Secure Email Gateway (SEG) V2

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

Contents

Introduction to the Secure Email Gateway(V2)

The Workspace ONE UEM powered by AirWatch Secure Email Gateway V2 (SEG V2) helps to protect your mail infrastructure and enables VMware AirWatch Mobile Email Management (MEM) functionalities. Install the SEG along with your existing email server to relay all ActiveSync email traffic to Workspace ONE UEM-enrolled devices.

Based on the settings you define in the Workspace ONE UEM console, the SEG filters all communication requests from individual devices that connect to SEG.

Note This guide contains information about the SEG V2. The SEG Classic software is being discontinued and end of life has been announced. The Classic Secure Email Gateway (SEG) installer will reach End of General Support on May 5, 2019. On December 24, 2018, the Classic SEG installer will be removed from the Resources portal. After May 5, 2019, VMware cannot guarantee full support for Classic SEG. For more information about the End-of-Life terms, see https://kb.vmware.com/s/article/2960293.

Note To read about the Classic SEG information, see the *VMware AirWatch Secure Email Gateway 1811 guide* at https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/WS1-Secure-Email-Gateway/GUID-AWT-SEG-CLASSIC-REQS.html.

Secure Email Gateway Architecture

2

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 the 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.

The SEG is an On-Premises component that you install as part of your own organization's network. The SEG Proxy model requires an Exchange ActiveSync infrastructure. For example, Microsoft Exchange, 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.
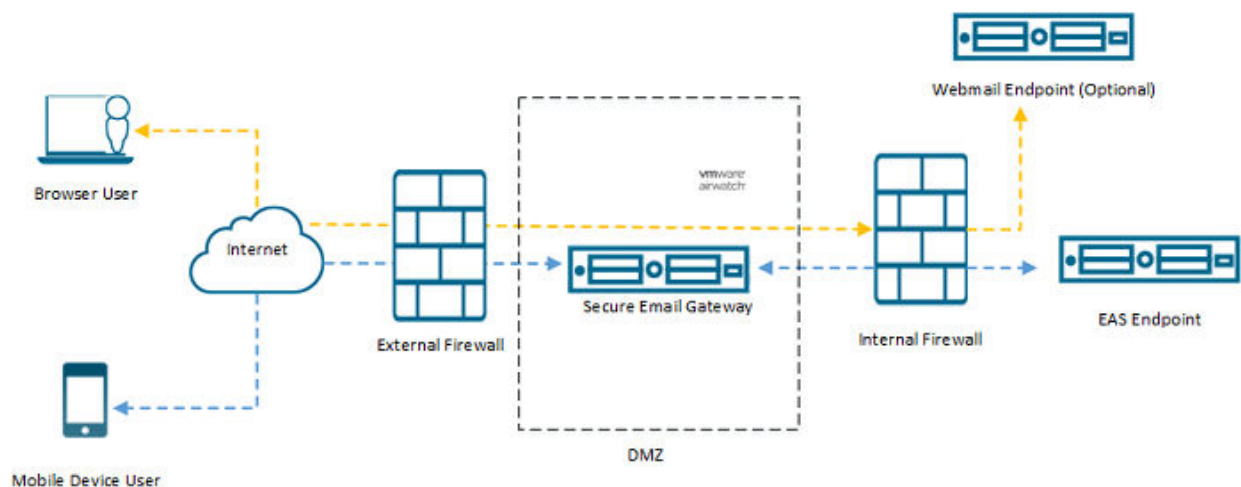
Alternative Supported Setup: Exchange ActiveSync SEG Using Optional Reverse Proxy Configuration
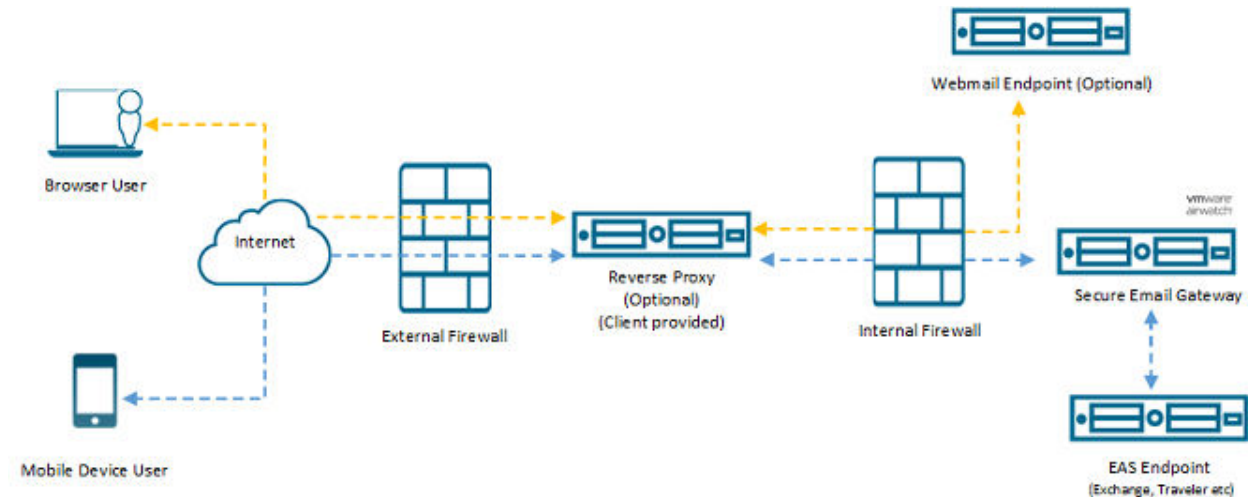
The reverse proxy configuration uses an optional reverse proxy to direct mobile device users to the SEG Proxy while routing browser users directly to their webmail endpoints. Use the following network configuration to set up the reverse proxy to communicate between devices and the SEG using the Exchange 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 the reverse proxy server. You can set up load balancing between the SEGs and the reverse proxy, but ensure that you 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.

