VMware Workspace ONE UEM Troubleshooting and Logging

for on-premises and SaaS deployments

VMware Workspace ONE UEM 2102

vmware®

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

VMware Workspace ONE UEM Troubleshooting and Logging

1

You may run into issues with your Workspace ONE UEM powered by AirWatch deployement. To help you diagnose the problem, Workspace ONE UEM provides detailed logging for all your services and applications. Learn how to generate these logs and where they're stored to help troubleshoot your issues.

Within Workspace ONE UEM, you can utilize logging for troubleshooting the core services of your platform, the services you've integrated in, and even your devices that run Workspace ONE UEM. Gathering and anyalyzing log data isn't just for troubleshooting; it can also be used to enhance performance and optimize settings for your unique environment.

Core vs Integrated Services

Your Workspace ONE UEM deployment consists of multiple services. These services can be considered either core services, which include the console, database, device services, API, and AWCM and are essential to the the functionality of Workspace ONE, or they can be integrated such as ACC, SEG, or other third-party integrated services.

You can learn more about troubleshooting and enhancing your your core and integrated components by reviewing the Core and Integrated Logging sections.

- Core Services Logging
- Integrated Services Logging

End-User Devices

Having trouble with your Workspace ONE UEM devices? If your device running Workspace ONE UEM needs troubleshooting, you can utilize the log information in VMware Workspace ONE UEM Device-Side Logging to analyze log data and help resolve your issues.

This chapter includes the following topics:

- Core Services Logging
- Integrated Services Logging
- VMware Workspace ONE UEM Device-Side Logging
- Workspace ONE UEM Logging Best Practices

Core Services Logging

Your Workspace ONE UEM deployment has several essential, or core, services that enable your deployment to run successfully. These services include the console, device-services, API, and AWCM. If you have issues with any of these core services, VMware provides logging data to help you diagnose the problem.

The core services of Workspace ONE UEM are its foundation, the pieces required for your deployment to run properly and efficiently. If the service you need assistance with does not display here, view the Integrated Services Logging section for an extensive list of integrated services and their log information.

There are two logging levels that proivide different levels of detail. If you are not troubleshooting a service, set the logging level to disabled to reduce use of hardware resources.

1 In the console, navigate to **Groups & Settings > All Settings > Admin > Diagnostics > Logging**.

2 Select any service that needs an increased logging level. Set the service logging to **Enabled**.

3 After you finish troubleshooting, revert the logging level back to **Disabled** to preserve hardware resources.

How to Read a Workspace ONE UEM Log Entry

The ability to read a Workspace ONE UEM log entry is key to succesfully analyzing and troubleshooting any issues you may encounter with your Workspace ONE UEM deployment.

Every log entry contains the following key information,

1 Date and time for the log entry.

2 Server identifier for the log entry.

3 Server communication thread identifier for the log entry.

4 Device or user identifier for the log entry.

5 VMware AirWatch internal code for the log entry.

6 Logging level for the log entry.

7 Associated service of the log entry.

8 Log message for the log entry.

Error Log Example

Workspace ONE UEM error logs use the following format:

```
2017/06/21 19:07:12.243[1]    EX-DS111[2]    11aaabbccc-dddee-1111-22ff-06gggg777777[3]
[0000000-0000000][4]   (14)[5]     Error[6]
```

```
AirWatch.CloudConnector.Client.AccServiceClient.SendRequest[7]     Received a Failure message from
AWCM: Destination not reachable at this moment[8]
```

Information Log Example

Workspace ONE UEM Information logs use the following format:

```
2017/09/07 14:46:57.852[1]             EX-DS111[2]           ca9562a7-c87c-4c3b-a1e1-
ca35a88555ab[3]               [0000052-0000000][4]   (20)[5]             Info[6]
WanderingWiFi.AirWatch.Console.Web.Controllers.HomeController[7]          Method:
WanderingWiFi.AirWatch.Console.Web.Controllers.HomeController.Index; LocationGroupID: 7; UserID: 52;
UserName: TEST_USER; Parameters: <N/A>;  69eddd96-9a81-47e9-a78a-dd20c845426b
```

Console Logging

Learn more about the Workspace ONE UEM logging functions available for the Console service. The API service is installed by default. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
AirWatch API	AW_Core_Api.log	Contains information on calls made to the API endpoint for available API commands.
AirWatch API	AW_MAM_Api.log	Contains information relating to specifically the /API/MAM endpoint.
AirWatch API	AW_MCM_Api.log	Contains information relating to specifically the /API/MCM endpoint.
AirWatch API	AW_MDM_Api.log	Contains information relating to specifically the /API/MDM endpoint.
AirWatch API	AW_MEM_Api.log	Contains information relating to specifically the /API/MEM endpoint.
AirWatch Services	AWServices.log	Contains information on the AirWatch SOAP API.
IIS>W3SVC1	u_ex####.log	Contains history of IIS web endpoints accessed and response codes delivered (Ex: /AirWatch & /Enroll).
Inetpub > Logs > FailedReqLogFiles	Fr####.xml	Contains failed IIS request log traces. You must enable this log as it is disabled by default.
Services	AirWatchGemAgent.log	Contains information on the GEM License assessing service and its back-end connections.
Services	ApiWorkflowService.log	This service log cites processed device commands from the REST API.

Folder	Log Name	Description
Services	AW.Meg.Queue.Service.log	Contains information on the email policy updates for SEG or Powershell integration, associated MSMQ reader information, SQL connection errors, and encryption ciphers.
Services	AW.IntegrationService.log	Contains information on all AW third-party integrations such as Apple School Manager APIs, VPP, and App Scan.
Services	BackgroundProcessorServiceLogFile.txt	Contains information on multiple different jobs that are processed in the background asynchronously such as console exports or report generation.
Services	BulkProcessingServiceLogFile.txt	Contains information on bulk commands such as SDK, certificates, APNS messages, DEP APIs, command queues, users, user groups, profiles, and apps.
Services	ContentDeliveryService.log	Contains information on content delivery and relay server communication for product provisioning.
Services	ChangeEventQueue.log	Contains information on event log entries, the batch save of those logs, syslog configuration loads, and policy updates for AW Tunnel.
Services	DirectorySyncServiceLogFile.txt	Contains information on directory user and group syncs such as member lists and LDAP mapping and definitions.
Services	EntityReconcileService.log	Contains information on reconcile and sync for entities linked to smart groups.
Services	MessagingServiceLog.txt	Contains information on notifications sent to the various 3rd party messaging services (APNs, GCM, WNS).
Services	PolicyEngine.log	Contains information on the device policies queue and products information related to user, OG and device compliance. It will also include information on product provisioning processing and delivery.

Folder	Log Name	Description
Services	SchedulerService.log	Contains information on the various jobs that are executed by the scheduler service such as Automatic sync, VPP user invite sync, bulk notification push, and AD sync triggers. For an exhaustive list please see Groups & Settings > All Settings > Admin > Scheduler.
Services	SmartGroupServiceLogFile.txt	Contains information relating to reconciliation of smart group mappings resulting from enrollments, changes in device or user state, and reports the resulting change for smart groups.
Services	SMSService.log	Contains information on batch SMS sent to devices.
Services	ComplianceSerivce.log	Logs Compliance service data
Services	ChangeEventOutboundQueueService .txt	Sends event notifications from source component to a central location (Ex: Syslog)
Services	PurgeUtility.log	Information about database blob file garbage collection
Services	Ws1.Tunnel.Kestrel.log	Tunnel services logs related to .net core based microservices
Web console	WebLogFile.txt	Contains information on the console user interface.
TargetedLogging	####Airwatch.log	Contains information on targeted logging enabled devices.

Device Services and Self-Service Portal Logging

Learn more about the Workspace ONE UEM logging functions available for Device Services. The API service is installed by default. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
AirWatch API	AW_Core_Api.log	Contains information on calls made to the API endpoint for available API commands.
AirWatch API	AW_MAM_Api.log	Contains information relating to specifically the /API/MAM endpoint.
AirWatch API	AW_MCM_Api.log	Contains information relating to specifically the /API/MCM endpoint.

