Secure Email Gateway (SEG) V2

VMware Workspace ONE UEM

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

https://docs.vmware.com/

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

Contents

Introduction to the Secure Email Gateway (V2)

1

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.

Requirements for the Secure Email Gateway (V2)

To successfully deploy the SEG, you must meet the UEM console requirements, hardware requirements, software requirements, and network recommendations.

UEM Console Requirements

- All currently supported UEM console versions. See the Workspace ONE UEM console release and End of General Support Matrix document for more details on the currently supported versions.
- REST API must be enabled for the 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 Workspace ONE UEM gets the API certificate from the REST API URL, that is, on the site URLs page located at **Groups & Settings > All Settings > System > Advanced > Site URL**. For SaaS deployments,the API URL must be in the `asXX.awmdm.com` format.

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 (preferred) 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 the 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
- Windows Server 2019

Networking Requirements

The SEG uses the following default ports:

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

Source Component	Destination Component	Protocol	Port	Description
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 and 41232	If SEG Clustering is used, then SEG communication 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 accessible from the browser on the SEG server and prompts for the credentials. `http(s)://<Exchange-Server-FQDN>/Microsoft-Server-ActiveSync`

The SEG V2 requires that TLS 1.1 or 1.2 is supported on the client's email server, preferably TLS 1.2. It is recommended that the client follow the guidelines of the email system and the OS manufacturer.

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. You can download the installer from the Microsoft download center.
Installation of Notepad++ (Recommended)	This application makes it easier to parse through the log files.
Ensure Exchange ActiveSync is enabled for a test account	
Ensure 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.	

The Secure Email Gateway Architecture

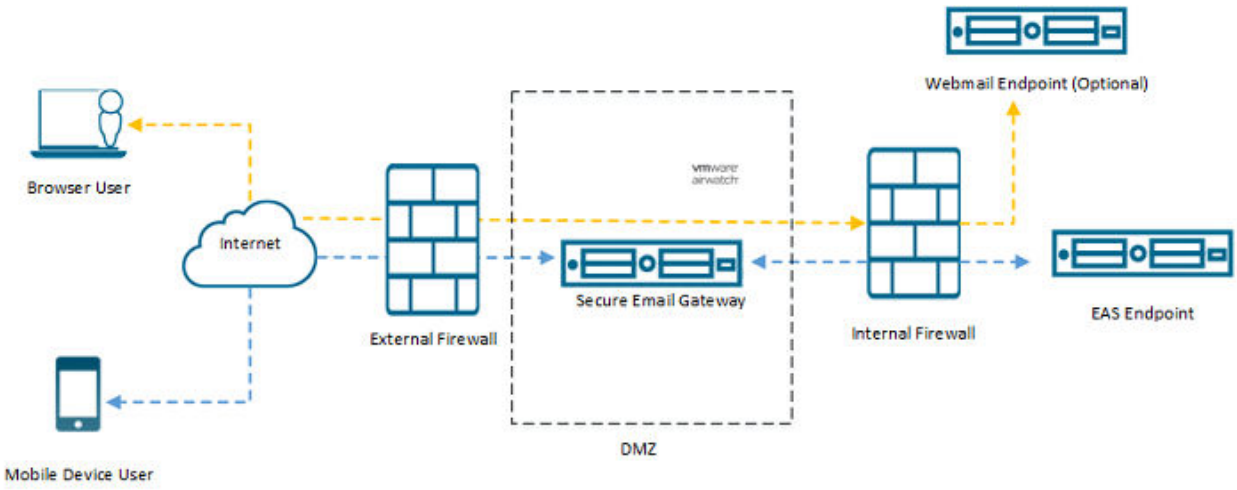
Deploy the SEG to enable the policy creation that determines how end-users access mail on their devices. It is optimal to install the Secure Email Gateway (SEG) in a Demilitarized Zone (DMZ) or behind a reverse proxy server.

The SEG is an on-premises component that you install as part of your organization's network. The SEG Proxy model requires an Exchange ActiveSync infrastructure like Microsoft Exchange, IBM Notes Traveler, or G Suite. For more information on SEG, contact Workspace ONE Support.

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.

SEG Setup with Exchange ActiveSync

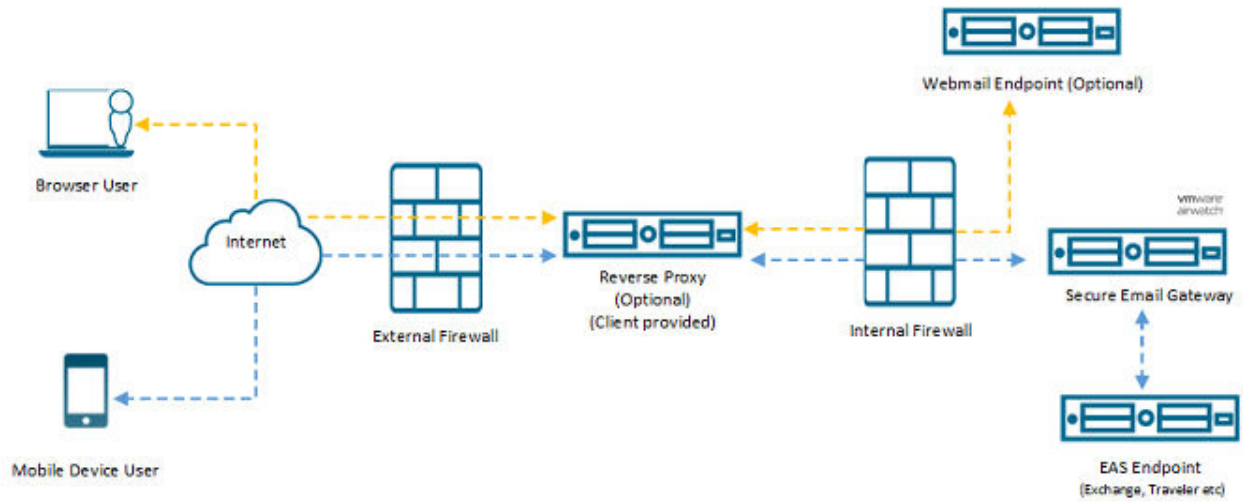
Workspace ONE UEM best practices support this configuration. The SEG is placed in the DMZ for routing mobile email traffic.



Note VMware recommends configuring the SEG with Exchange ActiveSync to route mobile email traffic.

Exchange ActiveSync SEG Using Optional Reverse Proxy Configuration

The reverse proxy configuration uses an optional reverse proxy to direct the mobile device traffic to the SEG Proxy while routing browser traffic directly to the 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.



Recommendations for Reverse Proxy Configuration

Exchange ActiveSync is a stateless protocol, and persistence is not explicitly required by Microsoft. The best load-balancing method might vary from different implementations. Use the following information to meet the recommended load-balancing requirements efficiently.

- **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.

Configure the SEG V2

2

The following topics describes the information related to configuration of 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 can download the SEG installer from the Workspace ONE resource portal.

1 In the UEM console, navigate to **Email** > **Settings** and select **Configure**. The **ADD** wizard displays.

2 In the **Platform** tab of the wizard:

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

   b Select the **Email Type** (Exchange, IBM Notes, or Google).

   c If you selected Exchange as the email type, then select the appropriate exchange version from the drop-down menu. Click **Next**. Example of email servers is 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 URL and port number for the incoming mail traffic to SEG.
Listener Port	The SEG listens for device the communication through this port. The default port number is 443. If SSL is activated for SEG, the SSL certificate is bound to this port.
Terminate SSL on SEG	Activate this option if you want the SSL certificate to be sent from the SEG instead of offloading on a web application firewall. Upload a .pfx or .p12 certificate file including the root and intermediate certificates.
Upload Locally	Select to upload the SSL certificate locally during installation.

Setting	Description
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. See, the *Upload the SSL Certificate after Renewal* section in the Chapter 3 Install the Secure Email Gateway (V2) topic to understand the methods to upload the SSL certificate after renewal.
Email Server URL and Port	Enter the email server URL and port number in the form *https://email server url:email* server port. The SEG uses the following URL for proxying email requests to the email server. If using Exchange Online, enter the *https://outlook.office365.com* URL.
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 the 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 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. **Note** A list of all the device records with the corresponding compliance status is provided. SEG does not calculate the compliance of a given device by itself, instead uses the data received from the Workspace ONE UEM console.
Enable Clustering	Select **Enable** to activate clustering of multiple SEG servers. When clustering is activated, policy updates are distributed to all SEGs in the cluster. The 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. Activate clustering to have multiple SEG servers operating as a cluster.

