VMware AirWatch Secure Email Gateway Guide

Securing Your Email Infrastructure

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to Secure Email Gateway

The Workspace ONE UEM Secure Email Gateway (SEG) helps protect your mail infrastructure and enables VMware AirWatch Mobile Email Management (MEM) functionality. Install SEG alongside your existing email server to relay all email traffic to AirWatch-enrolled devices.

Based on the settings you define in the Workspace ONE UEM console, the SEG takes allow or block decisions for every mobile device it manages. The SEG filters all communication requests, relays traffic from approved devices, and protects corporate email server by not allowing any devices to directly communicate with it. Through SEG, email attachments and hyperlinks can be opened only through VMware Content Locker and VMware Browser respectively, thus protecting your sensitive information.

Though SEG protects the email server and sensitive content, neither SEG nor any of the Workspace ONE UEM components stores emails and the attachments.

Secure Email Gateway Platforms

The Secure Email Gateway (SEG) is offered on two platforms; Classic and V2 that you can choose while configuring the SEG for your email architecture.

Though the basic functionalities of both the platforms remain the same, the V2 platform differs in certain aspects.

- Improved performance over Classic platform
- Use of standardized REST API over SOAP API
- Supports only Exchange environments
- Required installation of Java Runtime Environment

Features Supported on SEG Platform

The Classic and the V2 platform supports various compliance policies and the architecture. Refer the listed features to determine which platform best suits your need.

✓ Supported □ Not supported FR Future Release

	Classic	V2
Compliance Policies		
General Access Policies		
Sync Settings	✓	□
Managed Device User	✓	✓
EAS Device Type	✓	✓
EAS Mail Client	✓	✓
User	✓	✓
Managed Device Policies		
MDM Inactivity	✓	✓
Device Compromised	✓	✓
Device Encryption	✓	✓
Device Model	✓	✓
Device OS	✓	✓
Require EAS Profile	✓	✓
Email Security Policies		
Email Classification	✓	✓
Attachment Control	✓	✓
VMware Browser Integration	✓	✓
Architecture		
Mail Server		
Microsoft Exchange (2010+)	✓	✓
Office 365	✓	✓
IBM Notes Traveler (8.5+)	✓	✓
Google	✓	FR
Other ActiveSync	✓	□
Authentication		
Basic Authentication	✓	✓
Certificate Authentication (KCD)	✓	✓
Outbound Proxy		
To API	✓	✓
To Email Server	✓	✓

	Classic	V2
Sizing		
Without Email Security Policies	2 CPU Core per 4,000 devices	2 CPU Core per 8,000 devices
With Email Security Policies	2 CPU Core per 500 devices	2 CPU Core per 4,000 devices
For more information on sizing requirements, see Implementation of SEG (Classic Platform) on page 20 (Classic Platform) and Implementation of SEG (V2 Platform) on page 10 (V2 Platform).		

Chapter 2:
Secure Email Gateway Architecture

You can install the Secure Email Gateway (SEG) in a Demilitarized Zone (DMZ) or behind a reverse proxy server. The reverse proxy configuration is preferred when the DMZ configuration is not feasible.

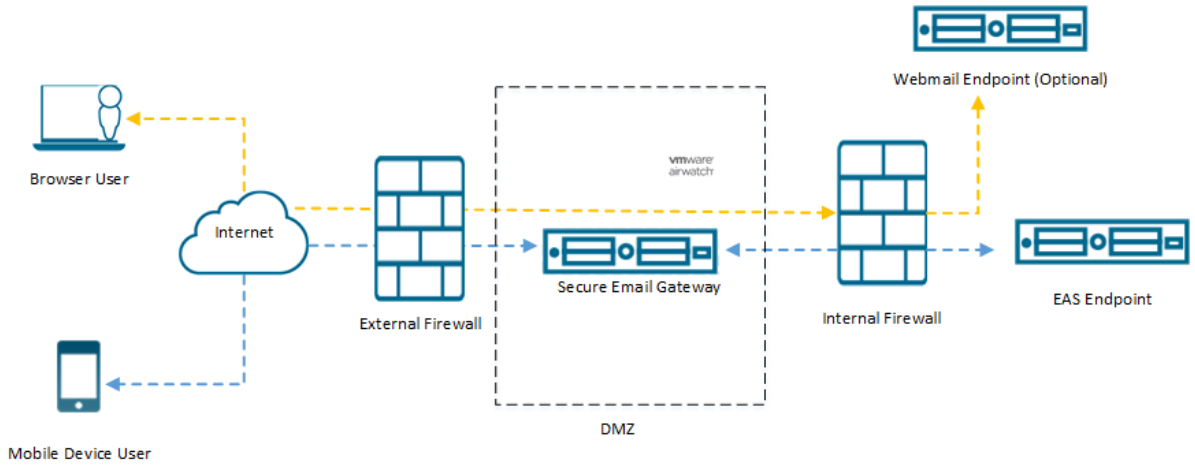
If SEG is installed in the DMZ, you can use an optional setting detailed in the installation wizard to proxy webmail traffic. In a reverse proxy server configuration, the reverse proxy handles webmail traffic.

SEG is an on-premises component that you install as part of your own organization's network. The SEG Proxy model requires Exchange ActiveSync infrastructure. For example, Microsoft Exchange 2010/2013/2016, Lotus Traveler, and Novell GroupWise Data Synchronizer. Please contact Workspace ONE Support for more information.

Note: Workspace 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 no longer supports integration with that version.

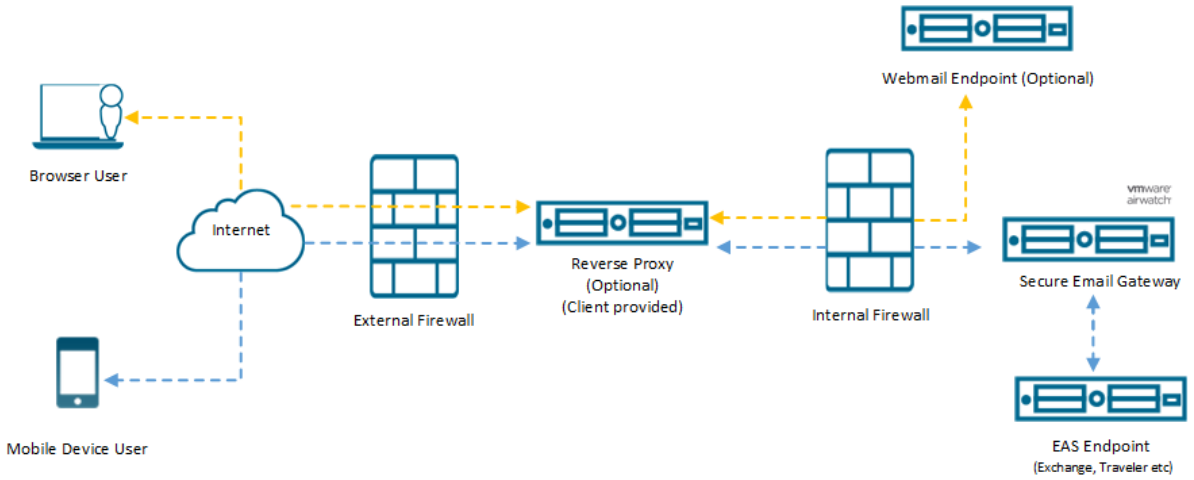
Recommended Setup: Exchange ActiveSync SEG Configuration

Workspace ONE UEM best practices support this configuration. The SEG is placed in the DMZ for routing mobile email traffic.



Alternative Supported Setup: Exchange ActiveSync SEG Using Optional Reverse Proxy Configuration

The reverse proxy configuration uses an optional reverse proxy to direct mobile device users to the SEG Proxy while routing browser users directly to their webmail endpoints. Use the following network configuration to set up the reverse proxy to communicate between devices and the SEG using the Exchange ActiveSync (EAS) protocol. This configuration should be used in cases where the recommended setup is not feasible.



Recommendations for Reverse Proxy Configuration

You can configure SEG to work with reverse proxy server in a normal fashion. You can set up load balancing between the SEGs and reverse proxy, but take care to configure the load balancers in front of the Central Authentication Service (CAS).

- **IP based affinity**: Configure IP based affinity if you are using Certificate authentication and there is no proxy or other component in front of the load balancer that changes the source IP from the original device.
- **Authentication Header Cookie based Affinity**: If you are using Basic authentication, especially if there is a proxy or other network component that changes the source IP from the original device.

For more information, please see:

- http://technet.microsoft.com/en-us/library/ff625248%28v=exchg.141%29.aspx
- http://technet.microsoft.com/en-us/library/ff625247

Exchange ActiveSync is a stateless protocol, and persistence is not explicitly required by MSFT. The best method of load balancing may vary from implementation to implementation.

Configuration

- Generally, they may be set to do a round-robin on the CAS with a persistence based on the source IP address. This works well when devices connect directly to the reverse proxy but causes issues when you place a SEG in front of it. Suppose you have one or two SEGs and the source IP as far as the load balancer in front of the CAS that is concerned will also be one or two. Hence, this can damage the load balancing and all the traffic can end up going to one or two CAS.

- Another issue that can arise is if there are some kind of limits set up on the reverse proxy server. For example, on an Internet Security and Acceleration (ISA) server, the default number of concurrent connections accepted from a single IP address is about 150. You need to set this to at least 5000 connections. On an ISA server, this can be set up under the Flood Mitigation settings.

Chapter 3:
Implementation of SEG (V2 Platform)

Requirements

You must meet the hardware, software, network, and general requirements to successfully deploy the SEG.

UEM Console Requirements

- AirWatch Console 9.0.3 or later
- REST API enabled for the Customer type Organization Group

Prerequisite: Enable REST API

To configure the REST API URL for your Workspace ONE UEM environment:

1. Navigate to **Groups & Settings > All Settings > System > Advanced > API > REST API**.
2. The UEM console gets the API certificate from the REST API URL that is on the Site URLs page. For SaaS deployments, use the format as 'XX.airwatchportals.com'.

You can configure the Secure Email Gateway (V2 platform) at a Container organization group that inherits the REST API settings from a Customer type organization group.

