Secure Email Gateway (SEG) V2

VMware Workspace ONE UEM 2005

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Introduction to 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.

The Secure Email Gateway Architecture

2

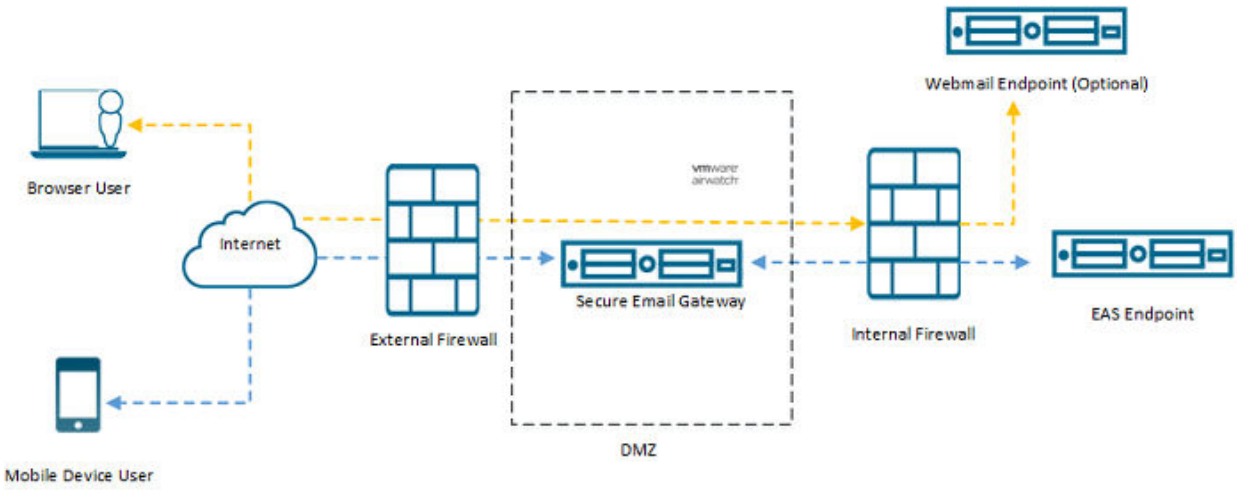
Deploy the SEG to enable the policy creation that determines how end-users access mail on their devices. It is optimal to install the Secure Email Gateway (SEG) in a Demilitarized Zone (DMZ) or behind a reverse proxy server.

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

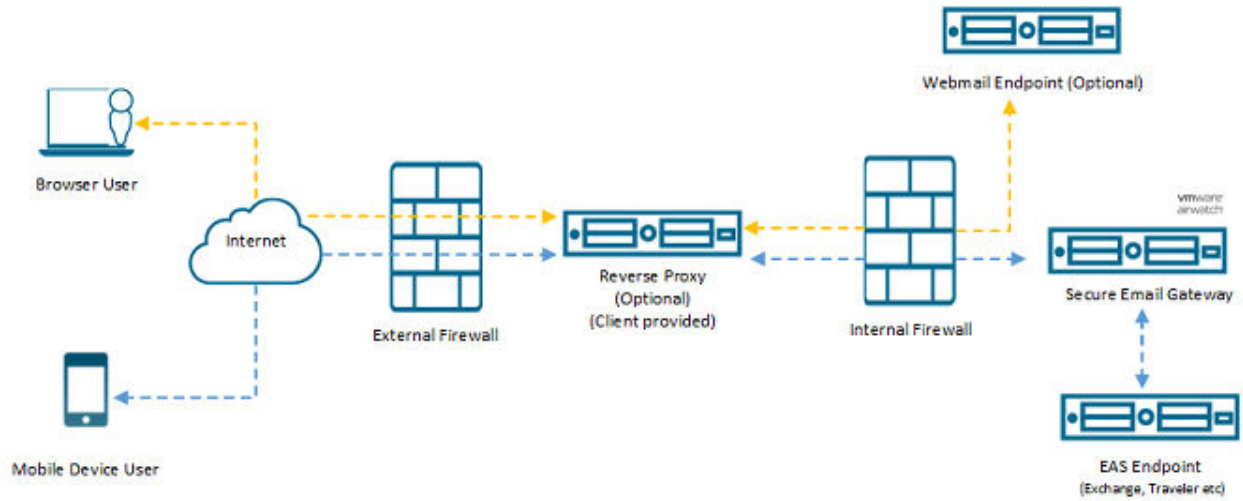
Workspace ONE UEM best practices support this configuration. The SEG is placed in the DMZ for routing mobile email traffic.



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.

Requirements for the Secure Email Gateway (V2) 3

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
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.	

This chapter includes the following topics:

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. The Workspace ONE team is evaluating the performance of combining SEG with other edge services on UAG.

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.

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.