4 Select **Next** in the **Profile** tab of the wizard. If necessary, assign an email profile to the MEM configuration. Select **Next** in the Profile tab of the wizard.

5 On the Summary tab, review the configuration that you have just created. Select **Finish** to save the settings.

6 Download the SEG installer from the Workspace ONE resource portal.

7 Configure any additional settings for your SEG using the **Advanced** option.

Setting	Description
Use Default Settings	The **Use Default Settings** check box is activated by default. To modify the advanced settings, you must uncheck this box.
Enable Real-time Compliance Sync	Activate this option to send the compliance information to the SEG in real-time. Without this, individual changes to the device policies are refreshed per the delta sync interval.
Required transactions	The **Required transactions** cannot be deactivated.
Optional transactions	Activate or deactivate the optional transactions such as Get attachment, Search, Move Items, and so on. The following are the Exchange Active Sync (EAS) transactions that the SEG reports to the console and are displayed on the **Email List View** in the **Last Command** column.
Diagnostic	Set the number and frequency of transactions for a device when the test mode is activated.
Sizing	Set the frequency of SEG and API server interaction.
Skip Attachment & Hyperlink transformations for S/MIME signed emails	Activate 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	Activate automatic lookup of the S/MIME certificate managed in a hosted LDAP directory. Enter the following values to configure the lookup. ■ **LDAP URL** - Specify the URL of the LDAP server hosting the S/MIME certificates. For example, `LDAP://certs.soandso.local/o=dept,c=company`. ■ **Authentication Type** - Specify the authentication type used by the LDAP server. **Anonymous** and **Basic** authentication are supported. If **Basic** authentication is selected, you must enter the username and password. ■ **Certificate Attribute** - The public key attribute used on the LDAP server to specify the S/MIME certificate. For example, `userCertificate;binary`. You must restart SEG service after enabling this feature.
Custom Gateway Settings	The SEG custom gateway settings are available as a key-value pair on the Workspace ONE UEM console. The commonly used properties are seeded on the Workspace ONE UEM console. For more information on the SEG supported key value pairs.

Setting	Description
Block Attachments	Used to control the default action when SEG is unable to communicate with the 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.

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. The high availability and disaster recovery setups are independent of the cluster configuration.

Use a load balancer to achieve the desired high availability and disaster recovery configuration. The same public host name must be used for the SEG servers across the data centers to ensure that the users need not reauthenticate when a SEG server failover occurs.

The following are the benefits of using SEG in a clustering and non-clustering server environments:

- Non-clustered server configuration:
  - Each SEG is updated independently.
  - Failover can be performed at the load balancer.
- Clustered server configuration:
  - Each data center must have its own MEM configuration and an external URL to update the MEM configuration's cluster.

    Note The external URL need not match the URL used by devices to access email, instead the UEM console uses the external URL to send policy updates to the appropriate cluster configuration.
  - Internal IP addresses or hostnames are applicable for clustering rather than public IP addresses only.
  - Device EAS profiles must use a third URL that can be failed-over between data centers.

SEG Custom Gateway Settings

The SEG v2 configurations are controlled at an individual node level. The custom gateway setting feature centralizes the configuration on the Workspace ONE UEM Console as part of the MEM configuration itself.

Prerequisites

The following table lists the requirements for the SEG custom settings feature:

Platform	Minimum SEG and UAG Supported Version	Workspace ONE UEM Console
Windows	2.17.0	20.10
UAG	UAG 2009 (SEG 2.17.0)	20.10

Configure SEG Custom Gateway Settings

The SEG custom settings are available as key-value pairs on the Workspace ONE UEM console. The commonly used properties are seeded on the Workspace ONE UEM Console. To configure the custom settings, perform the following steps:

1 Log in to the Workspace ONE UEM console.

2 Navigate to the **Email > Email Settings**.

3 Configure the **Email Settings** for SEG.

4 Configure the additional settings for SEG using the **Advanced** option.

5 Navigate to the **Custom Gateway Settings**, click **ADD ROW**, and enter the supported configuration as the key-value pair:

- **Key**: Enter the property or setting name.
- **Type**: Enter the type of value such as string, integer, and so on.
- **Value**: Enter the property or custom value.

6 Click **Save**.

Apply the Custom Gateway Settings on the SEG Service

During an installation or upgrade, if the custom settings are provided on the Workspace ONE UEM console, then the SEG service starts with the applied custom settings

If the custom settings are added or updated on the Workspace ONE UEM console when the SEG service is running, then a **refreshSettings** notification is triggered for SEG. The SEG fetches the latest custom gateway settings. A few of the custom settings are applied immediately, whereas the other custom settings might require you to restart the SEG service.

Supported Configuration for the Custom Gateway Settings

The following section lists all the supported SEG properties or settings for the custom settings feature.

Note The properties or settings are grouped based on feature or functionality. The custom settings can be added on the Workspace ONE UEM console in any order.

JVM Arguments or System Settings

The JVM arguments or system settings property keys start with **-D**. If the property value is modified, SEG updates the custom system settings in the **segServiceWrapper.conf** (for Windows) or **seg-jvm-args.conf** (for UAG). If the system setting is updated when the SEG service is running, then the SEG triggers a service restart.

You can configure the **seg.custom.settings.service.restart.code=0** property in the **application-override.properties** file to deactivate the automatic restart of the SEG service.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
-Djdk.tls.disabledAlgorithms	Comma-separated list of TLS algorithms, ciphers, and versions to be deactivated.	String	MD5, RC4, TLSv1, TLSv1.1, SSLv2Hello, SSLv3, DSA, DESede, DES, 3DES, DES40_CBC, RC4_40, MD5withRSA, DH, 3DES_EDE_CBC, DHE, DH keySize < 1024, EC keySize < 224	If the modified value is detected, restart automatically.
-Djdk.tls.ephemeralDHKeySize	Customize the strength of the ephemeral DH key size used internally during the TLS or DTLS handshake. The system property does not impact the DH key sizes in the `ServerKeyExchange` messages for exportable cipher suites. The following DH key sizes are impacted, the DHE_RSA, DHE_DSS, and DH_anon-based cipher suites in the JSSE Oracle provider. For more information, see Customizing Size of Ephemeral Diffie-Hellman Keys.	Integer	2048	If the modified value is detected, restart automatically.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
-Dsyslog.enabled	Flag to activate the syslog configuration for SEG.	Boolean	TRUE - For the UAG deployment FALSE - For the Windows deployment	If the modified value is detected, restart automatically.
-Dsyslog.host	Host address of the syslog server. The host address value can be configured with any remote syslog server hostname or IP address that listens over UDP. If syslog to the remote server is configured with the TCP or TLS, then point to a local host syslog listener that can retransmit using the required protocol over the wire. The in-built UAG syslog configuration can function as the local retransmitter.	String	localhost	If the modified value is detected, restart automatically.
-Dkerberos.process.recycle.time	Specify the Kerberos process recycle time, when activated. Process recycling can be activated using the property **-Denable.kerberos.process.recycle**.	Time in the hh24:mm:ss format	23:59:59	If the modified value is detected, restart automatically.
-Xmx	Maximum java heap memory for the service in Mebibytes (MiB). For example, 8 GiB of RAM can be configured as 8192.	Long	If the system property is not configured, dynamically identified during the SEG service installation based on the system configuration.	If the modified value is detected, restart automatically.
-Dsyslog.facility	Syslog facility as defined by the Syslog server.	String	USER	If the modified value is detected, restart automatically.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
-Dsyslog.port	Syslog listener port that the SEG points to.	Integer	514	If the modified value is detected, restart automatically.
-Denable.kerberos.process.recycle	SEG can be configured to recycle the native Kerberos client processes when the Kerberos based authentication is activated.	Boolean	FALSE	If the modified value is detected, restart automatically.

Support for EWS

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
enable.boxer.ens.ews.proxy	Flag to activate SEG to listen for the EWS traffic and proxy the same to the configured Exchange EWS endpoint. By default, SEG proxies the EWS requests to the email server host configured as part of the MEM configuration. However, a different host can be configured using the **ews.email.server.host.and.port** property.	Boolean	FALSE	Restart the SEG service.
ews.email.server.host.and.port	If the email server hostname for the EWS is different than the EAS, then use this property to configure the EWS email server hostname. When the host name for the EWS connection is used from the **ews.email.server.host.and.port** property, all the other HTTP connection parameters remain the same, similar to the EAS parameters. If the host is using a self-signed certificate, corresponding trusted certificate must be added to SEG separately.	URL	No user action required.	No user action required.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
	EWS proxy can be activated using flag **enable.boxer.ens.ews.proxy**.			
http.response.status.code.for.connection.terminated.with.ews	HTTP response code for the EWS request when a connection error occurs between the SEG and the Exchange.	Integer	503	No user action required.