Folder	Log Name	Description
AirWatch API	AW_MDM_Api.log	Contains information relating to specifically the /API/MDM endpoint.
AirWatch API	AW_MEM_Api.log	Contains information relating to specifically the /API/MEM endpoint.
AirWatch API	ws1.gateway.log	WS1-Services logs.
AirWatch Services	AWServices.log	Contains information on the AirWatch services including logging level and service details. This log also contains SOAP API related information.
AppCatalog	AppCatalogLogFile.txt	Contains information related to the application catalog such as application assignment, device requests when loading the app catalog, and user authentication.
DeviceManagement	DeviceManagement.log	Contains information on the early stages of enrollment including token or group ID validation, restriction checks, and authentication.
DeviceServices	DeviceServicesLog.txt	Contains information related to all device communications with Workspace ONE UEM.
DeviceService	DevicesGateway.log	Logging for the subset of APIs dedicated to devices.
Enroll Shortcut	EnrollShortcut.log	Information on URL redirects such as /enroll.
IdentityService	IdentityService.log	Information about the SAML web endpoint.
IIS>W3SVC1	u_ex####.log	Contains history of IIS web endpoints accessed and response codes delivered (Ex: /DeviceServices & /DeviceManagement).
Inetpub > Logs > FailedReqLogFiles	Fr####.xml	Contains failed IIS request log traces. This log must be enabled as it is turned off by default.
MyDevice	WebLogfile.txt	Contains information on actions taken within the self-service portal.
Services	ws1tunnel.kestrel	All the DB queries from Microservice. Log level is OFF by default.
Services	ws1.tunnel.log	Tunnel Microservice application/ functional logs. These logs also contain the equivalent of IIS logs about API status, time taken, etc.

Folder	Log Name	Description
Services	APIWorkflowService.log	Contains information on the API such as logging level, MSMQ reader errors and SQL connection errors.
Services	AW.IntegrationService.log	Contains information on all AW third-party integrations such as Apple School Manager APIs, VPP, and App Scan.
Services	AW.Meg.Queue.Service.log	Contains information on the email policy updates for SEG or Powershell integration, associated MSMQ reader information, SQL connection errors, and encryption ciphers.
Services	BulkProcessingServiceLogFile.txt	Contains information on bulk commands related to SDK, certificates, APNS messages, DEP APIs, command queues, users, user groups, profiles, and apps.
Services	ChangeEventQueue.log	Contains information on event log entries, the batch save of those logs, syslog configuration loads, and policy updates for AW Tunnel.
Services	EntityReconcileService.log	Contains information on reconcile and sync for entities linked to smart groups.
Services	InterrogatorQueueService.log	Contains information related to processed device samples for all platforms to be updated to the DB such as Application and Profile samples from device.
Services	MessagingServiceLog.txt	Contains information on sends and response times to the various third-party messaging services (APNs, GCM, WNS).
Services	ProvisioningPackageServicelogfile.txt	Logs provisioning package information for auto enrollment of applicable Windows 10 device
Services	ChangeEventOutboundQueueService.txt	Sends event notifications from source component to a central location (Ex: Syslog)
Services	SmartGroupServiceLogfile.log	Information relating to reconciliation of smart group mappings resulting from enrollments or changes in device or user state, and the resulting change for smart groups.

Folder	Log Name	Description
TargetedLogging	####Airwatch.log	Contains information on targeted logging enabled devices.
Trust Service	TrustService.log	Logging associated with an on-premises instance of the Trust Service that is used for Certificate Pinning.

API Logging

Learn more about the Workspace ONE UEM logging functions available for the API service. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
AirWatch API	AW_Core_Api.log	Contains information on calls made to the API endpoint for available API commands.
AirWatch API	AW_MAM_Api.log	Contains information relating to specifically the /API/MAM endpoint.
AirWatch API	AW_MCM_Api.log	Contains information relating to specifically the /API/MCM endpoint.
AirWatch API	AW_MDM_Api.log	Contains information relating to specifically the /API/MDM endpoint.
AirWatch API	AW_MEM_Api.log	Contains information relating to specifically the /API/MEM endpoint.
AirWatch API	CiscoiseLogfile.txt	Information about CiscoISE integration.
AirWatch Services	AWServices.log	Contains information on the Workspace ONE UEM services including logging level and service details. This log also contains SOAP API-related information.
IIS>W3SVC1	u_ex####.log	Contains history of IIS web endpoints accessed and response codes delivered (Ex: / ActiveSyncIntegrationServiceEndPoint).
Inetpub > Logs > FailedReqLogFiles	Fr####.xml	Contains failed IIS request log traces. This log must be enabled as it is turned off by default.
Services	APIWorkflowService.log	Contains information on handing bulk requests from the API server such as bulk commands to devices.
Services	AW.IntegrationService.log	Contains information on all AW third-party integrations such as Apple School Manager APIs, VPP, and App Scan.

Folder	Log Name	Description
Services	AW.Meg.Queue.Service.log	Contains information on the email policy updates for SEG or Powershell integration, associated MSMQ reader information, SQL connection errors, and encryption ciphers.
Services	BulkProcessingServiceLogFile.txt	Contains information on bulk commands related to SDK, certificates, APNS messages, DEP APIs, command queues, users, user groups, profiles, and apps.
Services	ChangeEventQueue.log	Contains information on event log entries, the batch save of those logs, and syslog configuration loads.
Services	EntityReconcileService.log	Contains information on reconcile and sync for entities linked to smart groups.
Services	MessagingServiceLog.txt	Contains information on sends and response times to the various third-party messaging services (APNs, GCM, WNS).
Services	ChangeEventOutboundQueueService .txt	Log file for entering information into the MSMQ to be sent to central outbound component (Ex: Syslog)
Services	SmartGroupServiceLogfile.log	Information relating to reconciliation of smart group mappings resulting from enrollments or changes in device or user state, and the resulting change for smart groups.
Services	DataPlatformService.log	Information about sending Windows 10 samples (requires Workspace ONE Intelligence)

AWCM Logging

Learn more about the Workspace ONE UEM logging functions available for the AWCM service. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
AWCM	Awcm.log	Contains information on AWCM such as status, history, properties, and additional sub-services.
AWCM	AWCMservice.log	Contains log information on AWCM Java service wrapper.

Integrated Services Logging

Having a Workspace ONE UEM powered by AirWatch deplpyment allows you to have many integrated services as well as the required core services. You may have issues with some of these services and require assistance troubleshooting your error. Learn more about how Workspace ONE UEM provides log information for your integrated services to help fix your issues.

Explore and implement logging for services that you have integrated into your Workspace ONE UEM deployment. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

VMware AirWatch Cloud Connector (ACC)

Learn more about the Workspace ONE UEM logging functions available for the VMware AirWatch Cloud Connector (ACC). All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
CloudConnector	CloudConnector.log	Contains information about ACC Services such as directory authentication, group syncs, communication with CA/PKI, PowerShell, syslog, and additional ACC services.

Change the Logging Level for ACC

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 Access the CloudConnector.exe.config file contained in the /Airwatch/CloudConnector/Bank# folder.

2 Make sure you compare the two bank folders to ensure you are editing the one with the most recent modified dates.

3 Change the level from error to verbose in the line <loggingConfiguration> line.

4 Allow the services a few minutes to pick up the logging change.

Secure Email Gateway v2 (SEGv2)

Learn more about the Workspace ONE UEM logging functions available for Secure Email Gateway v2 (SEGv2). All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
SecureEmailGateway	app.log	Contains information on device transactions and an analysis of each request passed through SEG and SEG application logs.
SecureEmailGateway	http-transaction.log	Contains information on overview of each email request passed through SEG (Transaction summary).
SecureEmailGateway	policy-update.log	Contains information on the policy updates performed by SEG.
SecureEmailGateway	active-sync-payload-reporting.log	Contains information active sync transaction reported to Email List view in console.
SecureEmailGateway	non-compliant-devices.log	Contains information on transactions for devices blocked by SEG and reasons for blocking.
SecureEmailGateway	cert-auth.log	Contains information of certificate authentication requests and certificate validation.
SecureEmailGateway	cache.log	Contains information about SEG policy cache.
SecureEmailGateway	content-transform.log	Contains information about content transformation (attachment and hyperlink transformation) processing
SecureEmailGateway	ews-proxy.log	Contains information about ews requests and proxy to ews endpoint
SecureEmailGateway	ews-transaction.log	Contains information on overview of ews transactions through SEG (Transaction summary).
SecureEmailGateway	resources-usage.log	Contains information about CPU and memory usage.
SecureEmailGateway	system-cpu-load.log	Contains CPU usage if it is exceeding the defined threshold for a given sustained period.
SecureEmailGateway	thread-dump.log	Contains information about thread dump.
SecureEmailGateway \kerberos	kerberos-service-manager.log	Contains information about Kerberos pipes availability.
SecureEmailGateway \kerberos	AirwatchKerberosClientPipe-#.log (# is pipe number)	Kerberos token retrieval requests.

Change the Logging for SEGv2

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 Access the admin page at https://localhost:44444/seg/admin.