Hardware Requirements

A Secure Email Gateway (V2 platform) server can be a VM or physical server with the following hardware.

SEG	CPU Core	RAM	Notes
SEG without content transformation	2	4 GB	Per 8,000 devices, up to a maximum of 32,000 devices (8 CPU/ 16 GB RAM) per application server.

SEG with content transformation (Attachment handling, hyperlinks security, tagging etc.)	2	4 GB	Per 4,000 devices (2,000 devices per core) per application server, up to a maximum of 16,000 devices (8 CPU/16 GB RAM) Performance varies based on the size and quantity of transforms. These numbers reflect a deployment with a high number of content transforms. Sizing estimates vary based on actual email and attachment usage.

Notes for both SEG deployments types:

- An Intel processor is required. CPU Cores should each be 2.0 GHz or higher.
- The minimum requirements for a single SEG server are 2 CPU cores and 4 GB of RAM.
- When installing SEG servers in a load balanced configuration, sizing requirements can be viewed as cumulative. For example, a SEG environment requiring 4 CPU Cores and 8GB of RAM can be supported by either:
  - One single SEG server with 4 CPU cores and 8GB RAM.

    or
  - Two load balanced SEG servers with 2 CPU core and 4GB RAM each.
- 5 GB Disk Space needed per SEG and dependent software. This does not include system monitoring tools or additional server applications.

Software Requirements

Requirement	Notes
Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	

Networking Requirements

Source Component	Destination Component	Protocol	Port	Description
Devices (from Internet and Wi-Fi)	SEG	HTTPS	443	Devices request mail from SEG
Console Server	SEG	HTTPS	443	Console makes administrative commands to SEG
SEG	Workspace ONE UEM REST API (DS or CN server)	HTTP or HTTPS	80 or 443	SEG retrieves the configuration and general compliance policy information
SEG (OPTIONAL)	Internal hostname or IP of all other SEG servers	TCP	5701 41232	SEG communicates to shared policy cache across other SEGs for updates and replication

Source Component	Destination Component	Protocol	Port	Description
SEG	localhost	HTTP	44444	Admin accesses the SEG server status and diagnostic information from the localhost machine
Device Services	SEG	HTTPS	443	Enrollment events and real-time compliance communicates to SEG
SEG	Exchange	HTTP or HTTPS	80 or 443	Verify the following URL is trusted from the browser on the SEG server and gives a prompt for credentials: **For Exchange:** http(s)://*Exchange_Activesync_FQDN*/Microsoft-server-activesync

Recommendations

Requirement	Notes
Remote access to Windows Servers available to Workspace ONE UEM and Administrator rights	Set up the Remote Desktop Connection Manager for multiple server management, download the installer from https://www.microsoft.com/en-us/download/details.aspx?id=44989
Installation of Notepad++ (Recommended)	
Ensure Exchange ActiveSync is enabled for a test account	

Remote Access to Servers

Ensure that you have remote access to the servers where Workspace ONE UEM is installed. Typically, Workspace ONE UEM consultants perform installations remotely over a web meeting or screen share. Some customers also provide Workspace ONE UEM with VPN credentials to directly access the environment as well.

Configure the V2 Platform

In order to implement the SEG (V2 Platform) for your email architecture, first configure the SEG (V2 Platform) related settings on the UEM console. Only after you configure the settings, you are provided with a link to download the SEG installer.

Procedure

1. In the UEM console, navigate to **Email** > **Settings** and select **Configure**. The **Add Email Configuration** wizard displays.
2. In the **Platform** tab of the wizard:

- Select **Proxy** as the **Deployment Model**.
- Select **V2** as the **Gateway Platform**.

- Select the **Email Type**.
- Select the **Exchange Version** and then select **Next**.

3. Configure the basic settings in the **Deployment** tab of the wizard and then select **Next**.

Setting	Description
Friendly Name	Enter a friendly name for the SEG deployment. This name gets displayed on the MEM dashboard.
External URL and Port	Enter the external URL and the port number to which Workspace ONE UEM sends policy updates in the form *https://<external seg url>:<external port>*
Listener Port	Enter the web listener port for SEG. By default, the port number is 443. The SSL certificate is bound to this port if SSL is enabled for SEG.
Terminate SSL on SEG	Select **Enable** to bind the SSL certificate to the port.
Upload Locally	Select to upload the SSL certificate locally during installation.
SEG Server SSL Certificate	Select **Upload** to add the certificate. The SSL certificate can be automatically installed instead of providing it locally. This is useful for larger SEG deployments
Email Server URL and Port	Enter the Exchange server URL and the port number in the form *https://<email server url>:<email server port>* This is the Exchange URL to which SEG proxies email requests to Exchange.
Ignore SSL Errors between SEG and email server	Select **Enable** to ignore the Secure Socket Layer (SSL) certificate errors between the email server and SEG server.
Ignore SSL Errors between SEG and AirWatch server	Select **Enable** to ignore Secure Socket Layer (SSL) certificate errors between the Workspace ONE UEM server and SEG server. Establish a strong SSL trust between Workspace ONE UEM and SEG server using valid certificates.
Allow email flow if no policies are present on SEG	Select **Enable** to allow the email traffic if SEG is unable to load the device policies from the Workspace ONE UEM API. By default, SEG blocks email requests if no policies are locally present.

Setting	Description
Enable Clustering	Select **Enable** to enable clustering of SEG servers. When clustering is enabled, single policy updates are distributed to all the SEGs. These updates include enrollment, profile updates, and compliance changes processed by AirWatch. The SEG servers maintain these policies in a distributed cache that is shared by all SEGs in a cluster. Bulk policy updates are distributed to not just one SEG but to all the SEGs in the cluster. These SEGs communicate with each other through the SEG clustering port.
SEG Cluster Hosts	Add the IPs or hostnames of each server in the SEG cluster.
SEG Cluster Distributed Cache Port	Enter the port number for SEG to communicate to the distributed cache.
SEG Clustering Port	Enter the port number for SEG to communicate to the other SEGs in the cluster.

4. Select **Next** in the **Profile** tab of the wizard. For SEG, there is no action required on the Profiles tab.
5. On the MEM Config Summary tab of the wizard, review the basic configuration that you have just created for the SEG deployment and select **Finish** to save the settings.
6. Select the link that appears under the SEG Proxy Settings to download the SEG installer.

The MEM Configuration screen shows options such as **Edit**, **Advanced**, and **Test Connection**. These options allow you to edit your configuration, configure advanced settings, and test the connectivity between SEG, Web, and the Workspace ONE UEM API servers.

Configure Advanced Settings

You can configure the additional settings that you require for your SEG (V2 Platform) such as diagnostics, enabling compliance sync, transactions, and sizing with the Advanced option.

The following table lists the advanced settings:

Setting	Description
Use Recommended Settings	By default, the **Use Recommended Settings** check box is enabled to capture all SEG traffic information from devices. Otherwise, specify what information and how frequently the SEG should log for devices.
Enable Real-time Compliance Sync	Enable this option to let the UEM console remotely provision compliance policies to the SEG proxy server.
Required transactions	Enable or disable the required transactions such as Settings, Provisions and so on.
Optional transactions	Enable or disable the optional transactions such as Get attachment, Search, Move Items and so on.
Diagnostic	Set the number and frequency of transaction for a device.

Setting	Description
Sizing	Set the frequency of SEG and API server interaction. Use Delta Sync for policy updates as it minimizes the amount of data sent to SEG, thereby improving the performance. Delta sync is refreshed at a default time interval of ten minutes to ensure that SEG has an updated policy set. This interval is useful when multiple SEGs are in use, as it is a maximum of ten minutes where SEG is out of sync with the UEM console.
S/MIME Options	
Skip Attachment & Hyperlink transformations for S/MIME signed emails	Enable to exempt the encryption of attachments and transformation of hyperlinks through SEG for emails that are signed with S/MIME certificates.
Enable S/MIME repository lookup	Enable to allow the automatic look up of the S/MIME certificate managed in a hosted LDAP directory. You must configure the S/MIME lookup settings before you begin the SEG installation.
LDAP URL	Enter your LDAP server URL.
Authentication Type	Select **Anonymous** or **Basic** authentication. In case of Basic authentication, enter the **User Name** and **Password**.
Certificate Attribute	Enter the name of the LDAP attribute corresponding to the S/MIME certificate on the email recipient object. For example, userCertificate; binary
Attachments	
Block Attachments	Block or allow the attachments when SEG fails to communicate with Workspace ONE UEM or when the local policy set is empty.
Default Message for Blocked Attachments	Configure the message that is displayed to end users when SEG blocks attachments.

Install the Secure Email Gateway

The Workspace ONE UEM REST API information that you provide during the installation process fetches your SEG configuration from the UEM console.

Java Runtime Environment (JRE) 8 (1.8.0.121) is required. You do not need to install JRE before installing SEG. The SEG installer prompts you to install JRE during SEG installation.

1. Run the installer as an administrator in the **AirWatch Secure Email Gateway - InstallShield Wizard** window. Click **Next**.
2. Accept the **End User License Agreement** and select **Next**.
3. Select **Next** to install the SEG to the default folder **C:\AirWatch** or select **Change** to choose a different folder. Select **Yes** to install JRE 8 (1.8.0.121).
4. Enter the **AirWatch API Information** and select **Next**

Settings	Description
HTTPS	Select the check box if the protocol for the Workspace ONE UEM API server is https.
API Server Hostname	Enter the URL of your Workspace ONE UEM API server. This is required to fetch the SEG configuration from the UEM console.
Admin Username	Enter the user name of a Workspace ONE UEM Admin user account.
Admin Password	Enter the password of a Workspace ONE UEM Admin user account.
MEM Config GUID	Enter the unique ID of your Mobile Email Management (MEM) configuration. This is shown on the MEM Configuration page on the UEM console.

5. If an outbound proxy is required for the communication from the SEG to the API server then select the **Outbound proxy?** check box and enter the proxy settings details as described in the table. Select **Next**.

Settings	Description
HTTPS	If the protocol for the proxy is https then select the check box.
Proxy Host	The address of the proxy host.
Proxy Port	The proxy port number.
Username Password	User name and password for proxy authentication. These fields are available once you select the Does the proxy require authentication credentails? check box.

