

VMware AirWatch Mobile Email Management Troubleshooting Guide

Workspace ONE UEM v9.6

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

- Chapter 1: Introduction to Troubleshooting Guide 3**
 - Overview 4

- Chapter 2: Troubleshooting Tips 5**
 - Troubleshooting Secure Email Gateway 6
 - Troubleshooting PowerShell 14
 - Troubleshooting Google Apps for Work 14

Chapter 1:

Introduction to Troubleshooting Guide

Overview 4

Overview

During or after integrating AirWatch Mobile Email Management's deployment models with your email infrastructure, you might experience some issues. The causes and the tips to troubleshoot such issues when they occur are discussed in this guide. The targeted audiences for this guide are the IT Administrators and the technical executives who manage your organization's email infrastructure that is integrated with AirWatch Mobile Email Management (MEM).

Chapter 2:

Troubleshooting Tips

Troubleshooting Secure Email Gateway	6
Troubleshooting PowerShell	14
Troubleshooting Google Apps for Work	14

Troubleshooting Secure Email Gateway

The errors that you might encounter while integrating the Secure Email Gateway (SEG) proxy deployment model with your email infrastructure are categorized in the tables.

Error	Cause	Solution
SEG Web Listener		
Touchdown does not receive email. All other mail clients do not have issues	An HTTP redirect is defined at the default website to redirect all traffic to Exchange. It is propagated down to all child applications	Remove redirect or limit to default website only
Users are unable to send large attachments	The default IIS settings limit file size is 4 Mb	Add the following in the listener web.config: <code><system.web> <httpRuntime maxRequestLength="10240" /></system.web></code>
The revocation function unable to check revocation as the revocation server was offline	You are using certificate authentication	The SEG listener server must be running in the same domain as the CA that has issued the identity certificate
HttpResponse status: 413 (RequestEntityTooLarge): Request Entity Too Large	The CAS server is most likely using IIS6. You are probably also using client certificates to authenticate or the attachment size is limited to 50 Kb	Increase the uploadReadAheadSize IIS setting on the CAS server. From IIS ->Microsoft-Server-ActiveSync web app > select ConfigurationEditor > system.webServer > serverRuntime > uploadReadAheadSize on the CAS server
Emails are not getting sent from the device. They disappear from the outbox but does not show up in the sent items folder	Weak device connection	Upgrade to 6.1 SP 1 or 6.1 HF4 or above

Error	Cause	Solution
415 Unsupported Media Type or 401 Unauthorized	You are trying to connect to a Lotus Domino server. The exchangeActiveSyncUrl setting in the listener web.config file is missing the Microsoft-Server-ActiveSync part	<ol style="list-style-type: none"> 1. Add Microsoft-Server-ActiveSync to the URL. i.e. <code>exchangeActiveSyncUrl=""https://lotuslab01.awmdm.com/servlet/traveler/Microsoft-Server-ActiveSync"</code> 2. This might also be caused if there is a trailing slash on the end of the URL
Cert Auth: Logged warning: System.Net.WebException: The remote server returned an error: (401) Unauthorized.	You are using KCD for certificate authentication and the CRL distribution list cannot be reached. Or the identity certificate is otherwise invalid.	Run the following command on the SEG server to validate the certificate chain of the identity certificate. The cert must be .cer and text file can be created at the current directory. <code>certutil -nse urlfetch -verify certname.cer > cert.txt</code>
Touchdown and Lotus Notes server issue: 449 Retry after provision keeps getting returned and the folder syncs never complete. Typically you can not finish the TD quick config setup process	–	The SEG installation only creates the first app path. Manually create the second app path and email should start syncing. Note that both app paths point to the same AppPool and the mail server URL defined in the SEG listener web.config remains unchanged and should have no trailing slash (<code>http(s)://mail-serverhostname/servlet/traveler/Microsoft-Server-ActiveSync</code>)
SSL Cert Errors	–	After changing the Ignore SSL Errors setting, you may need to do an App pool restart or IIS Reset for the setting to take affect.
Mails not syncing	The SEG version should be the same as the console version for the mails to sync. This is intermittent in nature.	Download the latest installer from the AirWatch Console and install it on the SEG server.