2 In the Logging tab, change the logging level from Error to Debug.

3 Wait a few minutes for the service to pick up the logging change.

Email Notification Service

Learn more about the Workspace ONE UEM logging functions available for Email Notification Service. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/	AW.Mail.Notification.Service.log	Contains information on ENS communication such as log subscriptions to the email server, transactions with API servers, notification status for user/device, and communications to CNS.

Change the Logging Level for the Email Notification Service

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

Note By default, ENSv2 runs at the most verbose level of logging. Logging for ENS Classic runs at the Error level, and can be changed to Verbose for troubleshooting.

1 Access the AW.Mail.Notification.Service.Config file contained in the Installation folder.

2 Change the level from **Error** to **Verbose** in the application configuration.

3 Wait a few minutes for the service to pick up the logging change.

Email Notification Service v2

Learn more about the Workspace ONE UEM logging functions available for Email Notfication Service v2. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/	ENS.log	ENS web application logging
/	ReSubscriptionMechanism.log	Logs for the subscription service that runs monitoring user's subscriptions and sending out notifications to have clients re-register
/	RSAKeysTracker.log	Logs for service that monitors the key repository in the DB and triggers creations of additional keys when necessary.
/tools/uploadrsakeys/	UploadRSAKeys.log	Contains information on the RSA Keys
/database/	AWDatabaseLog_MMDDYY.txt	Contains ENSv2 database transactions
/%Installdir%/	Airwatch_ENS_V2_InstallLog.txt	Contains information related to installation process for ENSv2

Change the Logging Level for the Email Notification Service

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

Note By default, ENSv2 runs at the most verbose level of logging. Logging for ENS Classic runs at the Error level, and can be changed to Verbose for troubleshooting.

1 Access the AW.Mail.Notification.Service.Config file contained in the Installation folder.

2 Change the level from **Error** to **Verbose** in the application configuration.

3 Wait a few minutes for the service to pick up the logging change.

VMware Tunnel

Learn more about the Workspace ONE UEM logging functions available for VMware Tunnel. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
VMware Tunnel Proxy	AirWatchDiagnosticService.log	Contains information on Tunnel diagnostic sample processing and saving.
VMware Tunnel Proxy /var/log/vmware/proxy/	proxy.log (Relay)	Contains information on Tunnel Proxy such as whitelisted devices entries, authentication, and certificate status from requesting device to AWCM.
VMware Tunnel Proxy	proxy.log (Endpoint)	Contains information on web requests through the proxy and to the listening endpoint.
VMware Tunnel Proxy /var/log/vmware/proxy/	proxy-request.log	Contains HTTP request information for requests going through the proxy.
/var/log/vmware/tunnel/vpnd/	tunnel.log	Contains information on VPN communications such as whitelisting devices, communication with API/AWCM, and health check status.
VMware Tunnel Proxy /var/log/vmware/proxy/	proxy-request.log	HTTP request information for requests going through the proxy.
/var/log/vmware/tunnel/vpnd/	tunnel_init.log	Contains information on Tunnel configuration and initialization.
/var/log/vmware/tunnel/vpnd/	reporter.log	Information about the test connection feature.
/var/log/vmware/tunnel/vpnd/	reporter_install.log	Information on the installation of vpnreportd service.

Change the Logging Level for VMware Tunnel

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 To change the logging levels for VMware Tunnel, in the console, navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration > Advanced**.

VMware Content Gateway

Learn more about the Workspace ONE UEM logging functions available for VMware Content Gateway. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
ContentGateway /var/log/airwatch/content-gateway/	CGContent.log (Relay)	Contains information on Content Gateway access such as authentication, trust relationship establishment, and repository structure services.
ContentGateway /var/log/airwatch/content-gateway/	CGContent.log (Endpoint)	Contains information on repository folder actions and user impersonation.
ContentGateway /var/log/airwatch/content-gateway/	Content-gateway-wrapper.log	Information about Content Gateway-related process lifecycle.
ContentGateway /var/log/airwatch/content-gateway/	content-gateway.log, 0.content-gateway-YYYY-mm.dd.log.zip	Contains log messages from Content Gateway.
ContentGateway /var/log/airwatch/content-gateway/	tunnel.log	Contains log messages from the tunnel process that is used as part of the XML API processing. You must have Tunnel enabled in the Horizon settings in order see this log.
ContentGateway /var/log/airwatch/content-gateway/	tunnel-snap.tar.gz	Tarball containing VMware Tunnel server and proxy logs.
ContentGateway /var/log/airwatch/content-gateway/	config.yml	Contains Content Gateway configuration and log level details.
ContentGateway /var/log/airwatch/content-gateway/	smb.conf	Contains SMB client configuration

Change the Logging Level for the Content Gateway

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 Access the logback.xml file contained in the Content Gateway Config folder /opt/airwatch/content-gateway/conf.

2 Change the level to **debug** in the <logger name="com.airwatch" level="info" /> line.

3 Wait a few minutes for the service to pick up the logging change.

Unified Access Gateway (System Information)

For UAG-based services using the Log Archive download option under the UAG Admin UI Support Settings page. Learn more about the Workspace ONE UEM logging functions available for Unified Access Gateway (System Information). All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/Opt/VMware/Gateway/Logs	*.ZIP	Collection of log files on the UAG appliance.
/Opt/VMware/Gateway/Logs	rpm-version.log	Contains system info versioning for UAG appliance
/Opt/VMware/Gateway/Logs	ipv4-forwardrules.log	Contains IPv4 forwarding rules on the appliance
/Opt/VMware/Gateway/Logs	df.log	Contains information about disk space usage on the appliance

Folder	Log Name	Description
/Opt/VMware/Gateway/Logs	netstat.log	Contains information on open ports and existing TCP connections
/Opt/VMware/Gateway/Logs	netstat-s.log	Contains network statistics form the time of creation of the appliance.
/Opt/VMware/Gateway/Logs	netstat-r.log	Contains static routes crated on the appliance
/Opt/VMware/Gateway/Logs	uag_config.json,uag_config.ini	Contains the configuration of the UAG appliance.
/Opt/VMware/Gateway/Logs	ps.log	Contains process running at the time of downloading logs.
/Opt/VMware/Gateway/Logs	ifconfig.log	Contains information on the network interface configuration for the appliance
/Opt/VMware/Gateway/Logs	free.log	Contains the amount of free RAM at the time of log gathering
/Opt/VMware/Gateway/Logs	top.log	Contains a list of processes sorted by memory usage at the time of log gathering
/Opt/VMware/Gateway/Logs	iptables.log	Contains IPv4 IP tables.
/Opt/VMware/Gateway/Logs	ip6tables.log	Contains IPv6 IP tables
/Opt/VMware/Gateway/Logs	w.log	Contains information about up time and users currently on the machine
/Opt/VMware/Gateway/Logs	systemctl.log	Contains a list of services running in the appliance
/Opt/VMware/Gateway/Logs	resolv.conf	Contains info on the local clients connections to known DNS servers
/Opt/VMware/Gateway/Logs	hastats.csv	Contains stats per node and total stats information for each back end type (Edge Service Manager, VMware Tunnel, Content Gateway)

Unified Access Gateway

For UAG based services using the Log Archive download option under the UAG Admin UI Support Settings page. Learn more about the Workspace ONE UEM logging functions available for Unified Access Gateway. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/Opt/VMware/Gateway/Logs	supervisord.log	Contains information on the Supervisor which manages the edge service manager, admin, and AuthBroker)
/Opt/VMware/Gateway/Logs	esmanager-x.log	Contains information on the Edge service manager which shows back end processes performed on the appliance
/Opt/VMware/Gateway/Logs	esmanager-std-out.log	Contains information on the Edge service manager which shows back end processes performed on the appliance

Folder	Log Name	Description
/Opt/VMware/Gateway/Logs	audit.log	Contains audits for all admin user operations
/Opt/VMware/Gateway/Logs	authbroker.log	Contains information from the AuthBroker process, which handles Radius and RSA SecurID authentication
/Opt/VMware/Gateway/Logs	admin.log	
/Opt/VMware/Gateway/Logs	admin-std-out.log	Contains information on the admin GUI logs and messages from the process that provides REST API.
/Opt/VMware/Gateway/Logs	bsg.log	Contains information from the Blast Secure Gateway.
/Opt/VMware/Gateway/Logs	SecurityGateway_xxx.log	Contains information from the PCoIP Secure Gateway
/Opt/VMware/Gateway/Logs	utserver.log	Contains information from the UDP Tunnel server
/Opt/VMware/Gateway/Logs	activeSessions.csv	Contains a list of active Horizon and WRP sessions
/Opt/VMware/Gateway/Logs	haproxy.conf	Contains information on the HA proxy configuration parameters for TLS port sharing
/Opt/VMware/Gateway/Logs	vami.log	Contains information from running vami commands to set network interface configurations during deployment
/Opt/VMware/Gateway/Logs	content-gateway.log, content-gateway-wrapper.log, 0.content-gateway-YYYY-mm.dd.log.zip	Contains log messages from Content Gateway.
/Opt/VMware/Gateway/Logs	tunnel-snap.tar.gz	Tarball containing VMware Tunnel server and proxy logs.
/Opt/VMware/Gateway/Logs	admin-zookeeper.log	Contains information on the data layer that is used to store the UAG configuration
/Opt/VMware/Gateway/Logs	aw-appliance-agent.log	Contains information on the Appliance agent which is responsible for starting AirWatch services.
	config.yml	Contains Content Gateway configuration and log level details.
	smb.conf	Contains SMB client configuration.
	smb-connector	Contain SMB protocol and log level details.

