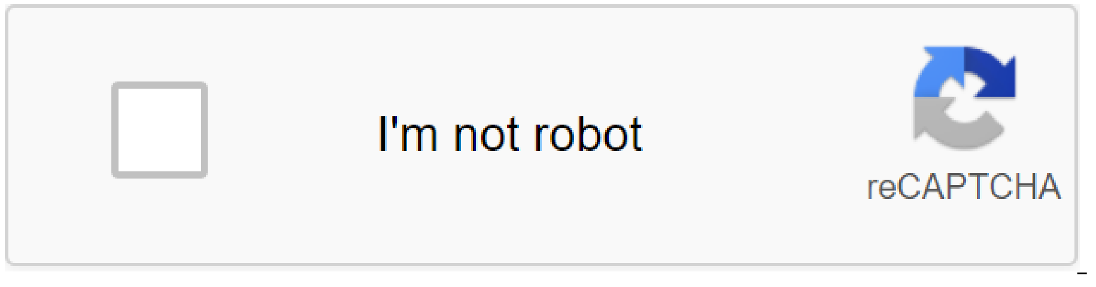
Airwatch seg configuration guide



Continue

Workspace ONE UEM based on AirWatch Secure Email Gateway V2 (SEG V2) helps protect your email infrastructure and allows VMware AirWatch Mobile Email Management (MEM) functionality. Install SEG along with your existing email server to transfer all ActiveSync mail traffic to devices registered in Workspace ONE UEM. Based on the parameters you define in the Workspace ONE UEM console, SEG filters all communication requests from individual devices that connect to SEG. Thank you for using our services. We are a non-profit group that manages this document-sharing service. We need your help to maintain and improve this site. To keep our site running, we need your help to cover our server costs (about $500/m), a small donation will help us a lot. Please help us share our service with your friends. You read free preview pages from 8 to 13 do not appear in this preview. You read free preview pages from 17 to 26 do not appear in this preview. You read free preview pages from 31 to 42 do not appear in this preview. You read the free 8 preview page not shown in this preview. You read free preview pages from 15 to 38 do not appear in this preview. AirWatch series post Number 3 today, we will be focusing on secure email gateway (SEG) and mobile access gateway (MAG) features AirWatch. By now you have a good understanding of what AirWatch is and how it works with a high level of view, today we're going to go a little deeper and discuss these two features and whether or not you need to install them. What is SEG and what does it do? As part of AirWatch's Enterprise Mobility solution, SEG provides an increased level of protection and control over your organization's corporate email. Everyone wants to access the email all the time and they want it in the palm of their hand. While 24/7/365 access to corporate email on the go is a good headache, there are inherent security risks that need to be addressed and mitigated and the inclusion of SEG will help you get there. Some of the known risks to corporate email are: Inappropriate devices - Leaving a BYOD/corporate device in a booth or restaurant gives strangers access to your email. Intercept Messages - With WiFi on your phones, you leave the front door open for your device for those who scan tools that have the know-how to intercept email traffic. Mobile malware - Yes, malware is mobile! Phones are very to malware attacks, especially root or ROMd phones that do not comply with your organization's BYOD program. So what does SEG do to hit these risks head on and apply a security blanket to your corporate email infrastructure? SEG can do a number of things to keep you safe, and when implementing all of them is not strictly necessary, you can find some features that will help you feel warm and fuzzy about your email on Here's how SEG saves the day: White List/Blacklist devices - SEG can be configured to allow certain devices access to corporate email. If you have corporate devices in your organization, you can create a white list and allow SEG to transfer mail traffic to all devices on the white list. Conversely, if you have devices that need to be blocked from accessing email, you can create a blacklist to seg block email traffic on those devices. Email Attachment Security - With email comes email attachments and one of the easiest ways malware and viruses are introduced into the corporate network. When you deploy SEG, you can be sure that you can set up and determine how you would like your email attachments to work within your organization. You can set up SEG to get email attachments to open up in an approved app, such as AirWatch's mobile content management tool, Content Locker's Advanced Administrative Control - SEG gives administrators more control over mail traffic that enters and exits the organization. You can monitor email activity dashboards as administrators to detect, isolate, and manage email according to your organization's policies. To give you an idea of how SEG is positioned in line with network resources and email infrastructure, check out the charts below; The first chart is the deployment of SEG with Exchange ActiveSync and without a proxy in the DMH. The second diagram shows the SEG proxy relay in the SEG with SEG behind the corporate firewall. Exchange ActiveSync SEG Configuration Exchange ActiveSync SEG Using a reverse proxy configuration in each organization There are certain internal resources that we do not want to be exposed to the Internet or devices that do not comply with the BYOD program. However, do you want to maintain an environment in which your employees can be productive when mobile, so how do you solve this problem? That's where the