Home > Secure Email Gateway V2 > Introduction to the Secure Email Gateway (V2)

Introduction to the Secure Email Gateway (V2)

Version: SaaS | Last Updated Apr 9, 2025 | 5 minute read | Summarize |

Omnissa Workspace ONE UEM Product Documentation SaaS

The Secure Email Gateway V2 (SEG V2) helps to protect your mail infrastructure and enables 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 Omnissa 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, Omnissa cannot guarantee full support for Classic SEG. For more information about the End-of-Life terms.

To read about the Classic SEG information, see the *Secure Email Gateway 1811 guide*.

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:

1. Navigate to **Groups & Settings** > **All Settings** > **System** > **Advanced** > **API** > **REST API**.

ON THIS TOPIC

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
- Windows Server 2022

Networking Requirements

The SEG uses the following default ports:

Source Component	Destination Component	Protocol	Port	Desc
Devices (from Internet and Wi-Fi)	SEG	HTTPS	443	Devi SEG
Console Server	SEG	HTTPS	443	Cons adm to SE
SEG	Workspace ONE UEM REST API (Device Services (DS) or	HTTP or HTTPS	80 or 443	SEG conf com infor

	Console Server (CN) server)			
SEG	Internal hostname or IP of all other SEG servers	TCP	5701 and 41232	If SE then shar othe repli
SEG	localhost	HTTP	44444	Adm serv diag from mac
Device Services	SEG	HTTPS	443	Enro time com
SEG	Exchange	HTTP or HTTPS	80 or 443	Verif acce brow and cred `htt Ser FQDI Ser`

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.

Note: You can download the latest SEG version directly from the Omnissa Customer Connect.

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

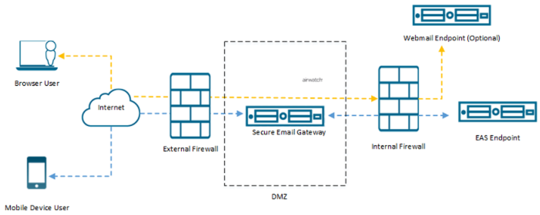
Deploy the SEG to enable the policy creation that determines how end-users access mail on their devices. It is optimal to install the Secure Email Gateway (SEG) in a Demilitarized Zone (DMZ) or behind a reverse proxy server.

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

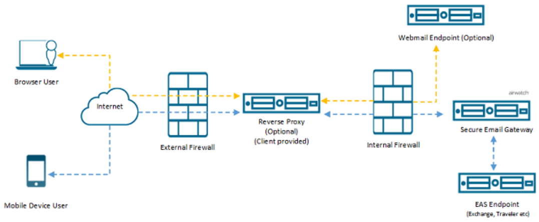
Workspace ONE UEM best practices support this configuration. For routing mobile email traffic deploy SEG in the DMZ .



Note: To route mobile email traffic, Omnissa recommends configuring the SEG with Exchange ActiveSync.

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.