Change the Logging Level for the Unified Access Gateway Service

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 n the Unified Access Gateway Admin UI, navigate to **Support Settings > Log Level Settings**

2 Select **INFO**, **ERROR**, **WARNING**, or **DEBUG** based on your requirements.

3 Wait a few minutes for the service to pick up the logging change.

Level	Type of Information Collected
INFO	Information messages that highlight the progress of the service.
ERROR	Error events that might still allow the service to continue running.
WARNING	Potentially harmful situations but are usually recoverable or can be ignored.
DEBUG	Events that would generally be useful to debug problems. You can enable the debug mode to view or manipulate the internal state of the appliance. The debug mode lets you test the deployment scenario in your environment.

4 Restart each service after saving changes.

Remote File Storage

Learn more about the Workspace ONE UEM logging functions available for Remote File Storage. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
RemoteFileStorage	Rfs-web.log	Contains information on RFS such as certificates, tokens, files, and storage file paths.

Content Rendering Engine

Learn more about the Workspace ONE UEM logging functions available for Content Rendering Engine. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/var/log/airwatch/cre/	Cre.log	Contains information on CRE such as Hazelcast, render requests, and associated manifests.

Change the Logging Level for the Content Rendering Engine

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 Access the logback.xml file contained in the CRE Configuration Folder.

2 Edit the file on using the Linux vi editor or on WinSCP.

3 Write text in the logback.xml file.

   a Enter `i` to begin writing text.

   b Change the logging level XML attribute value in both the **logger** and **root** XML elements.

   c Select **Esc** to exit edit.

d Press `wq!` to write and quit.

Change the Logging Level for the Content Rendering Engine

Advanced Remote Management

Learn more about the Workspace ONE UEM logging functions available for Advanced Remote Management. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
Program Files/RemoteManagement/Logs	*.log	Contains information on Remote Management communications including that of Registry Editor.

Change the Logging Level for Advanced Remote Management

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 To change the logging level for the Remote Management Service on the device change the apListener.application.config, FileManager.application.config and RemoteControl.application.config in the Config folder to ‘DEBUG

Workspace ONE Access Service

Learn more about the Workspace ONE UEM logging functions available for Worksapce ONE Access Service. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/.../opt/vmware/horizon/workspace/logs	Accessontrol-service.log	Access control service logging which handles role based access control for Workspace ONE Access admins
/.../opt/vmware/horizon/workspace/logs	Admin-Tool.log	Contains outputs from scripts called as admin tools.
/.../opt/vmware/horizon/workspace/logs	Analytics-service.log	Log for analytics service that managed audit events, reports, and search functionality.
/.../opt/vmware/horizon/workspace/logs	audit-service.log	Contains information on services and servlets including the API and elastic search functionalities.
/.../opt/vmware/horizon/workspace/logs	Calculator-deadletters.log	Contains information on anything that was not calculated.
/.../opt/vmware/horizon/workspace/logs	Calc-v2.log	Contains information on when the calculators were run. Calculators are responsible for completing entitlements of users/groups to app in the background.
/.../opt/vmware/horizon/workspace/logs	Catalina.log	Contains information on the Tomcat service. Date indicated roll-over.

Folder	Log Name	Description
/.../opt/vmware/horizon/workspace/logs	Cert-proxy.log	Contains certificate proxy information used by Android Mobile SSO. Date indicates roll-over.
/.../opt/vmware/horizon/workspace/logs	Certproxy-catalina.log	Stderr /stdout for cert proxy process.
/.../opt/vmware/horizon/workspace/logs	Certproxy-service.YYYY-MM-DD.log	Apache commons daemon wrapper logs for starting cert-proxy (date appended).
/.../opt/vmware/horizon/workspace/logs	Configurator.log	Contains information related to the configurator admin UI that runs on port 8443.
/.../opt/vmware/horizon/workspace/logs	Connector.log	Contains information related to the VMware Workspace ONE Access Connector.
/.../opt/vmware/horizon/workspace/logs	Connector-sync.log	Connector synchronization logs.
/.../opt/vmware/horizon/workspace/logs	Db-sql-and-tx.log	SQL and transaction database logs for IDM.
/.../opt/vmware/horizon/workspace/logs	Entitlement-calc-logic.log	Contains information on an additional background calculator specifically the entitlement calculations.
/.../opt/vmware/horizon/workspace/logs	Entitlement-calc-stats.log	Contains information on an additional background calculator specifically the entitlement calculations.
/.../opt/vmware/horizon/workspace/logs	Greenbox_web.log	Contains information of all Workspace ONE service side events.
/.../opt/vmware/horizon/workspace/logs	Group-calc-logic.log	Contains information on an additional background calculator specifically the group entitlement calculations.
/.../opt/vmware/horizon/workspace/logs	Group-calc-stats.log	Contains information on an additional background calculator specifically the group entitlement calculations.
/.../opt/vmware/horizon/workspace/logs	Horizon.log	Contains information related to Workspace ONE Access.
/.../opt/vmware/horizon/workspace/logs	Horizon-ceip.log	Contains information related to horizon and the device communications back to the service.
/.../opt/vmware/horizon/workspace/logs	Horizon-persist.log	Contains information on the DB Schema.
/.../opt/vmware/horizon/workspace/logs	Horizon-sockjs.log	Contains information of web socket communications between service and connector.
/.../opt/vmware/horizon/workspace/logs	Host-manager.log	Contains information on the Tomcat service. Date indicates roll-over. This log is not utilized in the latest release.
/.../opt/vmware/horizon/workspace/logs	Idm-service.YYYY-MM-DD.log	Apache commons daemon wrapper logs for starting IDM (date appended).
/.../opt/vmware/horizon/workspace/logs	Localhost.log	Contains information on the Spring framework. Date indicates roll-over.
/.../opt/vmware/horizon/workspace/logs	mtkadmin.log	Contains information related to Kerberos adapter

Folder	Log Name	Description
/.../opt/vmware/horizon/workspace/logs	Manager.log	Contains information on the Tomcat service. Date indicates roll-over. This log is not utilized in the latest release.
/.../opt/vmware/horizon/workspace/logs	Tcruntime-instance.log	Contains information on the Tomcat service. Date indicates roll-over. This log is not utilized in the latest release.
/.../opt/vmware/horizon/workspace/logs	tomcat.pid	Contains the PID for Tomcat
/.../opt/vmware/horizon/workspace/logs	vmwarecertproxy-stderr.log	Contains information on the certificate proxy component. This log is not utilized in the latest release.
/.../opt/vmware/horizon/workspace/logs	Workspace.log	Contains information related to the service including startup errors.
/.../opt/vmware/horizon/workspace/logs	Wrapper.log	Contains information on the Tomcat Wrapper service. This log is not utilized in the latest release.
/.../opt/vmware/horizon/workspace/logs	Wsadmin.log	Contains information on the admin servlet.
/Airwatch/VMwareIdentityManager	Idm-installer.log	Contains information on install history and status of the Workspace ONE Access service for Windows.
/.../opt/vmware/horizon/workspace/logs	connector-dir-sync.log	Contains information related to directory sync activities. (Embedded Connector)

VMware Workspace ONE Access Connector

Learn more about the Workspace ONE UEM logging functions available for Worksapce ONE Access Connector. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/VMware/IDMConnector/	Idm-connector-installer.log	Contains information on install history and status of the VMware Workspace ONE Access Connector Service.
/Opt/.../Workspace/Logs	Configurator.log	Contains information on the configurator admin UI that runs on port 8443.
/Opt/.../Workspace/Logs	Connector.log	Contains information related to the VMware Workspace ONE Access Connector.
/Opt/.../Workspace/Logs	Workspace.log	Contains information on service such as startup errors.
/Opt/.../Workspace/Logs	Catalina.log	Contains information on the Tomcat service. Date indicates roll-over.
/Opt/.../Workspace/Logs	Localhost.log	Contains information on the Spring framework. Date indicates roll-over.
\opt\vmware\horizon\workspace \logs\	connector-dir-sync.log	Contains information related to directory sync activities.