Certificate-based Authentication

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
proxy.email.request.on.kerberos.error	Flag to activate the proxy request to the email server, in case, an error occurs when generating the KCD token.	Boolean	TRUE	No user action required.
response.status.code.on.kerberos.error.for.non.ping	HTTP response code for commands, other than PING and OPTIONS, when the Kerberos token generation results fail.	Integer	503	No user action required.
response.status.code.on.kerberos.error.for.ping	If the **proxy.email.request.on.kerberos.error** property is set to false, then the **response.status.code.on.kerberos.error.for.ping** is the HTTP status code returned during a Kerberos error for the PING command request.	Integer	200	No user action required.
response.status.code.on.kerberos.error.for.options.method	HTTP response code for the OPTIONS command when the Kerberos token generation results fail.	Integer	401	No user action required.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
response.status.code.on.certificate.validation.fail	HTTP response code when the certificate authentication is activated and if SEG the client certificate validation fails. If the flag **force.client.cert.for.ssl.handshake** is activated, the request with the missing or invalid certificate might be rejected during the SSL handshake.	Integer	401	No user action required.
enable.upn.lookup.from.subject.cn	Flag to activate the UPN (used for Kerberos authentication) lookup from **Subject**, and **Common Name** when the UPN is not present in the SAN type extension of the client certificate.	Boolean	FALSE	No user action required.
generate.krb5.config.at.service.restart	Flag to generate the KRB configuration file (krb5.ini in Windows or krb5.conf in UAG) when restarting the SEG service.	Boolean	TRUE	Restart the SEG service.
kerberos.service.max.processes.size	Number of KCD client processes that SEG spawns.	Integer	10	Restart the SEG service.
kerberos.thread.pool.size.per.service	Number of threads used per KCD client process.	Integer	5	Restart the SEG service.
kerberos.service.health.check.frequency.in.seconds	Frequency of polling by SEG for each KCD client process.	Integer	5	Restart the SEG service.
kerberos.enable.performance.metrics.logging	Flag to activate time statistics for the Kerberos token handling.	Boolean	TRUE	Restart the SEG service.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
kerberos.process.kill.max.wait.time.in.seconds	The maximum wait time for a process to shut down, when you attempt to stop the native process.	Integer	60	Restart the SEG service.
kerberos.process.max.time.to.recover.in.seconds	Maximum time in seconds permitted for a process to be in any status (NOT_STARTED, STARTING, FAILED_TO_START, or BUSY) other than AVAILABLE. To recover processes in an unexpected situation and ensure a safer run.	Integer	120	Restart the SEG service.
kerberos.backpressure.queue.max.size	Maximum size of the backpressure queue to obtain the Kerberos token. If the backpressure queue is full, further requests are ignored.	Integer	2500	Restart the SEG service.
kerberos.backpressure.queue.max.wait.in.seconds	Duration in seconds for which a request waits in a backpressure queue for the Kerberos token generation before being stopped.	Integer	20	Restart the SEG service.
enable.cert.revocation.validation	Flag to activate the certificate revocation check using the CRL. The flag is used only when the CBA is activated.	Boolean	FALSE	Restart the SEG service.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
fail.hard.on.crl.download.failure.during.server.startup	Flag to prevent SEG from starting if SEG is unable to fetch the CRLs at start. The option is applicable only when any CRL distribution URL is configured using the **remote.crl.distribution.http.uris** key.	Boolean	TRUE	Restart the SEG service.
remote.crl.fetch.interval.in.minutes	Interval in minutes for a periodic timer that attempts to update SEG with the latest CRL data.	Long (the value type is integer)	1440 (24 hours)	Restart the SEG service.
remote.crl.distribution.http.uris	List of HTTP URLs of CRL Distribution Points (CDP). Use the value when SEG is configured to accept the client certificates, either by enabling the **Require Client Certificate** flag or the Kerberos based authentication. Applicable only if **enable.cert.revocation.validation** value is set to true.	String	NA	No user action required.
kerberos.linux.named.pipe.connect.delay.millis	Delay in milliseconds before the SEG Java process attempts to listen to the named pipes that are started by the Kerberos client native processes. This delay is to ensure smooth recovery of crashed Kerberos client processes. This property is applicable only for SEG on UAG. Since: UAG 21.03	Long	50	Restart the SEG service.

Certificate-Mapping LDAP Lookup

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
cert.mapping.ldap.enabled	The flag indicates if the certificate-mapping feature is activated for SEG. If the KCD authentication is deactivated in the email configuration, ignore the setting and consider as false.	Boolean	FALSE	Restart the SEG service.
cert.mapping.ldap.host	The remote LDAP host information in a proper URL format.	String	NA	Restart the SEG service.
cert.mapping.ldap.authType	The authentication type used with the LDAP server for the certificate-mapping feature.	Integer	0 (simple authentication)	Restart the SEG service.
cert.mapping.ldap.user	The LDAP user for authenticating the LDAP query. SEG uses the same service account credentials configured as part of the Kerberos authentication settings. However for the LDAP query, the user name must be provided in the Distinguished Name (DN) format.	String	NA	Restart the SEG service.
cert.mapping.ldap.attrs	List of LDAP lookup attributes used for certificate-mapping feature.	String	NA	Restart the SEG service.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
cert.mapping.ldap.server.base	Distinguished name of the base domain configured for running the LDAP query. The query fetches the matching results from the domain. By default, the query refers to the rootDSE of the LDAP setup. The field can be empty for the **userCertificate** and **userPrincipalName** attributes indexed and replicated to the global catalog.	String	NA	Restart the SEG service.
cert.mapping.ignore.ldap.ssl.errors	Flag to ignore any SSL errors when contacting LDAP server for the certificate-mapping lookup.	Boolean	FALSE	Restart the SEG service.
cert.mapping.max.query.executor.pools	Maximum number of LDAP services created to allow the maximum concurrent LDAP queries.	Integer	25	Restart the SEG service.
cert.mapping.ldap.connect.timeout.millis	LDAP connect timeout in milliseconds for certificate-mapping.	Integer	3000	Restart the SEG service.
cert.mapping.ldap.read.timeout.millis	LDAP read timeout in milliseconds for certificate-mapping.	Integer	3000	Restart the SEG service.
cert.mapping.ldap.service.pool.size	LDAP (executor) service thread pool size.	Integer	3	Restart the SEG service.
cert.mapping.backpressure.queue.size	Maximum size of requests that are allowed in back pressure queue, waiting for the LDAP service for certificate-mapping lookup.	Integer	1000	Restart the SEG service.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
cert.mapping.backpressure.max.ttl.in.seconds	Maximum time a request can stay in back pressure queue waiting for the LDAP service to be available.	Integer	60	Restart the SEG service.
cert.mapping.wait.delay.for.concurrent.query.millis	Fixed delay waiting for a request when another request for the same UPN is in progress for getting certificate mapping.	Integer	500	No user action required.