6. If your SSL certificate is provided when configuring the console MEM settings, skip this step and proceed with step 7. Otherwise, select **Browse** to upload the SSL Certificate, enter the **Certificate Password** and then select **Next**.

7. Select **Install** to begin the installation. The InstallShield Wizard takes few minutes to install the SEG.
8. Select **Finish** to exit the **AirWatch Secure Email Gateway - InstallShield Wizard**.

Configure SEG V2 Compliance for Email Notification Service

From the UEM console version 9.5, SEG provides authorization and compliance for Exchange Web Services (EWS) traffic used by VMware Email Notification Service (ENS). ENS adds Push Notification support to Exchange for providing real-time email notifications to VMware Boxer.

Both Cloud and On-premises ENS deployments are supported by SEG. SEG listens to the EWS traffic from ENS using */EWS* endpoint, applies the MEM compliance policies on incoming requests, and proxies the requests to Exchange. Certificate Based Authentication (CBA) using KCD is supported. If your deployment utilizes CBA using KCD, SEG acquires the Kerberos token (from KDC) required for Exchange authentication.

To enable SEG V2 compliance for ENS:

1. Navigate to **SEG > Config** folder.
2. Select the **application.properties** file and edit.
3. Select the **enable.boxer.ens.ews.proxy** value and update the value to **enable.boxer.ens.ews.proxy=true**.
4. Restart the SEG service.
   SEG now listens the /EWS and /ews endpoints for traffic from the ENS.

Secure Email Gateway V2 Platform Admin Page

You can use the Secure Email Gateway (SEG) V2 Platform Admin page to perform the maintenance tasks for your SEG without editing the configuration file. The Admin page is locally available on your SEG at https://localhost:44444/seg/admin. If SSL is enabled for SEG, the prefix of the localhost URL is *https* else it is *http*.

After you install SEG, you can perform the following tasks from the Admin page:

- Change the logging levels for the different SEG processes
- Call diagnostics endpoints
- Reconfigure the connections between SEG and API endpoints

The admin page displays two tabs: Logging and Diagnostics.

Logging

The information related to several SEG processes is recorded in a log file and each log entry is marked at a certain logging level. These logging levels control the amount of information that is logged in to the log file.

On the Logging page, you can adjust the logging levels for the SEG processes. The logging levels that you can set for the SEG processes are All, Trace, Debug, Warn, Error, Info, and Off.

The SEG processes for which you can set up the logging levels are listed in the table.

Settings	Description

Transaction Summary	Logs summary information about every device request that the SEG processes, such as the user, type of command, HTTP response code, and the time taken for processing the request.
Device Transactions (All)	Logs detailed information about individual EAS requests including allowed or blocked reason and HTTP headers.
Device Transactions (Blocked)	Logs detailed information about individual EAS requests including allowed or blocked reason and HTTP headers for blocked devices.
Policy Cache Policy Updates	Logs information about individual and bulk policy changes.
Transfer Handler Transfer Helper Encryption Helper MIME Type Conversion	Logs metadata used by email security policies for content security policies.
Console Transaction Reporting	Logs information about reporting data used by MEM dashboards in the UEM console.

Diagnostics

On the Diagnostics page, you can view the diagnostic information for SEG and run the various diagnostic REST API endpoints available locally on SEG. With the diagnostics endpoints that are readily available on SEG, you can view information about the SEG configuration settings, look up the policies in the SEG cache, and download records related to specific policy types in a .csv format.

Though the URI of the APIs on the SEG begins with *https://localhost:44444/seg/*, you must provide only the latter part of the URI after */seg/* as listed in the table. You can use the API endpoints to fetch SEG configuration settings, look up the policies, and download policy records.

API Endpoint	Description
/diagnostic/cluster	Returns SEG diagnostic information. By default, the SEG diagnostic information is displayed on the diagnostics page.
/policy/segconfig	Returns the SEG configuration settings.
/policy/<Policy Type> / <Policy Lookup Key>	Look up the policies in the SEG cache.
/download/ <Policy Type>	Download records related to policy types such as device, account, managedattachment, unmanagedattachement, and 451redirectmapping. The records are downloaded as a CSV file.

The following are the various policy types and the policy lookup keys to view the policies in the SEG cache. Replace the <Policy Type> and the <Policy Lookup Key> in the API endpoint, */policy/ <Policy Type> / <Policy Lookup Key>*

Policy Type	Policy Lookup Key	Description
segconfig	No lookup key required	Look up the SEG configuration settings.

generalaccess	No lookup key required	Look up the general access policy.
device	EAS Device Identifier	Look up the device policy by providing the EAS Device Identifier as the lookup key. For example, /policy/device/SMKG1KBHQ53H39TFTNQQ10JDES
account	User name	Look up the account policy by providing user name as the lookup key
easdevicetype	EAS device type	Look up the EAS device type policy by providing EAS device type as the lookup key.
mailclient	Mail Client	Look up the mail client policy by providing mail client as the lookup key. You must have all characters in the encoded URL form. For example, /policy/mailclient/Apple-iPhone5C3%2F1405.526000002
hyperlink	No lookup key required	Look up the hyperlink policy.
Encryptionkeydatapayload	AirWatch Device ID	Look up the encryption key data payload by providing the Workspace ONE UEM Device ID as the lookup key.

Chapter 4:
Implementation of SEG (Classic Platform)

Requirements

The factors such as hardware, software, network, and general requirements ensures uninterrupted SEG connectivity. Determine the requirements for your SEG using the following list.

UEM Console Requirements

- SOAP API enabled for the required organization group
- Exchange Active Sync profile created in the UEM console with the **Assignment Type** as Optional and **EAS hostname** as the SEG server URL

Prerequisite: Enable SOAP API

To configure the SOAP API URL for your Workspace ONE UEM environment:

1. Navigate to **Groups & Settings > All Settings > System** > **Advanced** > **API** > **SOAP API**.
2. The UEM console gets the API certificate from the SOAP API URL that is located on the Site URLs page. For SaaS deployments, use the format as XX.airwatchportals.com.

Hardware Requirements

Use the following requirements as a basis for creating your Secure Email Gateway (Classic Platform) server, which can be a VM or physical server.

SEG	CPU Core	RAM	Notes
SEG without content transformation	2	4 GB	Per 4,000 devices, up to a maximum of 16,000 devices (8 CPU/16 GB RAM) per application server

SEG	CPU Core	RAM	Notes
SEG with content transformation (Attachment handling, hyperlinks security, tagging, etc.)	2	4 GB	Per 500 devices (250 devices per core), up to a maximum of 2,000 devices (8 CPU/16 GB RAM) per application server Performance varies based on the size and quantity of transforms. These numbers reflect a deployment with a high number of content transforms. Sizing estimates vary based on actual email and attachment usage

Notes for both SEG deployment types:

- An Intel processor is required. CPU Cores should each be 2.0 GHz or higher.
- The minimum requirements for a single SEG server are 2 CPU cores and 4 GB of RAM.
- IIS App Pool Maximum Worker Processes should be configured as (# of CPU Cores / 2).
- When installing SEG servers in a load balanced configuration, sizing requirements can be viewed as cumulative. For example, a SEG environment requiring 4 CPU Cores and 8GB of RAM can be supported by either:
  - One single SEG server with 4 CPU cores and 8GB RAM.

    or
  - Two load balanced SEG servers with 2 CPU core and 4GB RAM each.
- 5 GB Disk Space needed per SEG and dependent software (IIS). This does not include system monitoring tools or additional server applications.

General Requirements

Status Checklist	Requirement	Notes
	Remote access to Windows Servers available to Workspace ONE UEM and Administrator rights	Set up the Remote Desktop Connection Manager for multiple server management, download the installer from https://www.microsoft.com/en-us/download/details.aspx?id=44989 See **General Requirements**.
	Installation of Notepad++ (Recommended)	Downloaded the installer from http://download.tuxfamily.org/notepadplus/6.5.1/npp.6.5.1.Installer.exe
	Ensure Exchange ActiveSync is enabled for a test account	

Software Requirements

Status Checklist	Requirement	Notes
	Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2 Windows Server 2016	
	Install Role from Server Manager	IIS 7.0 (Server 2008 R2) IIS 8.0 (Server 2012 or Server 2012 R2) IIS 8.5 (Server 2012 R2 only)
	Install Role Services from Server Manager	**Common HTTP Features**: Static Content, Default Document, Directory Browsing, HTTP Errors, HTTP Redirection **Application Development:** ASP.NET, .NET Extensibility, ASP, ISAPI Extensions, ISAPI Filters, Server Side Includes **Management Tools:** IIS Management Console, IIS 6 Metabase Compatibility Ensure WebDAV is not installed.
	Install Application Request Routing (ARR)	ARR component is available at http://www.iis.net/downloads/microsoft/application-request-routing ARR is mandatory for routing OWA traffic. For Lotus Notes, ARR is mandatory only when Traveler Mail Client is being used.
	Install Features from Server Manager	**.NET Framework 4.6.2 Features:** Entire module **Telnet Client**
	Install .NET Framework 4.6.2	The SEG Installer installs .NET 4.6.2 if it is not installed beforehand.
	Externally registered DNS	See **Server Requirements**.
	SSL Certificate from trusted third party with Subject or Subject Alternative name of DNS	Ensure SSL certificate is trusted by all device types being used. (i.e. not all Comodo certificates are natively trusted by Android) In addition, the SEG server must be able to connect to the SSL certificate CRL (For example: ocsp.verisign.com)
	IIS 443 Binding with the same SSL certificate	Validate that you can connect to the server over HTTPS (https://yourAirWatchDomain.com). At this point, you should see the IIS splash page. See **Server Requirements**.

Network Requirements

For configuring the ports listed below, all the traffic is uni-directional (outbound) from the source component to the destination component.