Folder	Log Name	Description
/User Auth Service/logs/	eas-service.log	Information about the activity on the Enterprise services, such as directory sync and logins.
/Directory Sync Service/logs/	eds-service.log	Information about the activity on the Enterprise services, such as directory sync and logins.
/Kerberos Auth Service/logs/	eks-service.log	Information about the activity on the Enterprise services, such as directory sync and logins.
/User Auth Service/logs/	eas-vertx-access.log	Information about the API requests on the Enterprise services.
/Directory Sync Service/logs/	eds-vertx-access.log	Information about the API requests on the Enterprise services.
/Kerberos Auth Service/logs/	eks-vertx-access.log	Information about the API requests on the Enterprise services.
/User Auth Service/logs/	UserAuthService.out.log	Information about the process running the Enterprise services.
/Directory Sync Service/logs/ DirectorySyncService	DirectorySyncService.out.log	Information about the process running the Enterprise services.
/Kerberos Auth Service/logs/	KerberosAuthService.out.log	Information about the process running the Enterprise services.
/User Auth Service/logs/	UserAuthService.err.log	Error information about the process running the Enterprise services.
/Directory Sync Service/logs/	DirectorySyncService.err.log	Error information about the process running the Enterprise services.
/Kerberos Auth Service/logs/	KerberosAuthService.err.log	Error information about the process running the Enterprise services.
/User Auth Service/logs/ UserAuthService	UserAuthService.wrapper.log	Information about the process running the Enterprise services such as Java options and process ID.
/Directory Sync Service/logs/	DirectorySyncService.wrapper.log	Information about the process running the Enterprise services such as Java options and process ID.
/Kerberos Auth Service/logs/	KerberosAuthService.wrapper.log	Information about the process running the Enterprise services such as Java options and process ID.

Change the Logging Level for the VMware Workspace ONE Connector

One of the functions available for Workspace ONE UEM integrated services is to change the log level to get more, or less information.

1 Access the l hc-log4j.properties file contained in /usr/local/horizon/conf/ .

2 Add “log4j.rootLogger=DEBUG,rollingFile,SYSLOG” to the first line of the file.

3 Wait a few minutes for the service to pick up the logging change.

Workspace One Intelligence

Learn more about the Workspace ONE UEM logging functions available for Worksapce ONE Intelligence. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/Airwatch/ETLService/Logs	Etl.log (YYYY-MM-DD)	Contains log information for WorkSpaceONE Intelligence Connector (ETL). Contains health status information and information around successful/failure events.

Memcached

Learn more about the Workspace ONE UEM logging functions available for Memchached. All Logs are located in the /VMware/AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/var/log/memcached-monitor/	Memcached-{mm-dd-yyyy}	Logs useful statistics about the Memcached solution

Dell Factory Provisioning Service

Learn more about the Workspace ONE UEM logging functions available for the optional Factory Provisioning component. All Logs are located in the /AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/Airwatch/Logs	FactoryProvisioning.Service.log	This file has any diagnostics (info, warnings, errors) messages generated during the runtime of the Factory Provisioning Windows Service which is the service performing the PPKG packages generation requested by admins.
/AirWatch/Factory Provisioning Services/Website/	VMware.WS1.FactoryProvisioning.API.log	This file has any diagnostics (info, warnings, errors) messages generated during the runtime of the Factory Provisioning Windows API which is the service accepting the PPKG packages generation requests by admins through different front-end components like the AW Console.
\AirWatch\Factory Provisioning Service\Services\	VMware.WS1.FactoryProvisioning.Service.exe.config	Configuration file

Airlift

Learn more about the Workspace ONE UEM logging functions available for the optional Airlift component. All Logs are located in the /AirWatch/Logs folder unless otherwise specified.

Folder	Log Name	Description
/Program Files/ Vmware/ VMware Airlift/Logs/	Airlift-YYYMMDD.log	Contains all AirLift information on calls made to the API endpoint of Workspace ONE UEM and Microsoft ConfigManager

VMware Workspace ONE UEM Device-Side Logging

In addition to core and integrated services, VMware provides logs to assist in troubleshooting your devices running Workspace ONE UEM. Learn more about the types of deivces supported, how to change log levels, and what log information is provided by VMware Workspace ONE UEM for your devices.

Explore and implement logging for end-user devices running the Workspace ONE Intelligent Hub. Some logging may require additional components or requirements to gather.

iOS Devices

Learn more about the Workspace ONE UEM logging functions available for iOS Devices.

Method	Log Name	Description
Console app on macOS	*.txt	Contains information related to all device side transactions including MDM, Enrollment, access, and application run history.
Hub App w/ Debug enabled in SDK	Agentlog####.txt	Contains information on system messages and stack traces when devices throw errors that are written from applications with the Log class.
Crash Logs	*.crash	Contains information on application crashes that is stored on iOS devices
sysdiagnose	*.tar.gz	Instructions available on Apple developer website. These logs will contain information from the past. If your issue has been reproduced in the last few hours, these logs should reference it.

macOS Devices

Learn more about the Workspace ONE UEM logging functions available for macOS Devices.

Method	Log Name	Description
Console.app	*.txt	Contains information related to all device side transactions including MDM, enrollment, access, and application run history.
/Library/Logs/DiagnosticReports	Intelligent Hub*.crash & hubd*.crash	Contains information on crashes related to the Hub daemon.

Method	Log Name	Description
Sudo Log collect (/var/log/)	System.log	Contains information on the mdmd and other OS-specific activities. Used only for macOS 10.12+
/var/log/	Install.log	Contains information on package installations including Munki
/Library/Application Support/AirWatch/Data/Munki/managed installs/logs/	ManagedSoftwareUpdate.log	Main Munki logging file which will contain information pertaining to macOS software deployment through UEM Internal Apps.
/Library/Application Support/Airwatch/Data/Munki/munki_repo/munkiData/	Munki_data.plist	Contains internal metadata information on current software being deployed through UEM Internal Apps.
/Library/Preferences/	AirWatchManagedInstalls.plist	Preference file used for VMware integration with Munki.
/Library/Application Support/AirWatch/Data/Munki/Managed Installs/	InstallInfo.plist	Contains status information on current software being deployed through UEM Internal Apps.
/Library/Application Support/AirWatch/Data/Munki/Managed Installs/	ManagedInstallReport.plist	Contains detailed status information on current software being deployed through UEM Internal Apps.
/Library/Application Support/AirWatch/Data	AppStatuses_WS1.plist	Used for displaying software download and installation statuses within Intelligent Hub.
/Library/Application Support/AirWatch/Data/Munki/Munki_Repo/catalogs/device_catalog.plist	device_catalog.plist	Contains metadata information about the internal apps like bundle id, installation criteria, pre/post-install scripts etc.
/Library/Application Support/AirWatch/Data/Munki/Munki_Repo/manifests/device_manifest.plist	device_manifest.plist	Contains all the assigned apps.
/Library/Application Support/AirWatch/Data/VPPApps.plist	VPPApps.plist	Contains information about assigned VPP apps like appurl, name, bundleid, status etc.
/Library/Application Support/AirWatch/Data/CustomAttributes/CustomAttributes.plist	CustomAttributes.plist	Contains the latest key-value pairs generated by Custom Attribute scripts. Contents in this plist will be sent to UEM in regular Hub samples.
/Library/Application Support/AirWatch/Data/com.vmware.hub.flags.plist	com.vmware.hub.flags.plist	Status of recently released features in the form of key-value pair. Key is the name of the feature and value can be either True/False.
/Library/Application Support/AirWatch/Data/ProductsNew	ProductsNew	Contains information about File/Action Products deployed through UEM Product Provisioning.

For more information on how to collect logs, see Request Device Log in *Introduction to Workspace ONE UEM powered by AirWatch for macOS*.

Android Devices

Learn more about the Workspace ONE UEM logging functions available for Android Devices.

Method	Log Name	Description
ADB/Android Studio/ RXLogger	*.txt	Contains information on app level traffic such as system messages and stack traces.
Hub Debug Logs	*.txt	Contains information on app level traffic such as system messages and stack traces filtered to the Workspace ONE Intelligent Hub and PackageManager.
DumpState Logs	*.txt	Contains information collected from Android Debug Bridge (ADB) without active connection to device and used for historical logging.

Android Enterprise Wipe Logs

If an Android device in your deployment is enterprise-wiped, additional logs are available.

To capture the latest set of logs, tap the Workspace ONE Intelligent Hub welcome screen header on the affected device 5 times. The device opens any available email app on the device where you can send the additional logging to administrators or support to help with investigation.