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.

Hardware, Software, and Networking Requirements for Secure Email Gateway (V2)

You must meet the UEM Console requirements as well as the hardware, software, and network recommendations to successfully deploy the SEG.

UEM Console Requirements

- AirWatch Console 9.0.3 or later

- REST API must be enabled for the Organization Group type, Customer.

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 SEG V2 at a container organization group that inherits the REST API settings from a customer type organization group.

Hardware Requirements

A SEG V2 server can be either a virtual or physical server .

Note the following when deploying SEG V2:

- 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 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 8 GB RAM can be supported by either:

  - One single SEG server with 4 CPU cores and 8 GB RAM.

  - Two load-balanced SEG servers, each with 2 CPU cores and 4 GB RAM.

- 5 GB disk space needed per SEG and dependent software. This does not include system monitoring tools or additional server applications.

Software Requirements

- 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 (Device Services (DS) or Console Server (CN) server)	HTTP or HTTPS	80 or 443	SEG retrieves the configuration and general compliance policy information
SEG	Internal hostname or IP of all other SEG servers	TCP	5701 or 41232	If SEG Clustering is used, then SEG communicates to shared policy cache across other SEGs for updates and replication.
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.

This chapter includes the following topics:

- Configuring for High Availability and Disaster Recovery

- Configure the SEG V2

- Install the Secure Email Gateway (V2)

- Configure SEG V2 Compliance for Email Notification Service

- Device Discovery

- SEG V2 Admin Page

- Upgrade Secure Email Gatewayto Secure Email Gateway V2

Configuring for High Availability and Disaster Recovery

SEG can be configured in high availability and disaster recovery environments with both clustering and non-clustering server configurations.

Following are the benefits of using SEG in Clustering and Non-Clustering server environments:

- Non-Clustered Server Configuration

    - Each SEG is updated independently.

    - Failover can be performed at load balancer.

    - External URL can be the same across servers and device EAS profiles.

- Clustered Server Configuration

    - Each data center uses a distinct MEM Config with distinct external URL and distinct cluster.

    - Device EAS profiles should use a third URL that can be failed-over between data centers.

Note   Workspace ONE UEM recommends using SEG in non-clustered server configurations.

Configure the SEG V2

To implement the SEG (V2) for your email architecture, first configure the settings on the UEM console. After you configure the settings, you are provided with a link to download the SEG installer.