SEG Policy and Cache

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
bulk.update.completion.threshold.in.seconds	The timeout value in seconds to complete bulk policy update flow. If the bulk policy update does not complete within this duration, the bulk policy update is marked as failure. Since: SEG 2.20.0, UAG 21.06	Integer	600	No user action required.
policy.data.not.ready.response.code	HTTP response code to be returned to the device if SEG is yet to receive all the policy data just after start, and the configuration prohibits email communication until policy data is ready.	Integer	503	No user action required.
ignore.duplicate.records.during.policy.update	Flag to ignore duplicate records returned from an API, and compare the size of a policy in the SEG cache with the size for only Unique IDs.	Boolean	TRUE	No user action required.
policy.update.eventbus.timeout.buffer.millis	Event bus timeout used during a policy update.	Long	30000	No user action required.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
disable.api.policy.count.match.during.policy.update	Maximum time in seconds that SEG waits for the cache to be asynchronously updated with the new policy records during a bulk policy update.	Boolean	FALSE	No user action required.
policy.async.cache.update.completion.threshold.seconds	Maximum time in seconds that SEG waits for the cache to be asynchronously updated with new policy records during a bulk policy update.	Integer	900	Restart the SEG service.
cache.index.validation.eventbus.timeout.millis	Timeout duration in milliseconds for validating the cache index on all the nodes after a bulk policy update. If failed, SEG retries before finally reverting the changes.	Integer	30000	No user action required.
cache.index.swap.wait.time.in.millis	Wait delay in milliseconds before swapping active and passive cache indexes after the latest policy from API is updated on the passive cache.	Long	60000	No user action required.
cache.index.validation.max.retry.count	Number of retry attempts to validate that the cache indexes are updated in all the nodes, when clustering is activated.	Integer	3	No user action required.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
wait.time.in.millis.before.passive.cache.cleanup.start	In case the policy update fails and the SEG is running in a clustered mode, the cache indexes in all the nodes must be updated to be in sync. The **wait.time.in.millis.before.passive.cache.cleanup.start**, is the time in milliseconds for which the SEG waits before cleaning the passive cache, so that all the nodes have sufficient time to swap the passive and active indexes, if necessary.	Long	30000	No user action required.
cache.async.update.status.check.timer.interval.millis	Interval in milliseconds for a periodic timer that validates async policy data update in cache.	Long	10000	No user action required.
full.bulk.update.interval.in.minutes (only when the delta is activated)		Integer	1440 (24 hours)	Restart the SEG service.
validate.resource.uri.in.jwt.auth	Interval in minutes for a periodic full bulk policy update, when the delta sync is activated.	Boolean	TRUE	No user action required.
jwt.allowed-clock-skew-in-seconds	Flag to activate validation of resource URL in the JWT token.	Integer	30	No user action required.
tcpip.discovery.timeout-seconds	Maximum allowed skew in JWT timestamp for the token to be successfully authenticated.	Integer	5	Restart the SEG service.
hazelcast.operation.call.timeout.millis	Timeout for Hazel cast cache read or write operation.		Long	60000

Content Transformation

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
disable.transformation.on.inline.unknown.attachment.bytes	Flag to deactivate the attachment transformation if the MIME type cannot be identified.	Boolean	TRUE	No user action required.
disable.transformation.on.inline.unknown.attachment.tag	Flag to ignore the transformation on the inline attachment tags that do not have a file extension or MIME type to be processed correctly.	Boolean	TRUE	No user action required.
enable.request.transformation.by.default	Flag to activate the content transformation on the request flow. If any of the transformation types are activated and the value is FALSE, the request transformation occurs. When the value is TRUE, request transformation always occurs. Activate the flag when the content the transformation is activated and the attachments are encrypted or hyperlinks are transformed. The content transformation is deactivated, but the outgoing emails are decrypted attachments and original hyperlinks.	Boolean	FALSE	No user action required.

HTTP Request or Response

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
email.server.request.timeout.millis	HTTP request timeout from SEG to the email server in milliseconds for the email traffic. Since: SEG 2.20.0, UAG 21.06	Integer	1200000	No user action required.
keep.http.client.connection.alive	Flag to keep a socket connection to the email server and the API server alive to reuse the same connection for any subsequent request. Since: SEG 2.20.0, UAG 21.06	Boolean	True	No user action required.
keep.email.server.client.connection.alive	Flag to keep a socket connection to the email server alive, to reuse the same connection for any subsequent request. **Note** This key is supported until SEG version 2.19.0 and UAG version 21.03.1. For SEG version 2.20.0 and UAG version 21.06, use key **keep.http.client.connection.alive**.	Boolean	True	No user action required.
api.server.connect.timeout.millis	HTTP connection timeout from SEG to the API server in milliseconds.	Integer	15000	No user action required.
email.server.connect.timeout.millis	HTTP connection timeout from SEG to the email server in milliseconds.	Long	15000	No user action required.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
force.client.cert.for.ssl.handshake	In the MEM configuration, when the **Require Client Certificate** is activated in the **Advanced Settings** option, setting the flag to **TRUE** forces the SSL handshake to fail. Due to the absence of a client certificate and the request not reaching the application layer, the SSL handshake fails. If the flag is set to FALSE, the request reaches the application layer before failing due to the lack of the client certificate.	Boolean	FALSE	No user action required.
http.client.max.idle.timeout.seconds	Maximum idle timeout in seconds after which any connection is closed to release the system resources.	Integer	3600	No user action required.
http.response.status.code.for.non.ping.on.connection.closed.failure	HTTP response code for the requests other than the PING command when the connection between the SEG and the email server closes unexpectedly. You can use this option only if the flag **return.http.response.status.for.non.ping.on.connection.closed.failure** is activated.	Integer	503	No user action required.
http.response.status.code.for.ping.on.connection.closed.failure	HTTP response code for the PING command requests when the connection between the SEG and email server closes unexpectedly.	Integer	200	No user action required.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
http.server.max.idle.timeout.seconds	Idle time in seconds after which an inbound connection to the SEG server is closed.	Integer	3600	No user action required.
max.http.buffer.chunk.size	Maximum HTTP chunk size.	Integer	8192 (that is, 8 KB)	No user action required.
max.initial.line.length	Maximum length of the initial line of the HTTP requests ending or originating at SEG.	Integer	4096 (that is, 4 KB)	No user action required.
return.http.response.status.for.non.ping.on.connection.closed.failure	Flag to decide if the SEG responds to the device in case a connection error occurs between SEG and the email server when serving a non-PING command. When activated, the **http.response.status.code.for.non.ping.on.connection.closed.failure** property determines the response code. Few email clients might show some error when the connection to SEG is abruptly closed.	Integer	TRUE	No user action required.

SMIME Certificate Lookup

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
smime.lookup.ldap.connect.timeout.millis	LDAP connection timeout in milliseconds for the SMIME certificate lookup.	Integer	3000	No user action required.
smime.lookup.ldap.read.timeout.millis	LDAP read timeout in milliseconds for the SMIME certificate lookup.	Integer	3000	No user action required.

Configuration Key	Description	Value type	Default value	Apply System Setting at Run Time
smime.lookup.ldap.server.base	Base path of the LDAP server that the SEG uses for the SMIME lookup.	String	NA	No user action required.
smime.lookup.ignore.ldap.ssl.errors	Flag to ignore any SSL errors when contacting the LDAP server for the SMIME lookup.	Boolean	FALSE	No user action required.

Custom Response Headers

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
resp-header.Strict-Transport-Security	The STS header with the preconfigured default value is overridden and a new SEG value is used.	String	Max-age=31536000;includeSubDomains	No user action required.
resp-header.X-Custom-Header	New header with a specified value is included for subsequent responses.	String	NA	No user action required.

KCD Client Configuration

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
kerb-conf.log_level	System log level for the **kcdclient** pipe processes that the SEG spawns. 0 - Off 1 - Error 2 - Warning 3 - Info 4 - Debug	Integer	2	No user action required.
kerb-conf.log_file_append	Flag to indicate if a process restart must append logs or discard old logs and truncate a file. 0 - Do not append 1 - Append	Integer	1	No user action required.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
kerb-conf.log_file_backup_count	Maximum number of backup log files to be created when the maximum file size is reached.	Integer	1	No user action required.
kerb-conf.log_file_size	Maximum file size of a Kerberos process log file in MB.	Integer	10	No user action required.
kerb-conf.refresh_config_interval	Time taken in seconds to refresh the settings and to load any updated configuration from a file.	Integer	30	No user action required.
krb5-conf.<property_name>	The properties are updated in the **krb5-base.conf** file.	NA	NA	No user action required.

SEG Statistics, Monitoring, and Troubleshooting

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
custom.response.text.for.root.and.health.api	Custom text to be sent as a response when the root path of the SEG V2 is accessed. If **hide.seg.info.on.health.monitor.response** is set to **true**, the text is also used in the response body of the health monitoring endpoints (/health and /lb-health). Since: SEG 2.20.0, UAG 21.06	String	OK	No user action required.
log.device.delta.sync.payload.in.debug.mode	Flag to activate the delta sync payload.	Boolean	FALSE	No user action required.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
api.server.connectivity.diagnostic.timeout.millis	When SEG verifies the connectivity to the API server to capture the diagnostic information, specify the HTTP connection timeout in milliseconds.	Integer	5000	No user action required.
email.server.connectivity.diagnostic.timeout.millis	When SEG verifies the connectivity to the Email server to capture diagnostic information, specify the HTTP connection timeout in milliseconds.	Integer	5000	No user action required.
high.cpu.monitoring.enabled	Flag to activate the CPU usage monitoring and to generate thread dumps beyond a threshold limit. Configure the threshold limit using the **cpu.monitor.trigger.threshold.percentage** property.	Boolean	FALSE	No user action required.
log.http.server.network.activity	Flag to activate the SEG HTTP server network activity.	Boolean	FALSE	No user action required.
enable.seg.metrics.collection	Flag to activate the SEG metrics collection. When the flag is activated with the UEIP flag on the Workspace ONE UEM console, SEG reports the diagnostic information to the VMware Analytics Cloud (VAC).	Boolean	TRUE	No user action required.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
log.active.sync.payload.in.debug.mode	Flag to activate logging active synchronization payload in **active-sync-payload-reporting.log** Since: SEG 2.18.0, UAG 20.12 .	String	FALSE	No user action required.
hide.seg.info.on.health.monitor.response	Flag to deactivate the SEG version and build information in the health monitoring endpoints (/health and /lb-health). Since: SEG 2.19.0, UAG 21.03	Boolean	False	No user action required.

