiles.
Login Information	
Domain	Enter the email domain.
User	Enter the email user name.
Email Address	Enter the email address. This text box is a required setting.
Password	Enter the email password.
Payload Certificate	Select the certificate for the EAS payload.

Settings	Descriptions
Settings	
Require Passcode	When enabled, requires a passcode when the AirWatch Inbox app is opened.
Type	Select the type of login credentials required: ■ **Passcode** ■ **Username and Password**
Complexity	Select the level of complexity for the passcode: ■ Simple ■ Alphanumeric
Minimum Length	Select the minimum number of characters the passcode must have.
Allow Simple Value	Enable to allow passcodes that do not meet complexity requirements.
Minimum Number of Complex Characters	Select the smallest number of non-alphanumeric characters allowed. Displayed when **Complexity** is set to **Alphanumeric**.
Maximum Age	Select the maximum number of days a passcode may be used.
History	Select the number of previous passcodes remembered. If a user changes a passcode and it matches a stored previous passcode, the passcode is not accepted.
Auto Lock When Device Locks	Enable to lock AirWatch Inbox automatically when the device locks.
Grace Period	Select the number of minutes the app remains open and unlocked before automatically locking.
Maximum Number of Failed Attempts	Select the number of incorrect passcode entry attempts allowed before the data in AirWatch Inbox is erased.
Passcode	
Require Passcode	Enable to require a passcode when the AirWatch Inbox app opens.
Type	Select the type of login credentials required: ■ **Passcode** ■ **Username and Password**
Complexity	Select the level of complexity for the passcode: ■ Simple ■ Alphanumeric
Minimum Length	Select the minimum number of characters the passcode must have.
Allow Simple Value	Enable to allow passcodes that do not meet complexity requirements.
Minimum Number of Complex Characters	Select the smallest number of non-alphanumeric characters allowed. Displayed when **Complexity** is set to **Alphanumeric**.
Maximum Age	Select the maximum number of days a passcode may be used.
History	Select the number of previous passcodes remembered. If the end user reuses a password within the number of recorded occurrences, they cannot reuse that password.
Auto Lock When Device Locks	Enable to lock AirWatch Inbox when the device locks.

Settings	Descriptions
Grace Period	Select the number of minutes the app remains open and unlocked before automatically locking
Maximum Number of Failed Attempts	Select the number of incorrect passcode entry attempts allowed before the data in AirWatch Inbox is erased.
Restrictions	
Disable Copy-Paste	Enable to restrict the copy/paste actions in AirWatch Inbox: ■ Disable ability to long press email text and copy it to the clipboard. ■ Disable ability to copy text from outside of the email client and paste it into a mail message.
Disable Attachments	Enable to restrict end user from opening attachments inside the AirWatch Inbox app.
Maximum Attachment Size (MB)	Enter the maximum size (in MB) that a received attachment may be.
Restrict Domains	Enable to restrict the mail flow to specific domains.
Restriction Type	Select the type of restriction for email domains.
Domain Name	Select **Add** to add a domain to the whitelist or blacklist.

7　Select **Save** to keep the profile in the console or **Save & Publish** to push the profile to the devices.

Configure an Exchange ActiveSync Profile (Windows Desktop)

Create an Exchange ActiveSync profile to give Windows Desktop devices access to your Exchange ActiveSync server for email and calendar use.

Note　Workspace ONE UEM does not support Outlook 2016 for Exchange ActiveSync profiles.

Use the following steps to create a configuration profile for the native mail client:

1　Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.

2　Select **Windows** and choose **Windows Desktop** as the platform.

3　Select **User Profile**.

4　Configure the profile **General** settings.

5　Select the **Exchange ActiveSync** payload.

6　Configure the Exchange ActiveSync settings:

Settings	Descriptions
Mail Client	Select the Mail Client that the EAS profile configures. Workspace ONE UEM supports the Native Mail Client and AirWatch Inbox.
Account Name	Enter the name for the Exchange ActiveSync account.
Exchange ActiveSync Host	Enter the URL or IP Address for the server hosting the EAS server.
Use SSL	Enable to send all communications through the Secure Socket Layer.