SEG can be configured in high availabilty and disaster recovery environments with both clustering and non-clustering server configurations.See Configuring for High Availability and Disaster Recovery.

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:

    a   Select **Proxy** as the **Deployment Model**.

    b   Select **V2** as the **Gateway Platform**.

    c   Select the **Email Type**.

    d   Select the **Email Server** from the drop-down menu and then select **Next**.

        Example of Email Servers are Exchange, IBM Notes, or Google.

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. The default 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. This setting is used when you do not have the certificate at the time of configuring the MEM config.
SEG Server SSL Certificate	Select **Upload** to add the certificate that binds to the listening port. The SSL certificate can be automatically installed instead of providing it locally. An SSL certificate in the .pfx format with a full certificate chain and private key included must be uploaded.
Email Server URL and Port	Enter the email server URL and port number in the form `https://email server url:email server port`. This is the URL which the SEG uses for proxying email requests to the email server.
Ignore SSL Errors between SEG and email server	Select **Enable** to ignore the Secure Socket Layer (SSL) certificate errors between the email server and the 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 the SEG server. Establish a strong SSL trust between Workspace ONE UEM and the SEG server using valid certificates.
Allow email flow if no policies are present on SEG	Select **Enable** to allow the email traffic if the SEG is unable to load the device policies from the Workspace ONE UEM API. By default, the SEG blocks all email requests if no policies are locally present on the SEG.

Setting	Description
Enable Clustering	Select **Enable** to enable clustering of multiple 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 VMware. 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 Summary tab of the Add Email Configuration wizard, review the configuration that you have just created. Select **Finish** to save the settings.

6   To download the SEG installer, click the link that appears in the SEG Proxy Settings section.

7   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 MEM Configuration screens shows options for **Add**, **Edit**, **Advanced**, and **Test Connection**. These options allow you to add another configuration, edit the current configuration, configure advanced settings, and test the connection between SEG, web, and the Workspace ONE UEM API servers.

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.
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.
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.

Setting	Description
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
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 (V2)

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

If Java Runtime Environment (JRE) is not already installed on your system, the SEG installer prompts you to install JRE during the SEG installation.

Procedure

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**.

3   Click **Next** to install the SEG to the default folder **C:\AirWatch** or click **Change** to choose a different folder.

4   Click **Yes** to install the JRE.

5   Enter the **AirWatch API Information** and click **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.

Settings	Description
Admin Password	Enter the password for the Admin Username.
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.

6   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. Click**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	User name and password for proxy authentication.
Password	These fields are available once you select the **Does the proxy require authentication credentails?** check box.

7   (Optional) Click **Browse** to upload the SSL Certificate, enter the **Certificate Password** and then click **Next**.

You can skp this step if the SSL certificate was already uploaded.

8   Click **Install** to begin the installation. The InstallShield Wizard takes a few minutes to install the SEG.

9   Click **Finish** to exit the **AirWatch Secure Email Gateway - InstallShield Wizard**.

Configure SEG V2 Compliance for Email Notification Service

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

Both Cloud and On-premises ENS deployments are supported by SEG. SEG listens to the EWS traffic from ENS using /EWS endpoints, 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.

Procedure

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.

Device Discovery

Before you can begin managing devices from the **Email Dashboard**, the configured MEM should discover the devices enrolled to the organization group. Depending on whether a device has an EAS profile or not, either a command or a broadcast message is sent to discover the devices.

With EAS profile

Workspace ONE UEM sends an allow command to the relevant EAS profile associated Secure Email Gateway server. The server then automatically starts connecting to the device.

Without EAS profile

Workspace ONE UEM sends a broadcast message stating that a device has enrolled. Workspace ONE UEM sends this message to all the SEG Proxy servers configured at the same organization group to which the device has enrolled. As soon as the device connects to a particular SEG server, the SEG recognizes the device as managed from the broadcast message sent earlier. The SEG Proxy then reports the device as discovered with its *memConfigID* to Workspace ONE UEM . MEM then associates the enrolled device to that *memConfigID* and displays it on the **Email Dashboard**.