SEG Logging

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
logger.app	The SEG application logs are applicable for the **app.log** and the **ews-proxy.log** files. Since: SEG 2.18.0, UAG 20.12	String	Error	No user action required.
logger.transactional	The transaction summary logs are applicable for the **http-transaction.log, kerberos-transaction.log** and the **ews-transaction.log** transaction log files. The default log level is **Debug** and you need not change unless you want to deactivate the transactional logging. Since: SEG 2.18.0, UAG 20.12	String	Debug	No user action required.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
logger.policy.cache	The policy update and SEG cache logs are applicable for the **policy-update.log** and **cache.log** files. Since: SEG 2.18.0, UAG 20.12	String	Info	No user action required.
logger.kerberos.service.manager	The Kerberos service manager log is applicable for the **kerberos-service-manager.log** file. Since: SEG 2.18.0, UAG 20.12	String	Error	No user action required.
logger.cert.auth	The certificate-based authentication log is applicable for the **cert-auth.log** file. Since: SEG 2.18.0, UAG 20.12	String	Error	No user action required.
logger.compliance	Transaction for blocked devices due to non-compliance. This is applicable for the **non-compliant-devices.log** log file. Since: SEG 2.18.0, UAG 20.12	String	Error	No user action required.
logger.content.transformation	Email content transformation such as hyperlink and attachment transform. This is applicable for the **content-transform.log** file. Since: SEG 2.18.0, UAG 20.12	String	Error	No user action required.

SEG Targeted Content Logging

SEG targeted content logging is activated to troubleshoot content transformation related issues. When you activate content logging, SEG starts writing email content (before and after transformation) in the `<SEG_Install_Dir>/tmp/content-logs` folder.

Note Activate content logging only for troubleshooting and remove the property keys from custom settings after troubleshooting. You must consent the customer before you activate content logging.

Configuration Key	Description	Value Type	Default Value	Apply System Setting at Run Time
content.logging.target.all	Activate content logging for all users and devices. Since: SEG 2.18.0, UAG 20.12	Boolean	False	No user action required.
content.logging.target.users	Activate content logging for targeted users. Comma separated list. For example, user1, user2, and so on. Since: SEG 2.18.0, UAG 20.12	String	NA	No user action required.
content.logging.target.easdeviceids	Activate content logging for targeted EAS device IDs. Comma separated list. For example device1, device2. and so on. Since: SEG 2.18.0, UAG 20.12	String	NA	No user action required.

Install the Secure Email Gateway (V2)

3

Install the Secure Email Gateway (SEG) to relay all email traffic to Workspace ONE UEM-enrolled devices.

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**.

Note The credentials used for accessing the API are only used for the initial setup and cannot be used again.

Settings Description	Description
HTTPS	Select the check box if the protocol for the Workspace ONE UEM API server is https.
API Server Hostname	Enter the hostname 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 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	Select the check box if the protocol for the proxy is https.
Proxy Host	The address of the proxy host.
Proxy Port	The proxy port number.
Username	Username for proxy authentication.
Password	Password for the proxy username provided. **Note** These fields are available once you select the **Does the proxy require authentication credentails?**

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

Note You can skip this step if the SSL certificate is 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**.

The SEG V2 Admin Page

On the Windows deployment of SEG v2, you can access the Admin page at `https://localhost:44444/seg/admin`. If SSL is not enabled for SEG, use `http`.

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

- Change logging levels for the different SEG processes
- Call diagnostics endpoints
- View health and statistics information

Note For SEG on UAG, the SEG Health and Diagnostic information is available under the **Edge Service Session Statistics** section of the UAG Admin UI. For more information about SEG Health and Diagnostic, see the *Monitoring the SEG Health and Diagnostics* section in the *Deploying and Configuring VMware Unified Access Gateway* guide.

Logging

The information related to the SEG processes is recorded in different log files. The level of logging determines the amount of information that is logged for a particular log file. The duration specifies how long an elevated logging level persists before reverting to the default level of the log.

The SEG generates the following logs:

Log Name	Description of the Log Contents
Application logs	The SEG application logs are applicable for the **app.log** and the **ews-proxy.log** files.
Transaction Summary	The transaction summary logs are applicable for the **http-transaction.log, kerberos-transaction.log** and the **ews-transaction.log** transaction log files. The default log level is **Debug** and you need not change unless you want to deactivate the transactional logging.
Policy Updates and Cache	The policy update and SEG cache logs are applicable for the **policy-update.log** and **cache.log** files.
Kerberos Service Manager	The Kerberos service manager log is applicable for the **kerberos-service-manager.log** file.
Certificate Authentication	The certificate-based authentication log is applicable for the **cert-auth.log** file.
Device Transactions (Blocked)	Transaction for blocked devices due to non-compliance. This is applicable for the **non-compliant-devices.log** log file.
Content Transformation	Email content transformation such as hyperlink and attachment transform. This is applicable for the **content-transform.log** file.

Diagnostics

On the Diagnostics page you can view the diagnostic information for the SEG and 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 following table into the REST API URI field on the diagnostic page and click the GET button. Information related to the endpoint is either displayed in the text area on the diagnostics page or a `.csv` file of the information is downloaded.

API Endpoint	Description
`/diagnostic`	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 attachments, and 451 redirect mappings.

The 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.

Configure the External Configuration File

In certain scenarios, you might want to override the default values provided in the `application.properties` file. Using the SEG V2, you can manually override the values in the `application.properties` file using an external configuration file, instead of modifying the `application.properties` file.

Note For SEG version 2.17.0 or later, with the Workspace ONE UEM console version 20.10 and later, you must use the SEG key-value pair settings instead of the external configuration file. To understand the SEG key-value pair settings, see the *SEG Custom Gateway Settings* topic.

Note When SEG is deployed on UAG, the default **application-override.properties** file already exists at `/opt/vmware/docker/seg/container/config/override/application-override.properties`.

Note The file or folder names used in this procedure are for your reference only. You can choose any file or folder names as per your choice.

Before you begin:

In addition to the configuration received from the Workspace ONE UEM console, the SEG V2 uses certain values from the local configuration file at `SEGDir/config/application.properties`. During a SEG V2 upgrade, the values in the older `application.properties` file are discarded and the external configuration file retains any overridden values when the new version of SEG is installed. In case, any values need to be modified, update the external configuration file. During a SEG upgrade this helps to retain the customer overridden configuration values.

About this task:

The following procedure describes the steps to configure the external configurations file.

1 Create a folder in the server machine where SEG V2 is installed, and create a subdirectory where the override file is located.

   Results: For example, create a subdirectory with name `config-override` under the SEG installation directory `C:\AirWatch\SEG\`.

2 Browse to the newly created folder and create a properties file.

   Results: For example, if the file name is `application-override.properties`, full path of the file might be `C:\AirWatch\SEG\config-override\application-override.properties`.

3 Navigate to **Control Panel > System and Security > System**.

4 Click the **Advanced System Settings** link on the left-side panel, and then click **Environment Variables**.

5 Create a system variable. Add the `additional.spring.config.location` value for the **Variable name** and provide the full path of the file created in Step 2 as **Variable value**.

6 Save the newly created file and click **OK**. As per the example in Step 2, the value of the system variable is **C:\AirWatch\SEG\config-override\application-override.properties**.

7 Open the properties file created in Step 2 in any text editor, add the property key-value pairs that you want to override and save the file. Any changes to this file take effect only after the SEG service is restarted.

8 Restart the SEG service and check if SEG is using the overridden values from the external configuration file.

What to do next:

After restarting SEG, the overridden values from the external configuration file is used. Verify that the functional behavior of SEG is as per the overridden values.