Configure the SEG V2

To implement the SEG (V2) for your email architecture, first configure the settings on the UEM console. After you configure the settings, you can download the SEG installer from the Workspace ONE resource portal.

Procedure

1. In the UEM console, navigate to **Email** > **Settings** and select **Configure**. The **Add Email Configuration** wizard displays.
2. In the **Platform** tab of the wizard:
   a. Select **Proxy** as the **Deployment Model**.
   b. Select 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 enabled for SEG, the SSL certificate is bound to this port.
Terminate SSL on SEG	Enable 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.
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 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 enable clustering of multiple SEG servers. When clustering is enabled, 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. Enable 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 enabled by default. To modify the advanced settings, you must uncheck this box.
Enable Real-time Compliance Sync	Enable 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 disabled.
Optional transactions	Enable or disable 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 enabled.
Sizing	Set the frequency of SEG and API server interaction.
Skip Attachment & Hyperlink transformations for S/MIME signed emails	Enable to exempt the encryption of attachments and transformation of hyperlinks through SEG for emails that are signed with S/MIME certificates.
Enable S/MIME repository lookup	Enable to permit the automatic lookup of the S/MIME certificate managed in a hosted LDAP directory. You must restart SEG after enabling this feature.
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.

Install the Secure Email Gateway (V2)

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

Procedure

1 Run the installer as an administrator. In the **AirWatch Secure Email Gateway - InstallShield Wizard** window. Click **Next**.

2 Accept the **End User License Agreement**.

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

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

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

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

Settings	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**.

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**.

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, disable 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 SNI configuration is not applicable.

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.

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.

Procedure

1 Navigate to **SEG > Config** folder.

2 Select the **application.properties** file and edit the file.

   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`

3 Add the **enable.boxer.ens.ews.proxy=true** entry in the **application-override.properties** file.

4 Save the file.

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

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.

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

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.

Prerequisites

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.

Procedure

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

   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.

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

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.

Procedure

1 In the SEG `applications.properties` file locate and modify the `ews.email.server.host.and.port` value.

2 Enter the hostname and port of the email server that handles the EWS requests.

3 Save the `applications.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 `seg-application-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.

The SEG V2 Admin Page

You can use the SEG V2 Admin page to monitor the health, logging levels, and diagnostics of your SEG.

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

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

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/cluster`	Returns SEG diagnostic information. By default, the SEG diagnostic information is displayed on the diagnostics page.
`/policy/segconfig`	Returns the SEG configuration settings.
`/policy/<Policy Type>/<Policy Lookup Key>`	Look up the policies in the SEG cache.
`/cache/<Policy Type>/`	Download records related to policy types including devices, accounts, managed attachments, unmanaged 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.

Channel SEG Logs to the Syslog Server

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.

Procedure

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.

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.

Procedure

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.

`–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.

Migrate from the Secure Email Gateway Classic to Secure Email Gateway V2

You can upgrade from SEG Classic to SEG V2.

Prerequisites

- You must have an older version of SEG already installed on the host machine.
- Ensure that the installer for latest version of SEG V2 is available on the host machine.
- MEM configuration for SEG V2 is available

Procedure

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

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

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

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

4 Verify the Workspace ONE UEM API information.

Settings	Description
HTTPS	Select the check box if the protocol Workspace ONE UEMAPI server is https.
API Server Hostname	The URL of your Workspace ONE UEM API server. This is required to fetch the SEG configuration from the Workspace ONE UEM console.
Admin Username	The user name of a Workspace ONE UEM Admin user account, that was used during earlier installation.

Settings	Description
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.

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

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

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

Email Management

4

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

Note

- Mail client compliance is not supported on Windows Phone.
- The Sync Settings policy is not applicable for SEG V2 architecture.

General Email Policies

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

Email Policy	Description
Sync Settings	Prevents the device from syncing with specific EAS folders. Workspace ONE UEM prevents devices from syncing with the selected folders irrespective of other compliance policies. For the policy to take effect, you must republish the EAS profile to the devices as this forces devices to re-sync with the email server.
Managed Device	Restricts email access only to managed devices.
Mail Client	Restricts email access to a set of mail clients.
User	Restricts email access to a set of users based on the email user name.
EAS Device Type	Allow or block devices based on the EAS Device Type attribute reported by the end-user device.

Managed Device Policies

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

Email Policy	Description
Inactivity	Prevents inactive and managed devices from accessing email. You can specify the number of days a device shows up as inactive before email access is disabled. The minimum accepted value is 1 and maximum is 32767.
Device Compromised	Prevents compromised devices from accessing email. Note that this policy does not block email access for devices that have not reported compromised status to VMware AirWatch.

Email Policy	Description
Encryption	Prevents email access for unencrypted devices. Note that this policy is applicable only to devices that have reported data protection status to VMware AirWatch.
Model	Restricts email access based on the platform and model of the device.
Operating System	Restricts email access to a set of operating systems for specific platforms.
Require ActiveSync Profile	Restricts email access to devices whose email is not managed through an Exchange ActiveSync profile.