Settings	Descriptions
Login Information	
Domain	Enter the email domain.
	The profile supports lookup values for inserting enrollment user login information. For more information, see the Username and Password section at the bottom of the page.
Username	Enter the email user name.
Email Address	Enter the email address. This text box is a required setting.
Password	Enter the email password.
Identity Certificate	Select the certificate for the EAS payload.
Settings	
Next Sync Interval (Min)	Select the frequency, in minutes, that the device syncs with the EAS server.
Past Days of Mail to Sync	Select how many days of past emails sync to the device.
Diagnostic Logging	Enable to log information for troubleshooting purposes.
Content Type	
Require Data Protection Under Lock	Enable to require data to be protected when the device is locked.
Allow Email Sync	Enable to allow the syncing of email messages.
Allow Contacts Sync	Enable to allow the syncing of contacts.
Allow Calendar Sync	Enable to allow the syncing of calendar events.

7   Select **Save** to keep the profile in the Workspace ONE UEM console or **Save & Publish** to push the profile to the devices.

Enable Certificate-Based Email

7

Configure email authentication using certificates.

Using certificates over the standard username and password credentials have certain benefits as the certificates provide stronger authentication against unauthorized access. It also eliminates the need for end users to enter in a password or renew one every month. Sensitive emails between recipients can be encrypted through S/MIME or prove your identity through a message signature.

To enable Certificate-based email:

1   Navigate to **Devices > Profiles & Resources > Profiles**.

2   Select **ADD > Add Profile** and then select the required platform.

3   Choose the **Credentials** profile setting and configure it.

4   ■   **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 drop-down menu for your organization group.

        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
    - ■   S/MIME Signing Certificate
    - ■   S/MIME Encryption Certificate

5   **Save & Publish** the settings.

Email Access Control Enforcement

8

Configure access control to provide secure access to your email infrastructure.

Email Compliance Policies

Once email has been deployed, you can further protect your mobile email by adding access control. The access control feature allows only secure and compliant devices to access your mail infrastructure. The access control is enforced with the help of email compliance policies.

Email compliance policies enhance security by restricting email access to non-compliant, unencrypted, inactive, or unmanaged devices. These policies allow you to provide email access to only the required and approved devices. Email policies also restrict email access based on the device model and the operating systems.

These policies are categorized as General Email Policies, Managed Device Policies, and Email Security Policies. The different policies that fall under each category and the deployments to which they are applicable are listed in the table.

✓ - Applicable ☐ - Not Applicable

	SEG	PowerShell	Gmail			
			Direct Integration using password management		SEG proxy using password management	Direct Integration using Directory API
General Email Policies			**Without SEG and without Password purge**	**Without SEG and with Password Purge**		
Sync Settings	✓	☐	☐	☐	✓	☐
Managed Device	✓	✓	☐	☐	✓	✓
Mail Client	✓	✓	☐	☐	✓	☐
User	✓	✓	☐	☐	✓	☐

	SEG	PowerShell	Gmail			
EAS Device Type	✓	✓	☐	☐	✓	☐
Managed Device Policies						
Inactivity	✓	✓	✓	☐	✓	✓
Device Compromised	✓	✓	✓	☐	✓	✓
Encryption	✓	✓	✓	☐	✓	✓
Model	✓	✓	✓	☐	✓	✓
Operating System	✓	✓	✓	☐	✓	✓
Require ActiveSync Profile	✓	✓	✓	✓	✓	✓
Email Security Policies						
Email Security Classification	✓	☐	☐	☐	✓	☐
Attachments (managed devices)	✓	☐	☐	☐	✓	☐
Attachments (unmanaged devices)	✓	☐	☐	☐	✓	☐
Hyperlink	✓	☐	☐	☐	✓	☐

This chapter includes the following topics:

- Activate an Email Compliance Policy
- Email Content, Attachments & Hyperlinks Protection
- Enable Email Security Classification
- Enable Email Attachment Protection
- Enable Hyperlink Protection

Activate an Email Compliance Policy

The email compliance policies available on the Workspace ONE UEM console are General Email Policies, Managed Device Policies, and Email Security Policies. You can activate any of these email compliance policies or edit the rules for these email policies to allow or block the devices.