SEG provides an API to verify if any invalid keys are configured in the external configuration file. Enter `/diagnostic/invalidconfigkeys` in the **Diagnostics** tab of the Admin UI to access the invalid keys.

Upload the SSL Certificate after Renewal

Each SSL certificate has a validity period and after the certificate expires you must renew and upload the latest SSL certificate. For SEG, you can upload the SSL certificate to the Workspace ONE UEM console, or locally when installing the SEG on Windows, or when configuring the SEG Edge service on the UAG. This topic describes the various options through which you can renew and upload the SSL certificate.

Upload the SSL Certificate through the Workspace ONE UEM Console

Perform the following steps when the SSL certificate is uploaded through the Workspace ONE UEM console:

1 In the UEM console, navigate to **Email** > **Settings** and edit the existing email configuration and click **Next**.

2 Navigate to the **Deployment** tab and click **Next**.

3 Upload the latest SEG server SSL certificate.

4 Enter the password when prompted, click **Next**, and save the settings.

5 Restart the SEGv2 service on all the servers to fetch the latest configuration and bind the updated SSL certificate.

Upload the SSL Certificate locally during the SEGv2 Installation for the Windows Server

Perform the following steps when the SSL certificate is uploaded locally during the SEGv2 installation for the Windows server:

1 Run the SEGv2 installer in the server box where the SEG is installed.

2 Select the **Modify** option to modify the installation when prompted.

3 Click **Next** to continue.

4 Upload the latest SEG server SSL certificate when prompted.

5 Enter the password and click **Next** to finish the setup.

6 SEGv2 service now binds to the updated SSL certificate.

Upload the SSL Certificate locally for the SEG Edge Service on the UAG Admin UI

Perform the following steps when the SSL certificate is uploaded locally for the SEG Edge service on the UAG Admin UI:

1 Log in to the UAG Admin UI.

2 Open the SEGv2 configuration under the **Edge Service** settings.

3 Enable the **Add SSL certificate** toggle button.

4 Click **Select** against the SSL certificate field.

5 Upload the latest SEG server SSL certificate and enter the password when prompted.

6 Save the configuration and wait for the appliance agent to complete the modification of the SEG Edge service.

7 SEG Edge service now binds to the updated SSL certificate.

Offloading SSL traffic on a Load Balancer or F5 network for a Windows-based Deployment

When the SSL traffic is offloaded on a Load Balancer or the F5 network for a Windows-based deployment, deactivate the **Terminate SSL on SEG** toggle button under the **Email Configuration** settings. The communication between the Load Balancer or the F5 network and the SEGv2 occurs in plain HTTP. In such a scenario, the SSL certificate rotation for the SEG is not applicable.

Offloading SSL traffic on a Load Balancer or F5 network for a UAG Deployment

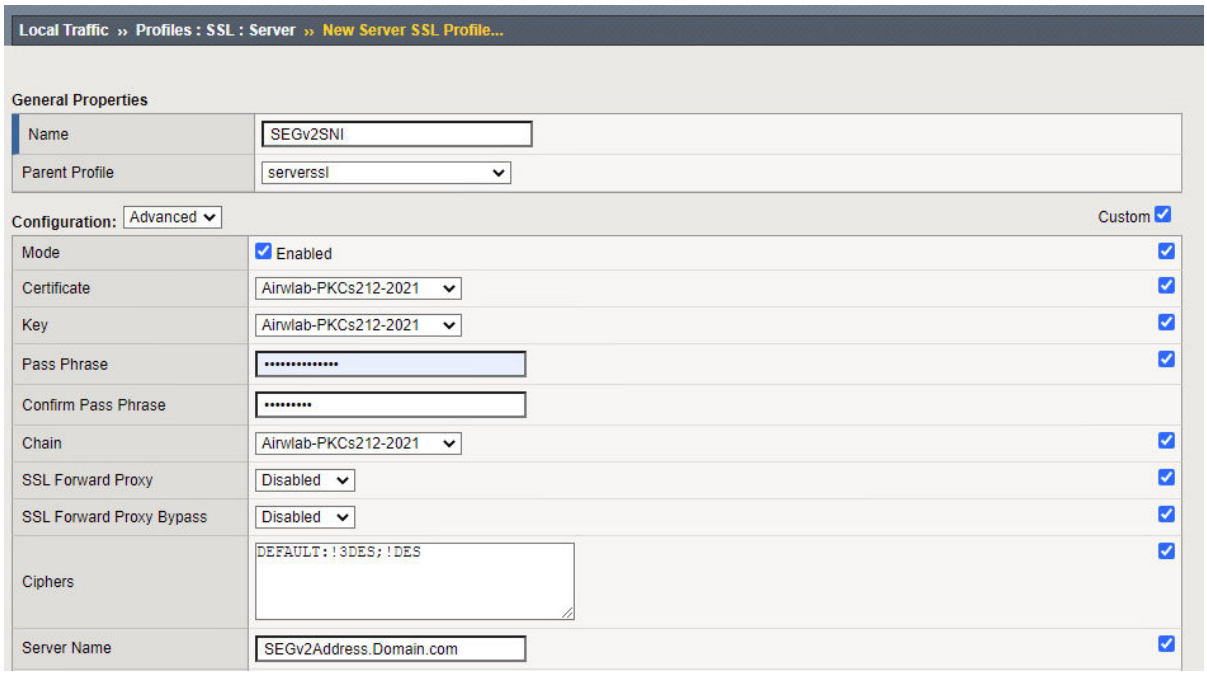
The SEG on UAG does not support a non-SSL configuration. If the SSL traffic from a device is offloaded on a Load Balancer or F5 network, the SEG must be configured with any SSL certificate to ensure that the traffic reaching the SEG from these network components is encrypted. In such a scenario, the SSL certificate rotation for SEG is applicable as explained in the *Upload the SSL Certificate Locally For SEG Edge Service on the UAG Admin UI* section.

Additionally, when the SEG on UAG is configured to listen on port 443, the UAG expects a valid Server Name Indication (SNI) extension during a TLS handshake, to enable the redirect requests to the SEG Edge service. When initiating a TLS connection with the SEG on UAG, the load balancer or the F5 network must be configured to use the correct value for the SNI field. The hostname which is configured as part of the external URL field in the Workspace ONE UEM Console (without port and protocol) is used as the SNI value for the SEG Edge service. The same value is used for the following fields while configuring the SEG Edge service on the UAG:

- The **airwatchServerHostname** field in the INI file when you configure through PowerShell and

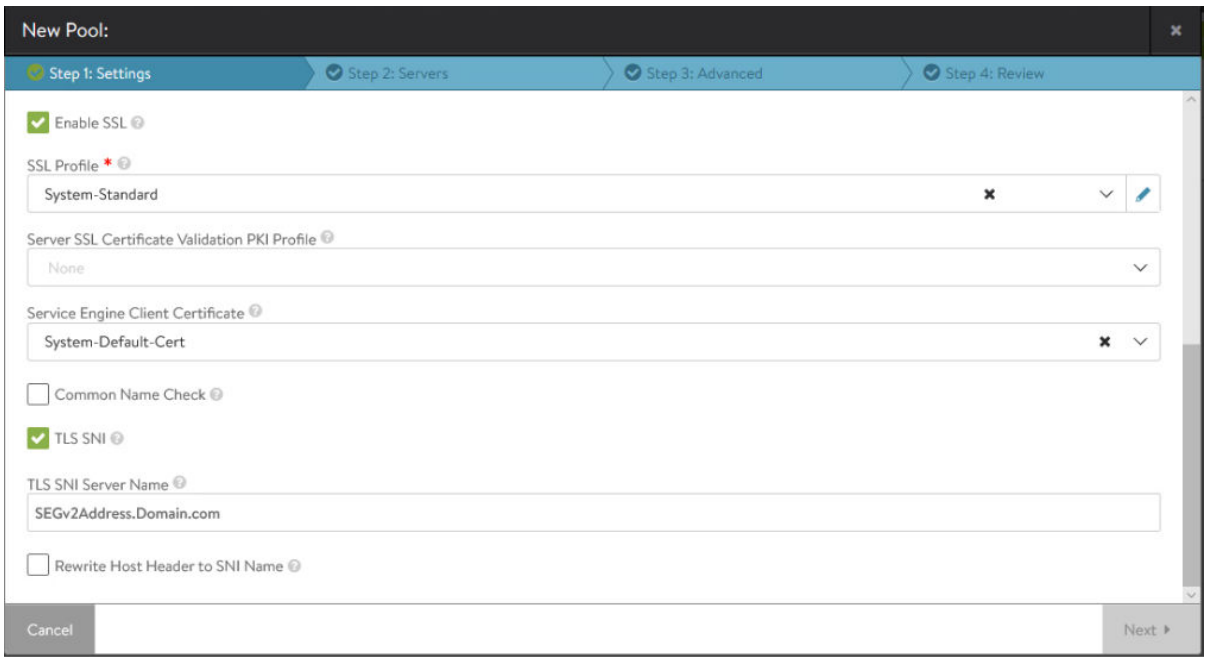
- The **Secure Email Gateway Hostname** field under the **Secure Email Gateway** settings when you configure through the UAG Admin UI.