	Source Component	Destination Component	Protocol	Port	Verification
	Devices (from Internet and Wi-Fi)	SEG	HTTPS	443	Telnet from Internet to SEG server on port
	Console Server	SEG	HTTPS	443	Telnet from Internet to SEG server on port
	SEG	Workspace ONE UEM SOAP API (DS or CN server)	HTTP or HTTPS	80 or 443	Verify that the following URL is trusted from the browser on the SEG server: https://<API URL>/AirWatchServices/Internal/0/ActiveSyncIntegrationServiceEndpoint.svc 'IP based Persistence' should be used in the event when there are more than one API server. When the communication between SEG and the API server is through a proxy, SEG cannot make use of the proxy details defined in the browser settings. Therefore, the proxy settings must be specified during SEG configuration. For more information on configuring proxy settings see Configure the Classic Platform with the SEG Setup Wizard on page 34.
	SEG (OPTIONAL)	Internal hostname or IP of all other SEG servers	UDP and TCP	9090 (Configurable)	If you are using SEG Clustering (multiple load balanced SEG servers) SEG Clustering across Data Centers is not supported.
	Device Services	SEG	HTTPS	443	Telnet from Device Services to SEG server on port

	Source Component	Destination Component	Protocol	Port	Verification
	SEG	AirWatch Cloud Messaging (AWCM) server	HTTPS	• 2001 (For on premise instance of AirWatch) • 443 (For SaaS instance of AirWatch)	Telnet from SEG server to AWCM on port

The following requirements apply based on the email configuration you are using:					
	SEG	Exchange	HTTP or HTTPS	80 or 443	Verify that the following URL is trusted from the browser on the SEG server and gives a prompt for credentials: **For Exchange:** http(s)://*Exchange_Activesync_FQDN*/Microsoft-server-activesync **For Lotus Notes:** http(s)://*LotusNotesTraveler_FQDN*/servlet/traveler **For Google:** https://m.google.com/Microsoft-server-activesync **For Groupwise (depending on version):** http(s)://*Groupwise_FQDN*/EAS or http(s)://Groupwise_FQDN/Microsoft-server-activesync Once you enter the credentials, verify that a 501/505 HTTP page displays. **Important:** If you are using SSL from the SEG server to the mail endpoint, ensure the SEG server is able to reach the Certificate Revocation List URL for the mail server's SSL certificate. Failure to reach this endpoint may result in performance issues.
	SEG	Lotus Notes	HTTP or HTTPS	80 or 443	
	SEG	Google	HTTPS	443	
	SEG	Novell Groupwise	HTTP or HTTPS	80 or 443	

If Windows authentication is enabled on your CAS Activesync Endpoint, then one of the following is required:
1. Certificate Authentication and KCD
2. SEG cannot be joined to the domain

Server Requirements

External DNS Name

The two main components of Workspace ONE UEM are the Device Services server and the Console server. In a single

server deployment, these components reside on the same server, and an external DNS entry needs to be registered for that server.

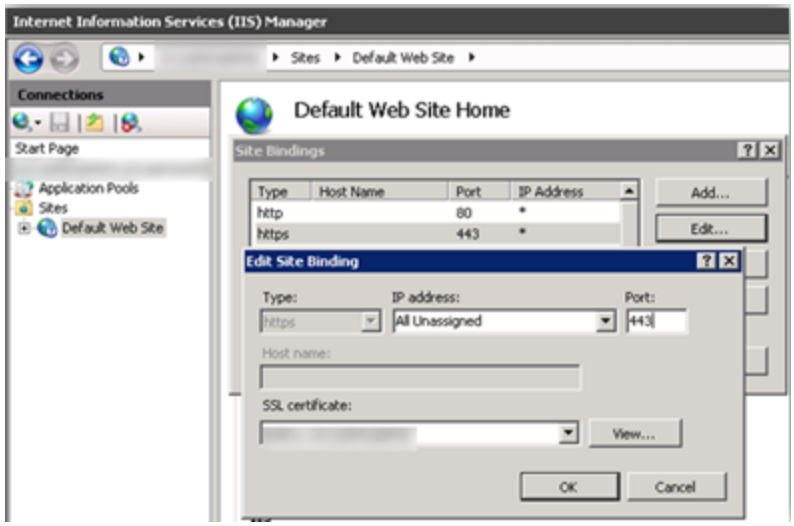
In a multi-server deployment, these components are installed on separate servers, and only the Device Services component requires an external DNS name, while the Console component can remain only internally available.

SSL Certificate

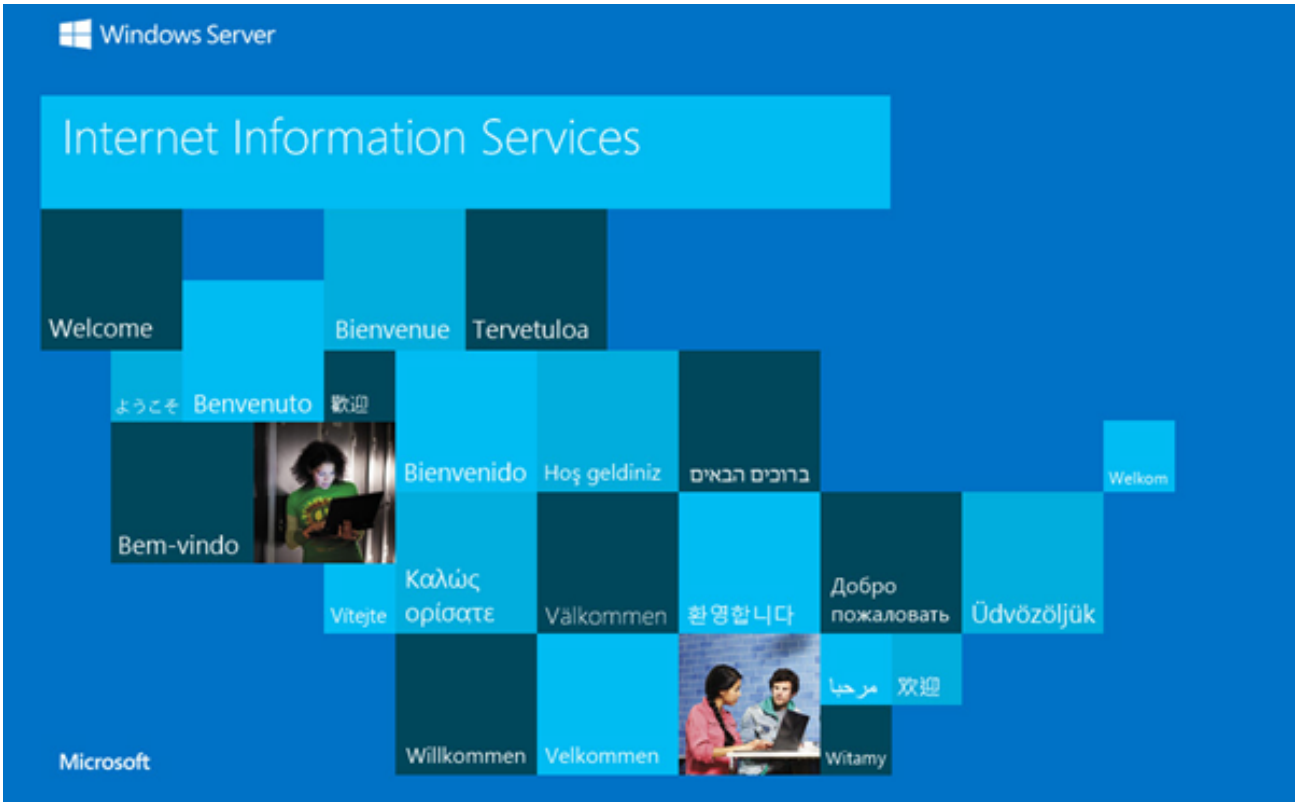
Set up the externally available URL of the Workspace ONE UEM server with a trusted SSL certificate. A wildcard or individual website certificate is required.

> **Note:** If SSL is used for admin console access, ensure that FQDN is enabled or the host file is configured.

1. Obtain SSL certificates for each of your external DNS entries. A list of root certificates natively trusted by iOS can be found here: http://support.apple.com/kb/HT5012
2. Upload your SSL certificate to the Workspace ONE UEM server(s). Your certificate provider has instructions for this process.
3. Once uploaded on your server you can use it to add a 443 binding to the Default Website in IIS. The bindings for a completed server look like the following. Your SSL certificate appears in the drop-down menu of available certificates.



4. Validate that you can connect to the server over HTTPS (https://yourAirWatchDomain.com). At this point, you see the IIS splash page.



URL Endpoints

Use the below mentioned URL Endpoint and the status code to check the SEG Connectivity.

Description	URL Endpoint	Status code
ActiveSync Connectivity	/Microsoft-Server-Activesync	HTTP/1.1 401

Configure the Classic Platform

To implement the SEG Classic platform for your chosen email architecture, first configure the basic Classic platform related settings on the UEM console. It is only after configuring these basic settings that you are provided with an option to download the SEG installer.

1. On the UEM console, navigate to **Email** > **Settings** and select **Configure**. The **Add Email Configuration** wizard displays.
2. On the **Platform** tab of the wizard:

- Select **Proxy** as the **Deployment Model**.
- Select **Classic** as the **Gateway Platform**.
- Select the **Email Type**.
  - If the email type chosen is Exchange, then select the version from the **Exchange Version** drop-down menu. If you want to deploy the SEG for Office 365, please contact Workspace ONE Support for additional information.
- Select **Next**.

3. On the **Deployment** tab of the wizard, configure the basic setting. Select **Next**.

Setting	Description
Friendly Name	Enter a friendly name for the SEG deployment. This name gets displayed on the MEM dashboard screen for devices managed by SEG.
Secure Email Gateway URL	Enter the URL for the SEG server in this field. This URL provisions email policies to the SEG server.
Ignore SSL Errors between SEG and email server	Select **Yes** to ignore the Secure Socket Layer (SSL) certificate errors between email server and SEG server.
Ignore SSL Errors between SEG and AirWatch server	Select **Yes** to ignore Secure Socket Layer (SSL) certificate errors between Workspace ONE UEM component and SEG server.
Use Basic Authentication	Select **Yes** if the SEG server is configured to enforce Basic Authentication. Workspace ONE UEM recommends using basic authentication. For more information on how to enable basic authentication, see Enable Basic Authentication on page 30.
Gateway Username **Gateway Password**	Enter the credentials to authenticate and secure traffic (including policy updates to the SEG server) between Workspace ONE UEM components and SEG. If disabled, anonymous authentication is used.