Email Security Policies

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

Email Policy	Description
Email Security Classification	Define actions for SEG to take against emails that are with or without security tags. You can either use predefined tags or create your own tags. You can enable restricted access to VMware AirWatch Inbox and Workspace ONE Boxer based on these tags and define the default behavior for other email clients. You can either allow or block emails. If you choose to block emails, you can replace the email contents with a helpful message using the available templates configured at Message Template settings. These configured templates can be selected from the Select Message Template drop-down menu. Also, lookup values are not supported for Block Email message template.
Attachments (managed devices)	Encrypt email attachments of selected file type with an encryption key unique to the device - user combination. These attachments are secured on the device and are only available for viewing on the VMware AirWatch Content Locker. This is only possible on managed iOS, Android, and Windows Phone devices with the VMware AirWatch Content Locker application. For other managed devices, you can either allow encrypted attachments, block attachments, or allow unencrypted attachments.
Attachments (unmanaged devices)	Allow encrypted attachments, block attachments, or allow unencrypted attachments for unmanaged devices. Attachments are encrypted for unmanaged devices to prevent data loss and maintain email integrity. The attachments of unmanaged devices cannot be opened in VMware AirWatch Content Locker.
Hyperlink	Allow device users to open hyperlinks contained within an email directly with VMware Browser present on the device. The Secure Email Gateway dynamically modifies the hyperlink to open in VMware Browser. The Modifications Types are All, Include, and Exclude. ■ **All** - Allows device users to open all the hyperlinks with VMware Browser. ■ **Include** - Allows device users to open only the hyperlinks through the VMware Browser. Mention the included domains in the Only modify hyperlinks for these domains field. You can bulk upload the domain names from a .csv file as well. ■ **Exclude** - Does not allow the device users to open the mentioned excluded domains through the VMware Browser. Mention the excluded domains in the Modify all hyperlinks except for these domains field. You can bulk upload the domain names from a `.csv` file as well.

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

This chapter includes the following topics:

- Email Dashboard
- List View
- Configure and Deploy Email Profile

Activate Email Compliance Policy

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

Procedure

1 On the UEM console, navigate to **Email > Compliance Policies**.

By default, the policies are disabled and are denoted by red color under the **Active** column.

2 Select the gray button under the **Active** column to activate the compliance policy.

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

3 Select **Save**.

Results

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

What to do next

Use the edit policy icon under the **Actions** column to allow or block a policy.

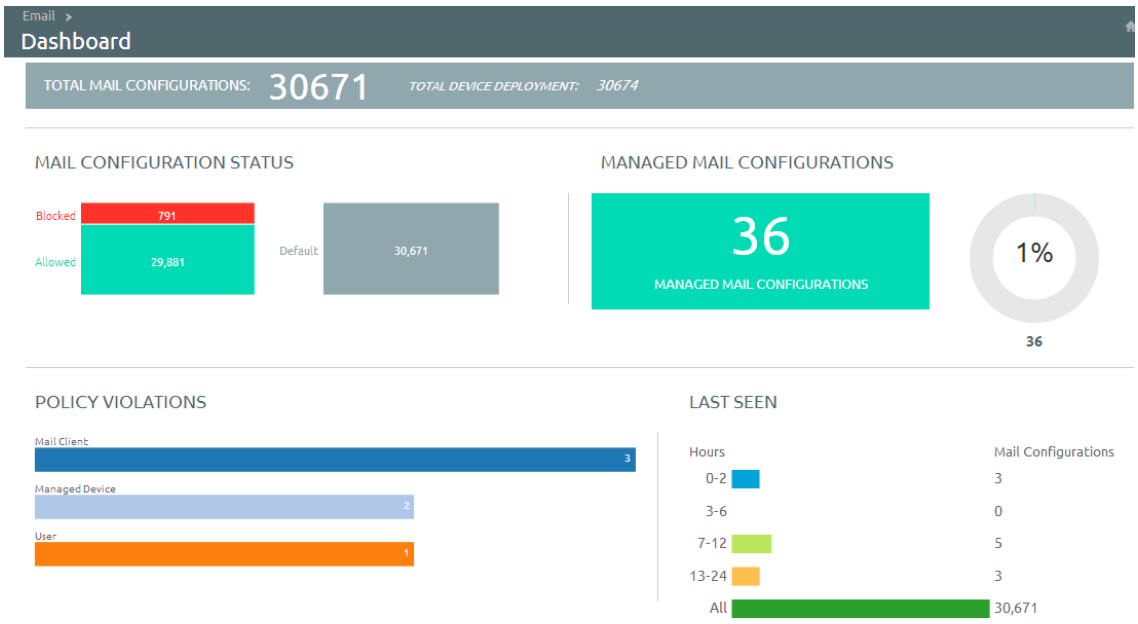
Email Dashboard

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

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

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

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



List View

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

The List View page enables you to:

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

Device and User Details

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

- **Last Request** - In SEG integration this column shows the last time a device synced mail.
- **User** - The user account name.
- **Friendly Name** - The friendly name of the device.
- **MEM Config** - The configured MEM deployment that is managing the device.
- **Email Address** - The email address of the user account.
- **Identifier** - The unique alpha-numeric identification code associated with the device.
- **Mail Client** - The email client syncing the emails on the device.