To activate an email policy:

1 Navigate to **Email > Compliance Policies**.

2 Use the edit policy icon under the **Actions** column to edit any of the rules for a policy.

- **General Email Policies** – Enforce policies on all devices accessing email. When you choose a user group, the policy applies to all the users of that group.

Email Policy	Description
Sync Settings	Prevent the device from syncing with specific EAS folders. ■ Workspace ONE UEM prevents devices from syncing with the selected folders irrespective of other compliance policies. ■ For the policy to take effect, it is necessary to republish the EAS profile to the devices (this forces devices to resync 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** and **Discovered** ■ You can also set default actions for the mail client and newly discovered mail clients that do not display in the Mail Client drop-down menu. For the custom client type, wildcard (*) characters and auto-complete are supported.
User	Restrict email access to a set of users. You can allow or block user type that includes Custom, Discovered, Workspace ONE UEM User Account, and user group. You can also set default actions for email usernames that do not display in the Username or Group drop-down menu. For the custom user type, wildcard (*) 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 devices based on the client type that includes Custom and Discovered mail client. You can also set default actions for the EAS device types that do not display in the Device Type drop-down field. For the custom client type, wildcard (*) characters and auto-complete are supported.

- **Managed Device Policies** – Enforce policies on managed devices accessing email.

Email Policy	Description
Inactivity	Prevent inactive, managed devices from accessing email. You can specify the number of days a device shows up as inactive (that is, does not check in to VMware AirWatch, before Workspace ONE UEM prevents email access. The minimum accepted value is 1 and maximum is 32767.
Device Compromised	Prevent compromised devices from accessing email. This policy does not block email access for devices that have not reported compromised status to AirWatch.
Encryption	Prevent email access for unencrypted devices. This policy is applicable only to devices that have reported data protection status to VMware 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.
Require ActiveSync Profile	Restricts email access to devices which are not managed with an Exchange ActiveSync profile.

■ **Email Security Policies** – Enforce policies on attachments and hyperlinks. This policy is applicable for SEG deployments only. For more information, see Email Content, Attachments & Hyperlinks Protection.

Email Policy	Description
Email Security Classification	Define the policy for the SEG to take on emails with tags and without tags. You can use the predefined tags or create tags using the Custom option. Based on the classification, you can either choose to allow or block the email in AirWatch Inbox and other email clients.
Attachments (managed devices)	Encrypt email attachments of the selected file types. These attachments are secured on the device and are only available for viewing on the VMware Content Locker. Currently, this feature is only available in managed iOS, Android devices, and Windows Phones with the VMware 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 unmanaged devices. Encrypted email attachments are not viewable on unmanaged devices. This feature is intended to maintain email integrity. If an email with an encrypted attachment is forwarded from an unmanaged device, the recipient can still view the attachment on a PC or another mobile device. For the maximum use of SEG, Workspace ONE UEM recommends using SEG for the attachment encryption and hyperlink transformation that can be accessed using AirWatch Inbox for iOS, Android, and the Native Mail Client for iOS and Android.
Hyperlink	Allow device users to open hyperlinks contained within an email directly with VMware Browser present on the device. The Secure Email Gateway dynamically modifies the hyperlink to open in VMware Browser. You may choose one of the following Modification Type: ■ All - Choose to open all the hyperlinks with VMware Browser. ■ Exclude - Choose if you do not want the device users to open the mentioned domains through the VMware Browser. Mention the excluded domains in the **Modify all hyperlinks except for these domains** field. You can bulk-upload the domain names from a `.csv` file as well. ■ Include - Choose if you want the device users to open the hyperlinks from specified domains through the VMware Browser. Mention the included domains in the **Only modify hyperlinks for these domains** field. You can bulk upload the domain names from a `.csv` file also.

3 Create your compliance rule and **Save**.

4 Select the gray circle under the **Active** column to activate the compliance policy. A page appears with a key code.

5 Enter the key code in the corresponding field and select **Continue**. The policy is activated and shows a green colored circle under the **Active** column.