Always establish a valid SSL trust between Workspace ONE UEM and SEG server using certificates. Also, ensure to restart IIS (on SEG) after changing the SEG settings 'Ignore SSL Errors between SEG and email server' or 'Ignore SSL Errors between SEG and Workspace ONE UEM server'.

4. On the **Profiles** tab of the wizard, select a profile for the device platform that you choose.

Setting	Description
Platform	Select device platform from the drop-down menu.
Mail Client	Select an email client from the drop-down menu.
Action	Select either **Use Existing Profile** to associate an existing profile of the chosen platform or **Create New profile** if the existing profile do not match your requirement.You can associate only one profile per device type and mail client.
Profile	if an existing profile is used for the chosen platform, select a profile from the drop-down menu.

5. Select **Next**. The MEM Config Summary form provides a quick overview of the basic configuration that you have just created for the SEG deployment. Select **Finish** to save the settings.

   You have completed the email configuration steps and can view the MEM configuration details displayed on the Mobile Email Management configuration screen.

6. To download the SEG installer, click the link provided under the SEG Proxy Settings.

   You can use the **Edit**, **Advanced**, and **Test Connection** options available on the Mobile Email Management Configuration screen to edit the settings, configure advanced settings, and also test the connectivity between the SEG, web, and the Workspace ONE UEM API servers. The test result shows the success or failure connectivity status from Web to SEG and from SEG to Workspace ONE UEM API. These test results, help you identify the cause of connection failure.

   
   For more information on test connection, see the Knowledge Base article: https://support.air-watch.com/articles/115001675588

7. (Optional step) Configure the advanced settings.

Setting	Description
Use Recommended Settings	By default, the **Use Recommended Settings** check box is enabled to capture all SEG traffic information from devices. Otherwise, specify the type and the frequency of the information that you want SEG to log for the devices.
Enable Real-time Compliance Sync	Enable this option to enable the UEM console to remotely provision compliance policies to the SEG Proxy server.
KCD authentication	Enable this if you want certificate based authentication when your SEG server and email infrastructure are in different domains
Required transactions	Enable or disable the required transactions such as Folder Sync, Settings etc.
Optional transactions	Enable or disable the optional transactions such as Get attachment, Search, Move Items etc.
Diagnostic	Set the number and frequency of transaction for a device.

Setting	Description
Sizing	Set the frequency of SEG and API server interaction. Workspace ONE UEM recommends utilizing Delta Sync for policy updates as it minimizes the amount of data sent to SEG, thereby improving the performance. Delta sync is refreshed at a default time interval of ten minutes to ensure SEG has an updated policy set. This is particularly useful when multiple SEGs are in use, as there is a maximum of ten minutes where SEG will be out of sync with the UEM console.
S/MIME Options	
Skip Attachment & Hyperlink transformations for S/MIME signed emails	Select **Yes** to disallow the encryption of attachments and transformation of hyperlinks through SEG for emails signed with S/MIME certificates.
Enable S/MIME repository lookup	Enable this option to allow the automatic look up of the S/MIME certificate managed in a hosted LDAP directory Configure the S/MIME lookup settings before you begin the SEG installation.
LDAP URL	Enter the URL of your LDAP server.
Authentication Type	Select **Anonymous** or **Basic** authentication. In case of basic authentication, enter the **User Name** and **Password**.
Certificate Attribute	Enter the name of the LDAP attribute corresponding to the S/MIME certificate on the mail recipient object. For example, userCertificate; binary

8. To confgure more deployments, select the **Add** option from the Mobile Email Management Configuration screen to configure more deployments. The Mobile Email Management Configuration screen shows the list of the configured deployments.

   To download the SEG installer or test the connection later, select the  icon corresponding to the MEM configuration and select **Download SEG Installer** and **Test Connection** options.

Enable Basic Authentication

Basic authentication assures enhanced security as this authentication type requires users to provide a valid user name and password to access content. You can use the basic authentication to secure the Secure Email Gateway (SEG) endpoint with the UEM console and enhance the security when sending policy updates.

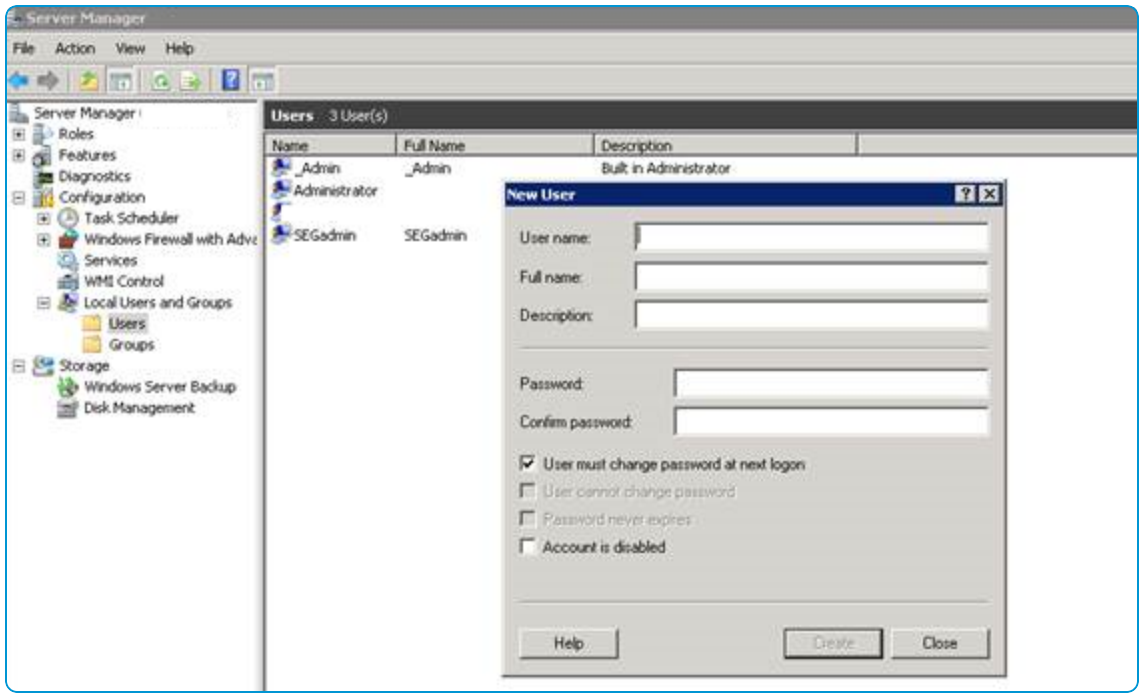
Procedure:

1. On the Secure Email Gateway server:

a. In the IIS Manager, expand **Default Web Site** and select **SEGConsole**.

b. Select **Authentication**, select Basic Authentication, and deselect **Anonymous Authentication**.

c. Navigate to **Server Manager** > **Local Users and Groups** > **Users**, and create a basic user name and password.



2. On the UEM console, when configuring the SEG deployment:
   a. Select the **Basic Authentication** check box.
   b. Enter the user name and password that you created in step c.

Install the SEG

After you download the SEG installer from the UEM console, run the SEG installer to start the SEG Setup Wizard. The SEG Setup Wizard helps you to complete the SEG Classic configuration

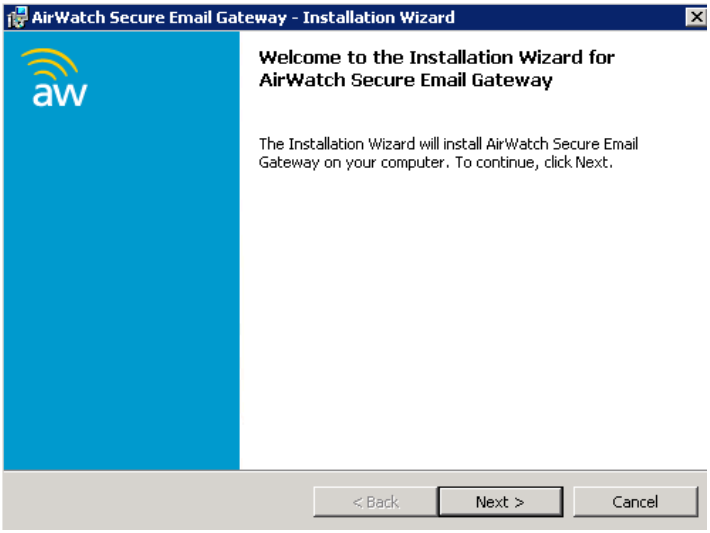
Prerequisites

- Disable User Account Control (UAC) for the installation process. However, you can re-enable UAC after the installation is complete. This is an environmental consideration that varies depending on the server deployment.
- Create an admin account for the SEG in the UEM console. This is required for the simple installation wizard. Configure the admin account at an organization group level at or above where you want to configure the SEG.

Procedure:

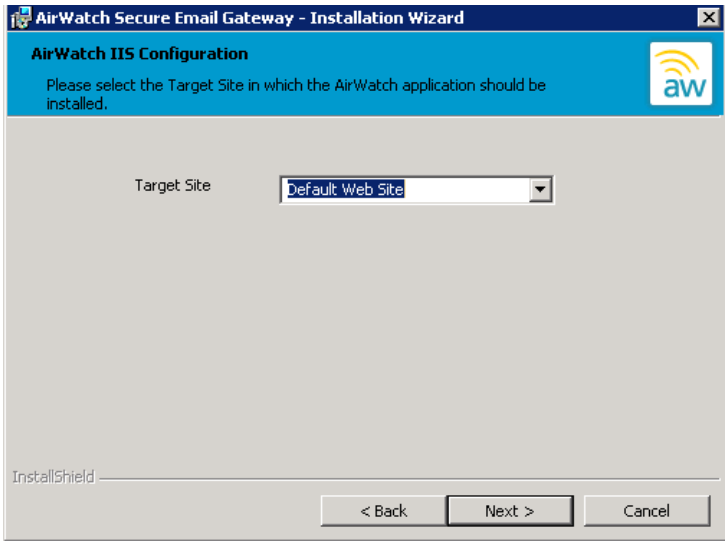
1. Double-click the **AirWatch SEG Installer.exe** file, or right-click to choose **Run as Administrator**. The **Setup** dialog box displays. If you receive a security warning choose **Run**.