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

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

Filters for Quick Search

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

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

Perform Actions

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

- **Override**

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

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

- **Actions**
  - **Run Compliance** - Triggers the compliance engine to run for the selected MEM configuration.
  - **Enable Test Mode** - Test email policies without applying them on devices. Once enabled, you can view a message displaying Test Mode Enabled on the List View screen. The enabling / disabling Test Mode does not require you to run compliance engine.
- **Administration**
  - **Dx Mode On** - Runs the diagnostic for the selected user mailbox.
  - **Dx Mode Off** - Turns off the diagnostic for the selected user mailbox.
  - **Update Encryption Key** - Resets the encryption and the re-syncs the emails for the selected devices.
  - **Delete Unmanaged Devices** - Deletes the selected unmanaged device record from the dashboard. This record may reappear after the next sync.

Configure and Deploy Email Profile

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

Procedure

1. Navigate to the **Devices** > **Profiles & Resources** > **Profiles** on the UEM console, and then select **Add** to create a new profile.
2. Select a device platform.

   If you are leveraging the SEG for multiple device operating systems, you must create a similar profile for each platform.
3. Enter the information about the profile on the **General** tab and assign the profile to the applicable organization groups and smart groups. Keep the assignment type as **Auto** or **Optional**.
4. Select **Exchange ActiveSync** and select **Configure**. Configure the following parameters to access corporate mail through the SEG.
   a. Select the **Mail Client** that your organization intends for end users to utilize from the drop-down menu.
   b. Ensure the **Exchange ActiveSync Host** is the host name of the SEG server and not the Exchange server.
   c. Leverage lookup values so each user can get their own distinct email.

      Leave the **Password** field blank. This prompts the end user to enter a password after the profile is installed on the device.
5. Click **Save and Publish** to begin using secure mobile email.

What to do next

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

SEG Migration (Classic)

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 disable or remove the existing configuration.
- **Upgrade an existing configuration** - You can edit the existing SEG configurations and upgrade it to include the necessary settings for the V2 platform. This migration maintains the existing Classic configuration settings and does not affect the existing SEG servers.

You can upgrade your existing SEG software to the V2 platform without interrupting the current SEG functionality. To upgrade, run the installer for the SEG V2 platform on the existing SEG server. After completing the installation, disable the World Wide Publishing service and restart the SEG service. This action transfers the device connections, refreshes the 443 listener from IIS, and allows the new SEG service to claim it. You can also run the V2 platform on a distinct port and connections transferred over at the network layer. To verify the SEG has properly restarted, check whether the localhost returns your IP address on the proper port.Attempt to access the Classic platform (IIS) displays the following screenshot:

The V2 platform displays the following screenshot:

This chapter includes the following topics:

- Migrate to the SEG V2 with Google

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.

Procedure

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

Configure Automatic Password Provision and Sync Passwords

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

Procedure

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

   The **Add Email Configuration** wizard displays.
2. Select **Add**.

   The wizard displays Platform tab.
   a. From Deployment Model, select **Proxy**.
   b. From Email Type, select **Google** and select **Next**.

      The Deployment tab opens and displays the basic settings.
3. In the Google Apps Settings section, you can see that the Automatic Password Provision is in Enabled mode. This is because Classic SEG uses Automatic Password Provision when integrating with Google.
   - If you are providing the SSO password and Google password to your device users, select **Disable**. The users must enter their credentials to access Google. When the automatic password management is disabled, the Google Sync password is managed within your organization, which provides more flexibility and control over the devices accessing Google.
   - If you want to use password provision using the UEM console, keep the Automatic Password Provision **Enabled**. The information you have entered when configuring Classic SEG with Google is used to provision the Google Sync Password. The password provisioning works without any interruptions to the user experience.
4. After selecting the required Automatic Password Provision setting, select **Next** to navigate through the wizard and select **Finish**.

5 If you have disabled the Automatic Password Provision setting, navigate to the device List View and select **Actions** drop-down menu.

6 Select **Sync Passwords** to synchronize the passwords on the device and Google Sync server. If you have kept the Automatic Password Provision enabled, the Sync Passwords function is not available from the Actions drop-down menu.

7 Restart the SEG service.