Email Content, Attachments & Hyperlinks Protection

Secure email using Workspace ONE Web, and Workspace ONE Content.

Workspace ONE UEM helps you protect and control the mobile email attachments that are vulnerable to data loss for both managed and unmanaged devices. Workspace ONE UEM allows device users to open hyperlinks in an email directly with VMware Browser present on the device. The Secure Email Gateway dynamically modifies the hyperlink to open in VMware Browser.

You must have installed the following applications before you can begin to proceed with protecting your email attachments:

- Secure Email Gateway (SEG)

- VMware Content Locker (iOS, Android, and Windows Phone)

- Support for Microsoft Exchange 2010/2013/2016, IBM Notes, Novell GroupWise, and Gmail

Enable Email Security Classification

Select the security classifications on the UEM consoleWorkspace ONE UEM console for which you want Secure Email Gateway to take action.

There is a list of pre-defined security classifications to choose from as well as the option to create your own custom classification.

To enable email security classification:

1   Navigate to **Email > Compliance Policies > Email Security Policies**.

2   Select the gray colored circle under the **Active** column for the **Email Security Classifications** compliance policy. A page appears with a key code.

3   Enter the key code in the corresponding field and select **Continue**. The policy gets activated and is indicated by a green colored circle under the **Active** column.

4   Select the **Edit** option under the **Actions** column.

5   Select **Add** and then select the type of tag from the **Type** drop-down menu. Options available are Pre-defined and Custom. Select the tag type as Pre-defined to get a list of available tags from the **Security Classification** drop-down menu. Select the tag type as Custom to enter your own custom tag in the **Security Classification** field.

6   Enter a **Description** for the tag and select **Next**.

7   Configure the actions that SEG should take against emails marked or not marked with a tag. You may choose to allow or block emails on AirWatch Inbox or other email clients. Select **Next**.

8   View the **Summary** and click **Save**.

Enable Email Attachment Protection

Protect email attachments using Workspace ONE UEM.

Email attachments are of various file types. On the UEM console, you can select the files types for which the email attachments must be encrypted by the Secure Email Gateway. These encrypted attachments are secured on the mobile devices and can be viewed using the VMware Content Locker application.

Granular settings are available for managed iOS, Android devices, and Windows Phone. For other managed devices and all unmanaged devices, attachments can be prevented (in-bulk) from being opened in third-party apps.

To enable email attachment protection:

1   Navigate to **Email > Compliance Policies > Email Security Policies**.

2   Select the gray colored circle under the **Active** column for the **Attachments (Managed devices)** or **Attachments (Unmanaged devices)**compliance policy. A page appears with a key code.

3   Enter the key code in the corresponding field and select **Continue**. The policy is activated and is denoted by a green colored circle under the **Active** column.

4   Select the **Edit** option under the **Actions** column.

5   Select whether to encrypt & allow or block or allow without encryption attachment for each file category (for managed iOS, Android and Windows devices only).

6   Select the check box **Allow Attachments to be saved in Content Locker** to save the attachments in Content Locker. The attachments remain encrypted and Content Locker policies applies.

7   Choose the policy for any **Other Files** not mentioned here.

8   Enter file extensions that are to be excluded from the actions configured in **Other Files** into the **Exclusion List**.