This logging function requires a minimum version of Workspace ONE Intelligent Hub for Android v8.1.

Google Bug Reports

To capture a Google bug Report, first navigate to **Device Settings > Software Information > Build Number** and tap **Build Number** 7 times to enable developer options. This will make an option available under **Developer Options > Take Bug Report**. After replication of the issue select this option and allow 1-2 minutes for the report to be generated. When the report generates, there a push notification appears that can be opened to select how to share the report (E-mail, Bluetooth, etc.).

Telecom Service App Reports

To capture a Telecom Service report, open the telecom service app and tap the screen 5 times. A notification appears that file logging is enabled. Open the application menu and select **Copy Log/DB**. Open the native file manager and navigate to **Internal Storage > Android > Data > com.airwatch.sampler > Files > telecom-log-dir > #.txt**. Transfer this file off of the device for further review.

Windows Phone Devices

Learn more about the Workspace ONE UEM logging functions available for Windows Phone Devices.

Method	Log Name	Description
Field Medic	*.etl	Contains information on enrollment and most other MDM related functions.

Widows Desktop Devices (Windows HUB)

For deployments using the VMware Windows HUB, you can use Remote Log collection to gather Windows Desktop logs.

1 In the Workspace ONE UEM Device List view, select the device you want to collect logs for.

2 Select **More ActionsRequest Device Log**.

3 Selectthe log source: **Hub** or **System**.

   a **Hub** - logs related to the Workspace ONE Intelligent Hub such as the Hub and application deployment logs

   b **System** - logs related to the system such as Event Viewer logs and registry export

4 Navigate to **More > Attachments > Documents**. Select the log name to download the log bundle and view the logs. The logs are contained in a .ZIP folder.

Method	Log Name	Description
/Hub/Agents/ ApplicationDeploymentAgent/	RegistryExport.txt	Contains information on application deployment flows.
/Hub/Agents/ ApplicationDeploymentAgent/	AirWatchMDM-*.etl	Contains information on application deployment flows.
Hub/Agents/WindowsUnifiedAgent/	AWProcessCommands.log	Contains information around installations that utilize the agent such as encryption and product provisioning.
Hub/Agents/WindowsUnifiedAgent/	NativeEnrollment.log	Contains information on agent based enrollments.
Hub/Agents/WindowsUnifiedAgent/	PowershellExecute.log	Contains information on PowerShell commands run through product provisioning.
Hub/Agents/WindowsUnifiedAgent/	TaskScheduler.log	Contains information on Task scheduler's local enforcement of policies, and samples sent to the console.
Hub/Agents/WindowsUnifiedAgent/	AwclClient.log	Contains information on communications between AWCM client and Workspace ONE UEM.
Hub/Agents/WindowsUnifiedAgent/	SSOCommunicationHandler.log	Contains information on agent post-enrollment single sign-on.
Hub/Agents/WindowsUnifiedAgent/	Updater.log	Contains information on agent auto update procedures.

Method	Log Name	Description
Hub/Agents/WindowsUnifiedAgent/	AwAirWatchIpc.log	Contains communication records between the Workspace ONE app and other services.
Hub/Agents/WindowsUnifiedAgent/	WorkspaceOneProvisioning.log	Contains information on Worksapce ONE app installations and downloads.
Hub/Agents/ProvisioningAgent/	awProvAgent.log	Contains the provisioning agent event logging.
System/Device/PCRefresh/	RegistryExport.txt	Contains registry exports related to Software and user provisioning
System/Device/PCRefresh/ or C:\Recovery\OEM\VMware\	*	Contains logs and application data with the app deployment cache, Hub database with all configurations and settings, and registry settings with MDM device ID.
System/Device/Windows/	Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provided_Admin_EventLogs.evtx	Contains information on MDM event logs
System/Device/Windows/	System_EventLogs.evtx	Contains information on system Event Logs
System/Device/Windows	RegistryExport.txt	Contains a list of successfully applies CSPs on the device (profiles and apps)
System/Device/Windows/Environment/	Processes.txt	Contains a list of currently running processes
System/Device/Windows/Environment/	Services.txt	Contains a list of currently registered services

Windows Desktop Devices (Without Windows HUB)

If your deployment does not include the VMware Windows HUB, use the following Windows Desktop logging options.

Method	Log Name	Description
Windows Event Viewer	*.evtx	Contains information on nrolment using Work Access and MDM functions that do not require the Unified Agent (Samples, Profiles, Commands).
/AirWatch/UnifiedAgent/Logs/	AwprocessCommands.Log	Contains information on installs that utilize the Unified Agent such as encryption and product provisioning.
/AirWatch/UnifiedAgent/Logs/	AWLPC.Log	Contains information related to the communications between the Unified Agent and AirWatch
/AirWatch/UnifiedAgent/Logs/	NativeEnrollment.log	Contains information around the Workspace ONE Intelligent Hub-Based nrolment method.
/AirWatch/UnifiedAgent/Logs/	PowershellExecute.log	Contains information on PowerShell commands that are run via product provisioning.

Method	Log Name	Description
/AirWatch/UnifiedAgent/Logs/	AwclClient.log	Contains information on communications between AWCM client and AirWatch.
/AirWatch/UnifiedAgent/Logs/	TaskScheduler.log	Contains information on the Task Scheduler's local enforcement of policies.
/AirWatch/UnifiedAgent/Logs/	SSOCommunicationHandler.log	Contains information on post nrolment SSO for Workspace ONE Intelligent Hub.
/AirWatch/UnifiedAgent/Logs/	RMService.log	Contains information around the Workspace ONE Intelligent Hub-Based enrolment method.

Windows Rugged Devices

Learn more about the Workspace ONE UEM logging functions available forWindows Rugged Devices.

Method	Log Name	Description
/AirWatch/Logs	Awregisterdevice	Contains information on device registration that occurs during the enrollment process.
/AirWatch/Logs	AWService.log	Contains information on communications between the device and AirWatch including managed beacon and interrogator samples.
/AirWatch/Logs	AWApplicationManager.log	Contains information related to product provisioning.
/AirWatch/Logs	AWProcessCommands.log	Contains information for commands sent from AirWatch such as profiles, applications, and product provisioning.
/AirWatch/Logs	FusionwlanSetup	Contains information on fusion Wi-Fi profile changes.
Root	AW_Setup	Contains information on the AWMasterSetup such as agent install and uninstall processing on a device.
/AirWatch/Logs	Awcmclient	Contains information on communications between AWCM client and AirWatch.
/AirWatch/Logs	Awapplauncher	Contains information on the application launcher executable. Only present if the App Launcher utility is assigned and utilized by device.
/AirWatch/Logs	Awapplyprofile	Contains information on agent settings SML file which is generated during enrollment.
/AirWatch/Logs	emScript	Contains information on the native system performance.
Program Files/RemoteManagement/Logs	*.log	Contains information on Remote Management communications including that of Registry Editor.

Enable Device-Based Targeted Logging

Device-based targeted logging is ideal for logging exercises on a small number of devices.

Procedure

1 Navigate to **Devices > List View**. Select the device you want to target. From the **Device Details** screen, navigate to **More > Targeted Logging**.

2 Select **Create New Log**.

3 Select the time frame you desire and select **Start**.

4 Once the specified time frame has elapsed, navigate to the configured file path and open the log.

What to do next

To see the configured file path, navigate to **Groups & Settings > All Settings > Admin > Diagnostics > Logging > Targeted Logging File Path**.

Enable Settings-Based Targeted Logging

Device-based targeted logging is ideal for logging exercises on a large number of devices.

Procedure

1 Navigate to **Groups & Settings > All Settings > Admin > Diagnostics > Logging**.

2 Select **Enabled** for the **Targeted Logging** setting, and provide a comma-separated list of Device IDs.

3 Once log gathering has concluded, reset **Targeted Logging** to **Disabled**.

Workspace ONE UEM Logging Best Practices

Leanring about your Workspace ONE UEM component logging allows your to better analyze and correct any issues you may have. Sometimes seeing examples of log files can greatly enhance your ability to understand its importnace while providing use cases on how to best use the information provided.

Best practices help piece together information by providing examples of how to use logging when troubleshooting or analyzing an issue with either a core component or an integrated component.

Capture Logs

Capturing accurate verbose logs helps diagnose errors and disconnections in your deployment.

1 Ensure that the logging is currently producing verbose entries after a logging level change. Verify that debug entries are logged to ensure that the correct logging levels have applied.

2 Rename the current log file to include the date and time the log was captured.

   a Changing the filename ensures that the log is not overwritten.

   b For Java based services, you must stop the service before renaming any files.