mobile access gateway comes into play. Let's first look at some things that you don't want to happen to your corporate assets. Data Leakage - In today's corporate world, I think we know all too well about the possibility of data leakage. Even high-level government data is not safe in some known recent cases, so it is important to take precautions against data leaks. Data Corruption - Many hackers today just want to get behind a firewall or use your employee's device in order to corrupt corporate data. Corporate Espionage - There Are there, and third-party partners who will be looking to collect all they can from your corporate data that are exposed to the web. Obviously hacking the network through the firewall is a criminal offense, but picking up the staff phone left in the bar and browsing is most definitely not an illegal crime. How MAG protects you that kind of threat? First, user training should be your first line of defense, and since you can't always trust end users to follow security guidelines, you need to take another active step. The introduction of MAG will allow users and devices to go through the firewall and get the corporate data they need to do their work on the go. Here are a few things you can customize MAG to do for your organization: Document repository - MAG can create internal document and content repositories in collaboration with AirWatch Locker Content. Secure Internal Websites - MAG will allow you to protect the company's internal websites by forcing users to use AirWatch Secure Browser. The Tunneling App - This is a feature that is only for iOS 7 and above devices. AirWatch Tunnel users can access internal resources through secure tunneling. To see if your typical and more advanced AirWatch deployment, including MAG, will show you what a typical AirWatch deployment with MAG might look like, and the second is a more advanced MAG deployment with the endpoint of the relay. Simple deployment of MAG Extended DEPLOYMENT MAG with relay and loadbalancer. Do you need one of them? If AirWatch is installed in your environment and you care about the security of your company's mobile mail and internal resources, then the answer is simple... Yes. If you don't have NI SEG or MAG deployed now, find out more about it, contact me or contact your AirWatch/VMware sales person for help in getting it deployed if you don't know how to do it. SEG is built into the AirWatch console, can be downloaded and deployed from the proxy section of the email. Be proactive with security, not reactive. As the late great President John F. Kennedy said, The time to repair the roof is when the sun is shining. Well, put it down. BlockLevelEncryption BlockLevelEncryption True if the block-level encryption is enabled; otherwise false. Boolean ComplianceStatus complianceReason Values: compatible, incompatible. String ComplianceStatus is true if the status corresponds to MDM policies; otherwise false. Boolean CompromisedStatus CompromisedStatus True if status is compromised; otherwise false. Boolean CompromisedStatus is compromised if the device is compromised; otherwise false. Boolean DataProtectionEnabled DataProtectionEnabled True if data protection is enabled; otherwise false. Boolean DeviceFriendlyName deviceName Concatenat name used to identify device/user combination. The EnrollmentStatus line is Edrolled True if the mdm value is registered; otherwise false. Boolean FileLevelEncryption True if file-level encryption is enabled; otherwise false. Boolean Id.Value deviceId Device ID. Line Imei IMEI DEVICE number. Line Line IsPasscodeCompliant True if the password is in line with THE MDM policy; false otherwise Boolean IsPasscodePresident IsPasscodePresident True, if the password was configured; otherwise false. Boolean LastComplianceCheckOn LastComplianceCheckOn Update Date and timestamp of the latest status reported. Timestamp LastCompromisedCheckOn LastCompromisedCheckOn Update Date and timestamp last status reported. Timestamp LastSeen lastSeen Date and the time of the device's last successful contact with the MDM group configuration value. Timestamp LocationGroupName LocationGroupName MDM. Line MacAddress macAdress Address Wi-Fi MAC. The string model Model is automatically reported by the device at the time of registration. String operating system osVersion OS version. Line property values: C, E or S (corporate, employees or general). PhoneNumber phoneNumber phone number entered at check-in. The String Platform Platform is listed at the time of registration. SerialNumber line serial numberNumber. String identifier of the Udid UDID device. UserEmailAddress userEmail e-mail address of the device user. UserName username name of the device. The Uuid UUID line is a universal unique identifier. String