If the SEG Edge service on the UAG is configured to listen on any port other than 443, then the Server Name Indication (SNI) configuration is not applicable. To enable the SNI configuration, a Server SSL profile must be created. For F5, enable the server SSL profile and the custom configurations. The **Certificate** and **Server Name** fields must be enabled and configured with the SEGv2. The following image shows an example of an SSL bridging configuration on F5 with SNI enabled in the server SSL profile.



Note The additional settings within the server SSL profile might be required based on your organizations security requirements.

For Avi Networks, enable SSL on the pool configuration and use the TLS SNI to specify the SEGv2 address. The following image shows an example of an SSL bridging configuration on AVI networks with SNI enabled in the pool configuration.


New Pool:
Step 1: Settings
Step 2: Servers
Step 3: Advanced
Step 4: Review
Enable SSL
SSL Profile *
System-Standard
Server SSL Certificate Validation PKI Profile
None
Service Engine Client Certificate
System-Default-Cert
Common Name Check
TLS SNI
TLS SNI Server Name
SEGv2Address.Domain.com
Rewrite Host Header to SNI Name
Cancel
Next

Additional Configuration on SEG V2

4

Configure the SEG V2 EWS Proxy for Email Notification Service

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.

About this task:

Both Cloud and On-premises ENS deployments are supported by SEG. The SEG listens on the EWS endpoint for traffic from the ENS, 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.

Note For SEG version 2.17.0 or later, with the Workspace ONE UEM console version 20.10 and later, perform the SEG configuration using the custom gateway settings. To understand the SEG custom gateway settings, see the *SEG Custom Gateway Settings* section in the Chapter 2 Configure the SEG V2 topic.

For SEG version before 2.17.0, SEG continues to use the default configuration (pre-defined configuration). If the custom settings feature is not available, manually update the respective files at the individual node and modify the SEG configuration.

1 Navigate to **SEG > Config** folder and open the **application-override.properties** file for editing. See the *Configure the External Configuration File* to understand how to configure the override properties file.

   Note When SEG is deployed on UAG, use the following path to edit the file: `vi /opt/vmware/docker/seg/container/config/override/application-override.properties`.

2 Add the **enable.boxer.ens.ews.proxy=true** entry in the **application-override.properties** file. See the *Configure the External Configuration File* to understand how to configure the override properties file.

3 Save the file.

4 Restart the SEG service. The SEG now listens to the `/EWS` endpoint for traffic from the email notification service.

Configure a Different Hostname for Exchange Web Service

Starting with SEG version 2.12, SEG supports the ability to configure a different hostname for processing Exchange Web Service (EWS) traffic. The following procedure describes the steps to configure a different hostname for processing EWS traffic.

Note For SEG version 2.17.0 or later, with the Workspace ONE UEM console version 20.10 and later, perform the SEG configuration using the custom gateway settings. To understand the SEG custom gateway settings, see the *SEG Custom Gateway Settings* topic.

For SEG version before 2.17.0, SEG continues to use the default configuration (pre-defined configuration). If the custom settings feature is not available, manually update the respective files at the individual node and modify the SEG configuration.

1 Navigate to **SEG > Config** folder and open the **application-override.properties** file for editing. See the *Configure the External Configuration File* to understand how to configure the override properties file.

2 Add the property **ews.email.server.host.and.port**. Set the value of this property to the hostname and port of the email server that handles the EWS requests.

3 Save the `applications-override.properties` file.

Note The email server related settings utilized by SEG such as server timeout, `ignoreSslErrorsWithExchange`, and so on is obtained from the email server provided in the MEM configuration wizard.

When you upgrade SEG, the `ews.email.server.host.and.port` always take the default value as false. On SEG upgrade, you can retain this setting in the `application-override.properties` file. See the *Configure the External Configuration File* to understand how to configure the override properties file.

For email servers using a self-signed certificate, you must add that certificate to the Java trustStore on the SEG server. If the certificate is added to the trustStore after SEG installation, you must rerun the SEG installer.

Configure Outbound Proxy between SEG V2 and the Email Server

When SEG cannot reach the email server directly due to network restrictions, the traffic from SEG is routed through the outbound proxy. The outbound proxy is accessible from SEG, and in turn the SEG can reach the email server.

About this task:

If SEG is configured to proxy the EWS requests, then the outbound proxy configuration is also applicable to the EWS traffic. The following procedure describes the steps to enable the outbound proxy between the SEG and the email server.

1 Log in to the SEG server.

2 Navigate to the `proxy-config.json` file and edit the file using any text editor.

Note For the Windows deployment, the **proxy-config.json** file is at the `<SEG_Install_Dir>\config` folder and for SEG on UAG deployment, the file is at the `/opt/vmware/docker/seg/container/config` folder.

3 In the JSON file, update the **emailProxy** field with all the details. The following table lists the description of each field shown in the sample entry.

```
"emailProxy" : {
"enabled" : true,
"host" : "http(s)://example.email.proxy.host:port",
"user" : "example_user",
"password" : "example_password.plaintext"
},
```

enabled	Value - Boolean flag Default value - false	Set this value to **true** to enable the outbound proxy for the email traffic.
host		Specify the FQDN of the proxy in the protocol://host:port format. The protocol can be http or https and the host can be the hostname or IP address of the proxy server.
user		Specify a user name if the proxy needs authentication. **Note** Only basic authentication is supported.
password		Specify a password if the proxy needs authentication. Enter the plain text password with the .plaintext suffix. For example, if **xyz_abc** is the password, then provide **xyz_abc.plaintext** as the value. Upon restart, SEG reads the configuration and overwrites the file with the encrypted password text.

4 Save the changes and restart the SEG service.

Channel SEG Logs to the Syslog Server on Windows

This procedure describes the steps to enable system logs (syslogs) to capture the SEG logs on a Windows platform.

After a SEG upgrade, repeat the steps to set the syslog properties.

1 Navigate to the SEG installation directory: `{SEG_DIRECTORTY}/service/conf`.

2 Edit the `segServiceWrapper.conf` file.

3 Check for the following properties to enable syslog: `wrapper.java.additional.27=-Dsyslog.enabled=false`.

4 Set the `wrapper.java.additional.27=-Dsyslog.enabled=false` property to `wrapper.java.additional.27=-Dsyslog.enabled=true`.

5 Configure syslog, enable the following syslog properties, and remove the `#` before the properties.

```
#wrapper.java.additional.28=-Dsyslog.host=
#wrapper.java.additional.29=-Dsyslog.port=514
#wrapper.java.additional.30=-Dsyslog.facility=USER
```

The syslog configuration in `logback.xml` directs the logs to the syslog host.

```
wrapper.java.additional.28=-Dsyslog.host=
```

The syslog configuration in `logback.xml` uses the port 514 on UDP by default.

```
wrapper.java.additional.29=-Dsyslog.port=514
```

The syslog configuration in `logback.xml` uses the USER as the default facility.

```
wrapper.java.additional.30=-Dsyslog.facility=USER
```

The `app.log` is directed to the syslog server by default.

6 Configure syslog for other loggers and add the syslog appender in the logger element.

```
<if condition="${syslog.enabled}">
    <then>
        <appender-ref ref="SYSLOG_ASYNC"/>
    </then>
</if>
```

7 Restart the SEG service.

Note For SEG version 2.17.0 or later, with the Workspace ONE UEM console version 20.10 and later, perform the SEG configuration using the custom gateway settings. To understand the SEG custom gateway settings, ssee the *SEG Custom Gateway Settings* section in the Chapter 2 Configure the SEG V2 topic.

For SEG version before 2.17.0, SEG continues to use the default configuration (pre-defined configuration). If the custom settings feature is not available, manually update the respective files at the individual node and modify the SEG configuration.

Channel SEG Logs to the Syslog Server on the Unified Access Gateway

This procedure describes the steps to enable the system logs (syslogs) to capture the SEG logs on the UAG platform.