3 Reproduce the event that cause the error, for example, an authentication failure.

4 Rename the new log file with a description of the observed error.

   a Add a –Description or –DateTime to help identify the contents of the log file.

5 Export the log file to a sharable location. If applicable, attach the log file to a support ticket.

Performance Logging

Explore and implement additional logs to troubleshoot and improve your Workspace ONE UEM deployment.

Some logging may require additional components or requirements to gather.

Table 1-1. Third-Party SDK App Logs

Method/Folder	Log Name	Description
ADB/Android Studio/RXLogger	*.txt	Contains real time logs for SDK application logging from developer run application.
Console app on macOS	*.txt	Contains real time logs for SDK application logging from developer run application.
Console (Apps&Book\Analytics\App Logs)	AppLog####.txt	Contains information from third-party SDK application integrations.

Workspace ONE UEM Troubleshooting Examples

The following table provides examples of the verbose logging that you can gather to troubleshoot an issue. These logs are Workspace ONE UEM-specific, so additional third-party logs may be required for troubleshooting. As a best practice, include replication time stamp information to expedite reviewing logging and aiding identification of pertinent errors.

Example	Log Files
Unable to enroll (AD user)	Deviceserviceslog.txt, u_ex####.log, DeviceManagement.txt, AWCM.log, and CloudConnector.log.
Unable to enroll (Basic User)	Deviceserviceslog.txt, u_ex####.log, and DeviceManagement.txt.
Unable to enroll (DEP)	Deviceserviceslog.txt, u_ex####.log, DeviceManagement.txt, AWCM.log, and CloudConnector.log.
Unable to enroll (AFW)	Deviceserviceslog.txt, u_ex####.log, DeviceManagement.txt, AWCM.log, and CloudConnector.log.
Unable to login to console (Admin)	WebLogFile.txt, AWCM.log, and CloudConnector.log.
Console UI errors	WebLogFile.txt.
Unable to upload application	WebLogFile.txt.
VPP sync failures	AW.IntegrationService.log and WebLogFile.txt.
Unable to upload content	WebLogFile.txt.
Unable to add repository	WebLogFile.txt, CGContent.log (relay) and CGContent.log (endpoint).

Example	Log Files
Device incorrectly reporting compliance violation	Deviceserviceslog.txt, AirWatch.log (targeted logging), and complianceservice.txt
Device incorrectly reporting email compliance violation	AW.EAS.IntegrationService.log and WebLogFile.txt.
Device not checking in	Deviceserviceslog.txt, MessagingServiceLog.txt, targeted logging (DS), and device side logging.
Profile will not install/push	Deviceserviceslog.txt, InterrogatorQueueService.log, SmartGroupServiceLogFile.txt, targeted logging (CN&DS), BulkProcessingServiceLogfile.txt, and device side logging.
Application will not install/push	Deviceserviceslog.txt, InterrogatorQueueService.log, SmartGroupServiceLogFile.txt, targeted logging (CN&DS), BulkProcessingServiceLogFile.txt, and device side logging.
Certificate will not install/push	Deviceserviceslog.txt, BulkProcessingServiceLogFile.txt, targeted logging (DS), and device side logging.
Products will not push	Deviceserviceslog.txt, ContentDeliveryService.log, BulkProcessingServiceLogFile.txt, PolicyEngine.log, targeted logging (CN&DS), and device side logging.
User group sync fails	AWCM.log, DirectorySyncServiceLogFile.txt, SchedulerService.log, and CloudConnector.log.
User attribute sync fails	AWCM.log, DirectorySyncServiceLogFile.txt, SchedulerService.log, and CloudConnector.log.
User group users missing	AWCM.log, DirectorySyncServiceLogFile.txt, SchedulerService.log, and CloudConnector.log.
DEP sync failures	WebLogFile.txt and BulkProcessingServiceLogFile.txt
Unable to receive email (New Device & SEGv2)	http-transaction.log, app.log, and policy-update.txt.
Unable to receive email (New Device & PowerShell)	AW.Meg.Queue.Service.log (DS), AWCM.log, and CloudConnector.log if enabled.
Unable to receive email (Existing Device & SEG)	AW.EAS.Web.Listener.log, AW.EAS.Web.log, and AW.EAS.Integrationservice.log.
Unable to receive email (Existing Device & SEGv2)	http-transaction.log and app.log.
Unable to receive email (Existing Device & PowerShell)	Third party logging.
Unable to browse internal sites	Proxy.log (relay), Proxy.log (endpoint), Access_Tunnel.log, targeted logging (DS), and device side logging.
Unable to connect to internal content	CGContent.log (relay), CGContent.log (endpoint), targeted logging (DS), and device side logging.
CA integration errors	WebLogFile.txt, AWCM.log, and CloudConnector.log if enabled.
SMTP integration errors	WebLogFile.txt, AWCM.log, and CloudConnector.log if enabled.
Enterprise system connector test connection failure	WebLogfile.txt, AWCM.log, and Connector.log.

Example	Log Files
ACC test connection failure	WebLogFile.txt, AWCM.log, and CloudConnector.log.
Directory services test connection failure	WebLogFile.txt, AWCM.log and CloudConnector.log if enabled.
AWCM test connection failure	WebLogFile.txt and AWCM.log.
Content Gateway test connection failure	WebLogFile.txt and CGContent.log (Relay).
File Storage test connection failure	WebLogFile.txt.
Syslog errors	WebLogFile.txt, ChangeEventQueue.log, AWCM.log, and CloudConnector.log if enabled.
Installer errors	%ServiceName%.log.
Service startup errors	Windows Event Logs and %ServiceName%.log.
ENSv2 Errors	ENS.log and ReSubscriptionMechanism.log
MAC DMG errors (Munki)	ManagedSoftwareUpdate.log

Syslog Integration

2

Security Information and Event Management (SIEM) technology gathers information about security alerts generated by network hardware and software components. It centralizes this data and generates reports to help you monitor activity, perform log audits, and respond to incidents. Workspace ONE UEM integrates with your SIEM tools by sending event logs using Syslog.

The event messages sent are the same that display from the Event Logs page in the AirWatch Console with the same Event Categories. During syslog configuration, you can opt to send Console events, Device events, or both. Any events generated by the AirWatch Console are sent to your SIEM tool according to the scheduler settings. The only way for you to control which events send messages is to customize the logging levels at the Events Settings system settings page.

On the Events Settings page, you can select a logging level for both the Console and Devices. Any logging level you select applies to what is shown in AirWatch, stored in the AirWatch database, and sent to your SIEM tool. Currently, you cannot opt to generate and store all events in AirWatch while sending a separate batch of select messages to your SIEM tool, or conversely.

Integrating Advantages

Event logs are sent to a SIEM tool for security and convenience:

- Security – Keep logs off site in a secure location in your SIEM systems.
- Convenience – Store logs in a central location for easy access.

This chapter includes the following topics:

Configure Syslog

During syslog configuration, you can opt to send Console events, Device events, or both. Any events generated by the Workspace ONE UEM console are sent to your SIEM tool according to the scheduler settings. Syslog can be configured for both on-premises and SaaS deployments.

Note For SaaS customers, ACC is highly recommend for Syslog integration even if Syslog is publicly accessible.

Procedure

1 Navigate to **Monitor > Reports & Analytics > Events > Syslog**.

2 If necessary, set the **Syslog Integration** to **Enabled** to display the settings table.

3 On the **General** tab, configure the following syslog settings,

Setting	Description
Syslog Integration	Enable or disable syslog integration.
Host Name	Enter the URL for the SIEM tool in the **Host Name** text box.
Protocol	Select the required protocol from available options (UDP, TCP, or Secure TCP) to send the data. It is to be noted that support for TLS v1.1 is provided.
Port	Enter the port number to communicate with the SIEM tool in the **Port** text box.
Syslog Facility	Select the facility level for the feature from the **Syslog Facility** menu. The syslog protocol defines the syslog facility. The widespread use and manipulation of the syslog protocol can clutter the meaning of the syslog facility. However, it can roughly suggest from what part of a system a message originated and it can help distinguish different classes of messages. Some administrators use the syslog facility in rules to route parts of messages to different log files.
Message Tag	Enter a descriptive tag to identify events from the Workspace ONE UEM console in the **Message Tag** text box. For example, "AirWatch".
Message Content	Enter the data to include in the transmission in the **Message Content** text box. This is how the message data gets formatted when sent using syslog to your SIEM tool. Use lookup values to set the content. For secure TCP, New line (CRLF) formatting using Enter, \n, \r does not work and gets automatically converted to tab, \t for secure TCP.