Error	Cause	Solution
Mails not syncing on the devices	Load on the SEG server	Increase the server cores and worker threads on the SEG server (VM Admin has to carry out these changes) Refer the link for more info on increasing the worker threads: http://stackoverflow.com/questions/4571118/how-to-increase-thread-pool-threads-on-iis-7-0
SEG mailbox crashing on iOS	SEG version not updated	Upgrade to the latest version of SEG

Error	Cause	Solution
SEG Integration Service		
Exceptions		
Insufficient resources to perform operation	MSMQ have queue level quotas and machine level quotas. The queue level quotas are usually not set. The machine level quota defaults to 1 GB worth of combined messages for all queues. If the quota exceeds you see this message.	Check MSMQ queues on the MEG Queue Reader server. If any of the queues are overflowing with messages, restart the related Queue Reader services and optionally purge the overflowed queue.
The private key is not present in the X.509 certificate	Private key for the client certificate is missing. The AirWatchServices API AppPool user (Network Service by default) must have access to the private key.Or permissions problem with the client certificate's private key	On the SEG server, make sure the client cert is in the Local Computer > Personal Store and has a private key with full permissions for the AppPool user (usually Network Service)
Keyset does not exist	The AirWatchServices API AppPool user (Network Service by default) must have access to the private key.	On the SEG server, make sure the client cert is in the Local Computer > Personal Store and has a private key with full permissions for the AppPool user (usually Network Service).
Could not establish trust relationship for the SSL/TLS secure channel with authority "Invalid hexadecimal string format"	Caused by copying a certificate thumbprint from the certificate properties dialog to the .config file. In some cases the certificate thumbprint has an invalid leading character.	The root issuing certificate authority cert for the SSL cert needs to be added to the Local Machine / Trusted Root Certification Authorities store on the MEG server.
An unsecured or incorrectly secured fault was received from the other party. See the inner FaultException for the fault code and detail.: An error occurred when verifying security for the message	1. Time Synchronization Issue. The EAS Integration Service and the AirWatchServices API must be UTC time synchronized to within 5 minutes. 2. Requests are being SSL Offloaded by the server. 3. Certificate Trust error (not common)	1. Sync server times. 2. Use bindingMode="Ssloffload" in the API web.config for the ActiveSyncIntegrationServiceEndpoint. 3. Add the SEG client certificate to Trusted People (and possibly Personal) store on AirWatchServices API and give rights to manage the private key. Please note this happens randomly with some certificates. Typically certificate chain trust is acceptable.

Error	Cause	Solution
<p>An unsecured or incorrectly secured fault was received from the other party. See the inner FaultException for the fault code and detail. At least one security token in the message could not be validated</p>	<ol style="list-style-type: none"> 1. Client certificate is missing from the Local Computer > Trusted People Store on the API server. 2. You are using username/password authentication and the user's role does not have the "Remote Services - Security - Allow Remote Access " permission set. 	<ol style="list-style-type: none"> 1. Add the client certificate to the Local Computer --> Trusted People store on the API server. A private key is not required. 2. Add the required permission.

Error	Cause	Solution
SEG Console		
Webpage shows error: Could not load type 'System.ServiceModel.Activation.HttpModule' from assembly 'System.ServiceModel...'	.NET version issue	http://msdn.microsoft.com/en-us/library/hh169179(v=nav.70).aspx
The test connection fails on the console even after fulfilling all the pre-requisites	You do not have a port binding for port 80	Created a port binding on the IIS that points to port 80.

Error	Cause	Solution
SEG queue		
(Gmail)Logged Exception: AW.Meg.Queue.S ervice.Processors.UserProvisioning Processor ... Captcha required	Administrator user is locked; wrong password might have been used many times.	Go to this page and unlock the Administrator: https://accounts.google.com/DisplayUnlockCaptcha . Make sure the correct Administrator password is entered in system settings for Mobile Email > Gmail.