   The Setup dialog box is followed by a **Welcome** dialog box. Click **Next**.

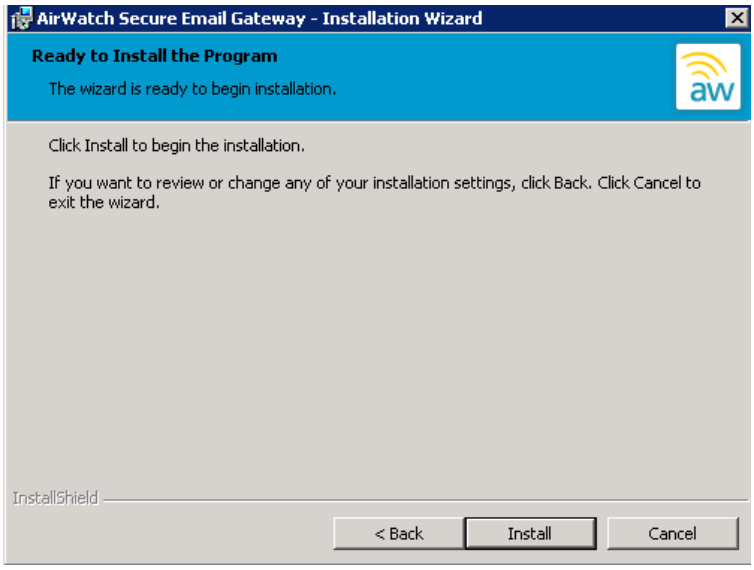


2. Accept the **End User License Agreement**, and then click **Next**.
3. Select the **Destination Folder** to install the SEG. The installer defaults to **C:\AirWatch**. However, for best performance, install Workspace ONE UEM on a partition separate from the OS.

4. Select **Default Web Site** as the IIS Website location for SEG in the **AirWatch IIS configuration** dialog box. Click **Next**.



5. Click **Install** to begin the SEG installation.



6. In the **SEG Installation Wizard** dialog box, click **Finish**. The **AirWatch SEG** setup shortcut icon is automatically created on the desktop, and the localhost URL opens in Explorer.

Configure the Classic Platform with the SEG Setup Wizard

The Secure Email Gateway (SEG) Setup Wizard starts automatically after you install SEG. The Setup Wizard helps you enable SEG server for Workspace ONE UEM Services, a proxy email server for email server communications, and configure SEG for specific deployments. You can also use the setup wizard to enable SEG clustering.

After the installation, if the **Secure Email Gateway Setup Wizard** does not start automatically, double-click the **SEG shortcut** icon on the desktop to open the wizard.

Note: The SEG setup wizard supports Internet Explorer 10 and later versions only.

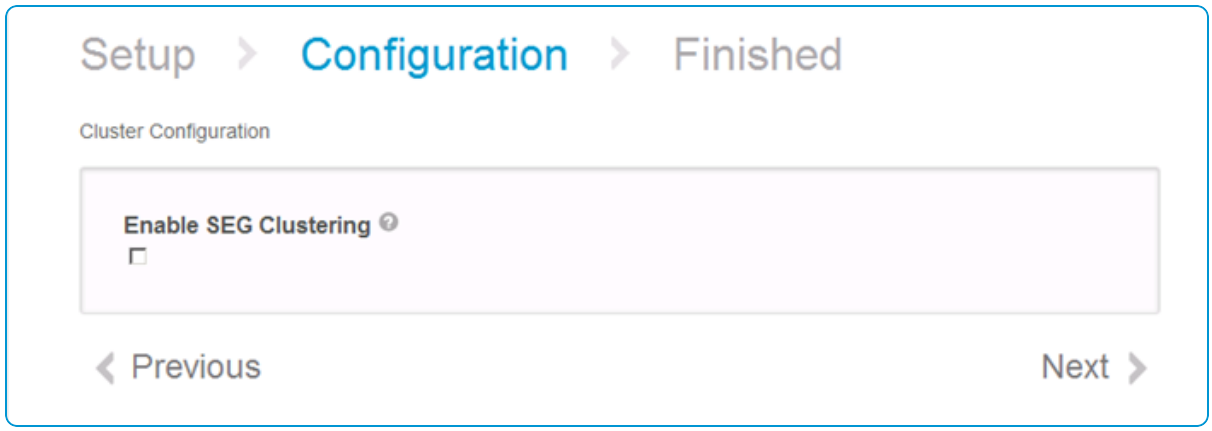
Procedure:

1. Specify the following information on the **Setup** page and click **Next**.
   - Enter the Workspace ONE UEM Server Host name that contains the API. This is usually the Workspace ONE UEM API Service URL.
   - Specify the SEG Admin Account **Username** and **Password** with the 'SOAP API General' role resource in UEM console that can be accessed from **Accounts** > **Administrators** > **Roles** > **Add Role** > **API** > **SOAP**. Create your SEG Admin Account at that organization group or at a level above the organization group where you want to configure the SEG.
   - If you have a proxy server, then enable **Proxy for AirWatch services communication**.
     - Enter the URL of the outbound **Proxy Host**.
     - Enter the **Proxy Port** number.
     - Choose the type of **Authentication**.
       - Anonymous Authentication. Unknown users can login based on the rights created by the admin
       - Basic Authentication. Enter the **Username** and **Password** to access.
   - If you have a proxy email server, then enable **Proxy for email server communication**.
     - Enter the URL of the proxy host server.
     - Enter the port of the proxy host server.
     - Select the type of authentication required to access this proxy server. Options include:
       - Anonymous Authentication. Unknown users can login based on the rights created by the admin.
       - Basic Authentication. Enter your username and password to access.
       - Windows Authentication. Enter windows credentials to access the server.
2. Configure the SEG for your specific deployment. Enter the following information:
   - Enter the Group ID of the SEG's organization group in the **Organization Group** field.
   - Select the MEM configuration from the drop-down menu.

3. Specify the following SEG Configuration settings and click **Next**. This information pre-populates with the setting that you have entered on the UEM console.

Settings	Description
Email Server **Email Server Hostname**	Select the Email Server type, Exchange version, and enter the Email Server Hostname for the SEG to communicate with your internal email servers.
Proxy web mail traffic through gateway	If you want to proxy webmail traffic in addition to EAS traffic through the SEG, select this check box.
Use Recommended Settings	Select this check box to capture all SEG traffic information from devices. Otherwise, specify the type of information and frequency at which the SEG can log for devices.
Ignore SSL errors With Email Server	Select this check box to ignore SSL errors created by certificates between the SEG and EAS server.
Rules Refresh Interval (min)	Enter the interval time, in minutes, for SEG to refresh rules.
Transfer Rate to Gateway (transactions) **Transfer Rate to Console (transactions)**	Set the transfer rate for the transactions happening between the SEG and the UEM console.
Friendly Name	Enter a **Friendly Name** to help identify the SEG in the logs.
Enable Real-time Compliance Sync	Select this check box so that the UEM console can send down compliance updates in a push-based mechanism instead of a periodically timed poll-based mechanism. This mechanism allows your compliance rule set to immediately update when actions occur instead at a specified rate.
Gateway Hostname	Specify the host name of the specific SEG Proxy server.

4. Select **Next** in the **Cluster Configuration** screen.



   If multiple SEG servers are load balanced, single policy broadcast messages apply to only one SEG. This includes the messages sent from the 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.

   SEG Clustering is also available to facilitate the sharing of single policy updates to all nodes of a SEG cluster.

   For more information on how to configure SEG clustering, see Classic Platform Clustering FAQs on page 37.

5. Select **Save** in the **SEG Service Settings** screen the to automatically restart the Integration service. The SEG Service Settings screen is a summary page that displays information such as Workspace ONE UEM Group, API Certificate, Certificate expiry date, and the log level. For troubleshooting purposes, select the **Log level** of the SEG Proxy server.

Any changes that were made to the SEG configuration are automatically updated in the console settings after the Setup wizard completes.

Upgrade the Classic Platform

Download the latest version of SEG from the UEM console and run the installer to upgrade your SEG.

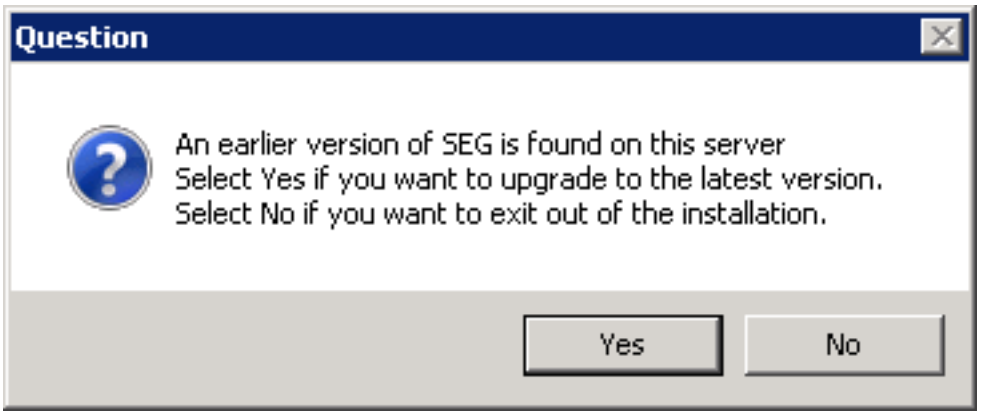
Prerequisites

- Run the MEM Configuration wizard again and associate the existing EAS profile to the SEG deployment.
- Download the SEG Installer from **Email** > **Settings** in the UEM console.

Procedure:

1. Double-click the AirWatch SEG Installer.exe file.

   The SEG Installer detects an earlier version is installed and prompts you to upgrade to the new version.



2. Select **Yes** and then select **Next**.
3. Select **Install** to begin the upgrade. The SEG Installer performs the SEG upgrade.
4. Select **Finish**.