SEG V2 Admin Page

You can use the SEG V2 Platform Admin page to perform 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 logging levels for the different SEG processes

- Call diagnostics endpoints

- Reconfigure the connections between SEG and API endpoints

The admin page displays the following tabs: Logging, Health, and Diagnostics.

Logging

Information related to the SEG processes are recorded in various log files. The amount of information logged can be controlled by setting the logging level of the log file. On the logging page, you can adjust the logging level and the duration of that logging level. The following logging levels are available: All, Trace, Debug, Info, Warn, Error, and Off. The duration drop-down is to specify how long an elevated logging level will persist before reverting to it's default level. Durations ranges can be set from a few minutes up to never reverting back to the default level

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

Settings	Description
Transaction Summary	Logs overview information of each email request that passes through the SEG including information such as user, HTTP response code and request processing time.
Device Transactions (All)	Logs detailed information about individual EAS requests including allow or block reasons and HTTP headers.
Kerberos Service Manager	Logs information from the Kerberos service manager.
Ews transactions (All)	Logs detailed information of each EWS request served by the SEG.
Ews Transaction Summary	Logs overview information of each EWS request served by the SEG.
Device Transactions (Blocked)	Logs detailed information about individual EAS requests including allowed or blocked reason and HTTP headers for blocked devices.
Policy Cache	Logs information on the state of the policy cache.
Policy Updates	Logs information related to real-time and bulk policy updates.
Console Transaction Reporting	Logs information about reporting data used by MEM dashboards in the UEM console.
Content Transformation	Logs details related to content transformations.
Certificate Authentication	Logs information related to certificate validation and retrieval of the UPN.

Diagnostics

On the Diagnostics page you can view diagnostic information for the SEG as well as invoke diagnostic endpoints to see other SEG related information such as the SEG configuration settings, look up the policies in the SEG cache, and download records related to specific policy types.

To use these endpoints, enter the API endpoints as shown in the below table into the REST API URI field on the diagnostic page and click the GET button. Information related to the endpoint will either be displayed in the text area on the diagnostics page or a `.csv` file of the information will be downloaded.

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.
`/cache/<Policy Type>/`	Download records related to policy types including devices, accounts, managed attachments, unmanaged attachements, and 451 redirect mappings.

TThe following table contains policy types and their respective lookup keys you use to view these 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.

Upgrade Secure Email Gatewayto Secure Email Gateway V2

You can upgrade from an older version of SEG that is installed on your system to SEG V2.

Prerequisites

■ You must have an older version of SEG already installed on the host machine.

■ Ensure that the installer for latest version of SEG V2 is available on the host machine.

■ MEM configuration for SEG V2 is available

Procedure

1 Run the VMware AirWatch Secure Email Gateway installer as an administrator.

   The install wizard verifies the existing installation and displays a popup notifying the user about the upgrade.

2 Follow the instructions on the install wizard and accept the End User Licence Agreement and click **Next**.

3 You may be prompted to upgrade to a new version of JRE. Follow instructions to reboot immediately or to reboot manually later.

4 Verify the Workspace ONE UEM API information.

Settings	Description
HTTPS	Select the check box if the protocol Workspace ONE UEMAPI server is https.
API Server Hostname	The URL of your Workspace ONE UEM API server. This is required to fetch the SEG configuration from the UEM console.

Settings	Description
Admin Username	The user name of a Workspace ONE UEM Admin user account, that was used during earlier installation.
Admin Password	Masked entry for password of Workspace ONE UEM Admin user account.
MEM Config GUID	The unique ID of your Mobile Email Management configuration. This is shown on the MEM configuration page on the UEM console.

5 (Optional) If Outbound Proxy was selected, verify the related information.

Settings	Description
HTTPS	Check if the protocol proxy is HTTPS.
Proxy Host	Address of the proxy host.
Proxy Port	Proxy port number.
Username Password	User name and password for proxy authentication. **Note** This option is displayed only if you had checked **Does the proxy require authentication credentials?** option

6 (Optional) If you had chosen to upload the SSL certificate locally when configuring the console MEM settings, upload the certificate and enter the certificate password.

7 Click **Install** to begin the installation.

Email Management

4

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.