Error	Cause	Solution
SEG Device Errors		
Device does not show up on the Email Management Dashboard	Log Error in Web Listener/EAS integration service/SEG Queue reader service	<p>On the Web Listener: Check for any errors and attempt to resolve these first. The device first hits this service, so this is the first checkpoint</p> <p>On the EAS Integration Service: Check for any errors, and attempt to resolve these. Typical issues are either a certificate issue or the fact that the Integration Service did not properly restart after installation. If the Web Listener does not show error, it is possible that the next step in the communication path, i.e. the EAS Integration Service has an issue</p> <p>On SEG Queue Reader Service: Check for any errors, this service writes device related information to the database, which is then read by the console and displayed on the dashboard.</p>
Policy update issues	—	<p>Change the following configuration files to verbose logging :</p> <ul style="list-style-type: none"> • SEG Queue Reader service (requires service restart) • SEG Console (requires app pool recycle) <p>Check the logs for errors pertaining to the following:</p> <ul style="list-style-type: none"> • Communication errors between the MEG Queue Reader service and the SEG console Check for network errors that might prevent successful communication. • Check for errors in the MEG Queue Reader service in reading the policies off the queue and provisioning them to the SEG server.

Error	Cause	Solution
Other Issues		
Test connections fails on an Office 365 setup	Office 365 was setup with DirSync and federated services, so AUTH for the cloud redirects to prospects servers. This causes the test connections to fail but the integration actually works	Verify this once the setup is done and mail flow happens normally
Test connection fails while installing SEG	The user does not have proper role	Check the user roles, the user should have EAS enabled to his ID. Also, right click on the user and grant access to EAS on Exchange
Test connection fail - connectivity between AirWatch and SEG	The Local DNS could not resolve the host	In the local machine (SEG) edit the host file (C:\Windows\System32\Drivers\etc\hosts) to redirect the as510.awmdm.sg to the corresponding IP address (as510.awmdm.sg)
Post upgrade to 7.1HF2, some customers reported that SEGs were incorrectly treating enrolled devices as unmanaged	A mailbox user had a very long name (256 characters) that resulted in a failure to migrate it correctly to a column whose max length was 255-characters This resulted in the migration script failing, hence all pre-existing, managed devices were not migrated to the new MEM table structure	Check the profile and disable Multi MEM
Test connection while configuring SEG failed between SEG and AirWatch	SEG was not able to communicate with API	The AirWatch API website was set to use the API app pool instead of the Default App Pool: The change had to be made, set the binding mode back to Default on the services web.config file and was able to confirm that the SEG Setup went past the API URL and username/password stage in my test SEG install.
Test connection fail - Connectivity between AirWatch and SEG	The service does not start some times, so before checking the logs, it is better to start the service and try test connection again.	Restart or force start the AirWatch EAS Integration Service

Troubleshooting PowerShell

Determine the causes and solve the errors by using the solutions mentioned in the table.

Error	Cause	Solution
Error running New-PSSession command: The SSL certificate is signed by an unknown certificate authority	Exchange SSL Cert missing from client computer.	Install the Exchange Server's SSL Cert on the calling computer in Trusted Root. You should be able to log into OWA without seeing a cert error
The WinRM client cannot process the request. The authentication mechanism requested by the client is not supported by the server or unencrypted traffic is disabled in the service configuration. Verify the unencrypted traffic setting in the service configuration or specify one of the authentication mechanisms supported by the server	Basic Authentication is not enabled for the PowerShell web application on the Exchange server.	Enable Basic Authentication.
Exception Message : A positional parameter cannot be found that accepts argument '[ActiveSyncAllowedDeviceIDs]'. + CategoryInfo: InvalidArgument: (:) [Set-CASMailbox], ParameterBindingException + FullyQualifiedErrorId: PositionalParameterNotFound,Set-CASMailbox	The executing user (the PowerShell admin defined in system settings) does not have appropriate permissions.	Make sure the PowerShell admin user has the necessary permissions for mail management. See the Shell Infrastructure Permissions section. http://technet.microsoft.com/en-us/library/dd638114.aspx

Troubleshooting Google Apps for Work

Google Apps integration (password retention) involves automatic policy provisions as well as manual actions.

Error	Cause	Solution
Web console error during Google Apps integration	-	<ol style="list-style-type: none"> 1. Change AW Web Console and AW SEG Queue Reader Service configuration files to verbose logging 2. Check whether commands are being written to the MEG Queue Reader properly 3. Check whether AW is able to make Google Apps connections and issue password provision commands successfully 4. Check whether data is being written to the DB properly