Create Target Logs

The Secure Email Gateway (SEG) targeted logging enables you to create Verbose Web Listener logs for specific users or devices. These log files help troubleshoot issues in a large environment setup. For security reasons, the targeted logging is available only on the SEG server through 'localhost/SEGConsole'.

To target logs for specific device or user:

1. Log in to the SEG server and navigate to **http://localhost/segconsole**.
2. Select the required query from the options **EAS Device Identifier** and **Username** in the **Targeted Logging** screen.
3. If you want to add more devices or users, select **Add Target**.
4. Select **Start Targeted Logging** to begin the process.
5. Select **Stop Targeted Logging**. By default, logs are written to the **Logs** > **EASListener** folder.

Classic Platform Clustering FAQs

The answers to some of the questions regarding SEG Clustering and the troubleshooting steps to follow in case of an error are listed here.

How do I enable SEG clustering?

You can enable SEG clustering while configuring SEG with the **Secure Email Gateway Setup Wizard**. In the SEG Setup Wizard:

1. Enter the setup details in the **Setup** page and select **Next**.
2. Enter the configuration settings details in the **Configuration** page and select **Next**. The **Cluster Configuration** page appears.

   To know the setup details and configuration settings that must be entered, see steps 1-3 of Configure the Classic Platform with the SEG Setup Wizard on page 34.
3. Select the **Enable SEG Clustering** check box.
   a. Specify the name you want to assign to the cluster in the **Cluster Directory Name** field.
   b. Define the default port for the SEG servers to communicate with each other in the **Default Port** field.
   c. Specify the host name of each SEG server in the cluster in the **Node Address** field.
4. Select **Next** when complete.

What is the app cluster directory XML?

The AppClusterDirectory.xml file (located in the same directory as the AW.Eas.IntegrationService.exe service) is created upon successful completion of the SEG setup process when clustering has been enabled. During the initial configuration, the first entry in the AppClusterDirectory.xml file is the master SEG. This file references other servers in the cluster, and is of the form as shown below (change node address, name, and port as needed):

```
<?xml version="1.0"?>
<applicationClusterDirectory name="Secure Email Gateway" port="9090">
<node address="servername1" name="seg@servername1" />
<node address="servername2" name="seg@servername2" />
</applicationClusterDirectory>
```

The value “name” in the initial applicationClusterDirectory tag reflects the name of the cluster as defined during configuration, and any changes to this will be reflected in different clusters being created. For example, if SEG1 is a member of SEG Cluster name= “SEG1” and SEG2 is a member of SEG Cluster name= “SEG2”, these two SEGs will never initiate communication.

Note: The value "name" will not be updated if a new SEG server is elected master.

What happens if the master SEG goes down?

If the master SEG goes down, all other SEGs in the cluster initiate a 'voting process' to elect a new master SEG. This process is initiated after the SEGs miss the maximum number of 'heartbeats' from a particular server; in this case the master SEG server. Once a new master is chosen, the cluster has successfully recovered and functionality returns to a steady state for all SEGs that are in active communication.

At this point, though the master SEG is not shown in the first position in the AppClusterDirectory.xml file, the EAS Integration service logs that a new master has been chosen and specify that SEG.

If a slave server goes down, it is removed from the cluster, and the slave server stops receiving or sending updates to the other members of the cluster.

How should the SEGs be re-clustered in the event the cluster breaks?

Clustering issues are typically seen when communication between the SEG servers is broken. In such scenarios, perform the following steps:

1. Verify if the EAS Integration Service is configured properly for clustering on all servers.
   - EAS Integration Service Config file (\AW.Eas.IntegrationService\AW.Eas.IntegrationService.exe.config):
     - In the configSections section, the cacheConfiguration field should be set equal to 'Clustered'.

```
<clusterConfiguration nodeAddress="servername1" nodeName="seg@servername1"
directoryLocation="AppClusterDirectory.xml" sharedKey="AirWatch"/>
<cacheConfiguration cacheType="Clustered" />
```

2. Choose one of the SEG servers to be the master SEG.
   - Verify cluster name and port details of the chosen SEG in the AppCluster Directory.xml
   - Add the node address of the chosen SEG in the AppCluster Directory.xml. This should be the only node listed in the AppCluster Directory.xml.
3. Restart the EAS Integration Service for the chosen SEG server. This SEG server now becomes the master node.
   - **Verification** - In the Integration service log file for this SEG server, verify if this server joins the cluster as the Master.
4. For all the other SEG servers:
   - Verify cluster name and port details in the AppCluster Directory.xml
   - Configure the AppClusterDirectory.xml identical to the master SEG. This means the AppClusterDirectory.xml of other SEG servers should only show the master SEG listed in it.
5. Restart the EAS Integration Service for the other SEG servers in the cluster.
   - These SEG servers now act as slave nodes and seeks the master node. The AppClusterDirectory.xml lists the information of the master SEG and the slave SEG servers.
   - **Verification**:
     - In the Integration service log file for each SEG server, verify if the server joins the cluster as a Slave server.
     - Verify if the AppClusterDirectory.xml is updated with information regarding all servers in the cluster, with the Master node on top of the server list.

Monitoring the cluster

After re-clustering the SEGs:

1. Monitor if the AppClusterDirectory.xml is identical across all SEG nodes.
2. Monitor the Integration service log files for each SEG server to check if any errors pertains to the following:
   - Communication errors between the SEG servers.
   - Policy update errors (perform a manual update of policies from the SEG console or UEM console).
3. Enter the command *netstat -an | find "9090"* to return a listener for both TCP and UDP.

What is the best practice for upgrading clustered SEGs?

To ensure the cluster is stable post upgrade, stop the integration service on all SEGs, then start the integration service on each SEG one by one (beginning with the first node in the AppClusterDirectory.xml). After starting the service on each SEG, check EAS Integration Service Logs (Verbose) to ensure the SEG joins the cluster. See How should the SEGs be re-clustered in the event the cluster breaks? for more detail.

> **Note:** While the integration service is not running, SEG falls back to the default setting in the Web Listener web.config file.

Compare SEG Policies

The Device Policies feature provides troubleshooting of clustered SEGs.

From the SEG console (localhost), you can download a file listing all devices that the SEG allows for email receipt. You can compare this list between the clustered SEGs to determine if the device policy sets are in line with one another.

1. Login to the SEG server and navigate to 'http://localhost/segconsole'.
2. Select **Export Device Policies** from the Device Policies section. The .csv file gets downloaded to the default location.
3. Select **OK**.

Chapter 5:
Email Management

Email Security with Email Policies

Email policies enhance security by restricting access based on the device status and general mail client characteristics. These policies allow for granular control over the devices that are approved for accessing email.

Important: a. Mail client compliance is not supported on Windows Phone.
b. The Sync Settings policy is not applicable for SEG V2 architecture.

General Email Policies

The general email policies used to restrict email access to devices are listed in the following table.

Email Policy	Description
Sync Settings	Prevents 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, you must republish the EAS profile to the devices as this forces devices to re-sync with the email server.
Managed Device	Restricts email access only to managed devices.
Mail Client	Restricts email access to a set of mail clients.
User	Restricts email access to a set of users based on the email user name
EAS Device Type	Allow or block devices based on the EAS Device Type attribute reported by the end-user device.

Managed Device Policies

The managed device policies that restricts email access to devices based on factors such as device status, model and operating system are listed in the following table.

Email Policy	Description
Inactivity	Prevents inactive and managed devices from accessing email. You can specify the number of days a device shows up as inactive before email access is disabled. The minimum accepted value is 1 and maximum is 32767.
Device Compromised	Prevents compromised devices from accessing email. Note that this policy does not block email access for devices that have not reported compromised status to AirWatch.
Encryption	Prevents email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to AirWatch.
Model	Restricts email access based on the platform and model of the device.
Operating System	Restricts email access to a set of operating systems for specific platforms.
Require ActiveSync Profile	Restricts email access to devices whose email is not managed through an Exchange ActiveSync profile.

Email Security Policies

The email security policies that take actions against devices accessing attachments and hyperlinks are listed in the following table.

Email Policy	Description
Email Security Classification	Define actions for SEG to take against emails that are with or without security tags. You can either use predefined tags or create your own tags. You can enable restricted access to AirWatch Inbox and VMware Boxer based on these tags and define the default behavior for other email clients. You can either allow or block emails. If you choose to block emails, you can replace the email contents with a helpful message using the available templates configured at Message Template settings. These configured templates can be selected from the Select Message Template drop-down menu. Also, lookup values are not supported for Block Email message template.
Attachments (managed devices)	Encrypt email attachments of selected file type with an encryption key unique to the device - user combination. These attachments are secured on the device and are only available for viewing on the VMware Content Locker. This is only possible on managed iOS, Android, and Windows Phone devices with the VMware Content Locker application. For other managed devices, you can either allow encrypted attachments, block attachments, or allow unencrypted attachments.
Attachments (unmanaged devices)	Allow encrypted attachments, block attachments, or allow unencrypted attachments for unmanaged devices. Attachments are encrypted for unmanaged devices to prevent data loss and maintain email integrity. The attachments of unmanaged devices cannot be opened in VMware Content Locker.

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. The Modifications Types are All, Include, and Exclude. • **All** - Allows device users to open all the hyperlinks with VMware Browser. • **Include** - Allows device users to open only the hyperlinks 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** - Does not allow the device users to open the mentioned excluded 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.

Note: Enable the **Test Mode** option on the Email Dashboard to test the compliance capabilities of the email policies even before applying the polices on the devices.

Activate Email Compliance Policy

Email compliance policies help to restrict email access to unmanaged, non-compliant, unencrypted, or inactive devices.

Procedure:

1. On the UEM console, navigate to **Email > Compliance Policies**. By default, the policies are disabled and are denoted by red color under the **Active** column.
2. Select the gray button under the **Active** column to activate the compliance policy.
3. Depending on the email policy that you want to activate, additional pages appear where you can specify your choices. Select **Save**.
4. The policy is activated and is denoted by green color under the **Active** column. Use the edit policy icon under the **Actions** column to allow or block a policy.