9   Enter a **Custom Message for Blocked Attachments**to inform the recipient that an attachment has been blocked.

10 **Save** the settings.
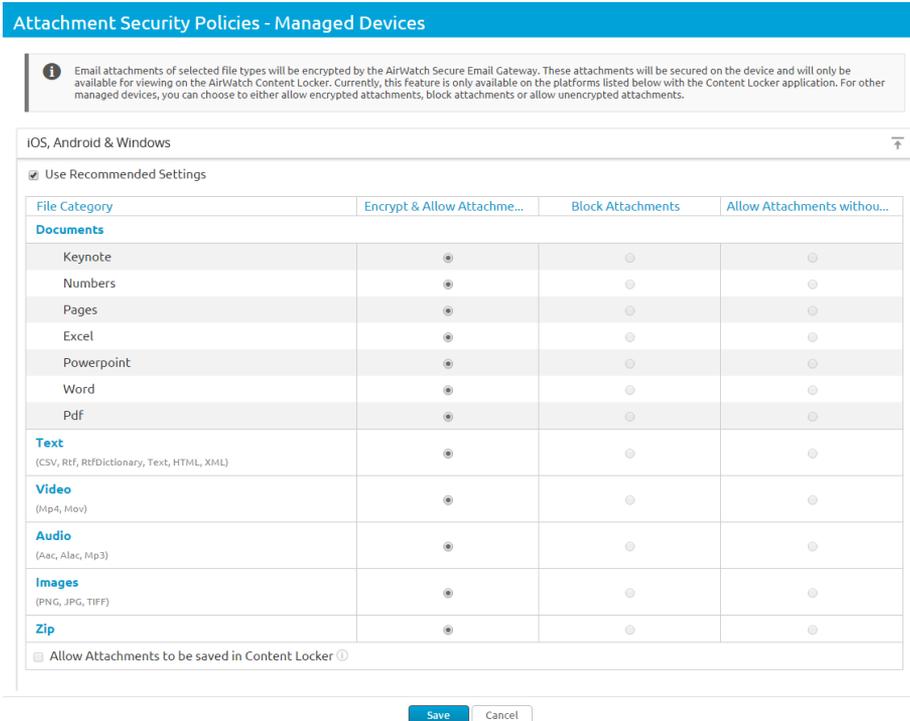
Enable Hyperlink Protection

Protect hyperlinks in emails.

Using the hyperlink email security policy, you can control the hyperlinks in the emails to be modified so that these can be opened directly with VMware Browser.

To enable hyperlinks protection:

1 Navigate to **Email > Compliance Policies > Email Security Policies**.

2 Select the gray colored circle under the **Active** column for the **Hyperlink** compliance policy. A page appears with a key code.

3 Enter the key code in the corresponding field and select **Continue**. The policy is activated and is denoted by the green colored circle under the **Active** column.

4 Select the **Edit** option under the **Action** column.

5 Select the platform for which you want to ignore the hyperlink transformations for AirWatch Inbox.

6 Select one of the **Modification Type**:

7 ▪ All - Choose to open all the hyperlinks with VMware Browser.

   ▪ Include - Choose if you want the device users to open the hyperlinks from specified domains through the VMware Browser. Mention the included domains in the **Only modify hyperlinks for these domains** field. You can bulk upload the domain names from a CSV file as well.

   ▪ Exclude - Choose if you do not want the device users to open the mentioned domains through the VMware Browser. Mention the excluded domains in the **Modify all hyperlinks except for these domains** field. You can bulk upload the domain names from a CSV file as well.

8 **Save** the settings.

Email Management

<div style="text-align: right">9</div>

Monitor your user group's email traffic and devices through the **Email Dashboard** .

The **Email > Dashboard** dashboard gives you a real-time summary of the status of the devices connected to the email server.