Starting with UAG version 3.7, by default, the SEG is configured to follow the syslog configurations done as part of the UAG system settings. To enable the syslog for UAG, see the *Configure Unified Access Gateway System Settings* topic in the *Deploying and Configuring VMware Unified Access Gateway* guide.

When SEG is deployed on UAG version 3.6, enable the syslog on SEG in addition to the UAG system settings. For more information about enabling syslog for SEG on UAG version 3.6 see the following steps.

1 Open your SSH client and initiate an SSH connection.

2 Edit the SEG java arguments for SEG using the `vi /opt/vmware/docker/seg/container/config/seg-jvm-args.conf` command.

3 Search for the syslog properties, update the values as shown in the example and save the file.

Results: `-Dsyslog.enabled=true`, `-Dsyslog.host=localhost`, `-Dsyslog.port=514`, and `-Dsyslog.facility=USER`.

4 Save the SEG edge service on the UAG admin UI to apply the changes.

5 Enable the syslog for UAG under the **System Settings**.

Note To configure SEG on UAG to log individually any remote syslog server over UDP, update the following properties listed in the `seg-jvm-args.conf` file:

- Update the `-Dsyslog.host` value to the remote syslog server host.
- Update the `-Dsyslog.port` value to the syslog server listener port.
- Save the SEG edge service on the UAG Admin UI to apply the changes.

Note For SEG version 2.17.0 or later, with the Workspace ONE UEM console version 20.10 and later, perform the SEG configuration using the custom gateway settings. To understand the SEG custom gateway settings, see the *SEG Custom Gateway Settings* section in the Chapter 2 Configure the SEG V2 topic.

For SEG version before 2.17.0, SEG continues to use the default configuration (pre-defined configuration). If the custom settings feature is not available, manually update the respective files at the individual node and modify the SEG configuration.

Override Default Heap Memory Allocation

During the SEG v2 installation, by default, SEG v2 dynamically configures a portion of the system RAM as the maximum heap allocation.

Note The JVM heap allocation configuration does not block all the allocated memory. Instead, the configuration defines the maximum limit on the Java heap memory. The Java process starts with the minimum required amount of memory. Based on the requirement, the process might consume more memory from the allocation. The JVM periodically runs garbage collection to free up the space.

You can configure a specific amount of memory for the SEG java process to override the default behavior:

- For SEG version 2.17.0 (UAG 2009) and Workspace ONE UEM Console 20.10 or higher: Override the default memory allocation using the custom gateway settings key **-Xmx**. To reflect the changes made, restart the service. For more information about the custom gateway settings, see the *SEG Custom Gateway Settings* section in the Chapter 2 Configure the SEG V2 topic.
- For SEG version 2.16.0 (UAG 3.10) or Workspace ONE UEM Console 20.06 and earlier: To configure a property value to override the default memory allocation, perform the following steps:

1 In the **application-override.properties** file, add the following entry:
`custom.heap.memory.allocation.in.mb=<value in MiB>`

The value is represented in MiB. For example, you can configure 8 GiB of RAM as `custom.heap.memory.allocation.in.mb=8192`.

2 For Windows deployment, rerun the SEG installer. For SEG on UAG, resave the edge service settings.

SEG Support on UAG

SEG provides secure access to your organization's on-premise email as part of the Unified Access Gateway (UAG) platform. Before deploying SEG on UAG, you must complete the MEM configuration using the Workspace ONE platform.

SEG has the following constraints when deployed on UAG:

- The SEG service on the UAG appliance listens on the port as configured under the **Server Settings** in the MEM configuration.
- The UAG does not support any non-encrypted protocols. Therefore, SEG only supports SSL re-encryption (SSL bridging) or SSL pass through.
- If your API server or email server is using self-signed certificates, the corresponding trusted certificates must be uploaded through the UAG Admin UI or referenced during the PowerShell deployment.
- SEG on UAG always uses port 5701 and 41232 for the clustering ports in the MEM configuration. You cannot configure clustering ports other than 5701 and 41232 with UAG.
- Consider deploying SEG on dedicated UAG instances as SEG requires additional resources that might strain your existing deployment.

For more information about the SEG support on UAG, see the *Secure Email Gateway on Unified Access Gateway* topic in the *Deploying and Configuring VMware Unified Access Gateway* guide.

SEG Migration (Classic)

5

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 deactivate 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, dectivated 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 from the Secure Email Gateway Classic to Secure Email Gateway V2

You can upgrade from SEG Classic to SEG V2.

Before you begin:

- 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

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 UEM API server is https.
API Server Hostname	The hostname of your Workspace ONE UEM API server. This is required to fetch the SEG configuration from the Workspace ONE UEM console.
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 Workspace ONE UEM console.

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

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 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.

Migrate to the SEG V2 with Google

You can migrate from the Classic SEG that is integrated with Google to the SEG V2. SEG V2 does not support the credential impersonation that was available on 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.

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 **Devices > Mobile and endpoints > Universal settings > Data Access > Google Sync**.

3 Select the **Google Sync IP Whitelist** text box and enter the external SEG IPs that you want to allowlist.

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 activate or deactivate 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 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 deactivated, 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 deactivated 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 Restart the SEG service.

Email Management

6

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 deactivated. 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.
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 activate 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.

Email Policy	Description
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 Airwatch Browser present on the device. The Secure Email Gateway dynamically modifies the hyperlink to open in Airwatch Browser. The Modifications Types are All, Include, and Exclude. ■ **All** - Allows device users to open all the hyperlinks with Airwatch Browser. ■ **Include** - Allows device users to open only the hyperlinks through the Airwatch 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 Airwatch 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 Activate 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.

1 On the UEM console, navigate to **Email > Compliance Policies**. By default, the policies are deactivated 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**.

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

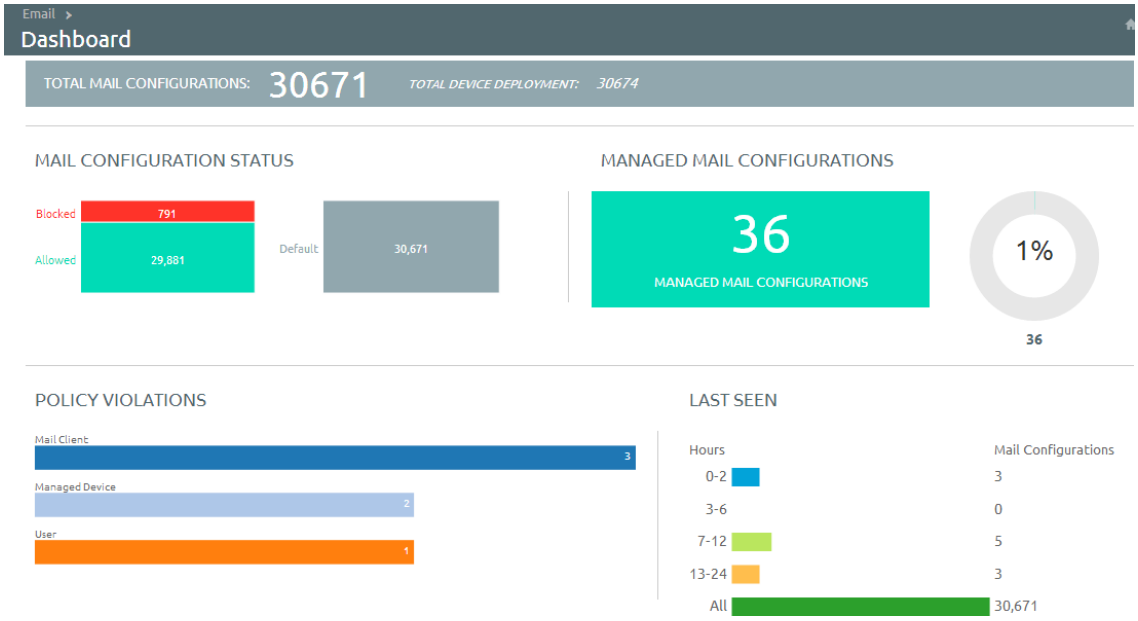
The **Email Dashboard** helps you to gain visibility into the email traffic and helps monitor the devices.

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:

■ Allowlist or denylist 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 allows 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, Blocked, Approved, 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.

- **Allowlist** - Allows a device to receive emails.
- **Denylist** - 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 activated, you can view a message displaying Test Mode Enabled on the List View screen. The activating or deactivating 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.

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. For Android Hub 4.2 and above, the end users have to install the Lotus Notes manually.

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.

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