Note

- Mail client compliance is not supported on Windows Phone.

- 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 VMware AirWatch.

Email Policy	Description
Encryption	Prevents email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to VMware 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 VMware AirWatch Inbox and Workspace ONE 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 AirWatch Content Locker. This is only possible on managed iOS, Android, and Windows Phone devices with the VMware AirWatch 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 AirWatch 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.

This chapter includes the following topics:

■   Activate Email Compliance Policy

- Email Dashboard

- List View

- Configure and Deploy Email Profile

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.

   Depending on the email policy that you want to activate, additional pages appear where you can specify your choices.

3 Select **Save**.

Results

The policy is activated and is denoted by green color under the **Active** column.

What to do next

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.
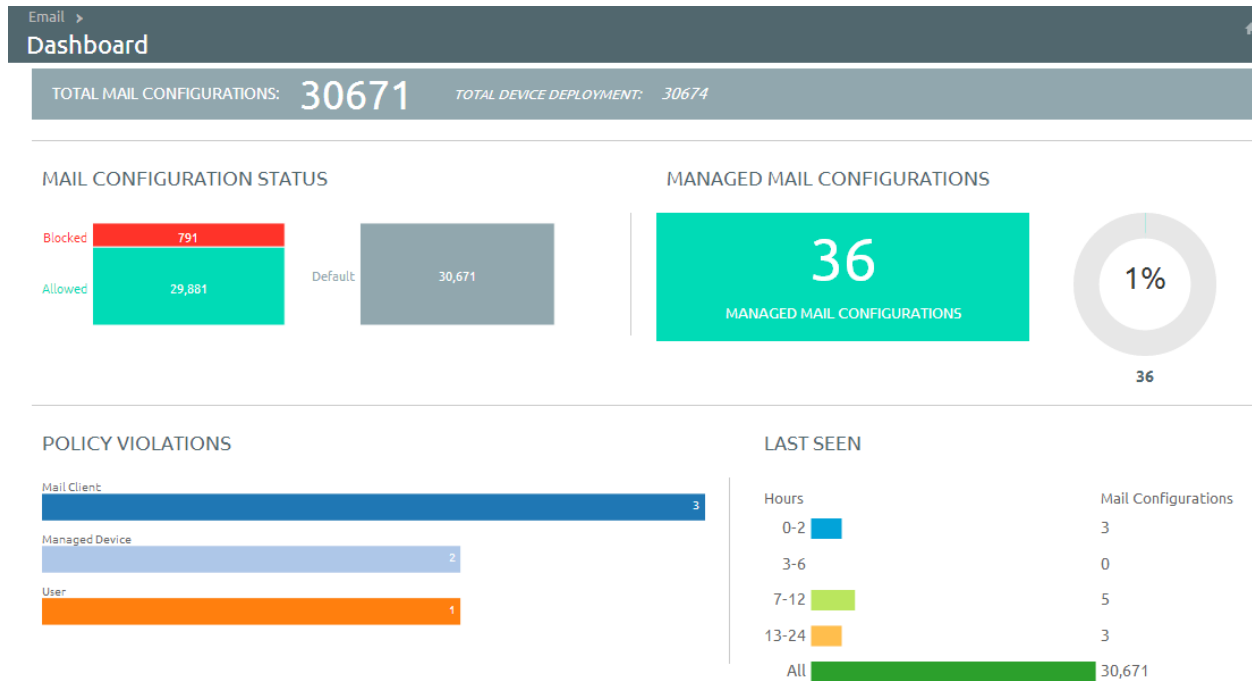
List View

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 operating systems, 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**. Configure the following parameters to access corporate mail through the SEG.

   a Select the **Mail Client** that your organization intends for end users to utilize from the drop-down menu.

   b Ensure the **Exchange ActiveSync Host** is the host name of the SEG server and not the Exchange server.

   c 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.

What to do next

Create additional profiles for each device platform for which you want to provision mobile email.

SEG Migration (Classic)

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** - 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:

This chapter includes the following topics:

- Migrate to SEG V2 with Google

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.

Procedure

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.

Procedure

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.

- 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.

- 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.