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. The graphs display the results in the List View page.
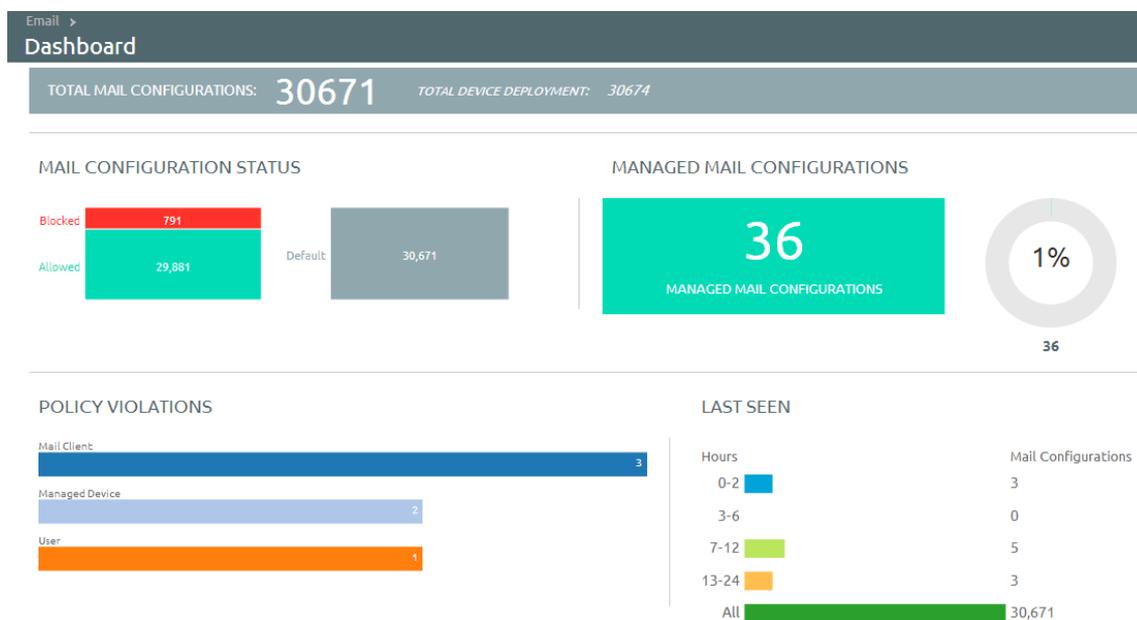
View Device and User Information

View detailed device and user-specific information.

You can view all the real-time updates of the end-user devices that you are managing with Mobile Email Management (MEM) from the **Email > List View** page.

Switch between the **Device** and **User** tabs to view the user and device information. In order to view the summary or the customized list of the information, change the Layout.

■   View the devices which are managed, unmanaged, compliant, non-compliant, blocked, or allowed.

■ View the device details such as OS, Model, Platform, Phone Number, IMEI, and IP address.

You can view the device or user-specific information either as a summarized list or as a customized one based on your requirement.

The **List View** page provides the following detailed information:

Settings	Description
Last Request	The last state change of the device either from Workspace ONE UEM 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. ■ The reason code is 'Global', if the default organization's Allow, Block, or Quarantine policies define the access state. The reason code is 'Individual' when the device ID is explicitly set for a given mailbox by Exchange admin or Workspace ONE UEM. The reason code is 'Policy', if any EAS policy blocks the device. ■ Workspace ONE UEM provides you with the option to block emails on non- compliant devices (such as devices with blacklisted apps). Emails are enabled once the devices become compliant. You can view the list of non-compliant devices on the **Email Dashboard** marked with the reason tag as 'MDM Compliance'.

■ **Platform, Model, OS, IMEI, EAS Device Type, IP Address** - The device information is displayed in these fields.

■ **Mailbox Identity** - The location of the user mailbox in the Active Directory.

Filters

Narrow the device search using the **Filter** option on the List View page.

Settings	Description
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.
EAS Device Type	Filter based on the device type.
Email Address	Filter based on email address.
Last Gateway Server	Filter based on the available Secure Email Gateway server.

Email Actions

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

Important These actions 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 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 Workspace ONE UEM or you manually whitelist or blacklist a device, so initiating a state change command.

  Workspace ONE UEM 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.

When the Direct PowerShell Model is configured, Workspace ONE UEM communicates directly to the CAS array using remote signed PowerShell sessions established from the console server or VMware Enterprise Systems Connector (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 Workspace ONE UEM.

- **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.

Settings	Description
Enrollment Email	Sends an email to the user with all the details required for enrollment.
	On discovering an unmanaged 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 providing you the history of the device activity. This feature is available for SEG only.
Dx Mode Off	Turns off the diagnostic for the selected user mailbox.
Update Encryption Key	Resets the encryption and then resyncs the emails for the selected devices.
Remote Wipe	Resets the device to factory settings.
	Perform an Enterprise Reset (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.
Migrate Devices	Migrate devices across organization groups and MEM deployments.
Sync Selected Mailbox	Syncs the selected device mailbox. Only one device mailbox at a time can be synced.

Note This record may reappear after the next sync.

Checking for Unmanaged Devices

To make sure all your devices are managed and monitored, navigate to the List View page. From List View page, filter the unmanaged devices and then send an enrollment mail from the Administration drop-down menu.