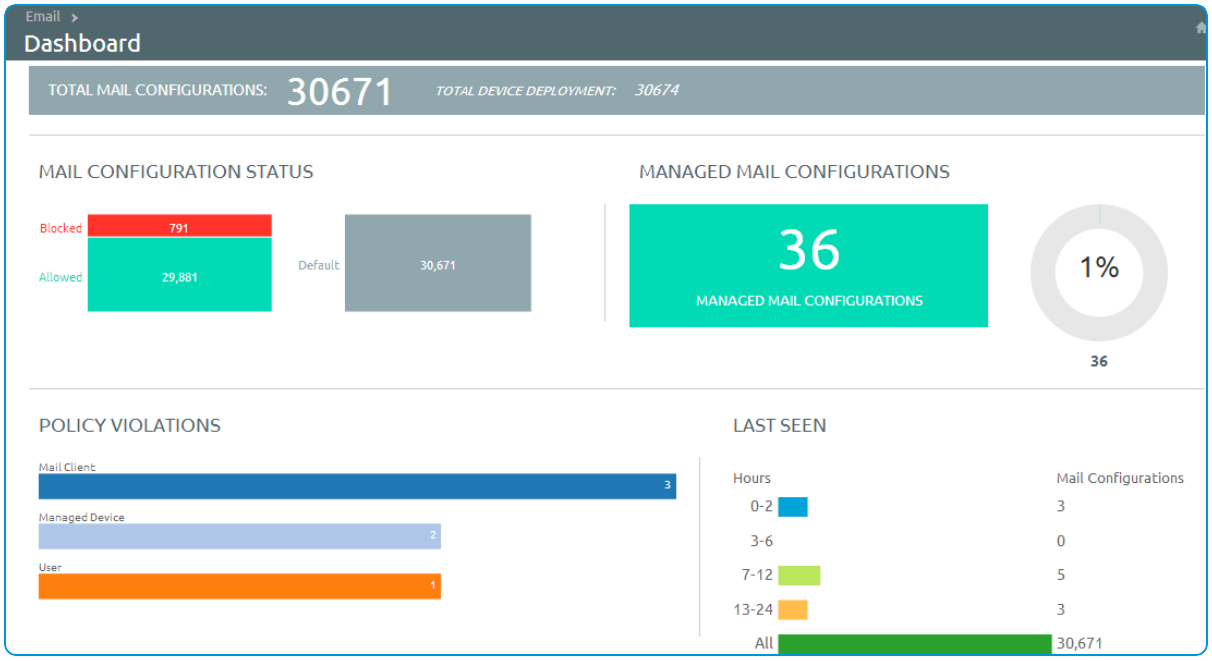
Email Dashboard

The **Email Dashboard** helps you to gain visibility into the email traffic and helps monitor the devices.

Email Dashboard gives you a real-time summary of the status of the devices connected to the email traffic. You can access the Dashboard from **Email > Dashboard**. From the Email Dashboard, you can access the List View page that helps you to:

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

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



List View

The List View page on the UEM console helps you to view all the real-time updates of your end user devices that you are managing with VMware AirWatch Mobile Email Management (MEM).

The List View page enables you to:

- View the device or user specific information by switching between the Device and User tabs.
- Search and narrow down a device using the Filter option.
- Change the layout to either view the summary or the detailed list of the device or user information based on your requirement.
- Perform multiple actions such as run compliance and sync mailboxes on the device.

Device and User Details

Switch between the Device and User tabs on the List View page to view the information about device and user. The Layout drop-down menu provides the option to display the information as a summary or as a detailed list.

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

Note: In the Email Dashboard, an iOS device shows mailbox record if at the time of enrollment a native email client is already configured on the device or when an EAS profile is pushed for other email clients. An Android device shows mailbox record when a device enrolls or when the email clients are installed on the enrolled device with the exception of AirWatch Inbox.

Filters for Quick Search

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

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

Perform Actions

The **Override**, **Actions**, and the **Administration** drop-down menu provides a single location to perform multiple actions on the device. Note that these actions once performed cannot be undone.

Override

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

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

Actions

- **Run Compliance** - Triggers the compliance engine to run for the selected MEM configuration.
- **Enable Test Mode** - Test email policies without applying them on devices. Once enabled, you can view a message displaying Test Mode Enabled on the List View screen. The enabling /disabling Test Mode does not require you to run compliance engine.

Administration

- **Dx Mode On** - Runs the diagnostic for the selected user mailbox.
- **Dx Mode Off** - Turns off the diagnostic for the selected user mailbox.
- **Update Encryption Key** - Resets the encryption and the re-syncs the emails for the selected devices.
- **Delete Unmanaged Devices** - Deletes the selected unmanaged device record from the dashboard. This record may reappear after the next sync.

Configure and Deploy Email Profile

Exchange ActiveSync (EAS) is a communication protocol designed for email, calendar, and contacts synchronization between the email server and the mobile devices. Configure the EAS profile on the UEM console such that the devices fetches the mails through the SEG server instead of the EAS server.

Procedure:

1. Navigate to the **Devices** > **Profiles & Resources** > **Profiles** on the UEM console, and then select **Add** to create a new profile.
2. Select a device platform. If you are leveraging the SEG for multiple device OS's then you must create a similar profile for each platform.
3. Enter the information about the profile on the **General** tab and assign the profile to the applicable organization groups and smart groups. Keep the assignment type as **Auto** or **Optional**.
4. Select **Exchange ActiveSync** and select **Configure**. From here, configure the following parameters to access corporate mail through the SEG:
    - Select the **Mail Client** that your organization intends for end users to utilize from the drop-down menu.

- Ensure that the **Exchange ActiveSync Host** is the host name of the SEG server and not the Exchange server.
- Make sure to leverage lookup values so each user can get their own distinct email.

  Leave the **Password** field blank. This prompts the end user to enter a password after the profile is installed on the device.

5. Click **Save and Publish** to begin using secure mobile email. Create additional profiles for each device platform for which you want to provision mobile email.

Chapter 6:
SEG Migration (Classic)

Migration to SEG (V2 Platform)

Migrating the SEG from the Classic platform to the V2 platform is simple, as the existing SEGs continue to function without interruption to the end-user experience.

You must first update the Mobile Email Management (MEM) configuration in the console in order to support the V2 platform. You can update the MEM configuration in one of two ways:

- **Create a new MEM configuration** - To create a new MEM configuration, see Configure the V2 Platform on page 12. If you use the same external URL there can be some delay in the policy updates. This delay is reconciled as part of the regular SEG policy refresh as configured in the advanced settings. After configuring the V2 platform, you can disable or remove the existing configuration.
- **Upgrade an existing configuration** - You can edit the existing SEG configurations and upgrade it to include the necessary settings for the V2 platform. This migration maintains the existing Classic configuration settings and does not affect the existing SEG servers.

You can upgrade your existing SEG software to the V2 platform without interrupting the current SEG functionality. To upgrade, run the installer for the SEG V2 platform on the existing SEG server. After completing the installation, disable the World Wide Publishing service and restart the SEG service. This action transfers the device connections, refreshes the 443 listener from IIS, and allows the new SEG service to claim it. You can also run the V2 platform on a distinct port and connections transferred over at the network layer.

To verify the SEG has properly restarted, check whether the localhost returns your IP address on the proper port.

Attempt to access the Classic platform (IIS) displays the following screenshot:

The V2 platform displays the following screenshot:

Migrate to SEG V2 with Google

You can migrate from the Classic SEG that is integrated with Google to SEG V2. SEG V2 does not support the credential impersonation as Classic SEG. Instead, SEG V2 uses the IP restriction that is configured in the Google Admin console. To support use-cases where users do not know their passwords, Workspace ONE can still provision passwords directly to devices. The information provided in this section helps you migrate from Classic SEG to SEG V2 with Google without service interruptions for your users.

Prerequisites

- Upgrade MEM configuration to SEG V2.
- Install SEG V2.
- Classic SEG services are not switched.

  For more information about migrating to SEG V2, see the *Migration to SEG (V2 Platform)* section of the *VMware AirWatch Secure Email Gateway Guide*.

Configure IP Restriction on Google Admin Console

Configure Google Sync to accept traffic only from SEG. Restricting the communication to SEG ensures that the devices that attempt to bypass SEG are blocked.

1. Log into the Google Admin console.
2. Navigate to **Device Management** > **Advanced Settings** > **Google Sync** .
3. Select the **IP Whitelist** text box and enter the external SEG IPs that you want to whitelist.
4. Select **Save**.

Configure Automatic Password Provision and Sync Passwords

When migrating from Classic SEG with Google to SEG V2 with Google, you are provided with an Automatic Password Provision feature. You can enable or disable the Password Provision as per your requirement.

1. Navigate to **Email > Email Settings** and select **Configure**.The **Add Email Configuration** wizard displays.
2. Select **Add**. The wizard displays Platform tab.
   a. From Deployment Model, select **Proxy**.
   b. From Gateway Platform, select **V2**.
   c. From Email Type, select **Google** and select **Next**. The Deployment tab opens and displays the basic settings.
3. In the Google Apps Settings section, you can see that the Automatic Password Provision is in Enabled mode. This is because Classic SEG uses Automatic Password Provision when integrating with Google.
   a. If you are providing the SSO password and Google password to your device users, select **Disable**. The users must enter their credentials to access Google. When the automatic password management is disabled, the Google Sync password is managed within your organization, which provides more flexibility and control over the devices accessing Google.
   b. If you want to use password provision using the UEM console, keep the Automatic Password Provision **Enabled**. The information you have entered when configuring Classic SEG with Google is used to provision the Google Sync Password. The password provisioning works without any interruptions to the user experience.
4. After selecting the required Automatic Password Provision setting, select **Next** to navigate through the wizard and select **Finish**.
5. If you have disabled the Automatic Password Provision setting, navigate to the device List View and select **Actions** drop-down menu.
6. Select **Sync Passwords** to synchronize the passwords on the device and Google Sync server. If you have kept the Automatic Password Provision enabled, the Sync Passwords function is not available from the Actions drop-down menu.
7. To switch to SEG V2 with Google, restart the SEG service. For more information on stopping Classic SEG and starting SEG V2 service, see SEG Migration (Classic) on page 49.