4 On the **Advanced** tab, configure the following settings.

Setting	Description
Console Events	Select whether to enable or disable the reporting of Console events.
Select Console Events to Send to Syslog	Visible if you enable Console Events. For each sub-heading, select the specific events that you want to trigger a message to syslog. Use **Select All** or **Clear All** to select or unselect all the events all at once. To select or unselect specific events, enable or disable the checkboxes. **Note** On enabling the **Console Events**, by default, all events under all categories of console events are selected.

Setting	Description
Device Events	Select whether to enable or disable the reporting of Device events.
Select Device Events to Send to Syslog	Visible if you enable Device Events. For each sub-heading, select the specific events that you want to trigger a message to syslog. Use **Select All** or **Clear All** to select or unselect all the events all at once. To select or unselect specific events, enable or disable the checkboxes. **Note** On enabling the **Device Events**, by default, all events under all categories of device events are selected.

5 Select **Save** and use the **Test Connection** button to ensure successful communication between the Workspace ONE UEM console and the SIEM tool.

Admin Scheduler Tasks

You can configure scheduler tasks by editing the frequency of individual tasks or by disabling tasks. Use the following table to get an understanding of what each task is for.

Scheduler Task	Description
Hub Package Process Repository	Watches the package repository directory for WinMo Hub packages and pulls them in to the database.
Android Work Google Device Id Validation Job	Upon enrollment into Android, the server waits for a Google generated deviceID, so that it can initiate the application assignment and push. There are a few minutes delay in getting this ID and this scheduler checks whether any new enrolled device has the ID updated and if yes, start the application sync process.
App EULA Update Notification	Accounts for all devices for which App EULA acceptance is pending and sends notifications. Once final notification is sent, app is removed from the device.
Auto Renew Expiring Profile	Checks for certificates that expired within a renewal grace period configured on Certificate Authority and renews them.
Auto-rotate Google Password	Handles password provisioning and purging for integration with Google Sync.
BitLocker Recovery Key Rotation Job	Rotates the BitLocker admin recovery key based on the values configured in the profile.
Command Publish Batch Job	
Console Notifications	Checks to see if any new notifications must be added to an admin's notification list (for example, APNs expiration notification). These notifications appear in the admin console and are emailed to the admins.
Device Based VPP Apps to Track Update	Checks which VPP applications at an organization group have device-based licensing and auto update enabled. This adds or removes apps from the list used by the VPP auto update scheduler job.
Device Enrollment Program Update	Initiates sync command from Apple to send the added and removed devices for a DEP token at a given OG to update our records.
Email Password Removal	Removes Google password generated for email from Workspace ONE UEM database.

Scheduler Task	Description
File Encryption Migration	Encrypts or decrypts the content stored in the file storage based on the settings in All Settings > Admin > Storage.
Install Application On Demand.	Triggers install of Apple VPP applications upon VPP invite acceptance and triggers install of failed-eligible Apple VPP applications.
List View Export	Checks if an export is requested by an admin for the device or user list view. If it has, it schedules a background job to run asynchronously. Once that background job is completed, the list view export is available for download.
MDM Application List Sample	Collects the status of applications that are marked as 'MDM apps' from all the devices. Applicable only for iOS apps and devices. Scheduler is turned off by default and is enabled only for customers who request the functionality.
MDM License Count Update	Checks device enrollment counts and updates the customer's license counts. Used to track product usage.
P2P license true-up with vendor	Identifies all the peer distribution server licenses that are about to expire, renews the licenses by communicating with the Adaptiva cloud licensing service and distributes the renewed license key to the peer distribution server.
Peer Distribution Software Notification Job	Identifies all the Peer Distribution servers that do not have the latest version installed and notifies the administrator to update.
Profile Publish Batch Job	Profile publishes for CA and Tunnel profile queues the install profile command in held status is by Profile Publish Batch Job in batches. Selects a batch and batch size, based on the settings configured in the UEM Console (under **Settings > Installation > Performance Tuning** for on-premise environments).
Purge Marked For Delete.	This job deletes repo(s)/folder(s)/file(s) under a repository that is marked for deletion.
Query Feedback Service	Checks Apple's Feedback Service for statuses and causes of failed APNs commands.
Re-queue Device Commands	Applicable only for Windows devices. Identifies devices with failed application installs and re-tries installation. The number of re-try attempts and the interval for the next attempt are identified from the performance tuning settings 'Max re-try attempts for failed app install' and 'Failed Application Install Retry Interval' respectively.
Run Compliance Engine.	The scheduler job evaluates compliance in scenarios where: ■ Compliance policy is created Post-enrollment. ■ Any subsequent changes are made to the compliance policy. ■ Any changes made to smart group ■ Device moves organization groups ■ Changes made to app groups ■ Certain Telecom based compliance policies are enabled ■ Apple Templates are used
S/MIME Certificate Cleanup	Checks for all SMIME certificates that have completed their retention period and purges them.
Scheduled Application Batch Release	Used to release internal application install commands created and held by 'Scheduled Application Publish' job. Selects queued application batch (roundrobin). Calculates device list using configured 'Batch Size' text box of performance tuning section. Releases install commands for batch.

Scheduler Task	Description
Scheduled Application Publish	Used to trigger the installation and removal of internal applications based on newly effective assignments. Creates held batch of install commands. Creates remove commands for the immediate release.
Send Apps to App Scan Vendor.	Send a unique list of applications installed across entire device fleet to the configured app scan vendor.
Send VPP Invites and Apps	Checks for users assigned user-based VPP apps and either sends email or device notifications inviting users or devices to participate in user-based licenses of the Volume Purchase Program.
Server Action Task	Handles Time Schedule profiles. The job runs at configured intervals and takes action of Install or Remove profile as per the time span configured for Time schedule profiles.
Staged Command Data Processing Job	Used to schedule the processing of bulk commands from the Device List View page.
Sync Chrome OS Devices	Retrieves new Chrome OS enrollments from Google and creates a corresponding device record in Workspace ONE UEM.
Sync Directory Groups.	Queries the directory to grab all members of synchronized directory groups. Stores users who are part of the group in the UserGroupEnrollmentUserMapSync table. Compares those users by Distinguished Name (DN) or other unique attribute in the UserGroupEnrollmentUserMapSync table to the Mobilemanagement.EnrollmentUser table. If group is configured with add missing users enabled and User does not exist with that DN, user details are pulled from the AD using user ExternalID and stored in the Mobilemanagement.EnrollmentUser table.
Sync Directory User and Admin Attributes	Queries the directory to sync user attributes based on eternalID.
Sync External Content.	Syncs admin repo metadata for all the repositories where admin user credentials are set in the MCM console.
Sync MEM Device Resource ID Job	Syncs Google device records with Workspace ONE UEM for approving new enrollments / mobile mail configurations
Telecom Assign Plans/Roll-up Usage	Calculate usage limits for devices whose Admin has enabled Telecom tracking. Necessary to run reports, populate dashboard, and have the accurate list-view for Telecom.
Temporary Session Key Clean Up	Clears temporary encryption keys used to encrypt the admin provided passphrase in a downloaded configuration file. The key is removed from the database so that it is impossible to retrieve the passphrase from the configuration file after the 48-hour key rotation window has passed.
VPP Auto Update	Checks iTunes for latest version of VPP applications from the list created by Device Based VPP Apps to Track Update job. Each app is checked once every 24 hours. If an update is available, the job kicks off the update command to assigned devices.
VPP Revoke Licenses	Checks for users with associated licenses but no corresponding assigned application. It then issues a revoke command of the license from the user to disassociate it from the license so it can be reused.

Scheduler Task	Description
Workflow Service	Used with the App store restriction, if the restriction is enabled then only one app workflow is active at a time. If there is any issue with the application installation, it deletes in 15 minutes and next one starts.
Purge Job	Removes orphan application blobs from the file storage, and CDN origin server if CDN is configured. Removes expired SDK application log files from the database. By default, the application log files expire every 14 days. Moves any application binary blobs to the file storage from the database if the file storage is configured. Moves non-expired SDK application log files from the database to file storage, if the file storage is configured. Global OG data does not get impacted with respect to the changes made to the blob purge.By default, the scheduler triggers every 24 hours and can either handle 2 GB of data from the database or actively perform tasks for 2 hours.

Configure the Scheduler Syslog Task

You can configure the Scheduler Syslog Task for on-premises deployments. This task sets the intervals at which the AirWatch Console sends request to the SIEM tool for data.

Procedure

1 Navigate to **Groups & Settings > All Settings > Admin > Scheduler**.

2 Select the **Edit** icon from the actions area for the **Syslog** task.

3 Define the interval at which the AirWatch Console sends data to the options configured in the **Syslog** feature in the **Recurrence Type** setting.

4 Define a limited time range for the AirWatch Console to send data in the **Range** setting.

This setting is optional.